

# *Safe Harbour Decision Implementation Study*

**prepared by**

**Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poullet**
**(Centre de Recherche Informatique et Droit,**
**University of Namur, Belgium)**

**with the assistance of**

**Prof. Dr. Joel R. Reidenberg**
**(Fordham University School of Law, New York, USA)**

**and Dr. Lee A. Bygrave**
**(Norwegian Research Centre for Computers and Law,**
**University of Oslo, Norway)**

**at the request of the**
**European Commission, Internal Market DG**
**Contract PRS/2003/A0-7002/E/27**

**Namur, 19 April 2004**

# Table of Contents


**I. INTRODUCTION ..... 5**

**II. OBJECTIVES AND METHODOLOGY ..... 6**

A. OBJECTIVES ..... 6
B. METHODOLOGY ..... 7
1. Theoretical Overview ..... 7
1.1 Scope of Application ..... 7
1.2 Involved Actors ..... 7
2. Self-certification Page Analysis ..... 7
3. In-depth Implementation Analysis of the SH Regime ..... 8
3.1 Visible Compliance/Implementation ..... 8
3.1.1 Selection of Organizations and Collection of Documents ..... 8
3.1.2 The Analytical Criteria ..... 9
3.1.3 Scoring ..... 10
3.2 Case-Study ..... 11
3.3 Implementation Experiences of Different Actors ..... 11
4. Impact of New US legislation ..... 12

**III. RESULTS OF THE STUDY ..... 13**

1. THEORETICAL OVERVIEW ..... 13
1.1 Scope of Application ..... 13
1.1.1 Geographic Scope of Application ..... 13
1.1.2 Material Scope of Application ..... 13
1.1.2.1 Relevance of the FTC and DoT Jurisdiction ..... 13
1.1.2.2 Transfers of "Personal Data" ..... 15
1.1.3 Personal Scope of Application ..... 17
1.1.4 Preliminary Conclusions ..... 18
1.2 Actors Involved ..... 18
1.2.1 Public Actors ..... 18
1.2.1.1 European Public Authorities ..... 18
1.2.1.2 US Public Authorities ..... 21
1.2.2 Private Actors ..... 23
1.2.2.1 European Private Actors ..... 23
1.2.2.2 US Private Actors ..... 24
1.2.3 Preliminary Conclusions ..... 25
2. SELF-CERTIFICATION PAGE ANALYSIS ..... 26
2.1 Results ..... 28
2.1.1 Industry Sector Information (see graphic 1 in Appendix V) ..... 28
2.1.2 Data Categories (see graphic 2 in Appendix V) ..... 30
2.1.3 Controller/Processor (see graphic 3 in Appendix V) ..... 30
2.1.4 Personal Data Covered (see graphic 4 in Appendix V) ..... 31
2.1.5 Privacy Policy Location Accuracy (see graphic 5 in Appendix V) ..... 31
2.1.6 Verification (see graphic 6 in Appendix V) ..... 32
2.1.7 Regulatory body (see graphic 7 in Appendix V) ..... 32
2.1.8 Privacy Program (see graphic 8 in Appendix V) ..... 32
2.1.9 Dispute Resolution Mechanisms/Programs (see graphic 9 in Appendix V) 34
2.1.10 Co-operation with EU Data Protection Authorities (see graphic 10 in Appendix V) ..... 35
2.1.11 Certification Status (see graphic 11 in Appendix V) ..... 35

2.1.12 DoC Self-certification Information ..... 35
2.1.12.1 Preliminary conclusions ..... 37
2.1.13 DoC Self-Certification form ..... 37
2.1.13.1 Preliminary conclusions ..... 45
3. IN-DEPTH IMPLEMENTATION ANALYSIS OF SH ..... 48
3.1 Visible Indicators and Trends on Compliance/Implementation ..... 48
3.1.1 Analysis of Adherent Organizations ..... 48
3.1.1.1 General Observations ..... 50
3.1.1.2 Organizations' Compliance Indicators ..... 51
3.1.2 Analysis of Privacy Programs and ADR Bodies ..... 56
3.1.2.1 Privacy Programs and ADRs' Compliance Indicators ..... 56
3.1.3 Main Findings ..... 58
3.1.3.1 Positive Trends ..... 58
3.1.3.2 General Observations ..... 60
3.1.3.3 Implementation Deficiency Trends ..... 62
3.2 Specific case-study ..... 78
3.2.1 Preliminary Conclusions ..... 81
3.3 Implementation experience by different parties ..... 81
3.3.1 Lawyers ..... 81
3.3.1.1 Preliminary Conclusions ..... 85
3.3.2 National DPAs ..... 85
3.3.2.1 Preliminary Conclusions ..... 87
3.3.3 Federal Trade Commission (FTC) ..... 87
3.3.3.1 Preliminary Conclusions ..... 91
3.3.4 Consumer Associations ..... 91
3.3.4.1 Preliminary Conclusions ..... 92
3.3.5 US Department of Commerce (DoC) ..... 92
3.3.5.1 Preliminary Conclusions ..... 95
3.3.6 ADRs ..... 96
3.3.6.1 Preliminary Conclusions ..... 97
3.3.7 DPA Panel ..... 98
3.3.7.1 Preliminary Conclusions ..... 98
4. IMPACT OF NEW US LEGISLATION ..... 98
4.1 Prevailing Laws that Conflict with SH Principles ..... 98
4.2 Significance of new US legislation for SH ..... 104
**IV. CONCLUSIONS ..... 105**
1. DEFICIENCIES OBSERVED ..... 105
1.1 SH Principles ..... 105
1.2 Self-Certification ..... 106
1.3 Privacy Programs ..... 107
1.4 Enforcement ..... 107
1.5 US legislation ..... 107
2. POSSIBLE MECHANISMS FOR IMPROVEMENT ..... 107
2.1 Implementation of the SH Principles ..... 108
2.1.1 Guidance on Privacy Policy Drafting ..... 108
2.1.2 Data Controller and /or Data Processor Capacity ..... 108
2.1.3 Clarification of Key Concepts ..... 108
2.1.4 SH Label ..... 108
2.1.5 Human Resources Data ..... 109
2.2 Enforcement ..... 109
2.2.1 FTC jurisdiction ..... 109
2.2.2 Minimal Standards for Privacy Programs and ADRs ..... 109
2.3 US Legislation ..... 109
2.4 Role of the different parties ..... 110

2.4.1 The US Department of Commerce ..... 110
2.4.2 The Federal Trade Commission ..... 110
2.4.3 The DPA Panel ..... 111
2.4.4 The DPAs ..... 111
2.4.5 Business Representatives and Intermediate Organizations (e.g. consumer and civil liberties organizations) ..... 111
3. DISCRIMINATORY APPLICATION ..... 111

**APPENDIX I – ANALYTICAL CRITERIA FOR SH ADHERENTS ..... 114**

**APPENDIX II – ANALYTICAL CRITERIA FOR PRIVACY PROGRAMS ..... 125**

**APPENDIX III – QUESTIONNAIRES FOR IN-DEPTH STUDY OF COMPANY PRACTICES ..... 129**

**APPENDIX IV – QUESTIONNAIRES TO DIFFERENT PARTIES INVOLVED IN THE SHA SYSTEM ..... 135**

**APPENDIX V – DATA TABLES AND GRAPHICS OF POINT 2 (CERTIFICATION PAGE ANALYSES) ..... 139**

**APPENDIX VI – DATA TABLES AND GRAPHICS OF POINT 3.1 (VISIBLE COMPLIANCE/IMPLEMENTATION) ..... 169**

# I. Introduction

The Safe Harbor scheme (SH), established under the auspices of the United States Department of Commerce (DoC) for the transfer of personal data from the European Union (EU) to the United States (US), is recognized by the European Commission as providing "adequate" protection under the terms of Directive 95/46/EC.[1] The scheme creates a voluntary mechanism enabling US organizations to qualify as offering adequate protection for personal data transferred to them from the EU. More specifically, SH defines a set of privacy principles and frequently asked questions (FAQs), allowing US organizations to commit that their information practices will conform to the defined principles, and requires the availability of independent recourse mechanisms for enforcement. The commitment by organizations must be made to the DoC through a certification that publicly identifies the organization's adherence to the principles. This commitment being made, companies are bound by the SH.

Article 4(1) of the Commission Decision on the scheme stipulates that implementation of the Decision shall be subject to evaluation three years after its notification to the Member States.

At the request of the European Commission, this report researches and reports on the implementation of SH. The specific objectives and methodology for the research are described in Section II. Section III describes the results of the study, and includes: (i) a brief theoretical overview of the SH regime; (ii) a factual analysis of the SH certification pages published on the DoC SH website; (iii) an in-depth analysis of the implementation of the SH principles; and (iv) a contextual analysis of the SH principles. The report concludes in Section IV with an evaluation of the current implementation of the SH in light of the findings.

[1] See Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (O.J. L 215, 25 August 2000, p. 7) – hereinafter "Commission Decision".

# II. Objectives and Methodology

## A. Objectives

The task assigned by the European Commission consists of an analysis of the *implementation* of the SH. More precisely, this study has the following goals:

First, it seeks to identify trends in the visible compliance of registered organizations with the terms of the SH and to determine the extent to which registered organizations generally:

1. feature a privacy policy which covers all SH principles and which is publicly displayed so as to trigger section 5 of the US Federal Trade Commission Act;
2. fulfil the requirements laid down in FAQ 6 (as regards their Self-Certification), FAQ 7 (as regards their verification procedures) and FAQs 5 and/or 11 (with regard to their independent dispute resolution system and enforcement mechanisms);
3. operate within the jurisdiction of the Federal Trade Commission (FTC) or Department of Transportation (DOT);
4. signal in their privacy policy whether and if so the extent to which prevailing laws in the US prevent them from applying the SHA.[2]

Secondly, the study seeks to report whether the independent dispute resolution mechanisms chosen by registered organizations generally appear to satisfy the requirements of FAQ 11 and, in particular, if seal organizations or privacy programs offering dispute resolution respect FAQ 11.[3]

Thirdly, this study seeks to assess the collateral impact of certain regulatory regimes on the SH principles. Analysis in this respect focuses upon the impact of new US federal legislation.

The study is primarily concerned with the *implementation* of the SH and does not directly review the SH Agreement itself other than in a brief theoretical introduction.

---

[2] These tasks replicate those of Joel R. Reidenberg & Privacy Laws & Business, "The Functioning of the US-EU Safe Harbor Privacy Principles" (Independent Consultant Study Report, 21 September 2001; available from the European Commission).

[3] *Id*.

## B. Methodology

### 1. Theoretical Overview

#### 1.1 Scope of Application

This part provides a brief overview of the scope of application of the SH regime (*ratione materiae*, *ratione personae*, *ratione loci*). It provides the background against which the factual, in-depth and contextual analyses have been conducted. The section does not aim to exhaustively explain the principles of the SH scheme but to help orient the reader who is not already acquainted with this framework.

#### 1.2 Involved Actors

Part 1.2 focuses on the role played by each actor involved in the SH system (i.e. public bodies in Europe and the United States, companies, dispute resolution bodies, intermediary associations, etc.). The section identifies these actors' functions within the SH framework. The aim of this part is to indicate the capacities and limits of each actor in order to understand their implementation responsibilities.

### 2. Self-certification Page Analysis

The description of the scope of the SH regime is complemented by an analysis of factual data extracted from the certifications available on the SH list that is published on the DoC website. This survey concerns all companies that have self-certified as of 3 November 2003. It is aimed at providing a "state-of-the-art" overview of SH self-certification. The analysis is a comprehensive review of the following elements as shown on the DoC certification form:

- The industry sector in which the certifying entity is active;
- Data typology;[4]
- Processing typology, i.e. on-line, off-line, manual, and processing of human resources data;
- Accuracy of privacy policy location;
- Type of verification, i.e. in-house, third party or both;
- Whether entities fall under the jurisdiction of either the Federal Trade Commission (FTC) or the Department of Transportation (DoT);
- Whether entities adhere to a privacy program;
- Type of dispute resolution mechanism to which entities adhere;
- Whether entities have declared an intention to co-operate with the European data protection authorities (DPAs); and

[4] From the declaration made in the item "Personal Information Received from the EU", data types can be roughly classified as: (1) commercial data; (2) human resources data; (3) research data (market and others); (4) travel data; and/or (5) medical data.

- The privacy policy's certification status.

## 3. In-depth Implementation Analysis of the SH Regime

In assessing the implementation of the SH regime, three paths of analysis have been followed. The first path consisted of a visible compliance/implementation study of publicly available information of selected companies' privacy policies, privacy programs, and alternative dispute resolution providers (ADRs). The second path consisted of a case-study of certain companies, based on their (voluntary) responses to a questionnaire. The third path took the form of analysis of the implementation experiences of different parties, again based on their (voluntary) responses to specific questionnaires.

### 3.1 Visible Compliance/Implementation

This part is based on a survey of publicly available privacy policies of US companies adhering to the SH, as referred to in the certification page. It is aimed at providing insight into the practical implementation of the SH principles. The research for this part consisted of three components:

#### 3.1.1 Selection of Organizations and Collection of Documents

The study selected 10% of all organizations that have self-certified their adherence to SH as of 3 November 2003. A sample of 10% was chosen since a thorough analysis of all SH companies was not feasible within the framework of this study. The companies subjected to this review were chosen randomly.

During the week of 3 November 2003, the self-certification statements and the publicly available privacy policies of each of the organizations were printed from the DoC website and the respective websites of each of the organizations. For one company, the relevant policy could not be immediately located, and was discovered and printed on 30 January 2004. Other policies (i.e. those declared to be available at physical addresses or Intranets) were requested from the companies by e-mails.

The 41 selected organizations listed the following organizations as privacy programs in their self-certifications to the US Department of Commerce:

1. American Arbitration Association ("AAA");
2. Better Business Bureaus Online ("BBBOnLine");
3. The Council of American Survey Research Organizations ("CASRO");
4. Coalition Against Unsolicited Commercial E-mail ("CAUCE");
5. Direct Marketing Association SH program ("DMASHP");
6. Online Privacy Alliance ("OPA"); and
7. TRUSTe.

Furthermore, the 41 selected organizations listed the following ADR organizations in their self-certifications to the US Department of Commerce:

1. AAA;
2. BBBOnLine;
3. DMASHP; and
4. TRUSTe

For the analysis, we have also considered the ADR organizations mentioned in the DoC website (beyond those listed above):

1. AICPA Webtrust (American Institute of Certified Public Accountants);
2. ESRB (Entertainment Software Rating Board); and
3. JAMS (Judicial Arbitration and Mediation Service)

The publicly available materials on the policies and dispute settlement mechanisms of each of these programs were printed from each of the respective program's websites during January and February 2004.

### 3.1.2 The Analytical Criteria

For the analysis, this part of the study adopted the criteria used in Joel R. Reidenberg & Privacy Laws & Business, "The Functioning of the US-EU Safe Harbour Privacy Principles" (Independent Consultant Study Report for the European Commission, 21 September 2001).

**Companies:** The SH Privacy Principles and the FAQs were distilled into a checklist of 66 criteria. For a company to conform to the requirements of SH, each of these analytical criteria must be satisfied from the aggregate of statements, disclosures and commitments made in the organization's self-certification, corporate privacy policy and independent dispute settlement mechanism.

These elements were divided into three categories:

1. those addressing *eligibility of organizations* to qualify for the benefits of SH, including procedural requirements;
2. those addressing the *substantive provisions* of fair information practices; and
3. those addressing *enforcement mechanisms and remedies.*

To the extent possible, the analytical criteria were defined as objective conformity or non-conformity indicators with the SH and FAQs. The criteria for each category are listed and briefly described in Appendix I.

**Privacy programs and ADR organizations:** In addition, for privacy programs and independent dispute resolution mechanisms, the SH and FAQ 11 were distilled into a checklist of 35 criteria. For the privacy program or dispute resolution mechanism to conform with the SH, these criteria must be found in the privacy program or dispute resolution body's rules.

These elements were divided into groups as follows:

A. incorporation of SH *notice* principle in privacy program rules;
B. incorporation of SH *choice* principle in privacy program rules;
C. incorporation of SH *onward transfer* principle in privacy program rules;
D. incorporation of SH *security and integrity* principles in privacy program rules;
E. incorporation of SH *access* principle in privacy program rules;
F. incorporation of SH *enforcement* principle in dispute resolution including FAQ 11.

The elements for each category are listed in Appendix II.

The study analyses the programs that were actually named as "privacy programs" by reviewed SH companies.[5] Further, dispute resolution mechanisms/programs which are mentioned in the reviewed companies' DoC certification pages and which do not constitute a "privacy program", are assessed with respect to the requirements set forth by FAQ 11.

### 3.1.3 Scoring

The research examined the publicly available information from each organization to ascertain if each element of the analytical criteria was satisfied.[6] The publicly available information consisted of the self-certification statements of each organization as found on the DoC website, the privacy policies referenced in those certifications, any other privacy policy found at each organization's website when the location of the privacy policy in the certification was inaccurate, any other relevant policies mentioned on the website of each organization or cross-referenced by the organization's privacy policy, and (when appropriate) any privacy policy that was requested by e-mail.

For privacy programs and independent dispute settlement mechanisms, the study examined each organization's available self-certification statement and the rules of each privacy program and dispute settlement mechanism as found on each program's web site.

Since the SH constitutes an alternative to statutory protection in the US, the analytical criteria were interpreted strictly. For example, SH requires that organizations disclose the public location of their privacy policies in the self-certification letter. If an organization provided only the URL location of the general website of the organization or an erroneous specific URL for its privacy policy, it was given a negative score on the criterion "accurate location."

At the same time, the terms of each organization's publicly available information were generally construed liberally. For example, the SH requires that organizations use reasonable security measures to protect personal information. If an organization indicated that it

---

5 See *infra*, section 2.1.8.

6 The scoring of corporate policies followed the approach taken in the study by Reidenberg and Privacy Laws & Business (*op. cit.*).

encrypted data or merely stated that its information was secure, then the organization was registered as satisfying this criterion.

Because the underlying goal of SH is to provide a clear, relatively high level of protection in the absence of an adequate, generally applicable data protection regime, any ambiguities or contradictions in an organization's publicly available information resulted in an adverse score. When an organization did not flag the SH obligations that are considered mandatory, the organization was registered as not satisfying the analytical element. When an organization's publicly available information was contradictory, the organization was registered as "unclear" on the point concerned. If the policy was not made publicly available, it scored an "unknown," while a "not applicable" ("napp") was registered for most US organizations that are data *processors*.[7] Finally, US organizations which are data controllers scored a "napp" for certain criteria if no obligations exist as a consequence of the absence of certain data processing activities. For instance, if an organization did not represent itself as processing "sensitive information" (as defined by the SH privacy principles), it is not required to operate with an opt-in consent mechanism. Consequently, such an organization would score a "napp" with respect to whether or not they offer opt-in consent.

### 3.2 Case-Study

Specific case-studies have been conducted with volunteering companies. Volunteering companies were asked to answer the questionnaire set out in Appendix III. The purpose was to gain a better view of companies' practices beyond the visible aspects established in a privacy policy and to understand better how the abstract principles are put into practice. Three companies volunteered to answer the questions.

### 3.3 Implementation Experiences of Different Actors

Finally, the study assesses implementation experiences of different actors involved in the SH scheme. The surveyed actors are: (a) lawyers who have experience with transborder data flows between Europe and the US (15 lawyers were approached, of which 6 answered); (b) national data protection authorities (DPAs); (c) the FTC; (d) the DoC; (e) consumer associations, and (f) ADR organizations. The various questionnaires sent out are included in Appendix IV.

Special attention was paid to the enforcement mechanisms and, in particular, the requirements of FAQ 11. The analytical criteria[8] already include specific issues to be evaluated with respect to the mechanisms that have to be present in the companies' Privacy Policies. A questionnaire was sent to 7 dispute resolution organizations referred to on the website of the DoC. The relevant page on that website mentions the following organizations: BBBOnLine, TRUSTe, AICPA WebTrust, DMA, ESRB, JAMS and AAA.[9]

---

[7] Many of the obligations of the SH, such as the provision of notice to data subjects, are not relevant for third-party processors.

[8] Reidenberg & Privacy Laws & Business, *op. cit*.

[9] See "Helpful Hints Prior to Self-Certifying to the Safe Harbor", DoC, available at <http://www.export.gov/safeharbor/helpful_hints.html> (last visited 23 February 2004). On "Safe Harbor

## 4. Impact of New US legislation

This part assesses whether and how certain new US legislation affects the level of protection provided for by the SH privacy principles.[10] Attention has been paid to the legal framework adopted after the events of 11 September 2001, as well as to any other sector-specific Acts. Only legislation in force as of 3 November 2003 has been taken into consideration.

Workbook", the DoC adds: "A third-party dispute resolution mechanism assures your customers that your organization is complying with its stated policies. While programs vary, organizations such as BBBOnLine, the Direct Marketing Association, the Privacy Council and the Entertainment Software Rating Board have indicated that they have developed privacy programs that allow companies to comply with the Safe Harbor privacy principle on enforcement. Other programs such as an outside arbitration and mediation service (e.g. JAMS or the American Arbitration Association) may also be used, so long as every complaint is heard in compliance with the enforcement principle and FAQ 11. (***Note: Organizations self-certifying to the Safe Harbor are responsible for ensuring that they have chosen a dispute resolution provider that will satisfy the requirements of the framework. The Department of Commerce does not certify programs in order to serve as dispute resolution mechanisms under Safe Harbor. Therefore, the Department of Commerce cannot guarantee that a particular program will meet all Safe Harbor requirements, including those under FAQ 11)"***. See <http://www.export.gov/safeharbor/sh_workbook.html> (last visited 23 February 2004).

[10] It is pertinent to refer to comments of the Article 29 Data Protection Working Party in relation to Binding Corporate Rules : "Mandatory requirements of national legislation applicable to the members of the corporate group which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, are in principle not in contradiction with the binding corporate rules. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax reporting requirements or anti-money laundering reporting requirements. In case of doubt, corporate groups should promptly consult the competent data protection authority". See Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU data Protection Directive to Binding Corporate Rules for International Data Transfers*, 3 June 2003, WP 74, p. 14.

# III. Results of the Study

## 1. Theoretical Overview

### 1.1 Scope of Application

#### 1.1.1 Geographic Scope of Application

Directive 95/46/EC (hereinafter "the Directive"), on which the Commission Decision is based, applies to the 15 EU Member States and the French overseas departments, the Azores, Madeira and the Canary Islands. At the same time, the Directive has been formally incorporated into the 1992 Agreement on the European Economic Area (EEA) so that the three States which are not members of the EU but party to the EEA Agreement – i.e. Norway, Iceland and Liechtenstein – are bound by the Directive and, hence, the Commission Decision.[11] The data transfer rules in the Directive and, thus, potentially the SH arrangement, apply to transfers conducted from those States.

The SH principles apply to US organizations which voluntarily subscribe to them. The Commission Decision does not contain any specific definition of "US organization". However, Article 2 specifies that the Decision "concerns only the adequacy of protection provided in the United States under the Principles (...)." Apparently, a US organization must be established in the USA to be eligible to join up to the SH scheme.[12] For instance, a Mexican subsidiary of a US organization cannot enjoy the benefits of SH – which implies that the subsidiary will have to utilize other data transfer exemptions (as set out in Article 26 of the Directive).

#### 1.1.2 Material Scope of Application

##### 1.1.2.1 Relevance of the FTC and DoT Jurisdiction

The material scope of application of the SH principles is determined to an important extent by the jurisdiction of the FTC and the DoT. The SH regime applies only to sectors and/or data processing which fall(s) under the jurisdiction of the FTC or DoT.[13] To put it differently, a

---

[11] Although a member of EFTA, Switzerland is not a Party to the EEA, having voted against EEA membership in December 1992. Switzerland maintains and develops its relationship with the EU through broadened bilateral agreements.

[12] See Article 1(1) of the Commission Decision (referring to "organizations established in the United States …"). This can also be deduced from the e-form published on the DoC website, <http://web.ita.doc.gov/safeharbor/shreg.nsf/safeharbor?openform> (last visited 23 February 2004).

[13] See Recital 6 of the Commission Decision.

US organization can qualify for the SH regime only if its failure to comply with its statement to adhere to the SH principles is actionable under the Federal Trade Commission Act section 5 (prohibiting unfair and deceptive acts) or Title 49 United States Code (USC) section 41712 (also prohibiting such acts).

A deceptive practice is defined as a "representation, omission or practice that is likely to mislead reasonable consumers in a material fashion."[14] According to Annex III of the Decision, the FTC claims broad jurisdiction over misrepresentations about the collection and use of consumer data.[15] Consequently, a US organization that self-certifies its adherence to the SH principles without actually respecting the regime may fall within the FTC's jurisdiction, since this would constitute a "deceptive practice" within the meaning of section 5 of the FTC Act.

Some qualifications need, however, to be made:

First, courts have not confirmed so far the FTC's broad claim of jurisdiction regarding privacy representations.[16] Although some cases may undoubtedly constitute deceptive practice,[17] other cases may figure in a gray zone and leave the controller as well as the data subject in a state of uncertainty. Under 15 USC section 45(n), a practice is deemed "unfair" if it "causes or is likely to cause *substantial injury* to consumers which is not reasonably avoidable by consumers themselves and *not outweighed by countervailing benefits* to consumers or to *competition*" (emphasis added). The control exercised by the FTC is only marginal and allows the balancing of a commercial practice with the commercial benefits the data subject gets in exchange. Although processing practices must be assessed case-by-case, the FTC has in its letter to the EC pointed out that "a company's failure to abide by a stated privacy policy is likely to be a deceptive practice."[18] Secondly, the FTC's jurisdiction extends to unfair or deceptive acts or practices "in or affecting commerce." Personal data collected and processed by corporations that are promoting goods and services, including collecting and using data for commercial purposes, would presumably meet the "commerce" requirement.[19] However, there exists considerable doubt about the FTC's competence

---

[14] A practice is unfair if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition: see 15 USC section 45(n) and letter of 14 July 2000 from FTC Chairman Mr. Robert Pitofsky to Mr. John Mogg, Director, DG XV, European Commission (set out in the Commission Decision, Annex V).

[15] The letter from FTC Chairman Pitofsky, *op cit.*, gives the example of a website that falsely claims to comply with a stated privacy policy or a set of self-regulatory guidelines. It is further stated that the "(FTC) has taken the position it may challenge particularly egregious privacy practices as unfair under section 5 if such practices involve children, or the use of highly sensitive information, such as financial records and medical records." See also FAQ 6 stipulating that "[a]ny misrepresentation to the general public concerning an organization's adherence to the SH Principles may be actionable by the Federal Trade Commission or other relevant government body. Misrepresentations to the Department of Commerce (or its designee) may be actionable under the False Statements Act (18 USC § 1001)."

[16] See J.R. Reidenberg, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal*, 2003, vol. 54, pp. 877–898 at especially p. 888 ("Since all of the FTC's deceptive practices cases have settled prior to any court decision, the legal standards remain uncertain").

[17] See, e.g., the Geocities and ReverseAuction.com cases (referred to in, *inter alia*, Annex V of the Commission Decision). Those cases have been settled by the FTC; they are not the subject of court decisions.

[18] See also Decision, Annex III.

[19] Letter of FTC Chairman Pitofsky, *op cit*.

regarding the SH scheme.[20] For instance, the FTC will lack, in principle, jurisdiction over the collection and use of personal information for non-commercial purposes or charitable fund-raising.[21] According to Annex III of the Decision, one should take into account the commercial character of the purpose of the data collection, rather than the commercial nature of the data controller.

Processing of personal data for purposes of employment or research activities (e.g. use of personal information for developing and testing drugs) would then not fall within FTC jurisdiction and would ordinarily be outside SH. The FAQs contain, nevertheless, specific provisions concerning human resources data and transfers to the US for pharmaceutical research and/or other purposes. The Article 29 Data Protection Working Party confirmed that there may be uncertainty as to whether personal data processed for these purposes would be covered by the SH.[22]

Section 5 of the FTC Act excludes the FTC's authority with regard to: (1) financial institutions, including banks, savings and loans, and credit unions; (2) telecommunications and interstate transportation common carriers; (3) air carriers; and (4) packers and stockyard operators.

Personal data-processing operations conducted by organizations that come within the range of the DoT's jurisdiction can also certify for the SH Principles. The DoT can take enforcement based on 49 USC section 41712, which prohibits a carrier from engaging in "an unfair or deceptive practice or an unfair method of competition" in the sale of air transportation which results or is likely to result in consumer harm. Again, failure to maintain the privacy of information obtained from passengers would not per se constitute a violation of this section unless the organization has publicly committed to the principles.[23]

#### 1.1.2.2 Transfers of "Personal Data"

The SH arrangement applies only to transfers of "personal data" or "personal information." Those categories are defined rather vaguely as "data about an identified or identifiable individual that are within the scope of the Directive, received by a US organization from the EU, and recorded in any form."[24] This definition suggests some commonality between it and

---

[20] See generally J.R. Reidenberg, "Privacy Wrongs in Search of Remedies," *op cit.*; J.R. Reidenberg, "E-Commerce and Trans-Atlantic Privacy", *Houston Law Review*, 2001, vol. 38, pp. 717–749; Y. Poullet, "The Safe Harbor Principles – An Adequate Protection?", paper presented at International Colloqium organized by IFCLA, Paris, 15–16 June 2000, <http://www.droit.fundp.ac.be/textes/safeharbor.pdf> (last visited 28 February 2004).

[21] Decision, Annex III. The letter of FTC Chairman Pitofsky, *op cit.*, gives the example of a "chat room" operated by non-commercial entities, e.g. a charitable organization.

[22] The Article 29 Data Protection Working Party pleaded to expressly exclude these categories of data transfers from the SH: see *Opinion 7/99 on the Level of Data Protection provided by the 'Safe Harbor' Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce*, 3 December 1999, WP 27, pp. 4–5.

[23] See letter from Mr. Samuel Podberesky, Assistant General Counsel for Aviation Enforcement and Proceeding, to Mr. John Mogg, Director, DG XV, European Commission (set out in the Commission Decision, Annex VI).

[24] See Commission Decision, Annex I.

the definition of "personal data" in Directive 95/46/EC Article 2(a), which refers to "any information relating to an identified or identifiable natural person" and then notes that "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[25] However, the definition in the SH principles is formulated in such a way as to leave open the possibility that it is not *fully commensurate* with the Directive's definition; in other words, it is possible that some data which would be "personal" under the Directive will not be "personal" for the purposes of SH.

Information which is rendered relatively "anonymous" by an intermediary that can conduct without unreasonable difficulty a "reverse identification" (so-called "coded" or "pseudonymized" data) will fall within the scope of the Directive, yet there remains uncertainty whether the SH principles apply to such information. With regard to "employment data", FAQ 9 specifically excludes "anonymized" or "pseudonymized" data from the scope of application without further clarifying what these notions exactly mean. Furthermore, FAQ 14 regarding research data holds that a transfer from the EU to the US of data coded by the principal investigator would not constitute a transfer of personal data that would be subject to the SH principles. It is unclear if one may extend those limitations to the processing of other data categories under the SH regime.

More concretely, the question arises as to what should be understood by "anonymized" and "pseudonymized" data. There exists a continuum between clearly personal data and anonymous data; many categories of data fall between these two extremes. In a transfer context, if there exists interdependence between transferor and transferee, it is unlikely that data will be entirely "anonymized," unless, perhaps, anonymization would be guaranteed by a trusted third party.

An "adequate" level of protection does not necessitate endorsement of a definition of personal data which is identical to the definition of the Directive. Only if the impact of a narrower definition would burden the privacy and related freedoms of the data subject with an unacceptable risk would there be a problem. The SH text specifies that US law will apply to questions of interpretation and compliance with the SH principles and relevant privacy policies by SH organizations, except where organizations have committed themselves to co-operate with European DPAs (e.g. in the context of human resources transfers). Consequently, the interpretation by the FTC or DOC (or a US court) will be determinative in the end. However, the SH framework contains a subtle system of checks and balances. If the US authorities' interpretation would erode the adequacy finding of the Commission, the latter may re-adjust the principles pursuant to Article 3(4) of the Decision. In accordance with FAQ

---

[25] See also Recital 26 in the preamble to the Directive which specifies that, in assessing whether a person is identifiable from data, one should consider "all the means likely reasonably to be used either by the controller or by any other person to identify the said person". In the context of a medical research program, for instance, if a medical doctor replaces the personal identifiers of medical data sent to a pharmaceutical enterprise by a random number assigned by the computer, the Directive applies, since the supplier of the information, i.e. the doctor, can relate the data to a specific patient. For further discussion of the various issues thrown up by definitions of "personal data", see L.A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), pp. 41–50, 210–215, 315–319. On "aggregate data" see, *inter alia*, D.J. Solove "Privacy and Power: Computer Databases and Metaphors for Information Privacy", *Stanford Law Review*, 2001, vol. 53, pp. 1393–1462, particularly at pp. 1434 and 1452.

5, US organizations can co-operate with European DPAs in which case the line of interpretation of the latter will (in first instance) prevail.

### 1.1.3 Personal Scope of Application

The SH principles only apply to US organizations. The latter term is not defined in the SH documentation. The Commission Decision indicates on its face that the SH principles would not apply, as a point of departure, to individual natural/physical persons who receive personal data from the EU. However, a natural person who owns and operates a business as a sole proprietorship or partnership that engages in data transfer, can, by virtue of such a legal entity, qualify as an organization eligible for certification. On many occasions, the FTC has claimed jurisdiction over individuals when they have violated the FTC Act, imposed fines or entered into agreements with individuals. Only if these persons would not be within the scope of the FTC's or DOT's jurisdiction, could individuals not benefit from the arrangement.

The notion "US organization" may not be interpreted by simply referring to the definition of "data controller" in Directive 95/46/EC. The SH principles do not refer to the Directive as regards the definition of "US organization," and, as has been indicated above, the principles generally fall under the interpretation of the US authorities (whose margin of discretion with respect to interpretation is limited, nevertheless, by the adequate level of protection requirement).

Several hypotheses could be made regarding the scope of the term "US organization":

> (i) A department that forms an integrated part of the same legal entity of a corporation is unlikely to constitute a separate organization under the SH scheme. For instance, if personal data held in the EU by a corporation are forwarded to one of its departments, this would not trigger the onward transfer rules because, arguably, the information only circulates within the same organization. To put it in the terms of the Directive, the organization is a "controller" which determines the purposes and means of the processing, independent of the fact that the processing is, in effect, carried out by one of its departments;
>
> (ii) If data are shared between various companies that are members of the same group, the situation will be less clear-cut, since legal criteria are missing from the face of the SH documentation to determine the extent to which these companies constitute different "organizations". The companies are likely, nevertheless, to constitute different "organizations," even more so if no specific processing guidelines are imposed by the central management of the group;[26]
>
> (iii) An organization which, in the context of the SH arrangement, performs processing operations on behalf of an organization, is deemed to constitute a separate

[26] The Principles tend to connect an "organization" with a "separate legal entity," rather than with the decision-making power over a specific processing operation. This can be deduced from FAQ 6 where it is stated that "(a)n organization *that will cease to exist as a separate legal entity* as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance" (italics supplied).

entity, to be distinguished from the "organization." Thus, a "processor" under the Directive may qualify as a "third party" in the SH context, if it is acting as an agent to perform task(s) on behalf and under the instructions of the organization.[27] The fact that a corporation has a contractual relationship with another legal entity, does not exclude the latter from qualifying as a "third party". Alleging the contrary would undermine the principles. It can be deduced from a general reading of the principles that the notion of "third party", although unclear, denotes a separate legal entity.[28]

While the Directive pursues a functional approach, (i.e. the controller is defined by reference to the *de facto* powers it exercises over the purposes and means of data processing), the SH arrangement seems to be based on a corporate law approach which takes the "legal personality" as primary criterion for delineating what is a "US organization."

#### 1.1.4 Preliminary Conclusions

- Key concepts such as "US organization," "personal data," "deceptive practices" lack clarity. Moreover, the jurisdiction of the FTC with regard to certain types of data transfers is dubious. A reliable protection regime does require, however, conceptual transparency and it is advisable that guidance be provided on these concepts to ensure that companies do not certify for data transfers falling outside the scope of SH. Such guidance could be developed by the Article 29 Data Protection Working Party in co-operation with the FTC/DoC.

## 1.2 Actors Involved

A multitude of actors are involved in administering the SH scheme or are otherwise affected by it. The relevant actors are the following:

### 1.2.1 Public Actors

#### 1.2.1.1 European Public Authorities

a) Data Protection Authorities (DPAs)

---

[27] A "third party" does not *per se* mirror a "processor" under the Directive unless it *performs tasks on behalf of and under the instructions of the organization*. "It is not necessary to apply the notice and choice principles when disclosure is made to such a third party. The Onward Transfer Principle, on the other hand, will apply": see endnotes 1 & 2 to the SH Principles.

[28] The notion "third party" may be analogous to the definition set forth in Directive 95/46/EC (although there is theoretical room for some variance). Article 2 of the Directive defines "third party" as: "[…] [A]ny natural or legal person, public authority, agency or any other body than the data subject, the controller, the processor and the person who, under the direct authority of the controller or the processor, are authorized to process the data."

A prerequisite to a valid data transfer is compliance by the data exporter with the local data protection rules. In addition, data subjects will primarily consider filing a complaint with their local DPA. National DPAs are entrusted with the tasks set forth by Article 28 of Directive 95/46/EC, including the monitoring of the application of the national data protection rules. They can use in that context the powers described in Article 28(3) of the Directive, as specified by national law. In some EU/EEA Member States, DPAs may impose administrative sanctions. In other such States, DPAs may investigate data-processing activities and refer a complaint to the public prosecutor if: (i) a violation of the data protection law is established; and (ii) such violations are criminally sanctioned.

DPAs may be empowered to block data transfers pursuant to Article 3 of the Commission Decision.[29] Under this provision, DPAs may suspend data flows to an organization that has self-certified its adherence to the SH principles implemented in accordance with the FAQs, if: (i) the FTC or DoT, and/or independent recourse mechanisms (i.e. private sector privacy programs that incorporate the SH principles with associated enforcement mechanisms)[30] have determined that the organization is violating the SH principles; or (ii) there is a substantial likelihood that the principles are being violated.[31]

b) DPA Panel (FAQ 5)

US organizations may commit themselves to co-operate with European DPAs, as set forth in FAQ 5.[32] The panel, which consists of a number of DPA representatives, may advise US organizations on unresolved complaints from individuals about personal data transferred to the US under the SH pursuant to the procedure laid down in FAQ 5. Failure to comply with the panel's "advice" may constitute a deception or misrepresentation under the FTC Act. Companies must undertake to comply with the panel's advice (see FAQ 5). The panel's functions are to provide: (i) a harmonised and coherent approach for assuring compliance with the SH; (ii) advice to the US organizations on unresolved complaints from individuals about the handling of transferred personal data; (iii) follow-up for referrals from organizations and/or individuals (see FAQ 5).

There have yet not been any enforcement actions by the DPA Panel.[33]

c) Public Prosecutors

---

29 Article 3 uses the term "competent authorities" – thus, such power may be exercised by different authorities depending on the structure of each national legal system.

30 See FAQ 11.

31 This is the case only if: (i) there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; (ii) the continuing transfer would create an imminent risk of grave harm to data subjects; and (iii) the competent authorities in the EU/EEA Member State have made reasonable efforts under the circumstances to provide the organization with notice and an opportunity to respond.

32 Such co-operation is a prerequisite for the valid transfer of human resources data under the SH framework.

33 See <http://forum.europa.eu.int/Public/irc/secureida/safeharbor/home> (last visited 25 March 2004).

Public prosecutors are charged with the criminal enforcement of the national data protection laws. Violation of national data transfer provisions typically attract criminal sanction. Data subjects generally may also file a complaint with the public prosecutor's office in parallel with the DPA in case the data exporter violates the data protection law prior to or during a data transfer.

d) Courts (Criminal and Civil)

Civil and criminal courts have authority to decide on data exporters' compliance with local data protection law, and may, depending on the particulars of national law, block data transfers pursuant to Article 3 of the Commission Decision.

e) European Commission

The European Commission executes the following tasks:

- *Co-ordination of information*: EU/EEA Member States which block data flows are required to inform the Commission of the blocking action.[34] Additionally, Member States and the Commission inform each other about any failure of private US enforcement mechanisms;[35]

- *Notification of the DoC and/or modification of the Commission Decision in case of compliance failures*: if the Commission has evidence that "any body responsible for ensuring compliance with the SH principles (…) is not effectively fulfilling its role", the Commission is required to inform the DoC "and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope";[36]

- *Evaluation of the SH principles*: The Decision requires that the implementation of the principles is evaluated as well as any evidence (i) that could affect the adequacy finding inherent in SH, and (ii) that may demonstrate that the SH Decision is implemented in a discriminatory way. The implementation assessment is done by the current study;[37]

- *Presentation of draft measures*: the Commission may propose draft measures to improve the SH mechanism. Draft measures need to be agreed on by the Article 31 Committee.[38] The wording of the Decision connotes that the Commission can propose draft measures, if necessary, which implies that the review of the implementation is not a "one-shot" action.

---

34 Article 3(2) of the Decision.
35 Article 3(3) of the Decision.
36 Article 3(4) of the Decision.
37 Article 4(1) of the Decision.
38 Article 4(2) of the Decision.

f) Article 29 Data Protection Working Party and the Article 31 Committee

The Article 29 Data Protection Working Party delivered opinions on the level of protection provided by the SH which have been taken into account in the drafting of the Commission Decision.[39]

The Article 31 Committee will review the SH implementation report.

1.2.1.2 US Public Authorities

a) FTC/DoT

SH data transfers are valid only if they are conducted within the FTC's and the DoT's jurisdiction, and private SH recourse mechanisms will refer the case to the FTC/DOT if a complaint cannot be settled.

So far, there is no evidence that the FTC or DoT has undertaken enforcement actions.

b) State "Unfair and Deceptive Practices" Authority

Annex III in the SH overview refers to "Unfair and Deceptive Practices" Authorities at the State level ("mini-FTCs"). Violation of Article 5 of the FTC Act may also constitute a violation of State level legislation on unfair and deceptive practices.

c) The US Department of Commerce (DoC)

The DoC negotiated and developed the SH principles with the European Commission. US organizations must certify annually their adherence to the SH principles with the DoC. The DoC keeps a publicly available register of SH members. Further, the DoC co-ordinates and documents the entire registration process for US organizations.[40] The DoC has pointed out the following: "*In maintaining the list, the Department of Commerce does not assess and makes no representation as to the adequacy of any organization's privacy policy or its*

[39] Recital 10 in the preamble to the Decision. See *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government* (WP 15, 26 January 1999); *Opinion 2/99 on the adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19 April 1999* (WP 19, 3 May 1999); *Opinion 4/99 on the frequently asked questions to be issued by the US Department of Commerce to the proposed "Safe Harbor Principles"* (WP 21, 7 June 1999); *Working Document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles"* (WP 23, 7 July 1999); *Opinion 7/99 on the level of data protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce* (WP 27, 3 December 1999); *Opinion 3/2000 on the EU/US dialogue concerning the "SH" arrangement* (WP 31, 16 March 2000); *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"* (WP 32, 16 May 2000); and *Working Document on Functioning of the Safe Harbor Agreement* (WP 62, 2 July 2002).

[40] See <http://www.export.gov/safeharbour/sh_overview.html> (last visited 27 November 2003).

*adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.*"[41]

[41] Italics added by DoC; see "Safe Harbor Workbook", at <http://www.export.gov/safeharbor/sh_workbook.html> (last visited 23 February 2004).

d) US Courts

Data subjects may introduce a claim for a violation of the SH principles before US civil courts to obtain damages. However, data subjects will likely be successful only if they base their claims on breach of contract, i.e. in circumstances where acceptance of a privacy policy may be considered to constitute contractual rights and obligations.[42] Costs of such action are typically very expensive and generally not affordable to data subjects.

### 1.2.2 Private Actors

#### 1.2.2.1 European Private Actors

a) Data Exporter

The data exporter will be, under EU data protection law, a data controller (i.e. a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data).[43] Data processors (i.e. entities acting on behalf of the data controllers, and on the latter's instructions) can export personal data only if the data controller has given such instructions.

Data exporters need to comply with the local data protection rules to transfer personal data to a US SH organization. They will generally be the interface between the data subjects and the US data importer to handle data subjects' privacy concerns and/or complaints.

b) Data Subject

The SH principles primarily concern personal data which are sent to the US by EU-based data exporters. Although individuals' nationality is not a relevant criterion to decide whether personal data are protected by the principles, SH data transfers will generally concern European data subjects (this is not necessarily the case, for instance, if personal data of a Chinese citizen are transferred from a European database to the US under the SH regime). Of course, US organizations may use the principles to improve their privacy practices and also apply the principles to data pertaining to US nationals (or others). Data subjects generally will be natural persons as SH does not extend protection to data on corporations and other legal persons *per se*.

---

[42] Federal law does not provide any private right of action in the event of an unfair and deceptive trade practice: 15 USC section 45(a)(2). Hence, Safe Harbor does not create a federal private right of action before the US courts. See also J.R. Reidenberg, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal*, 2003, vol. 54, pp. 877 *et seq.* at 890. Private claims for a violation of Safe Harbor will only be available in either contract or tort. However,successful tort claims for privacy violations are very unlikely : *id.*, at 893–96.

[43] Article 2(d) of Directive 95/46/EC.

#### 1.2.2.2 US Private Actors

a) Data Importer (US organization)

Data importers are US organizations. The notion of US organization is not defined by the principles. Further on the scope of the notion, see *supra*, Part 1.1.3.

b) Data Importer's Agent

US organizations may use a "third party that is acting as an agent".[44] An agent is analogous to a data processor under Directive 95/46/EC. Agents may receive personal data only if the US organization ascertains that the agent subscribes to the principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that it provide at least the same level of privacy protection as is required by the relevant principles. The US data recipient may also be a data processor for the EU-based data exporter, in which case FAQ 10 applies.

c) Onward Transferee

Onward transferees may be: (i) other US organizations that are considered "data controllers" under EU data protection law; or (ii) agents or data processors.

d) Privacy Programs

Organizations may choose to adhere to a privacy program as a means of complying with the Enforcement Principle.[45] These programs are "private sector developed privacy programs that incorporate the SH Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle."[46] Depending on the type of privacy program, adherents may have latitude as to the modalities of implementation of the SH, or will need to respect rules specified by the privacy program service provider for specific data processing applications (for instance, online customer data-processing rules which specify the SH requirements to a specific data-processing scenario). Membership of a privacy program is not mandatory in the context of the SH.

---

44 See Onward Transfer principle.

45 FAQ 11.

46 *Id*.

e) Alternative Dispute Resolution Bodies (ADRs)

ADRs provide only for dispute settlement procedures without specifically requiring companies to implement privacy rules. In the context of data protection complaint handling, it is essential that such services are affordable and transparent to the data subject.[47]

### 1.2.3 Preliminary Conclusions

- The SH arrangement occupies the middle ground between a self-regulatory scheme and rules enforced by public authorities. As such, it may be viewed as a form for "co-regulatory" scheme. The SH regime is analogous to a state law regime since the principles have been adopted by the Commission, and private entities have no or little autonomy regarding the principles' substance – i.e. data controllers cannot choose their own principles and cannot go below the level of protection laid down by the principles. The principles show, however, more procedural autonomy than classic state regulation: (i) data importers are free to adhere to the principles; and (ii) enforcement can be handled by private enforcement programs. It also shows bi-cultural characteristics since it provides for a data protection regime that bridges regulation based on public law enforcement (EU) with a system relying primarily on the initiative of the private sector (US).

- This hybrid nature makes the SH system complex. Adding to the complexity is the multitude of actors involved in the system.

- At the same time, the complexity creates considerable potential for legal confusion and uncertainty for both companies and data subjects.

- Business representatives and intermediate organizations may have an important role to play in the SH scheme. They may provide for the institutional framework to develop and enforce privacy programs. Business organizations are important to inform member organizations of their obligations and to offer concrete tools and mechanisms to comply with the SH. For instance, the rules and principles set forth in the SH may be translated into codes of conduct to which member organizations represent adherence. They may also engage in complaint handling and have the organizational means to effectively sanction member organizations in case of violations.

---

[47] FAQ 11 reads: "[…] As required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organizations operating the recourse mechanism, but such requirements should be transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints […]."

## 2. Self-certification Page Analysis

This part provides for a factual analysis of representations in the self-certifications[48] made by SH companies on the DoC Certification page. All of the US organizations that were listed on the DoC SH certification list on 3 November 2003 have been reviewed.[49] At that date, 401 companies declared that they adhere to the SH principles.

---

[48] FAQ 6 on self-certification reads: "[…] To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:
1. name of organization, mailing address, e-mail address, telephone and fax numbers;
2. description of the activities of the organization with respect to personal information received from the EU; and
3. description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor, (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organization is a member, (f) method of verification (e.g. in-house, third party)(1), and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organization wishes its safe harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information that is listed in the annex to the Principles. In addition the organization must indicate this in its letter and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with FAQ 9 and FAQ 5 as applicable and that it will comply with the advice given by such authorities.

The Department (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of safe harbor benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. Such self-certification letters should be provided not less than annually. Otherwise the organization will be removed from the list and safe harbor benefits will no longer be assured. Both the list and the self-certification letters submitted by the organizations will be made publicly available. All organizations that self-certify for the safe harbor must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles.

The undertaking to adhere to the Safe Harbor Principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the safe harbor. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the safe harbor for any reason.

An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (1) continue to be bound by the Safe Harbor Principles by the operation of law governing the takeover or merger or (2) elect to self-certify its adherence to the Safe Harbor Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Safe Harbor Principles. Where neither (1) nor (2) applies, any data that has been acquired under the safe harbor must be promptly deleted.

An organization does not need to subject all personal information to the Safe Harbor Principles, but it must subject to the Safe Harbor Principles all personal data received from the EU after it joins the safe harbor.

Any misrepresentation to the general public concerning an organization's adherence to the Safe Harbor Principles may be actionable by the Federal Trade Commission or other relevant government body. Misrepresentations to the Department of Commerce (or its designee) may be actionable under the False Statements Act (18 U.S.C. § 1001)."

[49] <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list> (last visited 23 February 2004).

The paragraphs below summarize the factual findings which are tabled and visualized in the charts attached in Appendix V. Data have been collected on the following parameters:

1. Industry sector information: exhaustive overview of all the industry sectors represented by the companies importing personal information under the SH agreement;

2. Data categories: rough classification of the various categories of personal data transferred under the SH regime as declared in the box "Personal Information Received from the EU";

3. Personal data covered: on-line, off-line, manually processed, and/or human resources;

4. Controller-to-controller, and controller-to-processor data transfers;

5. Privacy policy location accuracy: assessment of whether companies provide for an accurate and/or direct link to the relevant data privacy policy from the certification webpage;

6. Verification type: distinction between in-house and third party verification;

7. Regulatory body: this parameter indicates whether the SH adherent falls under the jurisdiction of the FTC or DoT, or whether they have erroneously mentioned the FTC as having jurisdiction (considering that they import human resources data);

8. Privacy program: this parameter indicates the various "privacy programs" that have been mentioned on the companies' certification pages;

9. Dispute resolution mechanisms/programs: this parameter indicates the various dispute mechanisms/programs that companies have mentioned on their certification page;

10. Co-operation with EU Data Protection Authorities: this parameter indicates companies' willingness to co-operate with EU DPAs; *and*

11. Certification status: this parameter indicates the certification status (current/not current).

The results of the review are as follows:

## 2.1 Results

### 2.1.1 Industry Sector Information (see graphic 1 in Appendix V)

The participating companies belonged mainly to the IT sector (51% in total):

| Industry Sector Information | |
|---|---|
| Computer Servcies (CSV) | 16% |
| Information Services (INF) | 13% |
| Computer Software (CSF) | 12% |
| General Services (GSV) | 6% |
| Advertising Services (ADV) | 4% |
| Others | 49% |

The complete list of services as classified on the DoC website is as follows:

ACE: Architectural/Construction/Engineering Services
ACR: Air Conditioning & Refrigeration Eq.
ACT: Accounting Services
ADV: Advertising Services
AGC: Agricultural Chemicals
AGM: Agricultural Machinery & Equipment
AIR: Aircraft and Parts
APP: Apparel
APS: Automotive Parts & Service Equipment
ARW: Artwork
AUT: Automobiles & Light Trucks/vans
AUV: Audio/Visual Equipment
AVS: Aviation Services
BOK: Books & Periodicals
BTC: Biotechnology
BUS: Business Equipment (other than computers)
CEL: Consumer Electronics
COL: Coal
CON: Construction Equipment
COS: Cosmetics & Toiletries
CPT: Computer & Peripherals
CRM: Ceramics Fine Advanced
CSF: Computer Software
CSV: Computer Services
DFN: Defense Industry Equipment
DRG: Drugs and Pharmaceuticals
EDS: Education and Training
EIP: Electronic Industry Prod/Test
ELC: Electronic Components

ELP: Electrical Power Systems
EMP: Employment Services
FLM: Films Videos & Other Recording
FNS: Financial Services
FOD: Foods Processed
FOT: Footwear
GCG: General Consumer Goods
GFT: Giftware
GIE: General Industrial Equipment & Supplies
GST: General Science and Technology
GSV: General Services
HCG: Household Consumer Goods
HCS: Health Care Services
ICH: Industrial Chemicals
INF: Information Services
INS: Insurance Services
INV: Investment Services
LAB: Laboratory Scientific Instruments
LES: Leasing Services
MCS: Management Consulting Services
MED: Medical Equipment
MTL: Machine Tools & Metal Working Equipment
MUS: Musical Instruments
OGM: Oil & Gas Field Machinery
OGS: Oil Gas Mineral Production/Exp Services
OMS: Operations & Maintenance Services
PAP: Paper & Paperboard
PCI: Process Controls Industrial
PHT: Photographic Equipment
PMR: Plastic Materials & Resin
PRT: Port & Shipbuilding Equipment
PUL: Pulp & Paper Machinery
PVC: Pumps Valves & Compressors
REQ: Renewable Energy Equipment
RRE: Railroad Equipment
SPT: Sporting Goods Recreational Equipment
TEL: Telecommunication Equipment
TES: Telecommunications Services
TOY: Toy & Games
TRA: Travel and Tourism Services
TRK: Trucks, Trailers & Buses
TRN: Transportation Services (Except Aviation)
TXF: Textile Fabrics

### 2.1.2 Data Categories (see graphic 2 in Appendix V)

The analysis of this parameter is based on the certification pages' entry titled "Personal Information Received from the EU." Personal information could be roughly reduced to the following categories:

- C: Commercial (data used for advertisement purposes, in pre- and contractual relations, after-sale services, consumer data, etc.)
- HR: Human Resources
- RE: Research (including market research)
- T: Travel
- M: Medical
- RH: This category was included to refer to companies which represented themselves as receiving HR data from the EU in the item "Human Resource Data Covered," but did not make such a representation in the entry "Personal Information received from the EU".

Many companies did not define the categories of "Personal Information received from the EU", but explained how data are processed, the purpose, the business model, etc. In those cases, the data categories were inferred, to the extent possible, from the processing model description.

The approximate results of representations are as follows:

- Nearly half of the data types were Commercial data;
- More than one third concerned Human resources data[50];
- The remainder concerned Research data, Travel data and Medical data.

Note that the figures resulting from the Human Resources data category do not coincide exactly with the figures obtained in point 2.4 (Personal data covered), since in certain cases the representation made in that entry and in the one under analysis did not match.

### 2.1.3 Controller/Processor (see graphic 3 in Appendix V)

Eleven percent (11%) of the companies declared that they import personal information in a data processor capacity. The other 89% must be considered data controllers.

It should be stressed that the number of organizations importing personal data in a data processor capacity may be higher in reality, since the distinction between controllers and processors is not necessarily indicated on the certification page, and may appear only from the privacy policy.

---

[50] This includes the companies (9%) that did not specify this data type under the item "personal information received from the EU," but answered positively under the item "personal data covered". These are the companies that scored "RH".

2.1.4 Personal Data Covered (see graphic 4 in Appendix V)

The results are as follows:

| Personal Data Covered | |
|---|---|
| On-line Data | 37% |
| Off-line Data | 25% |
| Human Resources Data | 21% |
| Manually Processed Data | 17% |

The distinction between these four categories is set forth on the DoC certification page. It should be noted that this page blends data type with data-processing modalities (online, offline and manual).

2.1.5 Privacy Policy Location Accuracy (see graphic 5 in Appendix V)

Companies adhering to the SH agreement must specify in the certification page or letter where the privacy policy is made publicly available. Normally, they include a hyperlink to their privacy policy. However, the hyperlink sometimes led to a company's homepage and not directly to the privacy policy.

Certain companies give sometimes a physical address where the privacy policy is supposed to be available, or they mention "Available Upon Request." Those categories do not *per se* mean that the location is accurate or that the policy is truly available to the public. Only in the context of the in-depth analysis were such companies contacted by e-mail in order to get hold of their policy (see *infra*, part 3.1.1).

The categories applied in the analysis are as follows:

- Y: Yes (the hyperlink given in the certification page led directly to the relevant privacy policy);
- No: No (the hyperlink given did not work or no link was given);
- NDL: No Direct Link (the link provided did not lead directly to the privacy policy but to the homepage. It was necessary to search in the company's website to find the policy);
- PA: Physical Address (a physical address was given as location);
- Intranet: the company stated that its privacy policy is located on the company's Intranet); *and*
- AUR: Available Upon Request

The following results were scored:

- 40% of the companies provided a hyperlink in the certification page which led directly to the relevant privacy policy;

- 33% of the companies did not provide for a direct link to a relevant privacy policy but to their respective homepages;
- 13% did not provide any hyperlink or the one provided did not work;
- 6% of the companies declared that the policy is available on their intranet;
- 5% of the companies certified that the policy can be obtained at a physical address; *and*
- 3% specified that the policy is available upon request.

2.1.6 Verification (see graphic 6 in Appendix V)

- 86% of the SH companies opted for in-house verification.
- 14% chose a third party verification mechanism.

2.1.7 Regulatory body (see graphic 7 in Appendix V)

All but one company represented themselves as falling under the jurisdiction of the FTC. One US organization represented itself as regulated by the DoT. However, organisations importing human resources data scored "error", because FTC jurisdiction over human resources data is doubtful. Organizations which represented themselves as importing both human resources data and non-human resources data scored "both." As a consequence, approximately half of the companies, representing themselves as importing human resources data, doubtfully fall under FTC jurisdiction.

2.1.8 Privacy Program (see graphic 8 in Appendix V)

The SH does not provide for a positive definition of the term "privacy program." However, the meaning of the term can be deduced from FAQ 11, which states, *inter alia*, that privacy programs have to "incorporate the Safe Harbor Principles into their rules and … include effective enforcement mechanisms of the type described in the Enforcement Principle." Privacy programs must be distinguished from mere dispute settlement programs or services which do not set forth substantial privacy requirements. While most companies did not adhere to a privacy program, some did. Whereas the adoption of an independent recourse mechanism in order to satisfy the Enforcement principle is mandatory, the adoption of a privacy program is not mandatory.

Few of the items mentioned below can be considered privacy programs. The following chart indicates the organizations that have been certified as a "privacy program," whether true (privacy program) or false.

AAA: American Arbitration Association
AABB: American Association of Blood Banks
AIM: Association for Interactive Marketing
ASISP: American Society for Industrial Security's Privacy
BBB: BBBOnLine

BNI: Business Network International
BR: The Belmont Report
CASRO: Council of American Survey Research Organizations
CAUCE: Coalition Against Unsolicited Commercial E-mail
CFR: The Code of Federal Regulations
CIDE: Chemical Industry Data Exchange
CLSR: Center for Legal and Social Responsibility
CNIL member: "We registered our privacy policy to the Commission Nationale de l'Informatique" [*sic*]
COPPA: Children Online Privacy Protection Act
CRe-m: Council for Responsible e-mail
CSPSTI: Cyber Security Data Exchange
DHHSFAPHS: The Department of Health and Human Services Federalwide Assurance of Protection for Human Subjects
DMA Privacy Promise
DMA: Direct Marketing Association
DMACFCRe-mail: Direct Marketing Association Council for Responsible e-mail
DMAgui: Direct Marketing Association Guidelines
DMAshp: Direct Marketing Association SH Program
DoC: US Department of Commerce SH Program
Data Protection Authority for Human Resources
EPOF: European Privacy Officers Forum
EPON: European Privacy Officers Network
ESRBPOP: Entertainment Software Rating Board
GBCC: The Greater Boston Chamber of Commerce
GHEI: Guidelines for Handling Employee Information
HIPPA: Health Insurance Portability and Accountability Act
HON: Health on the Net
IAPO: International Association of Privacy Officers
IOPO: International Organization of Privacy Officers
KPMG: KPMG Security Seal
MRA: Marketing Research Association
NAI: Network of Advertising Initiative
NAITA: North Alabama International Trade Association
OPA: Online Privacy Alliance
P3P: Platform for Privacy Preferences
PAB : Privacy and American Business
PIMC: Personal Information Management Council
PrivacyBot
SHRM: Society for Human Resources Management
SSN: Secure Site Network
TPC : The Privacy Council
TRUSTe

The scores for adherence to SH privacy programs are as follows:

- 53% of the organizations were not members of a SH privacy program;
- 14% of the organizations were members of TRUSTe;
- 6% of the organizations represented themselves as adhering to the DMA privacy (or SH privacy) program;
- 5% of the organizations were members of BBBOnLine.
- 22%: others

### 2.1.9 Dispute Resolution Mechanisms/Programs (see graphic 9 in Appendix V)

In their self-certification letters, the participating companies are supposed to mention the independent recourse mechanism that is available to investigate unresolved complaints.

The following programs/services/associations were mentioned (whether or not they are actually ADRs):

DPA: Data Protection Authority
DMASHP: Direct Marketing Association Safe Harbour Program
DMA: Direct Marketing Association
TRUSTe
BBB: Better Business Bureaus
AAA: American Arbitration Association
HON: Health On the Net
USERTRUST
ESRBPOP: Entertainment Software Rating Board
Eftpeb: Exception for third party enforcement body
JAMS: Judicial Arbitration and Mediation Service
CFO: [meaning of acronym not apparent]
OR: Online Resolution
WWTS: SH Team at World Wide Travel Service

The scores for the most relevant categories are :

- Almost two thirds of the companies represented themselves as co-operating with the DPA panel;
- Less than a fifth of the companies were members of TRUSTe;
- Less than 10% of the companies were members of BBBOnLine;
- Less than 10% were members of the DMA (without specification to implement the DMA SH programme);

- Less than 5% represented adherence to AAA dispute resolution;
- Less than 5% adhered to the DMASHP.

2.1.10 Co-operation with EU Data Protection Authorities (see graphic 10 in Appendix V)

- 73% of the US organizations certified their willingness to co-operate with the EU DPAs;

- 27% did not certify such willingness.

Within the class of 27%, 5 companies (approx. 1% of the companies) imported human resources data, for which co-operation is mandatory.

2.1.11 Certification Status (see graphic 11 in Appendix V)

- 94% of the certifications were "current;"

- 6% were "not current".

2.1.12 DoC Self-certification Information

Further to the data above, it is useful to replicate below the DoC webpage that offers information for certification,[51] in order to provide a graphic view of certain tools provided to companies for the self-certification process:

**********

**Information Required for Safe Harbor Certification**

To expedite the certification process, please compile the following information before you go online to certify your organization's participation.

**1. Organization Information:**

**A.** Name
**B.** Address
**C.** City
**D.** State
**E.** Zip
**F.** Phone
**G.** Fax
**H.** Website (Optional)

[51] Available at <http://www.export.gov/safeharbor/sh_registration.html> (last visited 25 March 2004).

**2. Organization Contact Information (for the handling of complaints, access requests, and any other issues arising under the safe harbor):**

**A.** Contact Office
**B.** Contact Name (Optional)
**C.** Contact Title (Optional)
**D.** Contact Phone
**E.** Contact Fax
**F.** Contact Email

**3. Corporate Officer who is certifying the organization's adherence to the safe harbor framework:**

**A.** Corporate Officer Name
**B.** Corporate Officer Title
**C.** Corporate Officer Phone
**D.** Corporate Officer Fax
**E.** Corporate Officer Email

**4. Description of the activities of the organization with respect to personal information received from the EU.**

**5. Description of the organization's privacy policy for personal information:**

**A.** Effective date of your organization's privacy policy

**B.** Location of your organization's privacy policy

**C.** Specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Annex to the Principles): (Federal Trade Commission or Department of Transportation)

**D.** Information on any privacy programs relevant to the safe harbor in which the organization is a member

**E.** Method of your organization's verification (e.g., In-house, Third Party. (See FAQ 7))

**F.** Independent recourse mechanism(s) available to investigate unresolved complaints (e.g., private sector developed privacy program that incorporates the Safe Harbor Principles, legal or regulatory supervisory authorities that provide for the handling of individual complaints and dispute resolution, or EU data protection authorities. (See FAQ 11)

**G.** Data Covered by the safe harbor (e.g., off-line, on-line, manually processed data, human resources data)

**6. Additional Information Required**

**A.** EU Countries that you receive information from: (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom)

**B.** Industry Sector - you can select up to 3 sectors (View Safe Harbor Industry Sectors)

**C.** Level of organization sales (this information will not be posted on the website)
**D.** Number of employees (this information will not be posted on the website)

---

2.1.12.1 Preliminary conclusions

- It is advisable that, with respect to point 1.H (Website) of the certification information form set out above, the reference to the link be mandatory instead of optional (to the extent, of course, that the company has a website). With respect to point 2.B and C (Organization contact name and title), it is also advisable that the references be mandatory.
- The certification information can be made more transparent by adding clarifications (e.g. in the form of hyperlinks) particularly as regards: (i) key categories ("Personal data received from the EU", "Privacy programs", "Location of privacy policy", etc.); and (ii) main criteria to self-assess and register the processing ("Purpose", "controller/processor", obligation to comply with DPA advice, etc.), the understanding of which is problematic.
- It should be noted that, after May 2004, point 6.A will have to be extended to incorporate the 10 new EU Accession countries. It is also necessary to add references to Norway, Iceland and Lichtenstein (i.e. countries that are party to the EEA Agreement though not EU states).

2.1.13 DoC Self-Certification form

It is also useful to replicate below the form to be completed by companies that self-certify on-line.[52]:

OMB clearance number 0625-0239
Expire: 05/31/04

**To view the ITA Privacy Statement, click here.**

**CERTIFYING AN ORGANIZATION'S ADHERENCE TO THE SAFE**

[52] Available at <http://web.ita.doc.gov/safeharbor/shreg.nsf/safeharbor?openform> (last visited 25 March 2004).

## HARBOR

To expedite the certification process, prepare the required information before completing this form. **(See Information Required for Certification)** Please note that it is necessary to complete all fields except those with asterick(*).

Organizations that wish to submit their certifications on-line should file them between 6 am and 12 pm (EST) to avoid interference with routine maintenance that will be performed daily during early morning hours.

If you have any difficulty completing this form or have any other questions concerning the safe harbor, please contact Jeff Rohlmeier at the International Trade Administration, Department of Commerce, Jeff_Rohlmeier@ita.doc.gov or 202-482-0343.

Public reporting for this collection is estimated to range from 20-40 minutes per response, including the time for reviewing instructions, and completing and reviewing the collection of information. All responses to this collection of information are voluntary, and will be provided confidentially to the extent allowed under the Freedom of Information Act. Notwithstanding any other provisions of law, no person is required to respond to nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a current valid OMB Control Number. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Reports Clearance Officer, International Trade Administration, Department of Commerce, Room 4001, 14th and Constitution Avenue, N.W., Washington, D.C. 20230.

**ORGANIZATION INFORMATION**

| | |
|---|---|
| Organization Name: | |
| Address: | |
| City: | |
| State: | Minnesota |
| Zip: | |
| Phone: | |
| Fax: | |
| *Website: (Optional) | http:// |

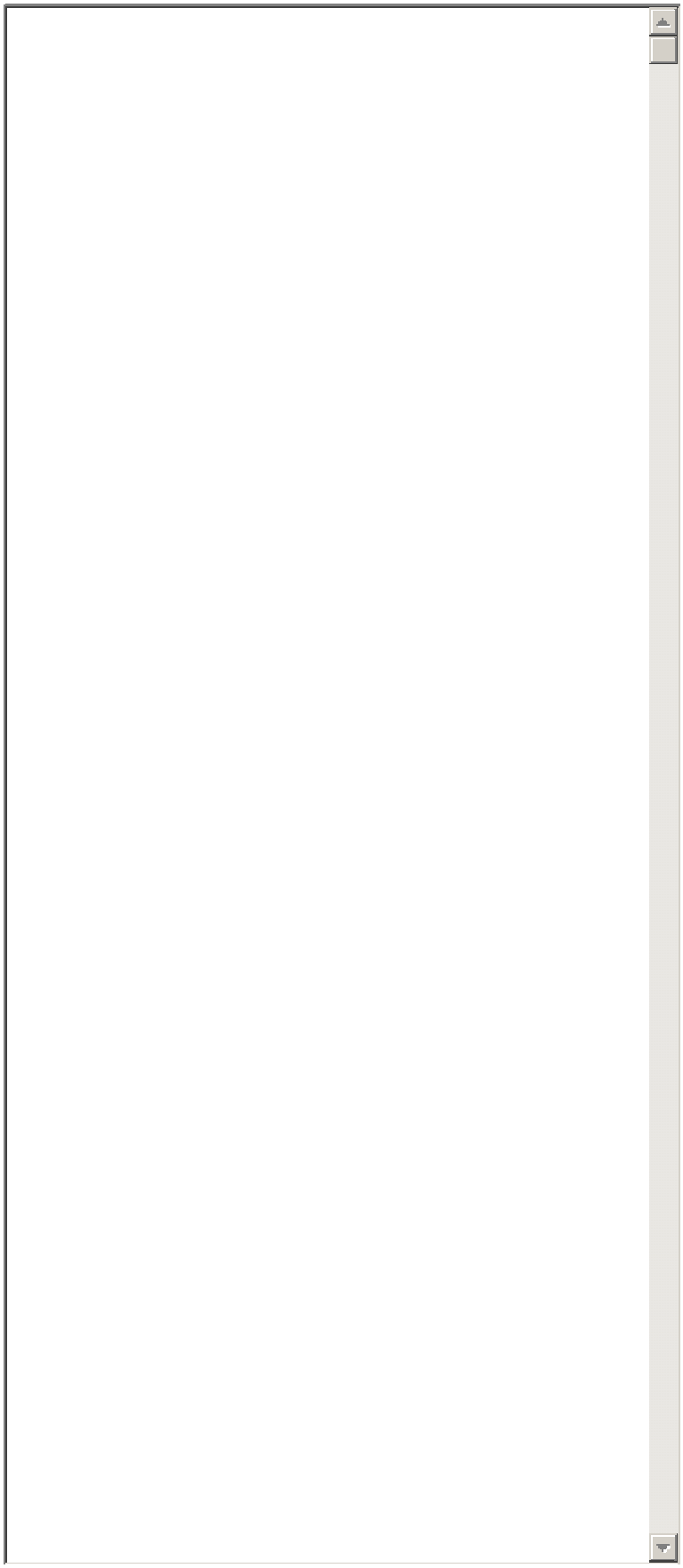
**ORGANIZATION CONTACT INFORMATION** (FOR HANDLING OF COMPLAINTS, ACCESS REQUESTS, AND ANY OTHER ISSUES ARISING UNDER THE SAFE HARBOR)

| | |
|---|---|
| Contact Office: | |
| *Contact Name: (Optional) | |
| *Contact Title: (Optional) | |
| Contact Phone: | |
| Contact Fax: | |
| Contact Email: | |

**CORPORATE OFFICER** WHO IS CERTIFYING THE ORGANIZATION'S ADHERENCE TO THE SAFE HARBOR FRAMEWORK

| | |
|---|---|
| Corporate Officer Name: | |
| Corporate Officer Title: | |
| Corporate Officer Phone: | |
| Corporate Officer Fax: | |
| Corporate Officer Email: | |

**DESCRIPTION OF THE ACTIVITIES** OF THE ORGANIZATION WITH RESPECT TO PERSONAL INFORMATION RECEIVED FROM THE EU



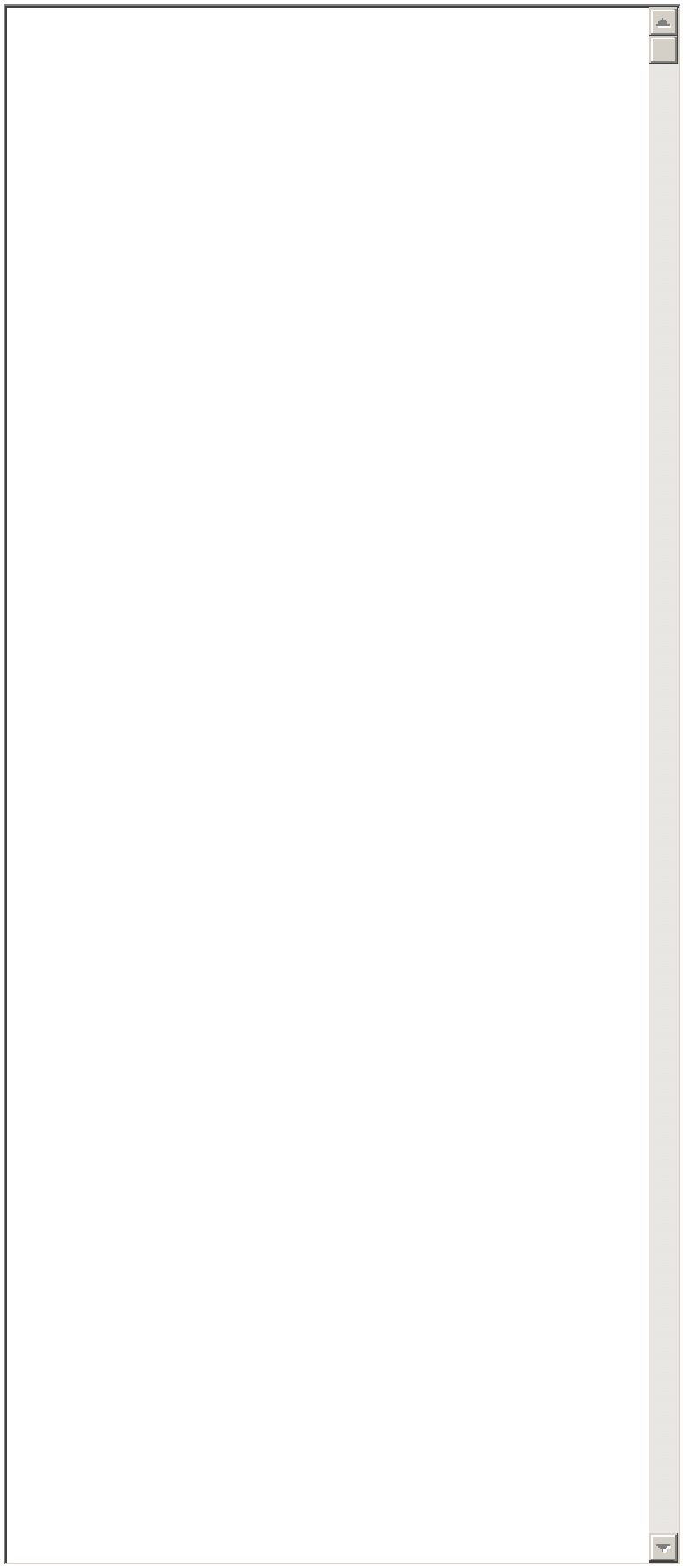
## DESCRIPTION OF THE ORGANIZATION'S PRIVACY POLICY FOR PERSONAL INFORMATION

Please enter the effective date of your organization's privacy policy:

Please provide the location of your organization's privacy policy: http://

Please indicate the appropriate statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy: Select Statutory Body

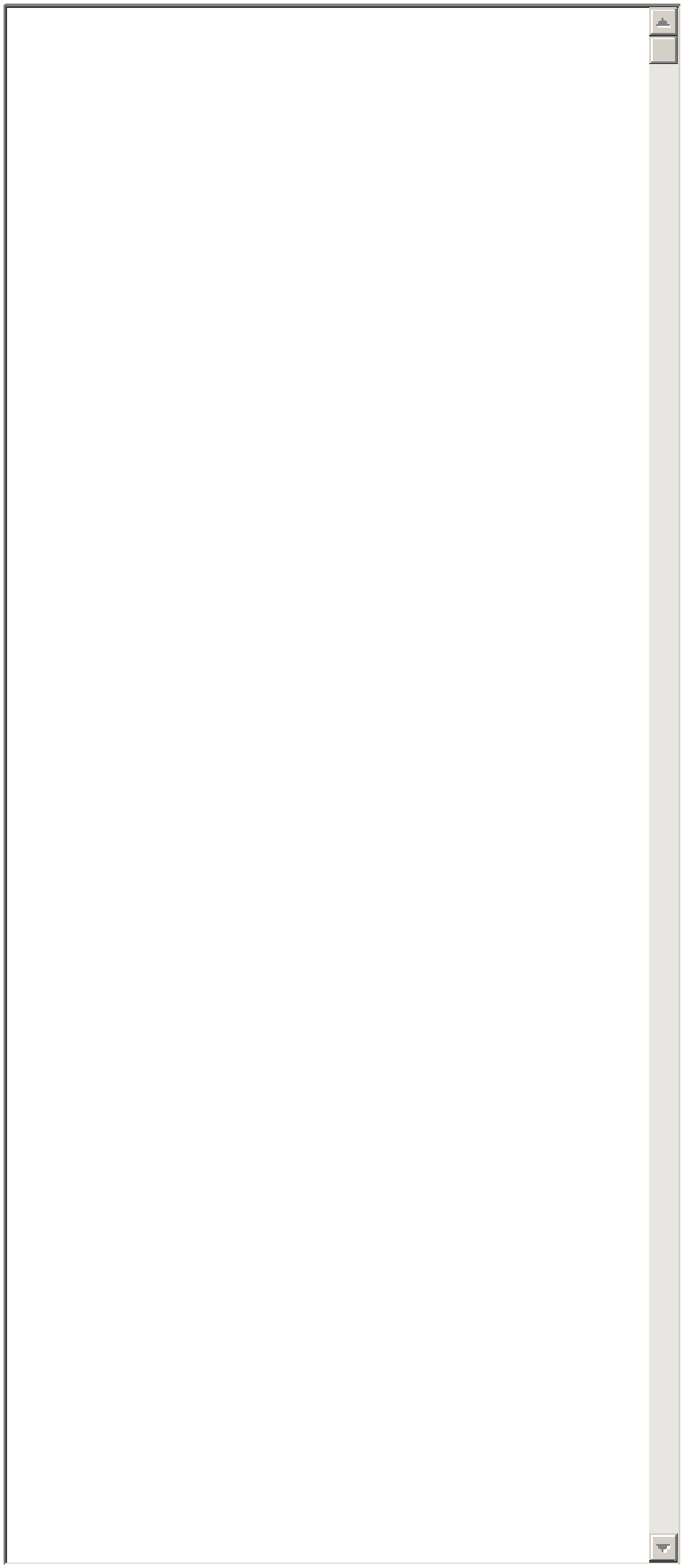
List any privacy programs in which your organization is a member for safe harbor purposes:



(See FAQ 6)

What is your organization's verification method (e.g., In-house, Third Party. **See FAQ 7**)

What independent recourse mechanism(s) is(are) available to investigate unresolved complaints (e.g., private sector developed dispute resolution mechanisms that incorporate the safe harbor framework or EU data protection authorities.
(**See FAQ 11**)?



What personal data processed by your organization is covered by the safe harbor? (e.g., off-line, on-line, manually processed data, human resources data)

Do you plan to cover human resources data?

Select Appropriate Response

If yes, you need to agree to cooperate with the Data Protection Authorities (See FAQs **5** & **9**).
Do you agree to cooperate with the EU Data Protection Authorities?

Select Appropriate Response

Which EU Countries do you receive information from? (Select all that apply)

☐ None ☐ Austria ☐ Belgium ☐ Denmark ☐ Finland ☐ France ☐ Germany ☐ Greece
☐ Ireland ☐ Italy ☐ Luxembourg ☐ Netherlands ☐ Portugal ☐ Spain ☐ Sweden ☐ United Kingdom

Please select your appropriate Industry Sectors. (Select up to 3.)

Select 1st Industry Sector

Select 2nd Industry Sector

Select 3rd Industry Sector

Please select the appropriate level of sales?: Enter Sales Amount

How many employees does your organization have?: Enter Number of Employees

Please print out your completed form now to verify that the information provided is correct and to retain a copy for your files.

If you are ready to submit the self certification for your organization simply click the **SUBMIT** button below.

Return to Welcome | Safe Harbor Overview | Safe Harbor Documents Workbook | Safe Harbor List | Information Required for Certification

2.1.13.1 Preliminary conclusions

- The analysis of data categories was often difficult since certain companies described the activities conducted instead of the type of personal data imported. Transparency of processing would be improved if the DoC certification form includes entries for "data type", "activity/ies" and "purpose/s of processing". This information is also necessary in order to evaluate respect for the SH "Data

Integrity" principle, i.e., "personal information must be *relevant* for the purposes for which it is to be used" (italics added). Considering that the style of privacy policies is different, and that it may take some time for the concerned actor to recognize the suggested parameters ("data type, "activity/ies" and "purpose/s of processing") in a systematic way, it is important to include them in the certification page. This would be also important for an enforcement body in the event that questions arise about the "relevance" of data *vis-à-vis* usage purpose.

- A considerable proportion of the imported data concerns human resources. The jurisdiction of the FTC seems dubious as regards the importing and processing of human resources data. It is necessary to determine more accurately the scope of the FTC's competence in this context and to determine if there is another competent body to hear claims concerned with use of such data.

- The entry, "Personal Data Covered", blends data type ("human resources") with data-processing modalities ("on-line", "off-line", and "manually processed"). To increase coherence, it would be preferable to separate both categories, taking out the "human resources" option from the entry, "Personal Data Covered", and adding it to a new entry, "Data Type".

- A significant proportion of importers are data processors. However, the DoC certification form does not contain information fields for controller-to-processor transfers. Taking into consideration that the legal obligations of data processors are different from those of data controllers, it is advised that the certification form distinguishes between both categories. In case data importers act both as controllers and processors, it is desirable that the respective capacity for each data stream be specified.

- The requirement that there be accurate location of privacy policies is not always met. This detrimentally affects transparency. It should be ensured that under the entry, "Location", the proper link to the privacy policy be given. Furthermore, even if the US organization imports only human resources data, it would be preferable to provide a direct on-line access to the privacy policy, which would facilitate any necessary action by an enforcement body.

- The third party verification method has not been widely adopted. It is advisable that there remains some traceable proof of in-house verification audits (for instance, a copy of in-house verification audit could be filed with the DoC).

- The definition of a "privacy program" is not clear; consequently, companies may believe that they adhere to a privacy program which is not really such a program. The findings indicate some mistakes of this kind occurring. Clarification is needed of what constitutes a privacy program. Guidance from the DoC and the Article 29 Data Protection Working Party could help resolve this issue, by providing for: (i) a positive privacy program definition, (ii) minimal privacy program standards; and (iii) a privacy program recognition procedure. The DoC could also register a list of privacy programs, and conduct an analysis based on the minimal standards to be imposed.

- The majority of the companies have chosen to co-operate with European DPAs as their Dispute Resolution method. Nevertheless, "co-operation" as such may not be enough to guarantee respect for final decisions adopted by DPAs. It may be advisable to add to the DoC certification form an entry to be filled in by companies that choose a DPA-based Dispute Resolution mechanism, whereby they represent their commitment to "comply" with DPA decisions. Concomitantly, it is suggested that in the event that such a mechanism is the only Dispute Resolution method adopted, yet the company does not represent an intention to comply with a DPA decision, the DoC would refuse to accept self-certification due to the company's failure to comply fully with the Enforcement Principle.

- As in the case of privacy programs, the DoC could maintain a list of Alternative Dispute Resolution organizations that may be used for the purposes of SH. It is doubtful that all the organizations named by self-certifying companies and listed under point 2.9 provide ADR services that are appropriate in the SH context.

- Finally, on the issue of certification status, there is no possibility to track which companies have been deleted from the list (apart from those scoring "not current"). It is important to bear in mind that even if a company decides to withdraw its SH adherence, it will be bound by the terms of the privacy policy under which it imported data from the EU insofar as it retains records of those data. Therefore, it would be convenient to add to the DoC website a list of companies that have withdrawn adherence or failed to annually verify their adherence, and, as a consequence, have been deleted from the SH list.

## 3. In-depth Implementation Analysis of SH

### 3.1 Visible Indicators and Trends on Compliance/Implementation

This section describes the results of the analytical analysis and identifies some indicators and trends regarding the implementation of the SH regime.

#### 3.1.1 Analysis of Adherent Organizations

As indicated above (in section II on Methodology), the assessments concern 10% (41 companies) of the organizations that had self-certified as of 3 November 2003.

Within that sample, 6 organizations did not make their privacy policies available on the web. As a consequence, they scored "unknown" for the substantive criteria if they acted as data controllers (4 companies), and "not applicable" if they acted as data processor (2 companies).

| Privacy Policy not available | |
|---|---|
| Company number | Score |
| 4 | Not applicable (processor) |
| 18 | Unknown (controller) |
| 21 | Not applicable (processor) |
| 23 | Unknown (controller) |
| 25 | Unknown (controller) |
| 29 | Unknown (controller) |

Five (5) companies represented to locate their privacy policy on an Intranet, and 3 to make the policy available at a physical address. Of those 8 companies, 6 certified that they import human resources data (with the other 2 acting as data processors). Strictly speaking, the privacy policy of companies importing human resources data has to be made available to these organizations' employees (as concerned data subjects). Thus, the fact that the privacy policy was not available online did not necessarily result in a negative score for these companies. However, an e-mail was sent to these companies (all 8) asking for a copy of their respective policies. Three (3) answers have been received, with the privacy policy that covers human resources data attached. As a result, the companies that did not reply to the e-mail scored "unknown". There is one more company that scored "unknown" although it partly disclosed a privacy policy (scoring "yes/no" in the parameter "Public Disclosure of privacy Policy").

| Intranet | |
|---|---|
| Company | Score |

| number | |
|---|---|
| 2 | Unknown (no answer) |
| 5 | Unknown (no answer) |
| 19 | Analysed |
| 27 | Analysed |
| 32 | Not applicable (processor) |

| Physical Address | |
|---|---|
| Company number | Score |
| 8 | Analysed |
| 28 | Unknown (no answer) |
| 34 | Analysed |

In those cases where companies score "yes/no", the analysis was conducted on the available policy. However, in the case of company number 7 the available policy covered only data-processing practices in a data processor capacity. For that reason, this company scored "unknown" in the substantive criteria.

| Companies that score "Unknown" | |
|---|---|
| Company number | Reason |
| 2 | Intranet (no answer) |
| 5 | Intranet (no answer) |
| 7 | Yes/no |
| 18 | Privacy policy not available |
| 23 | Privacy policy not available |
| 25 | Privacy policy not available |
| 28 | Physical address (no answer) |
| 29 | Privacy policy not available |

In total, 8 companies scored "unknown". While it is not possible to attach statistical significance to the outcomes with such a high "unknown" rate, the SH regime requires complete compliance with every criterion since all its criteria/principles are essential to guaranteeing adequate protection.

The results function as valid indicators of general SH compliance and show trends regarding the implementation of the SH principles. The report utilizes below the notions "General Observations", and "Organizations' Compliance Indicators". The "General Observations" describe the categories that may show certain factual data, but concerning which a compliance analysis cannot easily be made since they have little or no positive normative (or mandatory) value pursuant to the SH framework. "Organizations' Compliance Indicators" describe findings dealing with mandatory SH requirements.

It appears from the company representations made that 7 companies imported personal data as "processors", while 2 acted as both "controller" and "processor". The "processors" are not taken into account for the item "Organizations' Compliance Indicators", and they scored "Not applicable". This is because (as set forth by FAQ 10) data processors do not need to comply with most of the SH principles. The entities which imported data both in a capacity of "controller" and "processor" were analysed in their "controller" capacity only, because it is in this capacity that their legal obligations and liability could be compromised. The certification criteria were analysed for all 41 companies, but the substantive and enforcement criteria were analysed only for those companies importing personal data as data controllers. This implies that in the assessment of the certification criteria, 41 companies have been taken into account (both data processors and controllers), while the assessment of the substantive and enforcement criteria considered 34 companies (data controllers only).

#### 3.1.1.1 General Observations

- Slightly more than half of the organizations' **privacy policies were published on the web in a printable format**. For approximately one quarter of the policies, it was not possible to determine whether they were printable or not since they were not posted on the website. The remaining companies published a privacy policy covering only part of the certified data streams; [see Appendix VI, Table 1.1, graphic 2]

- The great majority of the organizations **represented using the SH principles for specific data streams**, while a limited number of companies did not restrict the personal data covered (these organizations used the principles for online data, offline data, human resources and manually processed data); [see Appendix VI, Table 1.1, graphic 3]

- Approximately one fifth of the reviewed privacy policies showed that the SH framework was used to send personal information to US organizations in their **capacity of data processors**. A very small minority were acting both as data controller and processor (with respect to different data streams), while the remaining companies were importing personal information exclusively as data controllers; [see Appendix VI, Table 1.1, graphic 6]

- Approximately three quarters of the SH organizations made no representation concerning any **US law preventing compliance** with the SH principles. Some of them made general references to the obligation to co-operate with law enforcement agents; [see Appendix VI, Table 1.1, graphic 5]

- More than one third of the companies claimed to participate in a **privacy program**; [see Appendix VI, Table 1.3, graphic 3]

- Nearly all of the companies chose an in-house **verification method**; [see Appendix VI, Table 1.3, graphic 4]

- More than half of the companies chose DPAs as an **independent recourse mechanism**. The order in popularity of the selected private sector recourse mechanisms was as follows: first TRUSTe, second DMA (non-specific SH program), third AAA, fourth BBBOnLine, and last DMASHP; [see Appendix VI, Table 1.3, graphic 5]

- Nearly half of the companies used the SH principles for importing **human resources data**; [see Appendix VI, Table 1.3, graphic 6]

- Approximately three quarters of the companies had decided to **co-operate with the European DPAs** (this does not necessarily imply that these companies agreed to implement DPA decisions). Note that very few (less than one fifth of the companies) had represented in their privacy policies an intention to co-operate with the DPAs. [see Appendix VI, Table 1.3, graphic 7]

- Less than half of the organizations described the **personal data type** received from the EU. Approximately one fifth provided for a description that is unclear.[53] [see Appendix VI, Table 1.2, graphic 6]

- Nearly half of the companies represented **third party disclosures**. One quarter scored "unclear", while a minority did not represent that they disclose personal data to third parties. One quarter scored "unknown"; [see Appendix VI, Table 2.1, graphic 4]

- More than one third of the companies did not give **notice for secondary use**. Approximately one third provided such notice. One quarter scored "unknown"; [see Appendix VI, Table 2.1, graphic 3]

- Approximately three quarters of the companies had chosen to provide **independent recourse mechanism pursuant to FAQ 5** (DPAs). [see Appendix VI, Table 3.1, graphic 1]

#### 3.1.1.2 Organizations' Compliance Indicators

(a) Eligibility indicators

- Approximately half of the organizations **publicly disclosed their privacy policy** on the web. The policies of 6 companies were not publicly available on the web. Five (5) organizations certified to have their policy published on their intranet, 3 certified that the policies were available at a given physical address, and 6 organizations provided erroneous hyperlinks. Seven (7) companies made publicly available a privacy policy that covered only part of the data processing indicated on the

[53] FAQ 6 sets forth that "to self-certify for the SH, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the SH, that contains at least the following information: […] [d]escription of the activities of the organization with respect to personal information received from the EU. […]".

certification page. For instance, the privacy policy covered only data collected on an organization's website (i.e. online data), while the certification page represented that the organization processed also human resources data, manually processed and/or online data. E-mails have been sent to those companies representing a physical address and intranet as the location for their privacy policies. Of the 8 e-mails sent, 3 answers have been received with the proper privacy policy as attachment; [see Appendix VI, Table 1.1, graphic 1]

- Approximately half of the companies represented that they may **make changes in their policy**.[54] Approximately one fifth did not make a representation to that effect. Approximately one quarter scored "unknown"; [see Appendix VI, Table 1.1, graphic 4]

- Approximately one third of the companies provided for an **accurate location** of the privacy policy from the DoC certification list. Approximately one third did not provide for an accurate location. One quarter scored "unknown". A minority of companies scored "yes/no" because the privacy policy that was accurately located, covered only part of the certified data streams; [see Appendix VI, Table 1.2, graphic 8]

- Approximately one fifth of the companies did not state the **specific statutory body that has jurisdiction to hear claims against the organization**. They were companies importing human resources data and they made dubious statements in their certification letters since the FTC appears to have no jurisdiction over human resources data. Another fifth of the companies imported both human resources data and other data types, and scored "yes/no". More than half of the organizations correctly specified the FTC as the regulatory agency; [see Appendix VI, Table 1.1, graphic 2]

(b) Substantive indicators

- Less than half of the companies **specified the purpose** of processing activities. More than one quarter expressed it in an unclear fashion. Approximately one quarter scored "unknown"; [see Appendix VI, Table 2.1, graphic 1]

- Approximately two thirds of the companies included **organization contacts** in their privacy policy. A small minority did not include contact information. The remaining scored "unknown"; [see Appendix VI, Table 2.1, graphic 2]

- Nearly half of the companies provided **notice of choice for use**. Approximately one fifth of the companies provided notices in an unclear manner or did not provide choice at all. Approximately one third scored "unknown";[55] [see Appendix VI, Table 2.1, graphic 5]

---

[54] This indicates potential non-compliance.

[55] Figures based on 21 companies.

- Approximately two thirds of the companies explicitly stated in their relevant published privacy policy that they **adhere to the SH Principles**. A small minority did not make such a declaration. The remaining organizations scored "unknown"; [see Appendix VI, Table 2.1, graphic 7]

- Only 8 companies represented that they import **sensitive data**. One (1) company failed to represent that it provided opt-in for sensitive data, and 2 made unclear representations regarding opt-in. Another 5 companies represented opt-in;[56] [see Appendix VI, Table 2.2, graphic 7]

- Approximately half of the companies represented that they took **reasonable security measures**. Approximately one quarter of the companies did not make representations regarding security measures or made unclear representations. The remaining scored "unknown";[57] [see Appendix VI, Table 2.4, graphic 1]

- Approximately one third of the companies expressed the **notice in an unclear manner**. Less than half of the companies expressed it clearly. The remaining scored "unknown"; [see Appendix VI, Table 2.2, graphic 3]

- Approximately half of the companies expressed **notice in a conspicuous manner**. Approximately a quarter of the companies did not express it conspicuously. The remaining scored "unknown"; [see Appendix VI, Table 2.2, graphic 4]

- Less than half of the companies did not provide **notice of choice for dissemination of personal data to third parties,** or did not provide it in a clear manner. One third did provide such notice, and the remaining scored "unknown";[58] [see Appendix VI, Table 2.1, graphic 6]

- More than half of the **notices of choice** were not **readily available**. A minority were readily available. The remaining scored "unknown";[59] [see Appendix VI, Table 2.2, graphic 5]

- Nearly two thirds of the reviewed policies did not make representations regarding **affordability of choice**. The remaining scored "unknown";[60] [see Appendix VI, Table 2.2, graphic 6]

- More than one third of the companies did not represent their **third party processor's commitment to respect the SH**. Approximately one quarter did give such information. The remaining scored "unknown";[61] [see Appendix VI, Table 2.3, graphic 3]

---

[56] Figures out of a total of 16 companies since only data controllers that represented themselves as importing sensitive data and the companies scoring "unknown" were taken into account.

[57] Figures out of 41 companies.

[58] Figures based on 30 companies

[59] Figures based on 26 companies.

[60] Figures based on 26 companies.

[61] Figures based on 25 companies.

- Approximately half of the companies ambiguously specified the **relevance of the data for the specified purpose** ("unclear"), or did not specify it at all. A minority expressed it clearly, and the remaining scored "unknown"; [see Appendix VI, Table 2.4, graphic 2]

- Nearly half of the companies did not (or did not clearly) represent the adoption of any **steps to ensure reliability for the intended use**. Approximately one third represented to take such steps. The remaining scored unknown; [see Appendix VI, Table 2.4, graphic 4]

- Approximately half of the companies did not provide for **reasonable access**, while one quarter did provide access and the remaining scored "unknown"; [see Appendix VI, Table 2.5, graphic 1]

- Approximately two thirds of the reviewed policies represented that **cost for access** is reasonable/affordable or free; [see Appendix VI, Table 2.5, graphic 2]

- Approximately half of the companies represented to offer an opportunity for correction or amendment. Approximately one third of the companies did not provide for the possibility to make **correction/amendment** of inaccurate data, or made unclear representations. The remaining scored "unknown"; [see Appendix VI, Table 2.5, graphic 3]

- Approximately half of the companies did not provide the possibility to **delete inaccurate data** or made unclear representations on this point. Approximately one quarter provided that possibility, and the remaining scored "unknown". [see Appendix VI, Table 2.5, graphic 4]

(c) Enforcement Indicators

- Almost two third of the companies had represented to **co-operate with the DPAs** only on the DoC certification page.[62] Approximately one fifth had represented their co-operation on both the certification page and in their privacy policy. The remaining quarter did not represent to co-operate with the DPAs; [see Appendix VI, Table 3.2, graphic 2]

- More than two thirds of the companies did not agree to **comply with the advice** of the DPAs. Less than 10% (2 companies) agreed to comply with DPA advice. The rest scored unknown; [see Appendix VI, Table 3.2, graphic 3]

- None of the companies had elected an **US legal or regulatory supervision body other than the FTC**;[63] [see Appendix VI, Table 1.1, graphic 1]

---

62 This arguably indicates that the commitment is questionable.

63 See FAQ 11.

- All of the companies had represented to opt for **independent recourse mechanisms**.[64] [see Appendix VI, Table 3.3, graphic 2] All of these mechanisms are **readily available**; [see Appendix VI, Table 3.3, graphic 3]

- More than half of the companies **transparently set forth a dispute resolution procedure in their privacy policy**, while approximately one quarter did not transparently mention or describe such procedures. The remaining scored "unknown." [see Appendix VI, Table 3.3, graphic 4]

- Nearly three quarters of the companies did not agree to **reverse the effects of a breach**, or expressed their agreement in an unclear manner. A minority offered reversal, and the remaining scored "unknown"; [see Appendix VI, Table 3.3, graphic 5]

- Nearly three quarters of the companies had not represented adherence to a dispute resolution proceeding that foresees a **remedy compelling future processing** to conform with SH, or the existence of such a remedy was "unclear". A minority did offer such a remedy, and the remaining scored "unknown"; [see Appendix VI, Table 3.3, graphic 6]

- More than three quarters of the companies did not represent as a remedy the **cessation of processing** of the personal data, or the existence of such a remedy was "unclear". A minority did offer such a remedy and the remaining scored "unknown"; [see Appendix VI, Table 3.3, graphic 7]

- Almost three quarters of the companies did not include as an available sanction **publicity for findings** of non-compliance or scored "unclear". A minority provided for a publication measure, and the remaining scored "unknown"; [see Appendix VI, Table 3.3, graphic 8]

- Less than half of the companies did not provide for **sanctions** either in the privacy policy or through the ADR entity chosen. Nearly half represented sanctions or a sanction regime, and the remaining scored "unknown". [see Appendix VI, Table 3.3, graphic 9]

[64] Further research is needed to determine whether these mechanisms are *effectively* independent, by analyzing concrete decision-making.

### 3.1.2 Analysis of Privacy Programs and ADR Bodies

#### 3.1.2.1 Privacy Programs and ADRs' Compliance Indicators

(a) Substantive indicators

Of the 7 organizations mentioned by the 41 sampled companies, only 4 are really "privacy programs" (the other 3 scored "not applicable"). The following remarks pertain only to those 4 organizations:

- Most privacy programs provide for **program contacts**;
- Most of the programs did *not* require their members to make a **statement on SH compliance**;
- Most of the programs required members to draft their **privacy policies in a clear and conspicuous manner**;
- Most of the privacy programs required their members to **specify the processing purposes** in their privacy polices;
- Most of the privacy programs required their members **to disclose third party r**ecipients;
- Most of the privacy programs required their members to provide the data subject **choice for data use and dissemination**;
- Less than half the privacy programs required their members to provide **choice in a clear and conspicuous manner**;
- Most of the privacy programs did *not* require their members to provide **readily available choice**;
- Most of the privacy programs did *not* require their members to provide **affordable choice**;
- Most of the privacy programs did *not* require their members to provide **opt-in for sensitive data**;
- Most of the privacy programs did *not* require their members to provide third **party processor's commitment** to respect the SH in case a processor intervenes;
- Most of the privacy programs required their members to adopt **reasonable security precautions**;

- Most of the privacy programs did *not* require their members to process only personal information that is **relevant for the purposes** for which it is to be used;

- Most of the privacy programs required their members to adopt steps to **ensure reliability for intended use**;

- Most of the privacy programs required their members to provide for **reasonable access**;

- Most of the privacy programs did *not* require their members to provide for **affordable access**;

- Most of the privacy programs required their members to provide the possibility of **correction of inaccurate data**;

- Most of the privacy programs required their members to provide the possibility of **amendment of inaccurate data**;

- Most of the privacy programs did *not* require their members to provide the possibility of **deletion of inaccurate data**;

(b) Enforcement indicators

This part concerns the ADR organizations mentioned by the 41 selected companies, as well as the organizations mentioned in the DoC website.[65] One organization scored "unknown" because the rules of procedure were not found on its website. Other organizations scored "not applicable" because no dispute resolution services were offered.

- Most of the ADRs claimed to be **independent**;

- Most of the ADRs claimed to **investigate** each complaint;

- Most of the ADRs claimed to offer a **readily available and affordable recourse**;

- Most of the ADRs provided **transparency for the recourse procedures**;

- Most of the ADRs were unclear as to whether **the effects of breach are reversed**. One of them did *not* foresee that remedy;

- Some of the ADRs foresaw obtainment of SH compliance in **future processing activities**. Some were unclear on this point. One did *not* foresee it;

[65] See *supra*, section on methodology.

- Most of the ADRs were unclear as to whether they would obtain **cessation of illegal processing**. One did *not* foresee cessation, while another one did so;

- Some of the ADRs foresaw **compensation for harm.** Some were unclear in this regard. One organization did not foresee compensation.

- Some of the ADRs foresaw privacy program **sanctions**;

- Most of the ADRs did *not* foresee **publication of the imposed sanctions**. One organization did so, another was "unclear";

- Most of the ADRs did *not* foresee a **mandatory referral of sanctions**. Some were "unclear" on this point.

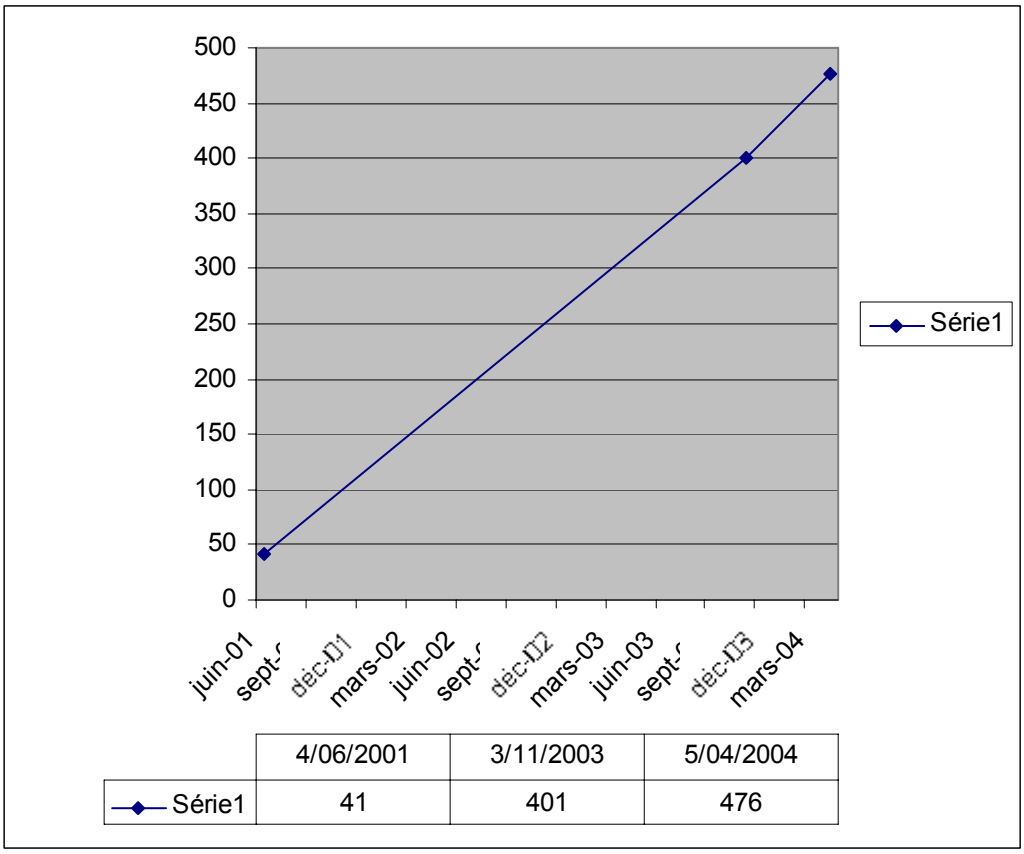
### 3.1.3 Main Findings

#### 3.1.3.1 Positive Trends

The analysis demonstrates that, despite many shortcomings, some companies invest in personal data protection. The following positive trends can be discerned:

- *Increased SH Participation*

At the time of the intermediate report, only 48 US organizations had signed up for the SH. As of 3 November 2003, 401 companies were mentioned in the DoC certification list. However, in order to be able to make an objective evaluation of this number, it would be necessary to know the total number of US organizations that import data from the EU.




- *Co-operation with DPAs*

A considerable number of companies certified that they co-operate with European DPAs. The analysis of the privacy policies indicates that certain companies agreed to co-operate with the DPAs even though they did not process human resources data. Although the concrete motives of these organizations could not be determined, and might be, for instance, simply a desire to limit legal uncertainty, such agreement is positive in itself.[66]

- *Additional Information in Privacy Policies*

Some companies provided information in their privacy policies which is not strictly required by the SH principles. For instance, a considerable number of companies that collect information online, explain in detail the use of cookies and log files.

- *Security Measure Compliance by Data Processors*

US data processors generally represent the existence of security measures.

[66] Since there have been no enforcement cases by the DPA Panel so far, it is difficult to appraise the meaning of such declarations of co-operation.

- *Contact Information (in the self-certification page)*

SH adherents generally provided full contact information in the DoC self-certification page. However, privacy policies did not always contain adequate contact information.

3.1.3.2 General Observations

- *The IT sector is the most represented industry sector within the US organizations that adhere to SH.*

- *Controller-to-Processor Applications*

Nine (9) of the reviewed privacy policies concerned controller-to-processor personal data transfers (2 of the organizations concerned also imported personal data in a data controller capacity). The analysis of the certification page[67] demonstrates that approximately 11% of the US organizations represented to import personal data as data processors.[68]

Although the SH principles were not specifically designed to accommodate this type of personal data transfer, FAQ 10 ("Article 17 Contracts") refers to this scenario. FAQ 10 recognizes that SH companies can participate in the SH framework but need to be further bound by a contract setting forth specific processing instructions, confidentiality requirements, and organizational and technical requirements as provided for in Article 17 of Directive 95/46/EC. US organizations that receive EU data for processing only, need not implement the other SH principles.

The SH principles were originally drafted for controller-to-controller data streams, and the text of FAQ 10 seems incompatible with the requirements set forth in the Commission Decision approving the model clauses for controller-to-processor transfers.[69] It appears that the same level of protection should be guaranteed as in those clauses, and that an Article 17 contract does not suffice.

Nevertheless, the SH policies of these companies which are publicly available showed generally that the companies had only implemented the security principle. More particularly, companies importing personal data as data processors generally represented to provide for specific security requirements entailing authentication, authorization measures, audits, system

---

67 See *supra*, point 2.3

68 This number may vary depending on the statements made in the privacy policies.

69 See FAQ 10: "[…]Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body who determines the purposes and means of processing, who retains full responsibility for the data vis-à-vis the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure.

A U.S. organization participating in the safe harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it vis-à-vis the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles)."

security, disaster prevention and recovery, physical security measures and confidentiality guarantees.

As already pointed out in the preliminary conclusions of point 2,[70] it is advisable to add an entry in the self-certification form for importers to identify their capacity either as controllers, processors, or both (and in the last case, for which processing activities). Although, the notions of data controller and data processor are European legal concepts, it is essential for reasons of transparency and legal certainty that guidance is provided on the obligations/requirements that a data importer needs to fulfil when acting in the capacity as data processor. It remains unclear what the expectations are regarding the implementation of SH principles by such organizations. One would expect that data importers which are data processors only need to provide for security and confidentiality requirements analogous to the requirements set forth in Articles 16 and 17 of Directive 95/46/EC. However, a close reading of FAQ 10 seems to exclude applicability of even the security principle and merely requires signing of a processing agreement. It is difficult to see what the added value is of certifying to SH if the principles need not to be respected. Also, it remains unclear what agreement needs to be signed (mere use of an Article 17 contract appears to be irreconcilable with the requirements set forth in the Commission Decision on controller-to-processor model clauses). In addition, transparency needs to be created since data subjects need to know to whom they can address any queries, complaints, etc., in short who is responsible for the processing of data pertaining to him/her.

To settle this matter, a dialogue between the US and EU authorities may be required to determine clearly the legal requirements for this kind of data transfers. Furthermore, if it is confirmed that SH can be used for controller-to-processor transfers, a separate DoC listing (or a specific template for this kind of transfers) could be introduced explaining the requirements. SH companies that are already importing personal data as a data processor should be informed of any rectifications they need to introduce.

- *Sensitive Data Transfers*

The number of companies that represented to transfer sensitive data under SH is relatively small (approximately one fifth of the reviewed policies). It should be noted that 6 of the 8 companies transferring sensitive data have represented to transfer human resources data.

These numbers may not be generalized since an important number of policies which concern human resources data streams, and which typically contain sensitive data, were not publicly available and thus were not reviewed.

- *In-house Verification*

A significant majority of the companies have self-certified to provide for in-house verification methods. FAQ 7 sets forth specific quality requirements for self-assessments.[71] Furthermore,

[70] See *supra*, point 2.1.13.1

[71] FAQ 7 provides: "Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate,

a statement verifying the self-assessment should be made available upon request by individuals. This obligation has not been evaluated.

- *Certification Status*

Most of the companies provided for a privacy policy that is current; only 6% of the importing organizations did not have a current policy. Even if a company loses safe harbour benefits, it is still supposed to be bound by representations with respect to imported personal data. According to FAQ 6: "The undertaking to adhere to Safe Harbor Principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the Safe Harbor. Its undertaking means that it will continue to apply the principles to such data for as long as the organization stores, uses or discloses them, *even if it subsequently leaves the Safe Harbor for any reason*" (italics added).

- *The FTC was (with one exception) the only US regulatory or supervisory authority selected*.[72]

3.1.3.3 Implementation Deficiency Trends

(a) Privacy Policies

- *Corporate policies were often hard to find*

Locating the privacy policy may be difficult for various reasons. First of all, it may be hard to locate the link to privacy policies on the homepage concerned. While there is a common practice consisting of putting the link at the bottom of the page, this was not the case for a significant number of companies; some placed it at the bottom of the web-page (left-hand corner, center, right-hand corner), at the top (left-hand, center, right-hand), or even in the center of the page, isolated or within a text. In some cases, the link was not included in the homepage, requiring a scroll through the sitemap to discover its location. Apart from the place of the hyperlink, another factor that rendered the localization difficult was the size of the characters, which were sometimes too small. In addition, there was no uniform way of titling privacy policies. Examples of titles given to privacy policies were: Déclaration de protection des données, Legal, Legal Notice, Internet Policy, Privacy, Privacy Statement, Privacy Notice, Site Policies, TRUSTe logo, EU-Site Privacy Statement, Legal Documents,

---

comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the safe harbor principles; that individuals are informed of any in-house arrangements for handling complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. […] Organizations should retain the records on the implementation of their safe harbour privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction."

[72] This finding covers all of the 410 companies.

Fair Information Privacy Statements, Terms of use, Use Policies, etc. A uniform typology and placement of (SH) privacy policy would help data subjects to locate the policy.

The following example from the research shows the time-consuming search process data subjects have to go through to locate the policy: A company provided a direct link in the SH self-certification to a webpage named "About the [the Company's] WebSite Notice." On this page the company represented itself as abiding by the SH principles but the Notice did not provide further information. Individuals who accidentally or successfully move with their mouse over a hidden icon labelled "SH" would be directed to this company's SH page. The relation between the two web-pages was not clear, and consequently, it remained ambiguous whether certain statements made on the initial page ("About [the Company's] Website Notice") covered data transferred from the EU or not. The webpage titled "About [the Company's] Website Notice" provided a clause that apparently alluded to onward transfers: "No matter what means you choose to communicate with [the Company], your E-mail and other personal information remain confidential. [the Company] do[es] not sell, rent, or give away such information to anyone, without a written permission obtained from the client and with the unique goal to develop the business interest of the client itself. […]". However, the web-page setting out the SH principles did not provide information as to whether personal information may be transferred onwards and under what conditions. Under the heading "onward transfer", it was stated: "Should [the Company] need the assistance of a commercial partner to develop the client's project, a co-finder agreement will be signed. It will cover all the aspects of privacy and security for the data received from the [the Company's] client and for their treatment".

Certain companies did not provide a direct link on the DOC certification page to their privacy policy. Other companies did not make their policies publicly available on the Internet, but required data subjects to contact the relevant office to obtain a copy of the policy. For instance, certain companies referred to their "Corporate headquarters" or mentioned that the organization can be contacted to obtain a copy of the privacy policy.

Difficulty in identifying the relevant privacy policy was also occasionally due to the fact that some companies did not develop their own policy but claimed to adhere to the privacy policy of an organization to which they belong. For instance, certain research organizations were members of the "Council of American Survey Research Organizations ("CASRO")." A member's certification page provided for a direct link to a CASRO webpage that provided for a privacy policy. However, this privacy policy was, according to the SH standard, incomplete and its scope not entirely clear (it set forth guidelines for both individuals and "members"). The CASRO website contained a link to the CASRO Code of Standards and Ethics for Survey Research, which set forth also certain privacy requirements. The Code did not, however, provide any reference in the title to "privacy," "data protection," "SH" or other relevant labels that could help inform data subjects that they are consulting the right web-page.

- *Self-certification despite non-existent or publicly unavailable policies*

One third of the companies under review did not have a policy which is publicly available on the Internet. These companies were mainly ones that import human resources data and/or were data processors. Other companies did not offer a functional link on the certification website.

Although publication on the Internet is not required by the SH agreement, and the transfer of human resources generally only affects employees, it is difficult to see why an online publication is not made available.[73] Online publication would facilitate direct availability of policies to the DPA Panel.[74]

- *Absence of publicly available privacy policy for certain data categories*

Certain companies certified for various data categories but only provided a link to a privacy policy for a particular data category, or they published a privacy policy concerning data categories that were not covered by the certification letter. For instance, a company certified for "company, product, and/or service related information" and "human resources data." The link published on the DoC certification page led, however, to a privacy policy concerning the collection and processing of personal information on the company's website visitors: "By displaying the [privacy seal] mark, [the Company] has agreed to notify you of: What personally identifiable information or third-party personally identifiable information is collected from you through our website. […]." Another company self-certified to cover "on-line, off-line, manually processed, and human resources data", while the privacy policy stated: "All personal information obtained from users of the *site* will be handled in accordance with the terms and conditions of this Privacy Statement" (italics added).

- *Style Differences and Lack of Clarity*

The reviewed privacy policies were marked by differences of style. A significant number of the reviewed policies required meticulous reading to clearly understand what the US data importing organizations did with the personal information. US organizations generally made efforts to describe how personal information is processed from a systemic point of view, but failed to give clear descriptions of data processing purposes. Further, a distinction must be made between privacy policies which constitute a notice, and privacy policies which do not. The first category, which was used by the majority of the companies, concerns privacy policies translating and delineating the SH principles into the corporate practice of the adherent. Such a policy will specifiy, for instance, the data processing purposes and explain how individuals can access their personal information. The second category simply paraphrases the SH principles without (consistently or clearly) indicating how the principles are implemented in practice. Such a policy will provide, for instance, a representation that personal data will be processed for specified purposes and that individuals have a right of access, but without specifying either the purposes or access modalities. In such cases, nevertheless, the policies have been awarded a positive score for the various criteria, since

---

[73] Companies may argue against such disclosures because they do not want to render public their business strategies and other secret corporate information. However, privacy policies need not contain such information nor would they, if properly worded, even indirectly reveal it.

[74] See Commission Staff Working Paper of 13 February 2002 on the Application of Commission Decision 520/2000/EC of 26 July 2000: "It would be preferable that even privacy policies only concerning employees be immediately and directly accessible by the relevant dispute resolution bodies (in this case the DPAs, as required by FAQ 9)."

they have made a representation, and if in the concrete case the companies concerned do not comply with the made representations they would be violating the FTC Act.

The significant deficiencies appear, accordingly, as follows: (i) privacy policies were drafted in difficult language and a non-transparent manner; (ii) processing purposes were omitted, not clear, too broadly formulated, or mentioned at dispersed parts within the policy; (iii) companies often used terms that were not clearly defined thereby rendering difficult comprehension as to how personal information is actually used; and (iv) third party disclosure and choice were often non-transparent.

(i) Privacy policies were drafted in difficult language and a non-transparent manner

For approximately one third of the companies, the notice lacked transparency. Privacy policies were often drafted in an eclectic manner, and data subjects may encounter difficulties in ascertaining data-processing risks.

A relatively small number of privacy policies seemed to be conceived as a contract. Certain "policies" provided for "disclaimer of warranties" and "limit of liability" or even imposed negative obligations (prohibitions) on individuals. For instance, a company that imported personal data in its capacity as a data processor set forth the following security provisions: "Client is prohibited from violating, or attempting to violate, the security of the [Company's network]. Violations may result in criminal and civil liabilities to the Client. [The Company] will investigate any alleged violations and will co-operate with law enforcement agencies if a criminal violation is suspected. Examples of violations of the security of the [Company's] network include, without limitation, the following: (i) Accessing data not intended for such Client; (ii) Logging into a server or account which the Client is not authorized to access; (iii) Attempting to probe, scan or test the vulnerability of a system or network; (iv) Breaching security or authentication measures without proper authorization; (v) Attempting to interfere with service to any user, host, or network including, without limitation, by means of "overloading," "flooding," "mail-bombing," or "crashing," taking any action in order to obtain services to which the Client is not entitled." While these requirements may be inherent in the service agreement that this processor entity concluded with its Clients, the relevance of the terms for the data subject is unclear.

Another company described its processing practices as follows: "Appropriate contact information for members may be given out to people requesting a referral for that profession. Referrals should be funnelled through the local Director. If the National Office has any reason to believe that the referral hasn't been followed up on, they may do so after seven days."

(ii) Processing purposes were not mentioned or too broadly formulated

A recurrent problem with the assessed privacy policies was that data categories and processing purposes were insufficiently defined. Approximately half of the reviewed companies either ambiguously described or did not describe the purposes for which personal data are collected and processed. "Insufficient" means that individuals needed to read the

entire policy to have a sense of the purposes and data categories, or, that it was impossible to clearly determine these elements.

The definition of the processing purposes is essential for data subjects to measure the risk of processing practices. Certain policies did not specify processing purposes or described them in cryptic language. For instance, a company provided that "personally identifiable information will only be collected to the extent that [the Company] deems reasonably necessary to serve a legitimate business purpose." To take another example, an organization indicated in its privacy policy the following relevant processing purpose: "[the Organization] collects limited personal data from different [Organization] regional offices and members worldwide in order to provide membership services to individuals". "Member Services" is further defined in the policy as follows: "[the Organization] uses personally identifiable information you have voluntarily provided on our Web sites, or by other means, to notify you via e-mail or printed material of [Organization] events or other relevant products and services offered by [the Organization]. Also, if you are a member of [the Organization] and/or part of an [Organization] specialty group or committee, [the Organization] will include your contact information in its directory of such members for networking purposes". The policy did not provide further clarification on the data processing purposes.

Another company's data processing purposes were described as follows: "[the Company] collects your information in order to record and support your participation in the activities you select. The information that you provide is also used as part of our effort to keep you informed about product upgrades, special offers, and other products and services of [the Company]." While the second sentence indicates that personal data are used for direct marketing services, the first sentence is not clear.

(iii) Use of unclear terms or incorrect definition

Privacy policies tended to use terminology that was not clearly defined. Examples of such terminology were "personal information," "technical data," "demographic information" and "aggregate information". Data subjects may encounter difficulties clearly understanding how their data are processed as illustrated by the following example: "[the Company] reserves the right to provide aggregate data to third parties for statistical analysis. Such data will not be linked to any particular individuals."

In other cases, key terms were defined differently than in the SH Decision. The SH Decision provides on this point that "personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a US organization from the European Union, and recorded in any form. However, some companies did not follow this definition. One company policy, for instance, set forth the following definition of personal data: "any information or set of information that identifies or could be used by or on behalf of the company to identify an individual. Personal information does not include information that is encoded or anonymized, or publicly available information that has not been combined with non-public Personal Information". In another case, anonymous information was defined as "information, which alone may not identify you, and includes both demographic and product ownership information. Demographic information is information such as a product owner's age, income, city, state, ZIP code, area code, gender,

purchase history, and so forth. Product ownership information is information about the specific products you own, such as the products' model numbers, serial numbers, places of purchase, and so forth".

Certain companies also tended to restrict the scope of application of their privacy policy to "personally identifiable information," without giving any guidance to data subjects about what this term concretely means.

(iv) Lack of transparency regarding third party disclosure and choice

Privacy policies tended to require careful scrutiny and more than one reading to impart a sense of the ways companies intended to re-use or disseminate personal data. For example, one company provided information unrelated to "opt-in" for data processing. It represented under "Sensitive Information Principle" the following: "[the Company] signs three types of documents with the clients: (i) a letter of intent, with the object of the collaboration, (ii) a non-disclosure agreement, (iii) a non-circumvention agreement. The information considered sensitive or confidential needs to be written on papers reporting the declaration "sensitive" on the page. The sensitive information transmitted electronically needs to be encrypted. At this regard both the parties involved in the electronic transaction will establish specific procedures. The collected data are stored in office computers or on paper." The mention of "procedures" was the indication that vaguely referred to choice, but no concrete representation was made regarding opt-in.

There may be different reasons for these style problems. First, US companies are not acquainted beforehand with the data protection principles and need to go through a learning process. Secondly, companies may prefer to make vague statements due to the nature of the enforcement system of the SH regime. Exposure to liability under the SH scheme is directly linked to explicitness and clarity of announced data protection practices.

To improve the current situation, the DOC could publish a set of guidelines on the drafting of SH privacy policies. The DOC could also publish a format that helps companies in their drafting process. Such guidelines could be developed in co-operation with the European DPAs, represented in the Article 29 Data Protection Working Party.

- *Ambiguous and contradictory policies (or parts of policies)*

A significant number of companies published privacy policies containing contradictory statements. In most cases, it was not the entire policy that suffered from this deficiency, only certain parts. However, the parts that lacked transparency were often those parts that are essential to offering adequate protection to individuals. The problem was not the amount of information provided, but rather the quality of insight given to data subjects about the collection and processing of personal information pertaining to them.

Organizations sometimes failed to issue clear statements concerning dissemination practices. The following example shows that it is not possible to determine the basic role of the said "partners" – whether they were data controllers or data processors: "Our site provides users

the opportunity to opt-out of receiving communications from us and our partners at the point where we request information about the visitor". In addition, this policy was patently contradictory when it also stated that "we will not rent, sell, or disclose information to a third party".

Furthermore, companies' privacy policies often used legal concepts that may be open to broad interpretation. For instance, a company set forth that "[b]eyond its representatives and affiliates, [the Company] does not offer or allow the selling of any user-provided information to third parties". Although this provides some indication to individuals, it is not exactly clear what is meant with "representatives and affiliates". The policy mentioned on the next page that "[the Company] may occasionally present a special contest or promotion that is sponsored by another company. To qualify for entry, we may ask you to provide personal information. If we plan to share that information with the sponsor(s), we will provide an up-front to that effect". No reference was made under this scenario to the individual's right to opt-out. It is not clear whether this company considered a sponsor as an "affiliate" or a "third party."

Another example is a third party disclosure clause setting forth that "[the Company] will not share any of your individual information with third parties outside of *strategic partners* (contracted email delivery form, or affiliates which we deem helpful to our member's experience on the site) unless you have specifically requested for [the Company] to share your information with *select companies*" (italics added). The paragraph dealing with "Limits of Confidentiality" only shed limited light on these concepts: "[the Company] may disclose personal information to special partners when it benefits our members. Special partners include companies that we have deemed to add value to our service and provide members with additional benefits. This type of partnership is rare, and is reserved only for those special partners that we have contracted with, who will provide additional benefit for our members. […]". The extent of choice offered here can only effectively be assessed if the meaning of "strategic partners" and "select companies" is clarified.

- *Incoherency between certification pages and privacy policies*

Certain companies stated on the DOC certification page that they process certain categories of personal data but the privacy policy to which the certification page refers covered other data types, or only one or certain data types of those listed on the certification page. For instance, a company certified to process both online and offline data, while the policy that was made publicly available only concerned the first category. Other companies certified to process both commercial and human resources data, but the policy only covered the collection of personal data via the company's website.

- *Incomprehensive description of data processing activities*

A considerable number of privacy policies scored insufficient as regards the description of their data processing practices, both in the certification letter as well as in the policy. Certain descriptions were too brief and opaque and imparted little meaning. Others provided descriptions which are inappropriate. For instance: "[the Company] is the sole owner of the

information collected on this site. We will not sell, share, or rent this information to others in ways different from what is disclosed in this statement. [The Company] collects information from our users at several different points on our website. With respect to any data transferred from the EU, [the Company] will hold such data for each customer securely and all data is the sole property of the customer. [The Company] will store and protect this data."

Certain descriptions of data processing practices were entirely irrelevant. An example is the following description: "[the Company] is a leading provider of proprietary and patented reservoir description, production enhancement and reservoir management services. These services enable [the Company] clients to optimise reservoir performance and maximise hydrocarbon recovery from their producing fills. The Company has affiliates in over 70 offices in more than 50 countries and its affiliates are located in every major oil-producing province in the world. The Company provides its services to the world's major national and independent oil companies."

- *False, misleading or irrelevant statements in certification statements or policies*

When giving information about how they implement SH requirements, some organizations described practices that were irrelevant to the particular requirement(s) concerned. For instance, one company translated the choice principle to its corporate practice as follows:

"[the Company] discusses the policy for personal/ technical treatment with the client itself; this claim is enclosed into the Agreement. The classic security triad referred to as confidentiality, integrity, availability is applied to the received information. In particular,

- confidentiality implies control possession
- integrity implies authenticity and non-repudiation
- availability implies the utility of information".

The policy did not indicate whether data subjects effectively have a right to opt-out. The relevant parts of the policy dealing with sensitive data, onward transfer and enforcement failed to specify whether individuals are effectively offered choice and the exercise modalities of such choice, if available.

Another company included the following contradictory clause: "**General.** This Policy constitutes the entire and only agreement between [the Company] and you regarding this subject matter and supersedes all prior or contemporaneous agreements, representations, warranties and understandings with respect thereto. You agree to review this Policy prior to reviewing any information or obtaining any documents from the Site. Any action related to this Policy shall be governed by the substantive laws of the State of California, without regard to conflicts of law principles. The State and Federal courts located in Santa Clara County, California, shall have sole jurisdiction over any dispute arising hereunder, and the parties hereby consent to the personal jurisdiction of such courts and to extra-territorial service of process. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Policy. Neither this Policy, nor any rights hereunder, may be assigned by operation of law or otherwise, in whole in part, by you without the prior, written consent of [the Company]. Any purported assignment without such permission shall be void. [The Company] may assign this Policy, in whole or in part, without notice to you. Any

waiver of any rights of either party must be in writing, signed by the waiving party, and any such waiver shall not operate as a waiver of any future breach of this Policy. In the event any portion of this Policy is found to be illegal or unenforceable, such portion shall be severed, and the remaining terms shall be separately enforced. The language in this Policy shall be interpreted as to its fair meaning and not strictly for or against either party. This Policy may be modified or amended by you only in writing, signed by both parties. Any purported modification or amendment inconsistent with the foregoing shall be void."

**"Grant of Rights.** You represent and warrant that all information provided by you in whatever format shall be non-proprietary to you or any third party, and [the Company] may use or disclose such information without notice to, or permission from, you or any other third party, subject only to the Policy. You hereby grant to [the Company] a worldwide, royalty-free, irrevocable, perpetual, non-exclusive, transferable license (with a right to grant sublicenses through multiple tiers of sublicensees) to use, execute, display, copy, perform and modify such information as [the Company] sees fit for internal business purposes."

Other examples concern enterprises that falsely certified to adhere to a privacy program.

- *Certain companies implemented the SH principles in part only*

The privacy policies of certain companies did not explicitly recognize all of the 7 SH principles.

1. Notice

    - Lack of clarity and conspicuousness

It was sometimes difficult to determine the actual purpose, type of third parties to which information is disclosed, and the choices the individual may have, mainly because those concepts were presented in an opaque manner. For instance, the following privacy policy did not include sub-titles to introduce each SH principle, and the processing purposes were unclearly formulated: "Member Communications from [the company] will address global issues that have an effect on the worldwide membership including, but not limited to: organizational statistics, new or revised organizational policies & guidelines (approved by the International Board of Advisors', and announcements about [the company] Conferences held around the world. (…)."

Another example of a minimal description of the purpose is the following: "In the course of providing users with [the company] imaging services, the Company needs to collect and store certain non-public information."

Lack of clarity was also evidenced when companies gave notice of data transfer(s) to "partners", "business partners", or "representatives and affiliates", since it remained unclear if the transferees would act as "processors" or "controllers".

Regarding lack of conspicuous presentation, some privacy policies did not divide the text into subtitles describing each SH obligation/right.

- Lack of specified purposes

The data processing purposes were often formulated in unclear language or described at different places in the privacy policy. The reason for this shortcoming is that US organizations tended to start from a description of their data processing practices rather than explaining how the principles are implemented in those practices. For example, a company provided the following information as regards the processing purposes (at different places over the policy): "[…] We may ask you for personal information at other times, including (but not limited to) when you enter a sweepstake contest or promotion sponsored by [the Company] and when you report a problem with our website. If you contact [the Company] we may keep a record of that correspondence. [The Company] also occasionally asks users to complete surveys that we use for research purposes. Wherever [the Company] collects personal information, we make an effort to include a link to this privacy policy on that page." "[The Company]'s primary goal in collecting personal information is to provide you, the user, with a customer experience on our website. This includes personalization services and many other types of services. By knowing all about you, [the Company] is able to deliver more relevant advertisements and content, and hence better service to you. We may use your personal information to contact you."

Instead of such long practice descriptions, the use of short but specific purpose descriptions should be promoted. This would enhance transparency.

- Lack of organization contacts in the privacy policy

Four (4) companies did not provide contacts at all. Some other companies, which scored positively anyway, provided e-mail contact only. Individual feedback would be facilitated if the privacy policy provides the same contact information as the self-certification page.

- Lack of clarity for choice

Description of the choice principle was generally found to be problematic. This was, firstly, because the description of purposes of the data processing often lacked clarity.[75] Secondly, more than one third of the reviewed policies simply did not provide for choice with respect to dissemination of personal data, or they provided it in an incomprehensible manner (because, *inter alia*, the notion of "third parties" tended not to be defined). A company's privacy policy provided in the paragraph entitled "Limits of Confidentiality" for the disclosure of personal information to "special partners" but did not mention any possibility for the data subject to opt-out from such an envisaged transfer. The same company's privacy policy offered choice to data subjects as regards the communication of information to advertisers. This scenario is, however, different from the disclosure of information to "special partners," regulated elsewhere in the policy.

Some companies provided for a mechanism whereby the effectiveness of the opt-out system was limited. This mechanism consisted of providing opt-out boxes that are pre-ticked to give permission to onward transfer of personal information. The online privacy policy of one

[75] See *supra* (Processing purposes were not mentioned or too broadly formulated).

company stated the following: "Except as otherwise noted in this policy [the Company] only discloses user information in aggregate form to marketing partners. For example, we might tell a marketing partner how many users visited [the Company] over a period of time, but we will never tell them who it was that saw or clicked on their offer, unless that user has given us permission to do so. [The Company] believes that consumers should be able to control the use of their data. We will not share personally identifiable information with marketing partners if you follow the simple opt-out procedure of removing the check mark located at the permission notice box appearing on the [company] registration and entry page. […]." This system does not comply with the opt-out requirement as described in the SH choice principle, pursuant to which onward transfer is the exception and not the rule.

- Lack of SH compliance statement

Four (4) companies did not incorporate in their privacy policy a statement of SH compliance. This affects directly the possibility of the individual to know (i) what would be the applicable regime to the data transfers concerning him/her, and, concomitantly, (ii) how to enforce his/her rights.

The problem could be mitigated by providing for a pre-published template (for instance, on the website of the DoC) with a specific SH label and containing mandatory statements as the one described in this paragraph.

2. Choice

Representations regarding choice of dissemination were lacking in 6 of the analysed policies. A recurrent problem was that choice tended to be formulated in vague terms, for instance: "We will share aggregated demographic information with 3rd parties in the case they would like to know aggregate demographics of our audience. This is not linked to any personal information that can identify any individual person. We do not share personally identifiable information with third parties." To understand concretely the extent of the choice offered in this instance, it would have been helpful to define key notions such as "third party" and "aggregated demographic information".

In situations where choice was provided, representations on the ready availability and affordability of choice were generally lacking.

3. Onward Transfer

The analysis demonstrates a consistent lack of third party processors' commitment to SH. The majority of the policies containing a reference to onward transfers to third party processors failed to specify under what conditions such a transfer would take place.

4. Security

Seven (7) companies did not set forth any representation on information security.

5. Data integrity

In all but 5 policies, it was impossible to determine whether the collected data were required for the data processing purposes. This deficiency is related to the problem of insufficient definition of the categories of personal data and/or the lack of specification of the data processing purposes. As a consequence, in cases where there were such deficiencies, it was virtually impossible for data subjects to assess whether the data integrity principle was being respected.

It is remarkable that nearly half of the reviewed privacy policies did not provide for a representation ensuring reliability for intended use (or did not provide for a clear representation). The data integrity principle requires, nonetheless, that the processed data be "reliable for its [*sic*] intended use, accurate, complete, and current". A standard statement to that effect could be inserted in a SH privacy policy template.[76]

6. Access

- Lack of reasonable access

Approximately half of the reviewed policies did not provide for reasonable access, and none of the policies made a statement on the affordability of access. Approximately one third of the companies did not provide for a right to correct data, or did not provide it clearly. With regard to online data collection and processing, the right of access was often restricted to contact data only. More specifically, the right of access was implemented in these cases by giving data subjects an opportunity to reset preferences in their personal accounts.

A recurrent failure was that, while companies granted an opportunity to individuals to amend personal information, no *explicit* right of access was foreseen. For instance, a company provided in its Privacy Statement that "Users can amend this information [i.e. collected information from its sites] through the web site on most [of Company's] sites, or if that feature is not available, by sending an e-mail to [questions@company.com]." This company, however, did not make a representation that individuals have a right of access independently of their wish to have personal information modified. Overall, provision for access rights seems problematic under the SH.

- Absence of reference to cost

None of the reviewed privacy policies explicitly provided that access is affordable or for free. Without such a representation, there is little guarantee that access is effectively affordable.

[76] See, for instance, the OECD Privacy Statement Generator, available at <http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm> (last visited 24 March 2004).

- Lack of correction, amendment or deletion of inaccurate data

One third of the policies failed to clearly provide for the right of correction and/or amendment of inaccurate data, or did not provide at all for these rights. Indeed, the right to delete inaccurate data was not even provided for in approximately half of the cases.

7. Enforcement

- Limited number of companies agreed to reverse effect of breach, SH compliance of future processing, cessation, publicity of decisions

Only 3 of the reviewed policies explicitly set forth that a breach of the policy will be remedied. Five (5) policies provided for future compliant processing in case of violation, 2 policies guaranteed for the cessation of wrongful data processing, and 4 provided for the publication of enforcement decisions. The policies themselves generally did not set forth these information categories and the data subject would need to conduct a time-consuming search on the website of the privacy program or ADR service provider to find out how the breach of the SH would effectively be remedied. It is advisable that these information requirements are included in privacy policies.

- Limited number of companies agreed to comply with the DPA advice

Although almost two thirds of the companies have represented to co-operate with the DPAs, only 2 US organizations represented to *comply* with the advice of the DPA panel. In cases where human resources data are transferred, this results in an absence of enforcement because the FTC has no clear jurisdiction to hear human resources data processing complaints. The DoC ought, strictly speaking, to delete all human resources data importers from the SH list that do no comply with this requirement.

- Absence of sanctions

Privacy policies generally did not provide for sanctions. More than one third represented sanctions or a sanction regime, but these sanctions were in most cases not explicitly found in the privacy policy, and accordingly required the data subject to check the sanctioning regime of the relevant privacy program.

- Remedy failure

A company included a clause on exclusion and limitation of liability: "**Damages**. In no event shall [the Company], its parent, subsidiaries, affiliated companies, agents, shareholders, employees or officers have any liability hereunder to you or any third party for any indirect, special, incidental or consequential damages (including damages for loss of business, loss of profits, litigation, or the like), whether based on breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages. In no event shall the aggregate liability of [the Company], its parent, subsidiaries, affiliated companies, agents, shareholders, employes and officers exceed one

hundred dollars ($100), regardless of the cause, whether in contract, tort, or otherwise. The foregoing limitations are fundamental elements of the basis of the bargain between [the Company] and you. This site and the materials would not be provided without such limitations."

(b) Privacy Programs

- *Dubious Status of Privacy Programs*

Fifteen (15) organizations/companies represented that they had enrolled in a privacy program, while the explanation they provided on this point demonstrated that this was most likely not the case, as they referred to either (i) non-verifiable in-house measures the description of which had nothing to do with a real privacy program; or (ii) mere dispute resolution programs, which clearly do not fall under the category of privacy program.

There exists confusion about the status of privacy programs, and certain US organizations have selected programs which do not fit with the SH privacy program definition. Pursuant to FAQ 11, privacy programs should (i) incorporate the SH principles into their rules, and (ii) include effective enforcement mechanisms of the type described in the enforcement principle. ADR mechanisms are sometimes confused with privacy programs, and US organizations have sometimes mentioned ADR service providers which can not be compared with privacy programs. In addition, the real privacy programs failed to comply with all the SH requirements.

In the case of CASRO, for instance, the primary, publicly accessible program was the "CASRO Code of Standards and Ethics for Survey Research",[77] which is not exactly what one would expect for a SH privacy program. However, another webpage stated that CASRO has created a Privacy Protection Program[78] (CASRO 3P) – "a single service developed to show research companies how to meet the privacy requirements for information collection, storage and dissemination under the following acts and directives: US Safe harbor, European Union Directive on Data Protection, […]". Nevertheless, the said program was not publicly available on the CASRO website.

It is advisable that (i) the Article 29 Data Protection Working Party sets forth minimum requirements for privacy programs (this could occur in co-operation with the DoC/FTC); (ii) privacy program service providers represent to be compliant with such requirements and are registered on the DoC website.

- *Incomplete incorporation of SH principles*

Privacy programs appeared in certain cases not to have implemented the choice principle. For instance, BBBOnLine and CASRO did not set forth the choice principle for onward transfers. Of the reviewed programs, only the DMA required choice to be affordable and readily

77 See <http://www.casro.org/codeofstandards.cfm> (last visited 27 February 2004).

78 See <http://www.casro.org/casro3p.cfm> (last visited 27 February 2004).

available, along with opt-in for sensitive data. The integrity principle was not completely implemented either since none of the reviewed programs, except for DMA, required their members to process only personal information that is relevant for the purposes for which it is to used. One would expect that privacy programs would completely implement the SH requirements so that their members are guaranteed to comply with SH. It is strongly advised that remedial action be undertaken by privacy program providers. Such action could begin by conducting an audit of the programs they offer.

Furthermore, the privacy programs' sanctioning regime was generally unclear and insufficient. For instance, descriptions were vague as to exactly which sanctions may be applied and which relief (e.g. damages) the data subject may expect. Moreover, no mention was made of *mandatory* referral to the FTC in case of non co-operation with the privacy program service provider.

(c) ADR Organizations

- *Lack of procedural transparency*

The reviewed ADR mechanisms showed important flaws with respect to procedural transparency and the sanctioning regimes.[79] For instance, JAMS is listed in the DoC Safe Harbor website, but it was virtually impossible to find and determine what complaint regime applies to SH complaints. Procedural transparency was missing because extensive research was required to learn what the rules of procedure are and how a complaint must be filed (the privacy policies of US organizations generally failed to explain how a complaint could be lodged). Further, the reviewed ADR programs did not explicitly provide guarantees about data protection expertise for the adequate handling of SH data-processing complaints. The programs also tended to reduce SH complaints to consumer complaints. Yet data protection is often more than consumer protection as it concerns fundamental human rights.

- *Lack of mandatory sanctions as foreseen in the SH*

Certain ADR mechanisms/procedures were not specifically designed to deal adequately with SH data protection issues. ADR service providers often referred to a consumer program, but it was not clear that such programs would be adequate to deal with data protection complaints. Such programs were often not entirely free and, as mentioned above, clear information about their procedures was often difficult to find. Sanctions that are explicitly required by the SH (reversal of the effects of breach, ensuring that future data-processing operations are SH-compliant, publication of sanctions, mandatory referrals to the FTC, etc.) were often not mentioned. For instance, AAA and JAMS did not provide for publication measures, reversal of effects of breach, or mandatory referral to the FTC in case of non-compliance.

It is strongly advised that ADR mechanisms claiming to have expertise to deal with data protection matters provide for specific data protection complaint procedures and that the

[79] See on privacy and dispute resolution, O. Rabinovich-Einy, "Going Public: Diminishing Privacy in Dispute Resolution in the Internet Age," *Virginia Journal of Law and Technology,* 2002, vol. 4, p. 1 - 55.

threshold to start proceedings is reasonably low. Furthermore, US organizations using an ADR service should provide clear information on how data subjects can start up a proceeding and what the other procedural steps are.

### 3.2 Specific case-study

What follows is a summary of the most relevant answers provided by the three companies that volunteered to respond to the questionnaire set out in Appendix III.

The reviewed companies used the SH chiefly for human resources data and commercial data transfers; one organization mentioned that it also transferred research data under the SH regime. The SH data streams had a regular and permanent character. As one company testified: "the frequency of the data transferred will depend on the type of data being transferred. For some functions transfers will occur on a frequent basis (e.g. employee services), for others (e.g; research data) transfer will be occasional". Data transfers were said to take place electronically via a private electronic network; one enterprise testified that, in exceptional cases, information may be sent via the Internet in an encrypted form and for small data sets only.

The three enterprises explained that personal data were generally preserved for limited time periods. One company specified that HR and research data were conserved, in compliance with its data retention policy, for maximum 1 to 3 years (and depending on the need to retain the information, for instance, "job applications are retained for 6 months and then destroyed"). The second company stated: "Data is retained for as long as required for the purpose and in accordance with data retention legislation: (1) Deletion of contact details provided by consumers in case of an un-subscribe request, (2) retention of accounting information for seven years, (3) retention of some employee information after employees left the company, e.g. to provide pensions." According to the third enterprise, "[a]s the data is constantly/periodically updated, previous records are generally discarded. An exception would be where proof of request or preferences is required. [the Company] avoids keeping unnecessary data." No concrete information was given on the preservation of commercial data.

The reviewed companies had seriously invested in security measures at various levels including the (i) software level, (ii) hardware level, (iii) safety of buildings and premises, and (iv) training to employees.

According to the representatives of the three companies, neither the Patriot Act nor other US national security regulations have had an impact on the SH data protection regime. All of them testified that they have never put restrictions on their adherence to SH in order to meet national security, public interest, or law enforcement requirements under any statute, government regulation, or case law that creates conflicting obligations or explicit authorizations.

Notice was said to be given prior to data collection or transfer. Notice was given in various ways. One company referred to the privacy statement on its website and "[a]dditional notices

[…] provided at the actual data collection point, such as a newsletter subscription service." It was also pointed out that the differences between national laws render the implementation of worldwide information practices difficult.

Two companies mentioned that they adhered to a permission-based approach to data collection. One company referred explicitly to opt-in as a fundamental principle for data processing, but did not specify whether opt-in was used for all data categories. Another company referred to "permission" without clarifying what is understood by the notion. The third company stated that as regards customer data, choice was guaranteed through its membership with a SH seal program, but it remains unclear whether choice posed problems with respect to processing of human resources data. A company also indicated encountering problems with differences in definitions of sensitive data, while another company mentioned that it had problems with the sensitive data opt-in principle "because the requirements from member state to member state are not fully articulated. More harmonisation is necessary to ensure that a multi-national company is able to comply with applicable laws."

Onward transfers do not seem to have created specific problems. It is interesting to note that 2 companies explained that if the data recipient (controller or processor) is not a member of SH, onward transfer will be administered via a contract or through subscription to the SH privacy policy of the transferor.

Two companies explained that the employees' rights of access are self-managed and facilitated by online self-help tools. For customer data, access rights were specified by 2 companies as being facilitated via the web/online, electronic or paper registration, or via direct individual request. One company stated that it received 3–4 data access requests per calendar year, a second 3–5 requests per month, while the third mentioned that it did not have aggregated numbers of access requests but stressed that additional harmonization and greater guidance on how to handle such requests would be welcome. It should be pointed out that the companies under review different in size and business activities – which may explain the differences in quantities of access requests. One company stated that access is exercised via the data exporter, another specified that access was administered both via the data exporter and/or data importer.

All of the three companies relied on privacy programs as a means of SH enforcement. BBBOnLine was selected by all of the organizations for online data collection/transfers. One company also adhered to the DMA safe harbor program, and all of them stated that they co-operate with the European DPAs as regards offline data or human resources data (2 relied also on the DPAs if BBBOnLine were unavailable). No specific co-operation with DPAs was reported as having been required so far. Two companies specified that they believed that enforcement mechanisms are to be readily available and gratis. One company reported that it had dealt with three complaints all of which had been settled without problems. The companies pointed out as important consequences of non-compliance, the loss of reputation or

relationship with the customer/individuals affected, damage to the corporate brand and additional sanctions.

All of the three companies used SH to transfer personal data to a data processor, and provided for the signature of an additional data-processing agreement. All of them had extensively invested in internal policies and guidelines and training courses to ensure that their employees concretely respect the SH principles. Such awareness training and self-assessment programs were reported to take place continuously.

According to the companies, the reasons (and advantages) for joining SH were, in summary: (i) creation of consumer confidence and trust; (ii) use of SH as a platform to build a global privacy program (the principles were applied beyond the specific EU-US relationship to provide a level of protection for data processed by establishments in countries that have no data protection regulations); (iii) ensuring continuity of data flows. One company pointed out that other data transfer options are problematic – global codes are currently not recognized, and the Commission model clauses are onerous and create uncertainty. Another company stated that "the model clauses reflect the EC legislation but their attempt to harmonize the national implementation is reversed by the requirement to also comply with national law. Thus, their use and the advantage of their implementation are fairly limited. Also, they do not take into account the corporate structure of multi-national companies." It was further stressed that the administration of onward transfers via contracts presents substantial administrative burden and is time consuming, and that alternatives such as code solution should be pursued.

Two companies reported that they had not encountered any problems after joining the SH (apart from the problems mentioned above). One company, however, was concerned about "the perceptions of the safe harbor in the EU and the heavy criticism it has received. In addition […] the fact that individual countries have varying interpretations of the directive creates extra work and increased cost." One company reported having encountered problems in the past due to the specificity of the SH regime compared to local laws, but that these problems had been resolved.

A reported disadvantage with SH was the fact that the scheme applies to US data imports only. Another disadvantage was the weak and inconsistent support for the SH by some EU member states (leading to data export restrictions in certain cases). Apart from these problems, the respondent companies viewed SH positively.

### 3.2.1 Preliminary Conclusions

- The companies considered SH as a viable framework on which they could build a global data protection regime;
- The companies pointed out that SH functions but would welcome more harmonization and support for SH in the data export policies of member states;
- The companies have not encountered enforcement problems so far, and testified that complaint levels have been very low;
- Onward transfers (to data controllers and/or processors) have been generally administered via contracts and may be onerous to administer in a multi-national context; pursuit of other solutions, such as the use of a global company data processing code, is considered worthwhile;
- The main SH principles, such as notice, choice and the right of access, seem not to have created operational difficulties.

## 3.3 Implementation experience by different parties

### 3.3.1 Lawyers

The questionnaire, attached to the report in Appendix IV, was sent to 15 lawyers all of whom are data protection experts practising in the EU and/or the US. We have received 6 answers. For reasons of confidentiality, the answers are rendered anonymous:

1) Regarding the perceived **advantages** of the SH regime, lawyer A answered: "SH has a number of advantages, in particular 1) broad coverage of (potentially) many types of data transfers to the US, 2) not requiring individual, ad hoc measures for each transfer (as is the case with the model contracts), 3) liberal rules concerning onward transfers, and 4) localization of the enforcement risk in the US (which also has a negative side, see the next question)."

Lawyer B stated: "Subscribing to SH means a solution for *all* future data transfers to the SH company in the United States. As for the affiliation to SH, the company can basically forget the prohibition on data transfers because after SH, the company becomes 'safe' and outside the scope of the prohibition. So, the advantage is that it is not necessary to ascertain on an ad hoc basic which legal grounds for transfer to such a company will be used because the SH provides for a unified solution for *all* the existing and forthcoming transfers." "Some provisions of SH, for example the access provision, are easier to comply with compared to if the company had decided to abide by local laws or Model contracts. Also, from a company perspective, the rule on onward transfers is very interesting. In this regard, the SH does not stipulate how a potential contract should be drafted in order to transfer data from a SH entity to another controller established outside the EU. This means that once a company has transferred data to the US, it can transfer the data from there to everywhere in the world. Because there is no enforcement or surveillance, this is standard practice." "It provides the

advantage of having a good reputation. It's a good marketing advantage (even if done for window dressing purposes)."

Lawyer C referred to the "[r]elative ease of enforcing requirements, and the ability to keep EU DPAs out of the matter when non-employee data is subject to the SHA."

Lawyer D stated: "In Spain, the main advantage of the SHA regime is that it is very easy to register a data transfer to the USA at the Spanish Data Protection Agency, unlike other transfers (for example based on the European Commission Standard Clauses)."

Lawyer F stated: "When adhering to the SH, our US clients, which are primarily multinational companies with presence in several EU Member States, do not have to negotiate and conclude a separate contract per EU country as per the Commission standard contractual clauses (or, alternatively, to conclude a single contract but with as many signatures as there are representatives in each relevant Member State) when they transfer data from the EU to the US."

2) The perceived **disadvantages** underlined are as follows:
Lawyer A: "The major disadvantages are (1) localization of liability risks in the US, with the risk of large damage awards that can bring, (2) the fact that SH only covers transfers to a single country, and (3) the fact that some important sectors (such as financial services and transportation) are excluded from it."

Lawyer B: "The SH places more burdens/obligations upon a company that uses it to legitimise transfers than if the same company uses consent as legal grounds. For example, if a company is able to obtain consent as legal ground for transferring data, from the company perspective, this is better because, generally speaking, the consent does not impose further obligations upon the company." "The fact that the company is under the jurisdiction of the FTC." "I find it to be a disadvantage that if a company wishes to use SH, this basically means that it will have to give SH treatment to all the data it receives from the EU (except for human resources data), (I realise that this may be an advantage as well). In contrast, if a company uses contracts, and, in the future it wants to use consent for other transfers, it still can do this. In sum, I find it to be a disadvantage that if a company subscribes to SH, then everything must be covered by SH."

Lawyer C pointed to the fact that the SHA is "[a]pplicable only to transfer from EEA to US."

Lawyer D added: "It is only valid for the transfers to the USA. If a corporate data transfer strategy requires data transfers to countries other than the USA, the European Union or countries that provide an adequate level of protection, the SHA regime only provides a partial solution, rather than a global one."

Lawyer E stated that "[t]he SHA regime may only be applied to US-entities and can therefore not be used when other third countries are involved. The SHA also excludes some business sectors. The SHA regime is a complicated regulation that is hard to understand."

Lawyer F commented: "[o]ur clients often have presence all over the world and the SH is only available to transfer data to the US, therefore not offering a global solution. Another important disadvantage of the SH is that it excludes certain sectors of the economy, such as financial services."

3) Regarding the question of whether the **EC Decision on Model Contractual Clauses has any impact on the TBDF strategy**, lawyer A responded: "Yes, certainly. The model contracts constitute another option for companies to provide a legal basis for transborder data transfers; I believe they are *per se* neither better nor worse than SH, since the decision to use a particular mechanism has to be determined based on the circumstances of each particular case. There are some cases for which SH is better suited (for instance, when a company in the US continually imports data from the EU), and others in which the model contracts may be more appropriate (e.g., when the importer is in a sector not covered by SH, or when the transfers are more limited in nature)."

Lawyer D added: "It is not feasible to seek global data protection compliance without taking into account the European regulations, and among others, the decisions on Model Contractual Clauses. Nevertheless, in some European Union member States (i.e. Spain), the European Standard Clauses are not as useful as they might seem, because they do not prevent a Spanish data exporter from having to seek prior authorisation for the transfer from the Spanish Data Protection Agency."

Lawyer F stated: "[i]n the majority of the projects we have handled so far, our clients have found that the model clauses are acceptable to deal with their multinational situation but they also advocate in favour of (industry-driven) alternatives and their recognition as offering an adequate level of protection. The corporate binding rules would obviously be a concrete answer to their concern."

4) When asked if they think that **the SHA system results in a dual regime within companies (one for EU data and one for other data), or an increase in the level of US data protection for all data**, lawyer A responded: "In my experience, what US companies want to avoid as much as possible is establishing multiple data protection regimes, since that creates substantial extra costs. Thus, they tend to adopt the SH principles as the basis of their data processing around the world. I can think of several large US-based multinational companies that have joined SH and applied the SH principles to their data processing globally even outside the US (except for countries such as the EU where mandatory national data protection law applies, of course)."

Lawyer B considered that "Safe harbor leads to a triple data protection regime: the EU regime, the SH regime, and the regime for 'US data' because I do not think companies provide SH rights to data gathered in the US."

Lawyer D pointed out: "I believe that companies that adhere to the SHA place their data protection regime in the USA at a similar level as that implemented in Europe."

Lawyer F stated: "[a]s far as we know, the SH often results in a double data protection regime. Given our clients' reluctance to adhere to the SH, we indeed assume that they do not increase the US data protection regime to the SH regime (although we are usually not involved in the US aspects of their projects)."

5) Lawyers A and B stated that companies normally conduct the **annual verification** internally, while lawyer C stated that sometimes it is conducted internally and sometimes by a third party. Lawyer F added: "[w]e are not aware of the way our clients implement the yearly certification and verification requirements. This part of the work is generally done by local in-house and/or external lawyers in the US."

6) 7) None of the respondents had any experience with **enforcement actions** either by **European DPAs** or by the **FTC**.

8) The respondents stated that they follow their client's choice concerning **alternative dispute resolution bodies (ADRs)**.

9) None of the respondents had any experience with **complaints before such ADRs**.

10) Concerning **the way access to data subjects is provided by the companies** they advise, lawyer A considered that "[t]his depends, of course, on which party has easiest access to the data – if the data is stored in Europe, then it is usually the exporter, and if it is in the US, the importer. In my experience, exporters and importers tend to work together in providing the most efficient mechanism for access."

Lawyer B commented that access occurred "[u]sually via the data exporter because it's closer to the individual."

Lawyer F stated that "[i]t depends upon the role of the parties. It is usually the data controller(s) who has/have to provide access to the data subjects. In practice, the data subjects located in the EU will find it easier to request access to the data exporter. Our experience shows however that such access is rarely requested by data subjects even when the required procedures are in place."

11) The lawyers were also asked whether they believe that the SH regime offers a feasible **solution to conducting processor-to-processor transfers and controller-to-processor transfers.** Lawyer A stated: "[i]n my view, the SH documents are ambiguous as to whether they only cover controller-to-controller transfers, or whether other types of transfers are covered as well. Of course, the distinction between a controller and a processor can often be artificial, and it can often happen that a party's role changes from one transfer to another. I also think that there is no clear prohibition in SH to covering data transfers to processors.

Thus, I believe that SH can cover transfers to processors as well. However, it would be useful if there was some clarification of this point in the documents."

Lawyer B stated: "I think that it does. In particular, if you compare it with the Model contract where the question of transfers to processors simply is not contemplated (this is a big mistake), I find that the SH provides a feasible and proper rule."

Lawyer F responded: "[y]es, as long as the SH rules are observed by all participants in the data transfer chain, with the geographical limit of the US."

12) None of their clients were reported as having experienced **limitations in the adherence to the SH principles** due to (a) necessity to meet national security, public interest, or law enforcement requirements, or (b) any statutes, government regulations, or case law that create conflicting obligations or explicit authorizations.

#### 3.3.1.1 Preliminary Conclusions

- The free flow of data after adherence was identified by the lawyers as one of the main advantages of SH. The liberal approach of SH with respect to onward transfers and ease of enforcement was also identified as advantageous.

- It was considered a disadvantage that SH regulates flows to just a single third country, and that certain industry sectors are excluded from SH.

- The model contracts constitute another option for regulating data transfer and companies have latitude to decide on the appropriate transfer regulation strategy. No comments were made concerning content issues of each legal instrument (for example, different approaches to enforcement, liability, etc.).

- There is no consensus as to the existence of a dual regime of data processing (one for US data, one for EU data).

- There is a paucity of enforcement actions or complaints.

- Controller-to-processor transfers are considered to be covered by the SH. However, clarification regarding the propriety of such coverage would be helpful.

### 3.3.2 National DPAs

The questionnaire was sent to the 18 EEA DPAs.

Thirteen (13) answers have been received.

In general, a full picture of the quantity and legal compliance of data transfers under the SH cannot be obtained because notification prior to transfers abroad is not required by all the DPAs. The figures received from those DPAs that do require notification are not representative for two reasons: (1) only Belgium and Spain specified numbers of SH data streams, (2) these numbers are substantially lower than the total number of companies that have self-certified. For instance, in Belgium, 18 data flows under the SH have been declared since September 2001, of which 14 deal with human resources data. In Spain, 16 data flows under the SH have been declared. All those DPAs that require notification answered that the received notifications concerned intra-company or intra-group transfers.

Most of the DPAs have elaborated guidelines on TBDF with specific reference to the SH, or have engaged in other kinds of educational activities, such as presentations to the business sector.

None of them report different treatment for those companies that have represented to co-operate with them compared with those that have not done so.

No DPA reported having: (1) received complaints dealing with the SH; (2) received communications from the FTC to investigate; (3) approached the FTC to monitor and/or investigate compliance with the SHA; (4) suspended data flows under the SH; or (5) initiated any informative procedure under Article 3(1)(a) of the Commission Decision.

The following remarks were added by the DPAs:

Belgium: "[i]t seems that the SHA and the standard contractual clauses are not broadly used yet. SHA is mentioned in less than 10% of TBDF notified. The main legal basis for TBDF is consent and the fact that the TBDF is necessary for the performance of a contract. In more than half of the cases, several legal bases are used in order to secure the validity of a TBDF."

Germany: "German companies tend to use the EU model clause or BDR for TBDF to the US rather than rely on the quite complex (and in respect of the categories of data non-concluding) SHA."

Italy: "Reference may be made to some cases addressed by the Italian Garante, in which US-based companies appeared to prefer to avail themselves of standard contractual clauses (SCC) for transferring data to the US because they found that the SCC were more in line with EU data protection principles compared with the SHA. Additionally, the standard contractual clauses were considered to provide more clear-cut guidelines as to liability issues and implementing mechanisms."

Portugal: "It is curious that controllers do not use SHA as a legal ground for TBDF to the US, which would be easier to get a permit for, but instead recourse [*sic*] to other instruments. We may say that SHA is far from being a successful solution in Portugal to TBDF to US."

Spain: "In general, it must be mentioned that companies established in Spain rather like other systems (mainly the use of contractual clauses or asking for the consent of data subjects) than the SH approach for legitimating the transfers of personal data to the US. This is even more true since the approval by the European Commission of the Model Contractual Clauses. The

most used argument in favour of this approach is that the legal certainty provided by the other methods is greater than the ambiguous, complex and less than clear provisions of the SH Agreement."

3.3.2.1 Preliminary Conclusions

- A complete overview of the quantity of SH data transfers (number of transfers per DPA) and their legal compliance cannot be obtained because not all the DPAs require that they be notified of third country data transfers.

- DPAs have not yet received any complaints nor been involved in any enforcement action.

- DPAs have not yet suspended data flows under the SH.

- Some DPAs believe that SH is not being broadly used. Some DPAs view the complexity of the SH regime as a cause of such limited use; others point to the fact that alternative mechanisms offer more legal certainty regarding liability and implementing mechanisms.

3.3.3 Federal Trade Commission (FTC)

The response of the FTC to the questionnaire was considerably delayed and came only after repeated requests. This suggests a serious lack of interest in SH administration and implementation.

The first question asked to the FTC was whether any **complaints concerning the application of the Safe Harbor framework** have been received, and, if yes, **from whom** (directly from the data subject, ADR/ODR bodies, competitor companies, data exporter, European DPA, consumer association, etc.). The FTC acknowledged that it received one SH complaint filed directly with FTC staff. No SH Referrals from European DPAs or self-regulatory bodies have been received.

The next question concerned the **procedures in place to deal with such complaints**. While no complaints have thus far been processed, the FTC reported that if "a Safe Harbor Referral is received by the FTC, the FTC will review the facts and determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in or affecting commerce has been violated. If the FTC concludes that it has reason to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order."

The FTC reported no similar investigative commitment for complaints brought directly by data subjects or other representative consumer groups. The FTC merely acknowledged that

"[a] complaint regarding a Safe Harbor company could be submitted to the FTC through the FTC's Consumer Response Center (CRC). The CRC processes complaints by telephone (1-877-FTC-Help); through the "file a complaint" link at the FTC website located at www.ftc.gov; and in writing at Consumer Response Center, Federal Trade Commission, Washington, D.C. 20580-0001. Complaints, which can be submitted by anyone of any nationality in any location, are handled by trained consumer response staffers who identify the nature of the complaint and try to respond with helpful consumer education information. The FTC periodically searches the CRC database to identify any Safe Harbor-related complaints. As of the date we last searched (December 3, 2003), no Safe Harbor-related complaints had been received by the CRC. A complaint regarding a Safe Harbor company could also be submitted to FTC staff directly, and not through the Consumer Response Center."

Concerning the **cost for submitting a complaint**, the FTC representative stated that "[t]here is no fee to submit a Safe Harbor Referral as described above, nor is there a fee to submit a complaint to the CRC or directly to the FTC."

With respect to **preliminary actions that might be taken during the procedure** the FTC provided an incomplete answer: "[y]es, assuming that the 'procedure' to which you refer is an FTC investigation resulting from a Safe Harbor Referral. Depending on the facts of each case and application of U.S. law to them, in certain situations the FTC may determine that specific action needs to be taken to halt particularly egregious behavior by a company that is likely to cause substantial injury to a consumer. In such cases, the FTC could ask a court to issue a preliminary injunction." Such a request to the court would occur subsequent to an administrative proceeding within the FTC. The FTC did not indicate whether it might pursue such actions for other complaints.

Concerning the **types of sanctions that the FTC can impose**, the agency stated: "[…] The FTC may bring a case in an FTC administrative court or in federal court. Generally, if an order against a company is issued in an administrative court, the sanction for violating the order is civil penalties. If an order against a company is issued by a federal court, the sanction for violating the order is an order of contempt by the court."

"Final decisions issued by the Commission may be appealed to the U.S. Court of Appeals and, ultimately, to the U.S. Supreme Court. If the Commission's position is upheld, the FTC, in certain circumstances, may then seek consumer redress in court. If the company violates the order while it is still in effect, the Commission also may seek civil penalties or an injunction."

In response to the question as to whether the FTC contemplates any type of **communication procedure with European bodies** (European Commission, European DPAs, Article 29 Data Protection Working Party, etc.) **to assure better implementation of the enforcement procedures**, the FTC provided a descriptive list of its contacts. The FTC reported that "[t]he Bureau of Consumer Protection Director, Howard Beales, met with the Article 29 Working Party on its visit to Washington in 2001, and again in Brussels in October 2003. He encouraged members of the Working Party to contact him personally (…) or his staff members in the Bureau's International Division of Consumer Protection, under the direction of Associate Director Hugh Stevenson (…). Contacts have been made by European Data

Protection Authorities on enforcement matters of mutual interest, but none have been Safe Harbor Referrals."

The FTC pointed out that it "has been in routine contact with the staff of the European Commission, formerly through Sue Binns and more recently through Philippe Renaudiere and Diana Alonso-Blas, as the Secretariat to the Article 29 Working Party. We have discussed Safe Harbor enforcement coordination with the European Commission staff, and we have advised them about general inquiries we have received from non-profit entities about opportunities for coverage under the Safe Harbor framework. In early February 2004, staff from the FTC's International Division, including the Associate Director, Hugh Stevenson, met with Rosa Barcelo. The Safe Harbor Framework, among other topics, was discussed at this time. On March 22, 2004, staff from the FTC, along with staff from the Department of Commerce, participated in a videoconference with Philippe Renaudiere and Rosa Barcelo regarding the European Commission's review of the Safe Harbor Framework."

"FTC Chairman Muris, several of our Commissioners, and Director Howard Beales have visited with members of the European Commission, European Commission staff, members of the European Parliament who have visited the FTC, and with the Article 29 Working Party in Washington and in Brussels, to discuss possible enforcement coordination on cases involving Safe Harbor companies. In October of 2003, Howard Beales met with the Article 29 Working Party in Brussels."

"(…) Recently, in February of 2004, Jose Luis Piñar Mañas, Director of the Data Protection Authority in Spain and Vice President of the Article 29 Working Party, met with Howard Beales and with staff from the FTC's International Division of Consumer Protection. Also in February 2004, Howard Beales and staff from the FTC's International Division of Consumer Protection, met with Richard Thomas, head of the United Kingdom's Information Commissioner's Office (the UK's Data Protection Authority). In addition, in March 2004, Commissioner Thompson and staff from the FTC's International Division of Consumer Protection met with officials from France's Data Protection Authority – the Commission Nationale de l'Informatique et des Libertés (CNIL)."

When asked **whether there is any special group/task force within the organization dealing with privacy issues**, the FTC responded : "[w]ithin the FTC's Bureau of Consumer Protection, many staff member hours and personnel are dedicated to privacy policy work, education and enforcement efforts. The work of three divisions is most closely involved with Safe Harbor enforcement coordination. They include the Division of Financial Practices (to investigate and pursue possible privacy-related enforcement actions), the Division of Enforcement (for monitoring compliance with privacy-related enforcement orders and the pursuit of follow up actions, as necessary), and the International Division of Consumer Protection (policy and liaison work)." For these divisions, however, privacy is not a main activity.

The last question was **whether any law passed after the adoption of the Safe Harbor framework could limit adherence to the principles** due to (a) necessity to meet national security, public interest, or law enforcement requirements, (b) any statute, government regulation, or case law which create conflicting obligations or explicit authorizations. If yes,

the FTC was asked to provide details, as well as to explain the parameters for the application of the "necessity test" that would have to be conducted as described by the exception included in the introduction to the SH principles. The response is as follows: "[t]he Federal Trade Commission Act[80], (FTC Act), the principal FTC legal authority relied on for the Safe Harbor Framework, has not been amended in any way that we believe would affect the operation of the Safe Harbor Framework. The principle behind the Safe Harbor Framework – that a company's failure to abide by commitments to implement the Safe Harbor Principles may be considered "unfair or deceptive acts or practices in or affecting commerce" under the FTC Act – remains intact."

"The FTC is an independent agency, rather than an executive branch agency, and therefore, it is beyond our scope to attempt to summarize or opine for the executive branch on local, state and federal laws or regulations that could have an impact on the Safe Harbor framework. The Department of Commerce, the executive branch agency within the U.S. government that has the lead authority for the Safe Harbor framework terms and implementation, would be better suited to address this particular inquiry. In the event that the FTC were to receive a Safe Harbor Referral and a Safe Harbor company asserted an excuse for justifiable non-compliance with the Safe Harbor principles, we would at that time apply our independent judgment in analyzing the case specific facts to determine whether an enforcement action is warranted under the application of the Federal Trade Commission Act, in light of legal defenses asserted."

*Other observations*

The FTC noted that it "periodically receives questions and comments from advocacy groups and from non-profit entities concerning the Safe Harbor framework. Bi-annually, the FTC has participated in the TransAtlantic Consumer Dialogue meetings and has answered questions and provided information about our enforcement and consumer and business education privacy agenda, including Safe Harbor enforcement, to European and U.S. consumer and privacy advocates." This illustrates a valuable educational role for the FTC.

However, the FTC also pointed out that "[a] number of non-profit entities have contacted the FTC to determine whether they are subject to the FTC's jurisdiction for purposes of qualifying for certification as a Safe Harbor registrant. These have included educational groups, arts organizations, non-profit medical service providers, genealogy and other research organizations, as well as associations of professionals. The FTC's jurisdiction relates to activities in or affecting commerce, thus, as you know, its enforcement jurisdiction applicable to non-profit entities is generally limited. The FTC does not have jurisdiction over the collection and use of personal information for non-commercial purposes. The comments that we often hear from non-profit entities is that a mechanism does not appear to be provided under the Safe Harbor framework for participation by non-profit entities to facilitate their transatlantic communications and operations." This highlights an important limitation for SH.

[80] See <http://www4.law.cornell.edu/uscode/15/41.html>.

#### 3.3.3.1 Preliminary Conclusions

As is largely the case for the other bodies, the way in which the FTC has fulfilled its role pursuant to SH is only partial, since the FTC has not dealt with any SH-specific complaints or enforcement procedure. Bearing that in mind, the following conclusions can be drawn:

- The FTC stated that "[t]o our knowledge, the FTC has only received one [SH] complaint". The FTC does not appear to have investigated that complaint. No further information was provided about this complaint which is unfortunate given that it would be of considerable importance. Furthermore, this statement contradicts the body of the answer where, when asked about "complaints", the FTC stated that no "referral" has been received.

- The FTC asserted that preliminary injunctions can be obtained if necessary.

- The FTC reported no formal procedure to investigate SH complaints other than those referred by DPAs or self-regulatory organizations.

- The FTC appeared to recognize an obligation to investigate SH complaints only if such complaints are made by DPAs or self-regulatory organizations. Direct complaints by data subjects or consumer groups appeared to have little weight. However, section 5 enforcement powers are not based on the status of the complainant and the FTC's exclusive interpretation of FAQ 5 contradicts paragraph 3 of the SH Principles and the requirement that any violation be actionable. Furthermore, section 5 of the FTC Act empowers the FTC to act on its own authority without the need for a formal complaint from a third party.

- Concerning sanctions, the FTC's response failed to mention two mandatory types of sanctions required by FAQ 11: publicity of findings of non-compliance, and deletion of data in certain circumstances.

The FTC showed little interest in responding to questions about enforcement and only returned the questionnaire after a videoconference with the EU on 22 March 2004. This suggests a lack of interest by the FTC in SH implementation and enforcement.

### 3.3.4 Consumer Associations

The BEUC (Bureau Européen des Union de Consommateurs) was contacted. The BEUC answered that they are not entitled to receive complaints, so they are not able to answer the questionnaire. They sent, however, position papers dated 1999, 2000 and 2001 which they have presented to the EC and to the press containing analysis of the SH from a European consumer point of view. Furthermore, they recommended contacting their national members. As a consequence, a fax and e-mail were sent to the members (25 organizations) containing the questionnaire. So far, two answers have been received – from the UK Consumers' Association (CA) and the UK National Consumer Council (NCC).

The representative from the CA stated that after having checked their data base they could confirm that complaints have not been received. However, the representative added that "this is not an area in which we would necessarily expect to receive complaints."

The representative from the NCC stated that they are a policy organization and do not deal with complaints from consumers. She stated that the organisation is publishing a book in autumn 2004 on consumer privacy.

#### 3.3.4.1 Preliminary Conclusions

- The BEUC has been quite active during the preliminary phases of SH discussions. BEUC explained that it is the role of its national members to follow up the implementation and actions concerning personal data with origin in their own respective countries.

- Twenty five (25) national consumer organizations were contacted, with only 2 responding. A more active role on the part of both consumers' organizations and civil society organizations (e.g. human rights' organizations, civil liberties' organizations) would be desirable.

### 3.3.5 US Department of Commerce (DoC)

When asked about a **description of the review procedure of the information contained in the Safe Harbour self-certification declarations,** the representative from the DoC answered: "U.S. organizations may self-certify their adherence by submitting their self-certification materials on-line (via the Safe Harbor web-site at http://export.gov/safeharbor) or by sending a letter to the Department of Commerce. If the organization chooses to submit its materials on-line, it will electronically transmit two documents: 1) the organization's self-certification form; and 2) a one-paragraph self-certification/affirmation statement from a company officer. If the organization chooses to send its self-certification materials through the mail, it must submit a cover letter from a company official along with its self-certification form. We receive between 10 and 30 self-certifications per month. Over 95% of self-certifications received have been submitted via the website."

"Upon receipt of an organization's self-certification materials, we review the submission in order to determine whether the organization should be placed on the Safe Harbor List. In making this decision, we will review the materials in order to determine: 1) Whether all of the required fields have been completed (Have the criteria specified in FAQ 6 been satisfied?); 2) If the organization's submission is responsive to the applicable fields on the form; and 3) If there are any inconsistencies on the face of the self-certification form (e.g. Does an organization list an inactive link as its privacy policy location?; Does the organization appear to fall outside the scope of Federal Trade Commission or Department of Transportation jurisdiction?)."

"An organization's self-certification to the Safe Harbor List, and its appearance on the list constitute a representation to the Department of Commerce and the public that it adheres to a

privacy policy that meets the Safe Harbor framework. It is ultimately the responsibility of the organization to ensure that its privacy policy reflects compliance with the Safe Harbor. Therefore, we often advise organizations that, before self-certifying for Safe Harbor, they consider carefully the ramifications of the False Statements Act and the Federal Trade Commission Act."

"Organizations that decide to adhere to the Safe Harbor principles must comply with the principles in order to obtain and retain the benefits of the Safe Harbor and publicly declare that they do so. FAQ 6 requires Safe Harborites to state in their relevant privacy policies that they adhere to the Safe Harbor principles. In addition, FAQ 6 requires Safe Harborites to provide a location where their privacy policy is available for viewing by the public. Organizations are often advised to state their adherence to Safe Harbor in their relevant privacy policies and/or to address each Safe Harbor principle and any applicable FAQ requirements within the text of the privacy policy."

"In addition, organizations should make their relevant privacy policies available to the general public. In certain cases, Internet-based privacy policies may satisfy this requirement. In other situations, including those where human resources data is covered in the self-certification, privacy policies housed on Intranet sites, in employee handbooks, or policies made available upon request (by contacting the organization) may satisfy the publicly available requirement."

"Our review of a self-certification normally takes one business day. If it is determined that an organization has submitted complete self-certification materials and that the materials are free of facial inconsistencies, an organization will be placed on the Safe Harbor List. There are currently 486 organizations on the Safe Harbor List.[81] On average, between 10 and 20 organizations are added to the list each month."

"If it is determined that a submission is incomplete, an organization will be notified and asked to complete any applicable field. If any inconsistencies are visible on the face of the form, the organization will be contacted and asked to clarify its response(s). In some cases, we have refused to post organizations to the Safe Harbor List because incomplete or inconsistent areas of the organizations' self-certifications were not resolved."

"The organization's self-certification is valid for one year subsequent to the organization's placement on the Safe Harbor List. In order to continue to enjoy Safe Harbor benefits, an organization will need to reaffirm its self-certification on an annual basis. This can be accomplished by sending the Department of Commerce a letter or an e-mail that reaffirms its commitment to Safe Harbor. (Organizations may also submit a new self-certification form in order to complete its annual self-certification/reaffirmation requirement). Safe Harbor organizations receive periodic letters from the Department of Commerce advising the organization that its self-certification 'Anniversary' is approaching and that the Department of Commerce will require a letter from the organization reaffirming its Safe Harbor commitments. Organizations that have not reaffirmed their self-certification by their anniversary date are designated as 'Not Current' on the Safe Harbor List and periodic e-mails are sent to the organizations to encourage their reaffirmation."

[81] The DoC certification list was last visited on 19 April 2004.

Concerning the **reception of any notification of company's persistent failure to comply with the Safe Harbor Agreement sent by any enforcement body (public or private)**, he stated that the DoC "have not received any notifications of an organization's 'persistent failure to comply' status, nor are [they] aware of any such findings having been made by a self-regulatory program, the Federal Trade Commission, or the European Union Data Protection Authorities."

A description was also given about the **procedure followed when a company does not respect the annual verification**: "Under Safe Harbor Frequently Asked Question #7, Safe Harbor organizations are required to retain their records on the implementation of their Safe Harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction."

"The Safe Harbor framework does not require the organization to submit its annual verification letter to the Department of Commerce and we are unaware of any failure of an organization to provide such a letter upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction."

"If we were to become aware of such facts indicating either that an organization has failed to complete its annual verification, or has failed to respond to a request in the context of an investigation about non-compliance, we would immediately contact the organization to determine the circumstances and if further action is warranted."

"In addition, under FAQ 11, if a relevant self-regulatory or government enforcement body finds an organization has engaged in a 'persistent failure to comply' with the principles, the organization is no longer entitled to the benefits of the Safe Harbor. In this case, the organization must promptly notify the Department of Commerce of such facts either by email or letter. Failure to do so may be actionable under the False Statements Act. That organization must also provide the Department of Commerce with a copy of the decision letter from the relevant self-regulatory or government enforcement body. Self-regulatory or government enforcement bodies are also encouraged to notify the Department of Commerce of such facts."

Regarding **withdrawal of organizations from the SH list**, the DoC representative answered: "Since the Safe Harbor's implementation, ten organizations have been removed from the Safe Harbor List at the request of the organizations. These withdrawals were mainly due to mergers or acquisitions or other cessation of the organizations' business and/or data collection activities." He added that "[they] do **maintain a record of organizations that have withdrawn** from the Safe Harbor List. A list of these organizations is available upon request. The Safe Harbor framework does not mandate that either the Federal Trade Commission or the DPA Panel be informed of such withdrawals as they occur. However, per Frequently Asked Question #6, organizations are required to notify the Department of Commerce. Withdrawal from the list terminates the organization's representation of adherence to the Safe Harbor, but this does not relieve the organization of its Safe Harbor obligations with respect

to personal information received during the time the organization is on the Safe Harbor List." Furthermore: "The Safe Harbor framework does not require the Department of Commerce to maintain a separate list of organizations that withdraw from the Safe Harbor List on the Safe Harbor website. However, we do maintain a record of the organizations that have withdrawn. This record is available upon request."

#### 3.3.5.1 Preliminary Conclusions

- It is noteworthy that the DoC spends one business day for the review of a self-certification. However, part 2 of the present study (i.e. the extensive analysis of certification pages) indicates that the certification pages published on the DoC website often contain important inconsistencies. In particular, there are problems with the exact location of the privacy policies and with references to privacy programs that are not really such programs.

- In the case of problems dealing with privacy policy location, a website may be working at the time that the DoC undertakes its verification procedure but may later cease to work. The DoC should consider carrying out periodic checks of websites subsequent to its initial verification procedure.

- In the case of privacy programs (as already pointed out), certain minimal standards should be applied, and a list of privacy programs should be provided in order to avoid companies choosing organizations that are not privacy programs.

- Even if the SH framework does not require the DoC to maintain a separate list of withdrawn companies, the DoC maintains such a list, which is available to the public upon request (in our experience, having requested it, that list has been sent via e-mail; however, three companies that were assessed for the Intermediate study,[82] were not mentioned in the list). Nevertheless, it would be advisable to make this list directly available on the DoC SH website, because even if a company decides to exclude itself from the SH system, it will still be obliged to respect the representations made for the data received during the period it was an adherent. That explains why, in the list of withdrawn companies, a link should also be provided to the privacy policy under which the company concerned imported EU data. This is necessary for reasons of transparency and the possibility for the individual to exercise the rights guaranteed by the SH principles.

- Finally, certain observations, going beyond the questionnaire, deserve to be made about the DoC website. Firstly, the website is poorly organized – the viewer can only see a small group of companies at a time. Secondly, there is no publicly available search function.

[82] See Reidenberg & Privacy Laws & Business, *op. cit*.

### 3.3.6 ADRs

The questionnaire was sent to the 7 ADR organizations mentioned on the DoC website.[83] Five (5) answers have been received, of which: (1) 1 (hereinafter "organization 1") answered the questionnaire in full; (2) 1 (hereinafter "organization 2") answered the questionnaire in part; (3) 1 answered that they "have not received even one consumer complaint"; (4) 1 answered that they are not involved in the SH scheme; and (5) 1 answered that their SH program is not fully developed.

Regarding the **way to deposit a complaint**, organization 1 provided a link whereby the procedure can be read, with examples of eligible complaints. In terms of **languages**, the information was only provided in English.

Organization 2 provided also links to the procedures, but was silent about languages.[84]

As for the **price** of the arbitration/ADR procedure, organization 1 stated that "ADR is included in the program benefits for [the organization] sealholders only. The pricing is on a sliding scale by company revenues and ranges from $599 per year for small companies under $5 million in revenue to $25,000 per year for companies over $5 billion. There is no cost to the consumer."

Organization 2 stated that "you pay for the services only if you use them. There are no upfront charges or Seal requirements".

Regarding the **selection criteria for panel members**, organization 1 stated: "Our process is entirely followed according to our program requirements and appeals are handled through an appeals board which is composed of half Board members and half independent privacy experts."

Organization 2 stated that "[their] arbitrators and mediators are highly trained professionals with privacy expertise."

When asked whether **there have been procedures** so far, and, if yes, whether they have **statistics**, organization 1 said that they receive 200 disputes per month, but the "US and EU Safe Harbour stats are blended and we do not track them separately".

Organization 2 was silent in this regard.

A question was also asked if a dispute settlement procedure leads to an **obligation of companies to reverse any effects of a violation of the safe harbor principles**, and, if yes, what **other sanctions** can be imposed to companies. Organization 1 responded: "[y]es.

---

[83] See section 3.3 (*supra*, p. 11).

[84] In one of the links containing the publicly available rules of procedure of the organization it can be read: "If the parties have not agreed otherwise, the language(s) of the mediation shall be that of the documents containing the mediation agreement."

Corrective action is determined according to the offence and reasonable satisfaction of the consumer."

Organization 2 was silent in this regard.

When asked whether **decisions/sanctions are made publicly available**, organization 1 answered: "[y]es, when appropriate. We will also notify the Department of Commerce if an EU Safe Harbor Seal Holder were in violation of the program requirements. If we have a significant investigation or corrective action against a company we will post it. […] If there were serious infringements we would publicly post and reserve the right under our license agreement to inform the FTC."

Organization 2 was silent in this regard.

#### 3.3.6.1 Preliminary Conclusions

The possibility to make firm conclusions on the basis of the responses to the questionnaire is rather limited considering that only one organization fully responded. However, other points can be considered:

- It is not advisable that the DoC's SH website mention examples of ADRs that are not involved in SH dispute resolution. Even if the SH regime accepts out-of-court enforcement via ADR organizations, the typical logic of a consumer or private law case would not always be applicable in a SH enforcement case. Specific expertise in privacy, personal data protection and the SH regime itself would be necessary to deal with SH cases. The two organizations that answered the questionnaire stated that the panel members are privacy experts (in the case of organization 1, half of the members).

- As mentioned above in this report, the DoC could maintain a list of ADR organizations with expertise in the SH system, and which offer their services in this context. The organizations would have to comply with SH standards to be registered therein (i.e. the standards provided by FAQ 11)[85].

- It would be preferable to find on the ADR organizations' websites specific reference to SH cases they have addressed (if they have done so, and in case they have not, to mention that as well), with specific statistics. Otherwise it is difficult to evaluate the way these organizations handle SH cases.

- From the answers received, we could infer that the number of complaints has been insignificant (though we cannot assume that there has been a complete absence of complaints because, in the case of organization 1, US and EU statistics are blended).

[85] Furthermore, consideration could be given to the Commission Recommendation of 4 April 2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes (2001/310/EC), O.J.E.C. L 109, 19.4.2001, p. 56 et seq. Even if that document is only dedicated to consumer disputes, the principles described – Impartiality, Transparency, Effectiveness and Fairness – are relevant for developing more elaborate standards for ADR bodies in the SH context.

- As a way of assuring that the system be known and understood by data subjects, multi-linguism of procedures (and rule descriptions) is to be recommended given the fact that not every European data subject understands English.

### 3.3.7 DPA Panel

In the case of the DPA Panel, no questionnaire was sent out since the panel is an *ad hoc* body. The DPA Panel's website provides little information and guidance to data subjects and SH actors. Apart from a complaint form in three languages (German, French and English), no other information seems available. It would be desirable that this form be available in all the EEA official languages.

The existence and role of the Panel should be more visible. For instance, a hyperlink on the respective websites of (i) the national DPAs, (ii) DG Internal Market –Data Protection Unit, (iii) the DoC, and (iv) privacy policies that choose the DPA Panel as an enforcement mechanism, is desirable to inform data subjects about the possibilities of lodging a complaint (the list of relevant US organizations, i.e. those organizations that have chosen DPA panel co-operation, could also be published on the Panel's website to avoid complaints that are outside the Panel's jurisdiction). Further guidance on personal data transfers to the US could also be available on the DPA Panel website.

#### 3.3.7.1 Preliminary Conclusions

The following conclusions can be made regarding the DPA Panel's functioning:

- The Panel is insufficiently visible. It is advised that links to the Panel's website be posted and that serious efforts be otherwise made to enhance awareness about the Panel's existence and role;

- The Panel is an important body since it allows data subjects to lodge their complaints in the EU. Therefore, the role of this entity should be better advertised.

## 4. Impact of new US legislation

### 4.1 Prevailing Laws that Conflict with SH Principles

Since the adoption of the SH, the United States has enacted several privacy laws and regulations that might enable subscribing organizations to disregard SH principles. According to the SH, if US law requires subscribing organizations to ignore SH principles, the protection of personal information transferred will still be deemed "adequate." The SH provides that:

> "Adherence to these Principles may be limited: … by statute, government regulation, or case law that create conflicting obligations or explicit authorizations".

The scope of this "escape clause" is confusing because there is no definition of "conflicting obligations or explicit authorizations".[86] Part B of Annex IV attempts to explain the meaning of the term "explicit authorization". The Annex notes that this exception to SH treatment would apply when US laws "affirmatively authorize the particular conduct by SH organizations" and that the exception "would not apply where the law is silent". However, the Annex also notes "specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorization to disclose the information without notice and consent)." In other words, this interpretative guidance seems to imply that exemptions from privacy protections that are contained in US law are tantamount to "explicit authorization."

As a general matter, this escape clause may be very broad. Typically, US privacy laws and regulations provide a minimum level of protection and, thereby authorize any non-prescribed conduct. Indeed, statutory obligations frequently contain specific exceptions for more permissive treatment of personal information such as affiliate sharing without consent. According to the interpretive guidance in Annex IV, these exceptions must be considered an "explicit authorization".

Organizations relying on the escape clause must demonstrate that "non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization" while "indicating in their privacy policies where exceptions to the Principles permitted by [statute]… will apply on a regular basis." In addition, the exception provides that if US law allows, "organizations are expected to opt for the higher protection where possible." To the extent that US law prescribes a minimum level of protection, organizations could always opt for higher protection.

Only a small number of organizations subscribing to the SH indicated the escape clause in their privacy policies. In general, such references were very vague such as:

> "[company] may disclose user information when we believe in good faith that the law requires disclosure";
> "[company] may make information available to law enforcement personnel and agencies as required by law … and may disclose such information if required by law or a judicial or governmental order or subpoena";
> "this privacy policy is subject in all respects to applicable legal and regulatory requirements and limitations that would dictate actions or policies different from those set forth herein".

These references do not provide sufficient transparency for data subjects to determine the exceptions that are applied to the company's privacy statement and to the SH principles. When one company did provide a more explicit reference, there was still no citation to any

[86] A prior report to the European Commission on the Safe Harbor has shown that the explanatory material in Annex IV, Part B is contradictory. See Privacy Laws & Business, "Report to the European Commission on US/EU Safe Harbor and the Financial Services Sector" (Dec. 2000).

particular statute and the reference was rather confused. This company prepared balloting packages and conducted voting for clients' officers and bylaws elections. The privacy statement indicated: "state laws vary with respect to public access and use of this voter registration information." This indication makes no sense. State laws governing public access to voter registration apply to public elections and are not relevant for private elections such as those for corporate officers. Securities regulation, however, might impose disclosure obligations for the identity of private election participants.

Since too few organizations make any reference in their privacy policies to overriding legislation or legal rules and none cite specific rules, this analysis will therefore identify potentially conflicting obligations arising from key new legal rules that have entered into force in the United States between the adoption of SH and the Study deadline of 1 November 2003.[87]

As an initial observation, there do not appear to be many new examples in US law where the escape clause affects data transferred from the European Union under SH. The most significant issues revolve around the USA PATRIOT Act.[88] This statute, adopted shortly after the terrorist attacks of 11 September 2001, created new law enforcement powers and modified many provisions of existing law to assist law enforcement in the deterrence and punishment of terrorist acts. The Act gives US law enforcement agents greater powers to access personal information and engage in surveillance activities. This expanded law enforcement authority remains controversial in the United States. Many of the Act's provisions are irrelevant for SH because most of the Act does not pertain to activities covered by SH. For example, Title III of the Act relates to financial services that are outside the scope of SH. Oddly, however, the Act does contain a provision directly relevant to human resources data. In that same context, a recent decision in connection with affiliate sharing and credit reporting[89] may have significant implications beyond the financial services sector with respect to data integrity and onward transfer for human resources information. In the area of sensitive data, the US Department of Health and Human Services issued health privacy regulations in August 2002 to implement the Health Insurance Portability and Accountability Act.[90] These regulations replaced the health privacy rules issued at the end of the Clinton Administration in 2000. Lastly, in the context of telecommunications services, several new rules or decisions affect the use of transmission data and personal privacy in a way that may have a tangential impact on data originating in the EEA.

---

87 The European Commission has previously undertaken an analysis of conflicting rules in effect as of December 2000 for the financial services sector even though this sector is not covered by the Safe Harbor. See Privacy Laws & Business, Report to the European Commission on US/EU Safe Harbor and the Financial Services Sector (Dec. 2000). Similarly, the European Commission has decided that conflicts regarding airline passenger data arising from the Aviation and Transportation Security Act, Pub. L. 107-71 (Nov. 18, 2001) and corresponding regulations have been resolved. See Communication from the Commission to the Council and the Parliament of 16 December 2003, COM (2003) 826 final, at <http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/apis-communication/apis_en.pdf>. Analysis of those issues is, therefore, unnecessary and they are not re-visited in this study.

88 Pub. L. 107-56 (Oct. 26, 2001).

89 *Bank of Am., N.A. v. City of Daly City,* 279 F. Supp. 2d 1118 (ND Ca. 2003).

90 Pub. L. 104-191 (1996).

Law Enforcement: USA PATRIOT Act

The USA PATRIOT Act contains a number of provisions that override the SH principles of choice, data integrity and onward transfer.[91] Specifically, the Act authorizes, and in many cases, requires electronic communications service providers to disclose personal information to government agencies in connection with law enforcement investigations without affording any choice to the data subject. These disclosures typically relate to communications services such as transaction records or emails. For example, section 203(a)(1) expressly authorizes the disclosure of grand jury information to a series of federal agents when the information relates to foreign intelligence or counterintelligence. Section 203(b) also allows the disclosure among law enforcement officials of the contents of electronic communications. The federal agents, however, may only use such information "as necessary in the conduct of that person's official duties." Section 210 expands the scope of information that may be obtained by a subpoena for records of electronic communications to include Internet connection information, payment information and information on types of services. Section 212(a) expressly authorizes the disclosure by communications service providers of users' data to governmental entities when the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." Section 212(b) requires an electronic communications service provider to disclose basic information about subscribers to a governmental entity on the basis of an administrative subpoena.[92] Section 214 specifically authorizes the government to obtain a court order for the installation of pen registers and trap/trace devices to gather data within the United States for the investigation of foreigners. Section 216 gives the government the right to require through court order that electronic communications service providers install pen registers and trap/trace devices to capture transaction records of Internet users without notice to those users. Section 215 empowers the FBI to obtain a Foreign Intelligence Surveillance court order requiring the production of business records from organizations in the United States for foreign intelligence and international terrorism investigations. The court order is confidential and the party disclosing business records to the FBI is prohibited from revealing the existence of the order and record disclosure to the data subject. This power is very broad as the FBI need not identify the target of the investigation and can seek wide range of business records.

In essence, these provisions of the Act "expressly authorize" disclosures to a third party – government agencies – without the choice of the data subject for purposes outside the scope of those related to the original data collection. These derogations from the SH principles are nevertheless justified on law enforcement and security grounds. Indeed, a separate escape

---

[91] The analysis of the USA PATRIOT Act does not address provisions of the law affecting data privacy for activities not covered by Safe Harbor such as financial services, education records maintained by US education institutions, immigration eligibility or the monitoring of foreign students studying in the US.

[92] The information is: name, address, local and long distance telephone connection records, or records of session times and durations, length of service, types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment. Section 212 also provides a more troubling authorization for service providers to disclose transaction records or other information relating to a subscriber or customer "to any person other than a governmental entity." This clause, however, is not an issue for Safe Harbor since the subscribers and customers will be US-based and the data in question will be of US origin.

clause of the SH allows organizations to derogate from the SH principles "to the extent necessary to meet national security, public interest, or law enforcement requirements."

### Human Resources Data: USA PATRIOT Act and Affiliate Sharing

One of the miscellaneous provisions of the USA PATRIOT Act provides an express authorization for employers in the financial services sector to disclose negative suspicions about employees in written employment references. Section 355 authorizes, but does not require, federally insured banks and uninsured branches and agencies of foreign banks to disclose in written employment references "information concerning the possible involvement of such … party in potentially unlawful activity."[93] This type of disclosure might contravene the data integrity provisions of SH because the Act provides no specific mechanism for an affected employee to challenge any inaccurate statements.

Similarly, the recent federal court decision in *Bank of Am., N.A. v. City of Daly City*[94] is likely to have an impact on human resources information. In a challenge to a state ordinance that required opt-in consent for financial institutions to share personal information among affiliates, the federal district court held that the federal Fair Credit Reporting Act (FCRA) pre-empted the stronger state law. The court found that the FCRA "expressly exempt[s] information shared among affiliates from the definition of a consumer report." As a result, the privacy protections of the FCRA expressly do not apply to data received by affiliates. Because the court's decision extended the affiliate-sharing clause to cover personal financial information in a context other than credit reporting, the decision means that the affiliate sharing exemption will apply to all areas covered by the FCRA. Since the FCRA expressly allows disclosure of personal information for employment purposes without consent,[95] the decision appears to allow the sharing of employment data among affiliates without limitation as to purpose and without consent. This apparent interpretation is contrary to SH principles and organizations are not likely to be able to show that non-compliance based on this statutory authorization is "necessary to meet the overriding legitimate interests furthered by such authorization."

### Sensitive Data: HIPAA Regulations

The initial regulations for health privacy were issued at the end of the Clinton Administration in December 2000. However, the Bush Administration modified the Clinton rules and promulgated new regulations on 14 August 2002 that took full effect on 14 April 2003.[96] The regulations protect "individually identifiable health information,"[97] though they exclude from protection health information maintained by an employer. Most of the HIPAA regulations will be inapplicable to EU data because they only regulate personal information held by

---

93 While financial services are excluded from Safe Harbor, this clause pertains to human resources data and is therefore relevant.

94 279 F. Supp. 2d 1118 (ND Ca. 2003).

95 15 U.S.C. § 1681b(a)(3)(C).

96 See 45 C.F.R. Parts 160 and 164. See also Dept. of Health and Human Services, General Overview of Standards for Individually Identified Health Information (2 Dec. 2002 as revised 3 April 2003), <http://www.hhs.gov/ocr/privacysummary.pdf>.

97 45 C.F.R. § 160.103.

"covered entities" such as US health care providers delivering services in the United States or health insurance plans. However, organizations that provide billing services or clearinghouse functions and that receive individually identifiable health information in the course of their processing are "covered entities."[98]

The HIPAA regulations authorize a "covered entity" to use and disclose personal information without the patient's consent for "treatment, payment … health care operations … public interest and benefit".[99] These exceptions from consent may conflict with choice requirements in the SH for sensitive data. Significantly, the regulations also exempt certain marketing activities from patient consent.[100] This explicit authorization for the use of sensitive data is in conflict with SH principles of choice and data integrity.

Telecommunications data

Several recent decisions may have an adverse effect on the SH principles of choice and integrity. In the context of choice, personal information of Internet users and telecommunications customers may now in certain circumstances be disclosed without the consent of data subjects for purposes that are outside those associated with the collection of the personal information. In particular, the identity of Internet users may be revealed to third parties without the consent of the Internet user. A number of court decisions under state law allow parties in a civil law suit to obtain a court order compelling the disclosure by Internet service providers of the identity of Internet users or anonymous posters on bulletin boards when those users are alleged to have engaged in illicit conduct.[101] Such derogation from the SH principles would, however, be justified as necessary to meet an overriding legitimate interest.

For telecommunications data, the Federal Communications Commission issued new regulations on "customer proprietary network information" in July 2002.[102] These rules followed an adverse court ruling against the previous opt-in regime.[103] The new regulations allow communications companies to use CPNI of subscribers without subscriber consent for marketing services in the same category[104] and with notice and opt-out for a variety of other uses as well as opt-in for certain specific cases.[105] While subscriber information will not be of European origin, these regulations have the odd effect of authorizing the use of third party data that might be of European origin without any protections. Third party data will be

98 45 C.F.R. § 160.103; 45 CFR § 164.500(b).

99 45 C.F.R. § 164.502(a)(1)(ii).

100 45 C.F.R. § 165.514(e)(1).

101 See e.g. *Immunomedics, Inc. v. Jean Doe,* 775 A.2d 773 (N.J. Super. 2001)(compelling ISP to disclose the identity of an anonymous poster who was alleged to have violated an employment agreement.) See also *John Doe v. 2TheMart.com Inc.*, 140 F.Supp.2d 1088 (W.D. Wash. 2001) (establishing a four part test to determine when the identification of an anonymous writer may be compelled).

102 In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, THIRD REPORT AND ORDER AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING Adopted: July 16, 2002 Released: July 25, 2002, <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-214A1.pdf>, codified at 47 CFR Part 64.

103 *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir., 2000).

104 47 C.F.R. § 64.2005(a).

105 47 C.F.R. § 64.2007.

contained in subscriber CPNI such as calling patterns between the subscriber and third parties. Yet, the regulations do not require any confidentiality with respect to the non-subscriber information. As such, the permissive use of non-subscriber data deviates from SH principles.

Most recently, the implementation by the Federal Trade Commission and the Federal Communications Commission of the National Do-Not-Call list for telemarketing[106] has the unintended consequence of authorizing outbound telemarketing to European phone lists and effectively exempts this use from the consent of those European subscribers. Telemarketers are permitted to make commercial solicitations to phone numbers as long as they have assured that the numbers are not registered on the national do-not-call list maintained by the Federal Trade Commission.[107] Registration on the do-no-call list is voluntary and 55 million US telephone numbers were registered during its first six months of operation.[108] However, non-US telephone numbers are not eligible for registration. Consequently, telemarketers are expressly authorized to use any European telephone lists for telemarketing without the consent any European telephone subscribers. While this would deviate from the SH principles of choice and, possibly data integrity, the transfer of European telephone lists under SH to US call centers for telemarketing is likely to be a rare occurrence.

### 4.2 Significance of new US legislation for SH

Since the new US legislation only rarely contradicts the SH principles for data covered by SH, these conflicts do not appear to undermine the level of protection for any significant flows of personal data to the United States. The controversial provisions of the USA PATRIOT Act are essentially irrelevant for SH data flows. Nevertheless, three particular points of concern remain from the new aspects of US law: (1) an obscure clause in the USA PATRIOT Act and a recent court decision under the Fair Credit Reporting Act may exempt certain human resources data from key protections; (2) the health insurance privacy regulations authorize processors of health information to escape SH requirements for some uses of heath data including the consent of patients for marketing; and (3) FCC regulations and FTC regulations authorize certain uses of personal information related to telecommunications in ways that may deviate from SH for European-origin data. While these points of concern illustrate new permissible exemptions from the protection of SH, they are isolated and do not appear at present to involve any significant amount of European data. However, the evolution of the exemption for human resources data may undercut SH in the future.

---

106 See Do-Not-Call Implementation Act, Pub. L. No. 108-10, 117 Stat. 557 (2003); 16 C.F.R. § 310.4(b)(1)(iii)(B) (FTC rule); 47 C.F.R. § 64.1200(c)(2) (FCC rule); *Mainstream Marketing Services, Inc. v. Federal Trade Commission*, 2004 U.S. App. LEXIS 2564, (17 Feb. 2004)(upholding the legality of the Do-Not-Call list against a Constitutional challenge).

107 16 C.F.R.§ 310.4(b)(3).

108 See FTC, Press Release: "Compliance with Do Not Call Registry Exceptional" (13 Feb. 2004), <http://www.ftc.gov/opa/2004/02/dncstats0204.htm>.

# IV. Conclusions

The SH implementation review[109] indicates that although participating US organizations have made efforts to accommodate privacy concerns, important improvements are required to ensure that safeguards for personal data streams under the SH are adequate. As a general observation, the majority of the reviewed US organizations seem to have difficulties in correctly translating the SH principles into their data-processing policies. Implementation deficiencies are not necessarily the result of bad faith but likely find their origin in confusion over the obligations of SH and perhaps a different perception of what personal data protection involves. These problems can be overcome by providing better guidance on the mechanics as well as the meaning of the SH data protection principles.

It is regrettable that the FTC's response to the questionnaire was considerably delayed and came only after repeated requests. The same can be said in respect of the 5 EU/EEA DPAs which have not answered the questionnaire. This weakness in responses does not reflect positively on the vitality of the SH.

SH participants generally scored well as regards formal requirements that need to be fulfilled in the certification process. The positive tendencies, as described in the report, are minimal but nonetheless important. They demonstrate that US organizations are sensitive to the data protection issue and are willing to invest resources in compliance. It should not be forgotten in this regard that a thorough understanding of data protection matters has also taken a long time to evolve in Europe and is an ongoing process.

## 1. Deficiencies Observed

From a legal point of view, however, there are numerous deficiencies in the way in which SH has hitherto been implemented. The most alarming deficiencies are as follows:

### 1.1 SH Principles

- Transparency and comprehensibility of **notices** or privacy policies were often deficient: privacy policies were generally difficult to read and were often not able to provide clear insight into data-processing activities and associated risks. While privacy policies showed important quality differences, all of them suffered from some deficiency (major or minor). The nature of the enforcement system of the SH regime may limit transparency. Exposure to liability under the SH scheme is directly linked to explicitness and clarity of announced data protection practices.

[109] The study task description did not include the impact of the CAN-SPAM Act on the SH framework since this Act became effective on 1 January 2004. See Letter of 27 October 2003 (ref. no. 5751) from Philippe Renaudiere (Head of Data Protection Unit) & Jacqueline Minor (Authorizing Officer by Sub-Delegation) of the European Commission to Dean Yves Poullet (Director) of the CRID.

- **Choice** was not clearly mentioned or lacking entirely. Choice is crucial for individuals to have minimal control over the processing of personal data pertaining to them. Without effective choice, personal data can be imported, used and distributed with little restriction. Representations regarding the affordability of choice were usually missing.

- With respect to **onward transfers**, the status of mentioned "third parties" was not always clear (e.g. "partner", "affiliate", etc.), and as a consequence, it was neither clear if those parties were acting in their controller or processor capacity. Express commitment of third party processors to respect the SH was lacking in certain cases. Apart from these problems, the flexibility offered by this principle could be used to circumvent EU law.

- Deficiencies were found also with respect to adoption of **security measures**. Certain companies did not represent adopting such measures.

- Regarding **data integrity**, the relevance of the data for the intended use was difficult to determine, since either the "purpose", the "data type" or the "activities" conducted were not specified at all or not clearly formulated.

- The principle of **access** tended to be weakly implemented. The right was often limited to contact information or not offered at all. Representations regarding the affordability of access were generally missing.

### 1.2 Self-Certification

- The entry, "Personal information received from the EU", in the DoC self-certification form presented many disparities in the answers given by companies. Some described the activities they conduct or gave a description of their business model, some described the purposes for processing, while some described the type of data imported.

- The requirement of accurate location of the privacy policy was not entirely fulfilled. Some of the provided hyperlinks did not work, some led to the home-page of the company where it was sometimes difficult to find the proper link to the privacy policy.

- The FTC was mentioned by the companies importing human resources data as the statutory body with jurisdiction to hear claims against the companies, yet the jurisdiction of the FTC in this respect is dubious.

- Many companies claimed to be members of privacy programs that are not really privacy programs.

### 1.3 Privacy Programs

- The analysed privacy programs did not incorporate all SH principles (or incorporated certain SH principles deficiently).

### 1.4 Enforcement

Whereas no concrete cases have been analysed (given the apparent paucity of enforcement cases or complaints received by enforcement bodies), only the implementation of the enforcement principle and FAQ 11 were assessed. Therefore, any statement as to whether enforcement bodies are fulfilling their role is limited to the application of the said SH obligations either in privacy policies or by ADR organizations' description of procedural rules. The following deficiencies were revealed:

- Organizations agreed to co-operate with the DPA Panel (even if they did not process human resources data), but generally did not represent their acceptance to *comply* with the DPA Panel's advice. This is alarming, especially with respect to data imports outside the jurisdiction of the FTC (arguably the case with human resources data).

- The different sanctions foreseen by FAQ 11 were not always available in the ADR mechanisms analysed.

- Publicity of findings was not fully guaranteed.

- For certain dispute resolution bodies/programs there was no indication or guarantee that the dispute would be heard by experts on SH or data protection. Enforcement mechanisms were insufficiently reflected in the privacy policies, and data subjects would have had to conduct extensive research to obtain information about the complaint procedure (mostly by checking the website of the privacy program/ADR organization).

### 1.5 US legislation

- As a result of new US legislation, European-origin health information, European-origin employee data, and European-origin data relating to communications services may be exempt from the protection of SH principles and risk, accordingly, being given a lower level of protection than provided by those principles.

## 2. Possible Mechanisms for Improvement

The answers of the different parties demonstrate a low awareness by data subjects of international data transfers since no complaints/claims have been received and treated with

respect to SH despite frequent and even flagrant inconsistencies and violations in implementation of SH. The tendency to draft privacy policies in English only does not enhance European data subject awareness.

It is believed that implementation of the SH system could be improved in various ways:

## 2.1 Implementation of the SH Principles

The following measures are suggested to guarantee a better implementation of the SH principles:

### 2.1.1 Guidance on Privacy Policy Drafting

- It is advisable that the DoC publishes a set of guidelines on the drafting of SH privacy policies. The DoC could also publish a format that helps companies in their drafting process. An ideal format is one that is fairly concise, and that clearly reflects the SH principles. Such guidelines could be developed in close co-operation with the European DPAs, represented in the Article 29 Data Protection Working Party. The advantage of a fixed format is that the policies can be easily reviewed, compared, and it may also have an important pedagogical value.

### 2.1.2 Data Controller and /or Data Processor Capacity

- While the assessment of the legitimacy of data transfers under the SH principles falls outside the scope of this study, it is considered appropriate to indicate that the DoC certification page requires companies to select whether they are importing personal information in their capacity as a data processor or as a data controller (or both). In this context, it would be helpful to provide further guidance as to the requirements with which US data processors need to comply. The DoC certification page should also reflect the dichotomy between US organizations that are data controllers and those that are data processors.

### 2.1.3 Clarification of Key Concepts

- Certain key concepts in the SH agreement remain unclear ("personal data", "privacy program", "aggregate data", "anonymous data", etc.). It is advisable that guidance be provided by the Article 29 Data Protection Working Party, in co-operation with the FTC/DoC, to create a better understanding of the field of application of the SH, through more precise definition of such concepts.

### 2.1.4 SH Label

- Adherent companies should post on their websites a specific SH label informing data subjects of their SH membership. The label would have to link to their SH privacy policy. This would avoid the confusion created by disparate titling of "privacy policies", the typography used, the placement on home-pages, etc. An official SH

label could be designed and required to be used upon certification. It could also be combined with the proposal to use a SH privacy policy template.

2.1.5 Human Resources Data

- Companies importing human resources data must be required to agree to *comply* with the DPA Panel decision in the self-certification form.[110]

## 2.2 Enforcement

2.2.1 FTC jurisdiction

- Clear guidance about the jurisdiction of the FTC is required with respect to human resources data and other personal data streams where the jurisdiction of the FTC is doubtful. This can come from a declaratory judgment by a federal court or express statutory modifications from Congress. Another solution is that US organizations which import and process data falling outside the jurisdiction of the FTC, are either required to accept the jurisdiction of the DPA Panel or to use another system that offers adequate protection (e.g. Model Contractual Clauses).

2.2.2 Minimal Standards for Privacy Programs and ADRs

- Privacy program service providers and dispute resolution service providers should be subject to minimum quality standards as regards data protection expertise, available sanctioning mechanisms, responsiveness, etc.

## 2.3 US Legislation

- Companies wishing to rely on the escape clause in SH for US legislation should clearly identify the relevant provisions of US law which will be used to justify a lower level of data protection.

[110] It should be noted that, at the time of the adoption of the SH, inclusion of human resources data was negotiated at the end, so there could remain certain inconsistencies in this regard. As a consequence, new tools for TBDF have to be considered in order to clearly determine the adequate way to transfer this kind of data, with important points of reference being the Commission Decisions on Model Contractual Clauses and the Article 29 Data Protection Working Party Document on Binding Corporate Rules.

## 2.4 Role of the different parties

### 2.4.1 The US Department of Commerce

- The DoC website needs to be designed in a more user-friendly manner (e.g. the SH list should provide a search function, the possibility to visualize the whole list in alphabetical order, listing by date of adherence, etc.).

- The webpage for self-certification should also accommodate controller-processor data transfers, entries to specify "data type" imported, "purposes" and "activities conducted" in processing such data. Furthermore, a non-exhaustive list of purposes could be given in the on-line form as a guidance for companies.

- Companies importing human resources data should represent their agreement to comply with the DPA advice. It is recommended that the self-certification form contain an entry for such a declaration.

- Regarding the location of the privacy policy to be declared in the self-certification, the DoC should control that companies do not provide a link to the home-page but to the relevant SH privacy policy.

- It is also advisable that companies importing human resources data provide a privacy policy that is available on the Internet. Even if this is not strictly mandatory, it is highly recommended that the policies be directly and readily available to the DPA Panel in case of dispute.

- The website should also contain a list of companies that have withdrawn from SH membership.

- The DoC website should contain a standard SH privacy policy format that contains minimum language and a structure which is concise and that reflects the principles (more than describing data processing practices). Privacy policies should be required to explain clearly the complaint/enforcement procedure; this should also be the case if US organizations are member of a privacy program.

### 2.4.2 The Federal Trade Commission

- The FTC should take concrete action in order to ensure that the adherent companies incorporate all of the SH principles in their privacy policies.

- Appropriate action should be taken to ensure that privacy program and ADR service providers clearly comply with the SH requirements.

2.4.3 The DPA Panel

- More visibility of the DPA Panel is advisable. Privacy policies, as well as websites of official SH authorities, such as the DoC, FTC, DPAs, the European Commission's relevant Data Protection website, should provide for a link to the DPA Panel website.

- The complaint procedure and the complain form to the DPA Panel should be more transparent and be translated into all EEA countries' respective languages.

- The DPA panel ought to be competent to act before the ADR bodies as a representative of the data subjects' interests.

2.4.4 The DPAs

- It is advisable that each national DPA provides a brief and simple description of the SH system and data subjects' rights under this system, as well as a complaint form in the national language in their websites.

- Their websites should also contain a direct link to the DPA Panel and the relevant SH webpages of the FTC/DoT and DoC.

2.4.5 Business Representatives and Intermediate Organizations (e.g. consumer and civil liberties organizations)

- Business representatives and intermediate organizations, including consumer and civil liberties organizations, have an important role to play in the SH scheme. They may provide not only awareness about the SH system but also the institutional framework to develop and enforce privacy programs and/or model privacy policies compliant with the SH principles.

## 3. Discriminatory Application

- Article 4 of the Commission Decision states: "The Commission shall … evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including (…) any evidence that the present Decision is being implemented in a discriminatory way."

While an analysis of discriminatory implementation was not included in the requested tasks of this Study,[111] the research arising from this Study suggests three different issues that should be considered for future work.

a) The existence of SH and the lax compliance by US organizations with SH mean that any third country's request for an adequacy finding on the basis of a SH-like agreement would result in discrimination if the EU insists on strict compliance and stronger enforcement than that implemented in the SH.

b) The deficiencies and laxity in the US implementation of the SH, combined with the lack of enforcement actions, suggest that the SH regime discriminates against EU companies in favor of US companies. The absence of effective enforcement mechanisms and actions despite the easily documented shortcomings of organizational policies and practices, means that the US companies are operating under a less stringent data protection standard and can, in effect, process European data in ways that are forbidden to EU companies without real risk of sanction. For example, given the way in which the onward transfer principle is applied, US companies can transfer European data more liberally than their European counterparts.

c) Where SH principles are applied strictly, there may be discrimination against US companies if such application is more exacting than the application of Directive 95/46/EC (or, more precisely, the member states' national laws transposing the Directive) to EU companies. To the extent that member states have not yet fully tranposed the Directive, the SH regime may have more onerous provisions for US companies.

[111] See Letter of 27 October 2003 (ref. no. 5751) from Philippe Renaudiere (Head of Data Protection Unit) & Jacqueline Minor (Authorizing Officer by Sub-Delegation) of the European Commission to Dean Yves Poullet (Director) of the CRID.

# APPENDIX I – Analytical Criteria for SH Adherents

The following criteria and descriptions are taken from: Joel R. Reidenberg & Privacy Laws & Business Independent Consultant Study Report, "The Functioning of the US-EU Safe Harbour Privacy Principles" (21 September 2001; available from European Commission).

## 1. Eligibility Criteria

The first category "Eligibility" identifies elements in the SH and FAQs that seek to establish whether a company's statements demonstrate that the company is, in fact, qualified to participate in SH.

The following elements provide a preliminary indication that an organization is eligible to benefit from the advantages of SH. The results of the analysis of these elements are included in Table 1.1 of Appendix VI.

*Public Disclosure of Privacy Policy*[112]

Commission Decision 2000/520/EC requires that the organization make a public disclosure of its privacy policy. Indeed, for the FTC to have jurisdiction over an organization under section 5 of the FTC Act for engaging in an "unfair or deceptive practice", the organization must make a public statement of its policy.

*Printable Policy*

As a practical matter, when an organization makes its public disclosure on the Internet, the policy must be printable so that data subjects, data exporters and data protection authorities can evaluate the privacy policy at a specific moment in time. If the policy is not capable of being printed, then there is no way to verify the terms of the policy applicable to data of European origin at any later point in time. This element indicates whether or not the policy can be printed.

*Jurisdiction*[113]

SH requires that an organization be subject to the jurisdiction of either the FTC or the Department of Transportation. This element identifies the relevant jurisdiction.

*Coverage*

Organizations may subscribe to the SH for the treatment of all their EU-origin data or for only some of their EU-origin data. This element seeks to identify the choices that organizations have made.

---

112 Recital 5; Art. 2(a).

113 SH Art. 1(2)(b).

*Policy Applies to EU Data Indefinitely*

FAQ 6 states that "the undertaking to adhere to the SH Principles is not time-limited …. [the] undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves SH". This element confirms whether organizations have made the commitment to apply their privacy polices to EU data for as long as the organization processes such data.

*Policy Signals US Law Preventing Compliance*

The SH allows US law to override provisions of the SH if there is an explicit conflict between the two. This element identifies whether the organization has indicated any such conflicts.

SH also requires that the self-certification letter of each adhering organization contain particular information. The elements of this procedural eligibility are found in FAQ 6. The results of the analysis for these elements are included in Tables 1.2 and 1.3 of Appendix VI.

*Name of Organizational Contact*
*Address of Organization*
*Telephone number*
*Fax number*
*Email*[114]
*Description of the Types of Processed EU Data*[115]
*Public Location of the Privacy Policy*
*Accurate Location of the Privacy Policy*[116]
*Date of SH Self-Certification*[117]
*Effective date of privacy policy*
*Organization's Contact Office*
*Identification of the Regulatory Agency that may hear claims*[118]
*Identification of the organization's membership in any privacy programs*[119]
*Verification Method of Organizational Compliance*
*Independent Recourse Mechanism*[120]
*HR Data + DPA Enforcement*[121]

---

[114] This criterion indicates if the Certification lists either a general organizational email address or a specific contact email address for SH issues.

[115] FAQ 6 requires that the certification include a "description of the activities of the organization with respect to personal information received from the EU".

[116] This indicates if the address shown on the Certification is an accurate and precise location for the privacy policy. When the Certification indicates a web site that is not the actual page for the privacy policy, the location will be marked as inaccurate.

[117] Although this is not precisely stated in FAQ 6, this element indicates when SH adherence takes effect.

[118] FAQ 6 requires that the organization state the specific statutory body that has jurisdiction to hear claims against the organization.

[119] FAQ 6 requires organizations to state the name of any privacy programs to which the organization belongs.

[120] FAQ 6 requires organizations to state the independent recourse mechanism that is available to investigate unresolved complaints.

[121] FAQ 6 requires organizations processing human resources data to declare their commitment to co-operate with the DPA and to comply with the advice of such authority.

2. Substantive Compliance Criteria

The second category "Compliance" identifies the elements of corporate privacy policies that show whether adhering organizations meet the substantive content requirements of the SH and FAQs. The Compliance criteria are divided into groups reflecting each of the SH principles (notice, choice, onward transfer, security, integrity, and access).

2.1 For the notice principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.1 of Appendix VI.

*Clear language*

SH provides that "notice must be provided in clear and conspicuous language". Clarity relates to the ease with which a data subject can understand the privacy policy. This element identifies whether the corporate policies are clear to an informed reader.

*Conspicuous Language*

SH provides that "notice must be provided in clear and conspicuous language". Conspicuous means that the notice is readily found. The certification of an inaccurate location, for example, would be an illustration of inconspicuous notice. This element identifies whether corporate policies are conspicuously posted.

*Specified Purpose*

SH requires that corporate policies notify data subjects of the purposes for the data processing. This element identifies whether corporate privacy policies contain purpose specifications.

*Organization Contacts*

SH requires that privacy policies provide contact information for the corporation. This element identifies whether corporate policies include contact information.

*Third Party Disclosures*

SH requires adherents to disclose if they transfer personal information to third parties. This element identifies whether corporate policies disclose third party disclosures.

*Notice of Choice for use/dissemination*

The SH Notice Principle requires that data subjects be informed of their choices and the means to limit use and disclosure of personal information. This element identifies whether the corporate policies provide such notice.

*Statement of SH Compliance*

FAQ 6 requires that "all organizations that self-certify for the SH must also state in their relevant published privacy policy statements that they adhere to the SH". This element identifies whether the corporate privacy policies make such affirmations.

2.2 For the Choice Principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.2 of Appendix VI.

*Opt-out (3rd party)*

SH requires an opt-out for the dissemination of personal data to third parties, other than those performing data processing services for the SH adherent. This element identifies whether corporate policies include an opt-out.

*Opt-out (secondary use)*

SH requires an opt-out for the secondary use of personal data. This element identifies whether the corporate privacy policies include such an opt-out.

*Clear language*

The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice".

*Readily Available*

The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice". This element identifies whether the corporate privacy policies provide a "readily available" mechanism to exercise choice. For this element, "readily available" will mean that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out) and that the opt-out mechanism be transparent for data subjects.

*Affordable*

SH requires that the means to exercise choice be affordable for data subjects. This element identifies whether the corporate privacy policies indicate affordable means to exercise choice.

*Opt-in (Sensitive Data)*

SH requires opt-in for data subjects. This element identifies whether the corporate privacy policy offers an opt-in for sensitive data.

2.3 For the Onward Transfer principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.3 of Appendix VI.

*Notice of Onward Transfers*

The SH provides that "to disclose information to a third party, organizations must first apply the Notice and Choice Principles." This element identifies whether company privacy policies provide notice of onward transfers.

*Choice*

The SH provides that "to disclose information to a third party, organizations must first apply the Notice and Choice Principles." This element identifies whether the company privacy policies offer choice with respect to onward transfers.

*3rd Party Processor's Commitment to SH*

SH requires that an organization may transfer personal data to third-party processors only if "the third-party subscribes to the Principles … or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles." This element identifies whether the corporate policies indicate that any third-party processors have made commitments either to SH or to a contract with at least the same level of protection.

2.4 For the Security principles, the single element found in SH will be included in Table 2.4 of Appendix VI.

*Reasonable Security Precautions*

SH requires that organizations take "reasonable precautions to protect [data] from loss, misuse and unauthorized access, disclosure, alteration and destruction." This element identifies whether the corporate privacy policies indicate reasonable security precautions.

2.5 For the Integrity principles, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.4 of Appendix VI.

*Relevance of Data for Specified Purpose*

SH requires that "personal information must be relevant for the purposes for which it is to be used". This element identifies whether the corporate policies indicate in some way that the data is relevant for the specified purpose.

*Compatible/Authorized Processing for secondary use*

SH provides that "an organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual". This element indicates whether the corporate privacy policy makes a commitment to finality and either opt-in or opt-out for secondary use.

*Steps to Ensure Reliability for intended use*

SH requires that "an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current". This element identifies whether the corporate privacy policies make any assertions regarding their steps to assure the reliability of their data.

2.6 For the Access principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.5 of Appendix VI.

*Reasonable Access Provided*

The SH requires that individuals "have access to personal information about them that an organization holds … except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy." FAQ 8 notes that "if information is used for decisions that will significantly affect the individual … then … the organization would have to disclose that information even if it is relatively difficult or expensive to provide." FAQ 8 also states that "it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information." This element identifies whether corporate privacy policies make the commitment to provide reasonable access for data subjects to stored personal information that is not publicly available to the public at large and not combined with non-publicly available information.

*Reasonable Cost for Access*

FAQ 9 permits organizations to "charge a reasonable fee" for access. This element identifies whether the organization indicates that it charges a reasonable fee. If the organization indicates that there is no fee for access, then the organization will also satisfy this element.

*Correction / Amendment of Inaccurate Data*

The SH stipulates that "individuals must … be able to correct, amend or delete information where it is inaccurate, except … where the legitimate rights of persons other than the individual would be violated." This element identifies whether the organization states that data subjects may have inaccurate data corrected or amended.

*Deletion of Inaccurate Data*

The SH stipulates that "individuals must … be able to correct, amend or delete information where it is inaccurate, except … where the legitimate rights of persons other than the individual would be violated." This element identifies whether the organization states that data subjects may have inaccurate data deleted.

3. Enforcement Criteria

The third category "Enforcement" identifies the elements satisfying the enforcement requirements of the SH with specific attention to FAQs 5 and 11.

3.1 The following elements provide an indication of the type of recourse mechanism chosen by the organization and the existence of remedies and sanctions. The results of the analysis for these elements are included in Table 3.1 of Appendix VI.

*Independent Recourse Mechanisms pursuant to FAQ 5*

SH requires "readily available and affordable independent recourse mechanisms". This may be satisfied either pursuant to FAQ 5 or FAQ 11. This element indicates whether the organization has stated its intent to satisfy the independent recourse requirement pursuant to FAQ5.

*Independent Recourse Mechanisms pursuant to FAQ 11*

SH requires "readily available and affordable independent recourse mechanisms". This may be satisfied either pursuant to FAQ 5 or FAQ 11. This element indicates whether the organization has stated its intent to satisfy the independent recourse requirement pursuant to FAQ 11.

*Obligation to remedy problem*

SH states that enforcement must include "obligations to remedy problems arising out of failure to comply with the Principles". This element identifies whether the organizational policy requires the organization to provide a remedy for non-compliance. If an organization belongs to a privacy program that requires its members to provide a remedy, then this element will be satisfied.

*Sanctions for Violations*

SH requires that "sanctions must be sufficiently rigorous to ensure compliance by organizations". Any company that has elected DPA as a recourse mechanism, but that does not fully satisfy FAQ 5, cannot satisfy the sanctions requirement.

3.2 For organizations that have chosen independent recourse pursuant to FAQ 5, the following elements indicate compliance with FAQ 5. The results of the analysis of these elements will be included in Table 3.2 of Appendix VI.

*Elects enforcement by the relevant Data Protection Authority*

FAQ 5 requires that the organization declare in its self-certification that it "elects to satisfy [the recourse obligation] …. by committing to co-operate with the DPAs." This element identifies whether the organization has made this requisite statement. [this obligation must be

fulfilled in the privacy policy. If a company has stated in its certification letter to elect DPA enforcement, but does not make such a statement in the privacy policy, then this requirement is considered not fulfilled].

*Agrees to co-operates with Data Protection Authority*

FAQ 5 requires that the organization declare in its self-certification that it "will co-operate with the DPAs in the investigation and resolution of complaints." This element identifies whether the organization has made this requisite statement.

*Agrees to comply with the advice of the DPA*

FAQ 5 requires that the organization declare in its self-certification that it "will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take remedial or compensatory measures." This element identifies whether the organization has made this requisite statement.

3.3 For organizations that have chosen independent recourse pursuant to FAQ 11, the following elements indicate compliance with FAQ 11. The results of the analysis of these elements will be included in Table 3.3 of Appendix VI.

*US Legal or Regulatory Supervision*

FAQ 11 allows the Enforcement Principle to be satisfied by "compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution". According to FAQ 11, this is in addition to any possible FTC recourse. This element identifies whether the organization has reported that it is subject to such US supervisory authority.

*Independence of Recourse Mechanism*

FAQ 11 states that "[w]hether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record". Under FAQ 11, a company may satisfy this requirement by making a commitment to co-operate with the DPA or by submitting to an independent dispute settlement mechanism. This element identifies whether the organization has stated its submission either to the DPAs or to an independent dispute settlement mechanism.

*Readily Available/Affordable Recourse*

FAQ 11 states, "as required by the enforcement principle, the recourse available to individuals must be readily available and affordable." This element identifies whether the organization has stated recourse that appears readily available and affordable.

*Transparency of Dispute Resolution Procedures*

FAQ 11 requires that "recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works". This element identifies whether an organization has made the recourse mechanism transparent. If a company has elected DPA dispute settlement and indicates such mechanism in its privacy policy, then the process will be considered transparent. Similarly, if an organization has elected another independent dispute settlement mechanism, indicates such mechanism in its policy, and the mechanism's procedures are available either through the organization or through the mechanism itself, then the recourse will be considered transparent.

*Company Agrees to Reverse Effects of Breach*

FAQ 11 requires that the dispute resolution proceeding remedy result in a reversal of the effects of non-compliance. This element identifies whether the organization commits to reversing the effects of non-compliance with the organization's policy.

*SH Compliant Future Processing*

FAQ 11 requires that the dispute resolution proceeding remedy result in future processing that will be in conformity with the SH Principles. This element identifies whether the organization commits to this remedy.

*Cessation of Processing of Data for Harmed Individual*

FAQ 11 requires that the dispute resolution proceeding remedy result in the cessation, when appropriate, of or processing the personal data of the individual who brought the complaint. This element identifies whether the organization commits to this remedy.

*Publicity for Findings*

FAQ 11 states that "sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances". This element identifies whether the independent dispute settlement mechanism elected by the organization is required to provide publicity for all findings of non-compliance.

*Sanctions*

FAQ 11 requires sanctions that "could include suspension and removal of a seal, compensation for individuals for losses … and injunctive orders". These sanctions must be in addition to any possible FTC action. Also, FAQ 11 requires that sanctions include "the requirement to delete data in certain circumstances" depending on the dispute resolution body's interpretation of the data's sensitivity. This element identifies whether an organization appears to be subject to such sanctions. Any company that has elected enforcement by a DPA, but has not agreed to abide by the DPA decision does not qualify for sanctions. Any organization that belongs to a privacy program whose rules provide for the removal of a seal in the event of non-compliance does qualify.

3.4 For organizations that rely on an independent dispute settlement mechanism, the following elements indicate whether the independent dispute settlement mechanism complies with FAQ 11. The results of the analysis of these elements will be included in Table F of Appendix VI.

*Investigation of each Complaint*

FAQ 11 states that "Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous." This element identifies if the dispute resolution body states that it investigates each complaint.

*Readily available/ Affordable Recourse*

FAQ 11 provides that "as required by the enforcement principle, the recourse available to individuals must be readily available and affordable." This element identifies if the recourse appears to be readily available and affordable.

*Transparency of Recourse Procedures*

FAQ 11 states that "recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices." This element identifies whether the independent recourse mechanism provides information on the procedures for filing a complaint and dispute settlement.

*DRB Obtains Reversal of Effects of Breach*

FAQ 11 states that "the result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization." This element identifies whether the independent dispute resolution body appears to have the authority to obtain the reversal of the effects of non-compliance.

*DRB Obtains SH Compliant Future Processing*

FAQ 11 states that "the result of any remedies provided by the dispute resolution body should be … that future processing by the organization will be in conformity with the Principles." This element identifies whether independent dispute resolution body appears to have the authority to compel that future processing by compliant with SH.

*DRB Obtains Cessation of Processing*

FAQ 11 states that "the result of any remedies provided by the dispute resolution body should be … where appropriate, that processing of the personal data of the individual who has brought the complaint will cease." This element identifies whether the independent dispute resolution body appears to have the authority to order the cessation of processing.

*Compensation for Harm*

FAQ 11 provides that "sanctions could include … compensation for individuals for losses incurred as a result of non-compliance." This element identifies whether independent dispute resolution bodies appear to have the authority to order such compensation.

*Privacy Program Sanctions*

FAQ 11 provides that "sanctions could include suspension and removal of a seal." This element identifies whether privacy program rules require the suspension or removal of the seal from organizations not in compliance with the program's privacy principles.

*Publication of Dispute Resolution Body's Sanction*

FAQ 11 requires that "sanctions should include publicity for findings of non-compliance" by the independent dispute resolution mechanism. This element indicates whether the dispute resolution body publicizes all findings of non-compliance.

*Mandatory Referral of Dispute Resolution Body's Sanctions*

FAQ 11 states that the "private sector dispute resolution bodies and self-regulatory bodies must notify failures of SH organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts … and to notify the Department of Commerce." This element identifies whether the dispute resolution body or privacy program has a mandatory referral provision in its rules.

## APPENDIX II – Analytical Criteria for Privacy Programs

The following criteria and descriptions are taken from: Joel R. Reidenberg & Privacy Laws & Business, Independent Consultant Study Report, "The Functioning of the US-EU Safe Harbor Privacy Principles" (21 September 2001; available from European Commission):

A. *Incorporation of SH notice principles in privacy program rules*

SH states "if an organization joins a self- regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor." According to FAQ 11, only "privacy programs that incorporate the Safe Harbor Principles into their rules" can be used to satisfy the Enforcement Principle. This first group of criteria identifies whether the privacy program incorporates the SH notice principles in the program's rules of membership. The results of the analysis of this group are included in Table A of Appendix VI. These elements are:

- Member's policy provide program contact information;[122]
- Member's policy must state compliance with SH;[123]
- Member's policy must be clear and conspicuous;[124]
- Member's policy must specify the purposes for data processing;[125]
- Member's policy must disclose 3rd party recipients;[126]
- Members must provide data subjects with notice of choice for use and dissemination of personal information.[127]

B. *Incorporation of SH choice principles in privacy program rules*[128]

This second group of criteria identifies whether the privacy program incorporates the SH choice principles in the program's rules of membership. The results of the analysis of this group are included in Table B of Appendix VI. These elements are:

- Member's policy must provide opt-out for 3rd party disclosures;[129]
- Member's policy must provide opt-out for secondary use;[130]
- Members must offer clear and conspicuous choice;[131]

---

122 SH Notice Principle & FAQ 6. See also Appendix I, at 2.1

123 *Id*.

124 *Id*.

125 *Id*.

126 *Id*.

127 *Id*.

128 SH states "if an organization joins a self- regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor." According to FAQ 11, only "privacy programs that incorporate the Safe Harbor Principles into their rules" can be used to satisfy the Enforcement Principles.

129 SH Choice Principle. See also Appendix I, at 2.2.

130 *Id*.

131 *Id*.

- Members must provide the choice in a readily available manner;[132]
- Members must provide choice in an affordable manner;[133]
- Member's policy must provide opt-in for sensitive data.[134]

C. *Incorporation of SH onward transfer principle in privacy program rules*[135]

The third group identifies whether the privacy program incorporates the SH onward transfer principle in the program's rules of membership. The results of the analysis of this group are included in Table C of Appendix VI. These elements are:

- Members must provide notice of onward transfers;[136]
- Members must provide choice for onward transfers;[137]
- Members must obtain 3rd party processor's commitment to comply with the SH principles.[138]

D. *Incorporation of SH security and integrity principles in privacy program rules*[139]

The fourth group identifies whether the privacy program incorporates the SH security and integrity principles in the program's rules of membership. The results of the analysis of this group are included in Table D of Appendix VI. These elements are:

- Members must take reasonable security precautions; [140]
- Members restrict their processing to relevant data;[141]
- Members only process data for purposes that are compatible with the specified purpose or that are authorized by the data subject;[142]
- Members must take steps to ensure the reliability if data for the intended use.[143]

E. *Incorporation of SH access principle in privacy program rules*[144]

---

132 *Id*. "Readily available" means that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out.)

133 *Id*.

134 Id.

135 SH states "if an organization joins a self- regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor." According to FAQ 11, only "privacy programs that incorporate the Safe Harbor Principles into their rules" can be used to satisfy the Enforcement Principles.

136 SH Onward Transfer Principle. See also Appendix I, at 2.3

137 *Id*.

138 *Id*.

139 SH states "if an organization joins a self- regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor." According to FAQ 11, only "privacy programs that incorporate the Safe Harbor Principles into their rules" can be used to satisfy the Enforcement Principles.

140 SH Security Principle. See also Appendix I, at 2.4

141 SH Data Integrity Principle. See also Appendix I, at 2.5

142 *Id*.

143 *Id*.

144 SH states "if an organization joins a self- regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor." According to FAQ 11, only "privacy programs that incorporate the Safe Harbor Principles into their rules" can be used to satisfy the Enforcement Principles.

The fifth group identifies whether the privacy program incorporates the SH access principle in the program's rules of membership. The results of the analysis of this group are included in Table E of Appendix VI. These elements are:

- Members must provide reasonable access to data subjects for their personal data;[145]
- Members may a reasonable fee for access;[146]
- Members must provide for correction of inaccurate data;[147]
- Members must provide for the amendment of inaccurate data;[148]
- Members must provide for the deletion of inaccurate data where appropriate.[149]

F. *Incorporation of SH enforcement principles in dispute resolution including FAQ 11*

The fifth group identifies whether the privacy program and its dispute resolution body, if any, incorporate the SH enforcement principles, including those specifically enumerated in FAQ 11. The results of the analysis of this group are included in Table F of Appendix VI. These elements are:

- The Privacy Program provides an Independent Dispute Resolution Body ("DRB") for individuals' complaints about members;[150]
- The DRB must investigate of each complaint;[151]
- Privacy Program offers readily available and affordable recourse;[152]
- Privacy program recourse procedures are transparent for data subjects;[153]
- DRB can require the reversal of the effects of non-compliance with the Member's privacy policy;[154]
- DRB can obtain a commitment that future processing be compliant with SH;[155]
- DRB can require the cessation of non-conforming processing;[156]

---

145 SH Access Principle & FAQ 8. See also Appendix I, at 2.6

146 FAQ 9. See also Appendix I, at 2.6

147 SH Access Principle. See also Appendix I, at 2.6

148 *Id*.

149 *Id*.

150 The SH Enforcement Principle requires the existence of "available and affordable independent recourse mechanisms." FAQ 11 requires an independent recourse body and states: "Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record".

151 The SH Enforcement Principle requires the existence of "available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved." FAQ 11 states: "Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous".

152 SH Enforcement Principle requires the existence of "available and affordable independent recourse." FAQ 11 states: "As required by the enforcement principle, the recourse available to individuals must be readily available and affordable".

153 FAQ 11 states: "recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint".

154 FAQ 11 states: "The result of any remedies provided by the dispute resolution body should be that the effects of noncompliance are reversed or corrected by the organization, in so far as feasible".

155 FAQ 11 states: "The result of any remedies provided by the dispute resolution body should be … that future processing by the organization will be in conformity with the Principles."

- DRB can order compensation for harm caused by non-compliant processing;[157]
- Privacy Program can sanction Members;[158]
- DRB publishes all decisions containing sanctions;[159]
- DRB refers sanctioned cases to governmental authorities when member fails to take corrective action.[160]

---

[156] FAQ 11 states: "The result of any remedies provided by the dispute resolution body should be ... where appropriate, that processing of the personal data of the individual who has brought the complaint will cease." FAQ 11 also requires that "sanctions should include … the requirement to delete data in certain circumstances."

[157] SH Enforcement Principle provides that "damages [be] awarded where the applicable law or private sector initiatives so provide". FAQ 11 states: "Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles …. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance …. Other sanctions could include … compensation for individuals for losses incurred as a result of non-compliance."

[158] SH Enforcement Principle requires that "sanctions … be sufficiently rigorous to ensure compliance by organizations."

[159] FAQ 11 requires that "Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances".

[160] FAQ 11 requires that "Private sector dispute resolution bodies and self-regulatory bodies must notify failures of safe harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce (or its designee)".

# APPENDIX III – Questionnaires for in-depth study of company practices

This questionnaire is based on the study conducted by Yves POULLET, Bénédicte HAVELANGE, Axel LEFEBVRE, Marie-Hélène BOULANGER, Herbert BURKERT, Cécile De TERWANGNE, "Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection es personnes physiques à l'égard du traitement de données à caractère personnel", Centre de Recherches Informatique et Droit (CRID). Commission Européenne – DG XV. Contrat ETD/95/B5-3000/165. Décembre 1996.[161]

1-Party responsible for the transfer in the country of origin (sender)

A. Type of business

2-Recipient of the data in the third country

A. commercial (specify)

B. HR (specify)

C. research (specify)

D. travel (specify)

E. other (specify)

3-Characteristics of the data transferred

What is the number of concerned persons on the file per transfer?

What is the number of items of information transferred?

What is the content of the data transferred?

*Identification data (name, address, telephone number, identity card, driver's license, etc.) provide details.

[161] This study is also available at the CRID's website, see <http://www.droit.fundp.ac.be/crid/privacy/default.htm> (last visited 10/08/02).

*Personal characteristics (age, sex, marital status, physical data, nationality, immigration status, military status, household composition, leisure and interests, consumption habits, education and training, etc.). Provide details.

*Data relative to profession and employment (current employment, details as to termination of employment, attendance and disciplinary history, salary, evaluation, etc.). Provide details.

*Medical data (relative to physical o psychological state of health, to the situations and behaviours at risk, to the medical background, etc.). Provide details.

*Data relative to the sexual behaviour of the person on file. Provide details.

*Data relative to the racial or ethnic origin of the person on file. Provide details.

*Data relative to the religious, philosophical or political convictions of the person on file. Provide details.

*Data relative to the union affiliation of the person on file. Provide details.

*Other data category. Provide details.

4-Purpose of the transfer

A. What is the purpose of the transfer?

*Company management (personnel administration, planning of activities, clientele management, management of litigations, public relations, technical-commercial information, etc.). Provide details.

*Commerce (mail order sales, customer profiling, direct marketing, etc.). provide details.

*Teaching and culture (student administration, library administration, etc.). provide details.

*Health care

*Scientific research (epidemiological research, bio-medical research, sociological research, etc.). Provide details.

*Other aims (to be identified).

B. Is the purpose of the posting in the third country identical to that pursued by the transmitter of the data?

5-Periodicity of the flow

A. What is the frequency of the transfers for which the authorisation is requested?

*Permanent (specify)

*Regular (specify)

*Exceptional (specify)

6-Duration of storage

A. No storage (immediate destruction).

B. Limited storage (in this case, specify the storage duration in months and in years, the aim of the storage, for example, for the purpose of proof).

C. Unlimited storage duration (specify the reasons).

7-Means of transfer

What is the chosen means of transfer (on-line network, physical, etc.)?

If it involves a network, does it involve a closed (e.g. Galileo) or an open (Internet) network? Provide details.

8-Security

A. Please describe the security measures that your organization has implemented to provide adequate technical and organizational security.

9-Patriot Act and other laws

A. Please describe the concrete impact of the Patriot Act (or other national security regulations) as regards personal data you receive from the EU.
B. Has your company ever limited the adherence to the SH principles (a) to meet national security, public interest, or law enforcement requirements, (b) due to any statute, government regulation, or case law that create conflicting obligations or explicit authorizations? If yes, provide details.

10-Notice

A. How does your organization implement the Notice principle?

B. At what moment does your organization provide notice?
C. How does your organization determine the purposes for which it collects and processes personal data?
D. What standard does your organization use to afford clear and conspicuous notice (e.g. have the notice read by non-lawyers before it is posted on the website)?

11-Choice

A. How does your organization implement the Choice principle?
B. How does your organization assess the (non-)compatibility of a subsequent purpose with the original one?
C. Does the opt-in requirement for sensitive data processing create practical problems?
D. Does opt-out permit an individual to exercise choice at any time?

12-Onward Transfers

A. In the case you transfer data to a third party, does this party subscribe to the principles, is subject to the directive, another adequacy finding or do you enter into a written agreement with that third party.
B. How do you conduct onward transfers to data controllers (under SHA)?
C. How do you conduct onward transfers to data processors (under SHA)?

13-Data Integrity

A. How do you apply the data integrity principle, given the fact that the SH principles do not contain the purpose specification principle?

14-Access and Rectification

A. How do you implement access and rectification? Could you please describe the procedures you offer to data subjects?
B. How many access requests have you received? Have you encountered problems in administering access and rectification?

15-Enforcement

A. What is/are the mechanism/s you have chosen for assuring compliance with the SH principles?
B. What recourse/s it/they provide for individuals affected by non-compliance?
C. Are these mechanisms readily available?
D. Are they affordable? How much would they cost to the data subject?
E. Are damages foreseen in the applicable law or private sector initiative?

F. What are the follow-up procedures for verifying that the attestations and assertions your company make about its privacy practises are true and have been implemented as presented?
G. What would be the consequences/sanctions for your organization in the case of non-compliance?

16-Sensitive data

A. In case you process sensitive data, do you give opt-in?

17-Journalistic exception

A. Have you ever applied the journalistic exception? If yes, under what circumstances?

18-Co-operation with European DPAs

A. Have you committed to co-operate with European DPAs? If yes, has any co-operation been concretely asked? If yes, what kind of co-operation? What was the outcome?

19-Certification

A. Do you provide self-certification letters on an "annual" basis?

20-Verification

A. Which verification procedure has your company chosen?
B. Do you provide for the "annual" verification?

21-Human Resources data

A. In case you transfer HR data, what is the purpose of such transfer?
B. Do you disclose it to third parties?
C. Do you use it for different purposes?
D. How do you implement "notice" and "choice" principles in those cases?
E. Do you anonymize certain data, assigned codes or pseudonyms when the actual names are not required for the management purpose at hand?
F. Have you ever denied an "access" requirement asked by an employee? If yes, under which basis?

22-Controller to processor

A. In case you transfer data to a processor located in the US under the SH principles, do you also signed a contract regulating this issue?

23-Travel data

A. Is travel data transferred?
B. If yes, have your company been asked access to these data by US public bodies?

24-Pharmaceutical and Medical data

A. In case you transfer pharmaceutical and/or medical data, is these data used for new scientific research activity?
B. Have individuals asked to withdraw from a clinical trial?
Which use do you make of these data?

25-Public record and publicly available information

A. Does your company transfer data from Public record or publicly available information?

26-Internal Communication and Management of the SH Principles

A. How do you concretely train your employees to ensure that your organization effectively respects the SH principles (internal guidelines, employee education, software architecture (e.g. pop=ups), employee notices, etc.)?

27-Reason for joining the SH

A. What has been the reason for your company to join the SH?

28-Procedure

A. Did you find the procedure for joining: difficult, bureaucratic, simple, etc.?

29-Problems

A. Have you experienced any problem after joining the SH? If yes, could you describe/explain the nature?

## APPENDIX IV – Questionnaires to different parties involved in the SHA system

a) Questionnaire to Lawyers (confidentiality of their names guaranteed)

1) What do you consider to be the advantages of the SHA regime when you contemplate a corporate data transfer strategy?
2) What do you consider to be the disadvantages of the SHA regime when you contemplate a corporate data transfer strategy?
3) Do you consider that the European Commission Decisions on Model Contractual Clauses has any impact on the strategy concerning TBDF? Why?
4) Do you believe that the SHA system results in a double data protection regime within companies (one for EU data and one for US data), or do you rather experience that companies increase the US data protection regime to the SH regime or beyond it?
5) How do you implement the yearly certification and verification requirements (internally or via a third party auditor; please describe the internal procedure)?
6) Have you been confronted with enforcement actions (including investigative questions) of European DPAs in the context of data transfers under the SH regime? If yes, what was the outcome?
7) Have you been confronted with enforcement actions (including investigative questions) of the FTC (or any other US public body) in the context of the SH regime? If yes, what was the outcome?
8) What complaint and mediation procedure do you prefer (BBBOnLine, TRUSTe, DMA, or other? Why? Which elements do you consider when you choose between these providers?
9) Do you have experience with data protection complaints before such private bodies? If yes, what was the result? Do you believe they function well?
10) How do you generally provide access to data subjects (via data exporters or data importers)?
11) Do you believe that the SH regime offers a feasible solution to conduct: =processor to processor transfers? =controller to processor transfers?
12) Have any of your clients experienced limitations in the adherence to the SH principles due to: (a) necessity to meet national security, public interest, or law enforcement requirements; (b) due to any statute, government regulation, or case law that create conflicting obligations or explicit authorizations? If yes, provide details.

b) Questionnaire to European DPA

1) Is notification of data transfers required pursuant to the data protection Act (or otherwise) of your country? If yes, please specify the legal basis and procedure of such notification. Does such notification require that you mention the legal basis (including the SHA) on which personal data is transferred to the third country?

2) If notification is required, please mention how many data transfers under the SHA regime have been declared to your institution.
3) Can you specify the data transfer categories that are notified to your institution, and the exact amount of notifications for each category (e.g. 25 HR data, 12 consumer data, etc.)?
4) Can you specify how many of the SH notifications concern intra-company transfers and how many concern third company transfers?
5) Do you treat SH transfers differently if the "harbourite" has announced not to co-operate with European DPAs? If yes, could you specify the differences?
6) Has your organization published any specific guidelines and/or opinions for companies that want to use the SH regime? If yes, could you provide a copy of them?
7) Has your organization received any complaint regarding the transfer of personal data under the SH regime? If yes, could you please specify how many complaints you have received and from whom you received the complaint (data subject, consumer protection organization, data exporter, other)? What was the nature/reason of the complaint? How are such complaints treated? Has your organization put procedures in place to investigate compliance with the SHA and to co-ordinate such investigations with the FTC? What has been the outcome of such a complaint procedure?
8) Has your organization received any communication from the FTC to investigate data streams under the SH regime (for instance, where a data subject's complaint is investigated by the FTC but needs input of your organization)?
9) Has your organization ever approached the FTC to monitor and/or investigate compliance with the SHA?
10) Has your organization ever suspended data flows under Article 3 of the SHA? If yes, why?
11) Is there any information procedure foreseen for the application of Article 3.1.a) of the SHA? If yes, could you describe it?
12) Are you assessing/have you assessed the extent to which the adherence to the SHA principles may be limited for purposes of national security, public interest, or law enforcement requirements, as mentioned in the introduction to the SH principles?
13) How many people within your institution work with international data transfers?

c) Questionnaire to the FTC

1) Have you received any complaint concerning the application of the SHA? If yes, from whom (directly from the data subject, ADR/ODR bodies, competitor companies, data exporter, European DPA, consumer association, etc.)? Can you describe the nature and outcome of the complaint/s?
2) Do you have procedures in place to deal with such complaints? If yes, can you please describe them?
3) Is there any fee for submitting a complaint? If yes, how much does it cost (approximately)?

4) Can you take preliminary actions during the procedure? If yes, please describe them.
5) What type of sanctions can the FTC impose?
6) Have you contemplated any type of communication procedure with European bodies (European Commission, European DPAs, Article 29 Working Party, etc.) for better implementation of enforcement procedures?
7) Is there any special group/task force within your organization dealing with privacy issues? If yes, can you please describe their function regarding the SHA?
8) Is there any law passed after the adoption of the SHA that could limit adherence to the principles due to: (a) necessity to meet national security, public interest, or law enforcement requirements; (b) any statute, government regulation, or case law that create conflicting obligations or explicit authorizations? If yes, provide details. What are the parameters for the application of the "necessity test" that would have to be conducted as described by the exception included in the introduction to the SH principles?

d) Questionnaire to Consumer Organization

1) Have you ever received a complaint connected to the use of personal data transferred under the SHA? If yes, could you please describe it? If no, what do you think is the reason for a lack of complaints?
2) In case you receive a complaint, what would/have you do/done?
3) Have you made any analysis/report/survey concerning the implementation of the SHA from a consumer law point of view? If yes, could you provide a copy of it/them or a description of the main findings/outcome?
4) Do you think that when a consumer is targeted in their own language, and data concerning them are transferred under the SHA, it would not be necessary to provide notice in the same language? If yes, what is the legal basis? Do you think this issue has an impact on complaints/enforcement of the SHA agreement? Why?

e) Questionnaire to the DoC

1) Do you make any kind of review of the information contained in the SH self-certification declarations?
2) If yes, could you please describe the review procedure (e.g are incomplete certifications refused; do you control consistency between the information provided in the self-certification form-letter and the privacy policy of the company; etc)?
3) Have you received any notification of a company's persistent failure to comply with the SH Agreement sent by any enforcement body (public or private)?
4) What is the procedure you follow when a company does not respect the annual verification?
5) Have you withdraw any company from the list?

6) If yes, do you keep record of those companies? Is this notified to the FTC and or DPA Panel?
7) Is the record of withdrawn companies (if any) made publicly available, for instance, on the webiste?

f) Questionnaire to ADRs

1) Has your organization competence to investigate SHA consumer privacy complaints?
2) Could you please explain how consumers may deposit a SHA complaint with your organization?
3) Does your organization provide for forms and procedures in different languages?
4) What is the price for an arbitration/ADR procedure (for both companies and consumers) in an SHA dispute?
5) What are the selection criteria for panel members/arbitrators?
6) Have there been any SHA procedures so far? Do you have any available statistics?
7) May a dispute settlement procedure lead to an obligation of companies to reverse any effects of a violation of the safe harbor principles? What other sanctions can be imposed to companies?
8) Are decisions/sanctions on SHA dispute settlements made publicly available?

## APPENDIX V – Data Tables and Graphics of Point 2 (Certification Page Analyses)

| Compan | a) Ind sect | b) Data type | Controller/ Processor | c) Personal data | d) Accur | f) verif | g) Reg | h) Priv. Prog | i) DR | j) Co | k) certif |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | CSV | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | ADV | C, pro | pro | on, off, MP | Y | in-h | FTC | DMAshp | DMAshp | no | Current |
| | TES | C | cont | off | NDL | in-h | FTC | N/A | DPA | no | Current |
| | MCS | C, RH, pro | pro | on, off, HR | No | in-h | both | no | DPA | Y | Current |
| | ADV | RE | cont | on, off | NDL | in-h | FTC | DMAguid | DMAshp | no | Current |
| | DRG, BTC, HCS | RE | cont | on, off, MP | NDL | in-h | FTC | HON, TRUSTe | DPA | no | Current |
| | CSV, INF | C, pro | pro | on, off, MP | NDL | in-h | FTC | no | DMAshp | no | Current |
| | CPT, CSF | HR | cont | on, HR | NDL | in-h | both | TRUSTe | DPA, TRUSTe | no | Current |
| | FNS | C | cont | off, MP | PA | in-h | FTC | no | DPA | Y | Current |
| | TEL, TES, CSF | HR | cont | HR | Intranet | in-h | error | N/A | DPA | Y | Current |
| | CSV, FNS | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | CSV, CSF | C, pro | pro | on, off | Y | in-h | FTC | no | DPA | Y | Not |
| | DFN, INF, TES | C | cont | on | Y | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | EIP, ELC, BTC | HR, C | cont | on, off, HR, MP | Y | in-h | both | BBB | BBB, DPA | no | Current |
| | TRA | T, pro | pro | on | NDL | TP | FTC | no | DPA | Y | Current |
| | INF | C, HR | cont | on, off, HR | Intranet | in-h | both | no | DPA | Y | Current |
| | GSV | RE | cont | on, off, MP | Y | in-h | FTC | CASRO | DPA | Y | Current |
| | HCS, INF | RE | cont | on, off | Y | in-h | FTC | no | BBB | no | Current |
| | INS, EDS, GST | ? | cont | on, off, MP | PA | in-h | FTC | no | DPA | Y | Current |
| | ADV, TRN, INF | C | cont | on | Y | in-h | FTC | AAA | AAA | no | Current |
| | CSV, INF, HCS | RE, M | cont | on | NDL | TP | FTC | BBB | BBB | no | Current |
| | GCG, INF | C | cont | on, off, MP | NDL | in-h | FTC | no | BBB | no | Current |
| | EDS, TRA | C RH, M | cont | on, off, HR, MP | Y | in-h | both | BBB, TRUSTe | BBB, TRUSTe, DPA | no | Current |
| | ACR, APS, PVC | C, HR | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | BTC | R, HR, C | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | MED, DRG | R, HR, C | cont | on, off, HR, MP | No | in-h | both | no | DPA | Y | Current |
| | CSF | HR | cont | on | Y | in-h | both | no | DPA | Y | Current |
| | CSF, CSV, INF | C | cont | on, off, MP | Y | TP | FTC | TRUSTe | TRUSTe | no | Not |
| | CSV | C, pro | pro | on, off | No | in-h | FTC | no | DPA | Y | Current |
| | BOK, ADV | C, pro | pro | on | No | in-h | FTC | DMAshp | DMAshp | no | Current |
| | APS | HR | cont | HR | Y | in-h | error | no | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | CSF, CSV, CPT | C RH | cont | on, HR | Y | in-h | both | no | DPA for HR | Y | Current |
| | ADV, CSF | C | cont | , | Y | TP | FTC | NAI, TRUSTe | TRUSTe | no | Current |
| | CSF | C RH | cont | on, off, HR | NDL | in-h | both | no | BBB, DPA | Y | Current |
| | ADV | C | cont | on, off | NDL | in-h | FTC | TRUSTe | TRUSTe | Y | Current |
| | GCG | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | TRA, GSV, MCS | C RH | cont | on, off, HR | Y | in-h | both | no | DPA | Y | Current |
| | EDS, CSV, CSF | C RH | cont | on, off, MP | NDL | TP | FTC | TRUSTe | TRUSTe | Y | Current |
| | MED, DRG, BTC | C, HR | cont | on, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | CSF | HR | cont | HR | Intranet | in-h | error | N/A | DPA | Y | Current |
| | ACE | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | CSV, INF, CSF | HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | ADV, INF | C | cont | on, MP | AUR | in-h | FTC | no | DPA | Y | Not |
| | INF, CSV | C | cont | on, off, MP | Y | in-h | FTC | BBBOnL | DMAshp | no | Current |
| | TRA | T | cont | on, off | NDL | in-h | FTC | BBBOnL | BBB | no | Current |
| | ADV, INF, GSV | C, pro | pro | on off | Y | in-h | FTC | CAUCE, AIM | TRUSTe | no | Current |
| | HCS MED | HR, C | cont | on, off, HR, MP | No | in-h | both | N/A | DPA | Y | Current |
| | INF,CFS | C | cont | on, off | NDL | in-h, T | FTC | NAI | BBB, DPA | Y | Current |
| | INF, CSV, TES | C | cont | on, off | NDL | in-h | FTC | no | DPA | Y | Current |
| | EDS | C | cont | on, off | Y | in-h | FTC | BNI | DPA | Y | Current |
| | APS | HR | cont | , | , | in-h | error | no | DPA | Y | Current |
| | ADV | C | cont | on | Y | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | INV, ADV, EDS | HR, C | cont | on, HR | Y | in-h | both | GBCC | BBB | Y | Current |
| | HCS | C | cont | on | NDL | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | CFS, CVS | C | cont | on | NDL | TP | FTC | TRUSTe, BBB | TRUSTe | no | Current |
| | ADV | C | cont | on, off | Y | in-h | FTC | no | DMAshp | no | Not |
| | EDS, CSV, MCS | HR | cont | HR | AUR | in-h | error | no | DPA | Y | Current |
| | CSF, CSV, GSV | HR | cont | on, HR, MP | PA | in-h | both | no | DPA | Y | Not |
| | CSV | C, pro | pro | on | PA | in-h | FTC | no | DPA | Y | Current |
| | CSF, MED | C RH, M | cont | on, HR | NDL | in-h | both | BBB | BBB, DPA | Y | Current |
| | ACE, TES, OMS | HR | cont | HR | Intranet | in-h | error | DoC | DPA | Y | Current |
| | CSF, CSV | C | cont | on, off, MP | NDL | TP | FTC | DMAshp, TRUSTe | DMA, TRUSTe | Y | Current |
| | INF | C | cont | on | Y | TP | FTC | TRUSTe, HON | TRUSTe, HON | no | Current |
| | CSV | C, pro | pro | on | Y | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | CSV, GSV, INF | HR, C | cont | on, off, MP | PA | in-h | FTC | no | DMAshp | Y | Current |
| | CSF, CSV, INF | C | cont | on | Y | in-h | FTC | no | DPA | no | Current |
| | INF | HR | cont | HR | Y | in-h | error | N/A | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | AGM, CON, FNS | HR | cont | HR | Y | in-h | error | no | DPA | Y | Current |
| | GIE, EIP, TEL | HR | cont | on, off, MP, HR | NDL | in-h | both | no | DPA | Y | Current |
| | CSV, CSF | R, pro | pro | off, MP | AUR | in-h | FTC | no | BBB | no | Current |
| | ARW, CSF, INS | C | cont | on, off, MP | Y | in-h | FTC | no | DPA | Y | Current |
| | CSF, CSV | HR, pro | pro | on, HR | No | in-h | both | no | DPA | Y | Current |
| | CSV, MCS, INF | HR, RE | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | CPT, CSC | C | cont | on | NDL | in-h | FTC | no | AAA | no | Current |
| | CSV | HR | cont | on, off, HR, MP | Intranet | in-h | both | no | DPA | Y | Current |
| | TES | C | cont | on | Y | in-h | FTC | no | AAA | no | Current |
| | INF | C, RH | cont | on, off, HR, MP | AUR | in-h | both | no | DPA | Y | Current |
| | GSV, GCG | C, pro | pro | off, MP | Y | in-h | FTC | no | DPA | Y | Current |
| | AVS | T | cont | on | Y | TP | DoT | BBB | BBB | no | Current |
| | OGS, OGM, CSF | HR, C | cont | on, off, HR, MP | NDL | in-H | both | no | DPA | Y | Current |
| | CSV, INF, CSF | C | cont | on | Y | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | CSV, INF | C, RH, pro | pro | on, off, HR | Y | in-h | both | no | DPA | Y | Current |
| | CSV, TRA | T, pro | pro | on | No | TP | FTC | N/A | TRUSTe | no | Current |
| | GSV, MCS, TRA | R RH | cont | on, off, HR | No | in-h | both | no | DPA | Y | Current |
| | CSV | C, pro | pro | on, off | NDL | in-h | FTC | DMA | DMAshp | no | Current |
| | APP, HCG, ARW | C RH | cont | on, off, HR | Y | in-h | both | no | DPA | Y | Current |
| | INF | C | cont | on, off | NDL | in-h | FTC | TRUSTe | TRUSTe | no | Not |
| | TRN, PRT, RRE | C, HR, RE | cont | HR | NDL | in-h | error | no | DPA | Y | Current |
| | APS, GIE, TRK | HR | cont | HR | No | in-h | error | no | DPA | Y | Current |
| | CSV, CSF, INF | C | cont | on | NDL | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | CSV, CSF | C, pro | pro | on | Y | in-h | FTC | ? | DPA | Y | Not |
| | INF, GSV, HCS | ? RH | cont | on, off, HR | No | TP | both | no | USERTRUST | Y | Current |
| | EDS, CSF, CSV | HR | cont | on, HR | NDL | TP | both | TRUSTe | TRUST, DPA | Y | Current |
| | MCS, ADV, GSV | RE | cont | on, off | Y | in-h | FTC | no | AAA | no | Current |
| | COL, ELP, FNS | HR | cont | HR | Intranet | in-h | error | N/A | DPA | Y | Current |
| | CSV | C, pro | pro | on, off | NDL | TP | FTC | DMAshp | DMA | no | Current |
| | DRG | ? | cont | on | PA | in-h | FTC | BBB | BBB | no | Current |
| | CSV | C, pro | pro | on, off | NDL | TP | FTC | no | DMA | no | Current |
| | EDS, INF, BOK | C RH | cont | on, off, HR, MP | Y | in-h | both | DMA | DPA | Y | Current |
| | BOK, EDS, CSF | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | INF | RE | cont | on | Y | in-h | FTC | CASRO, MRA, ESOMAR, TRUSTe | TRUSTe, DPA | Y | Current |
| | CSF, CSV | HR | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | MCS, ACE | HR | cont | on, off, HR, MP | Intranet | in-h | both | no | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | ADV, GSV | HR, C | cont | on, off, HR | Y | in-h | both | TRUSTe, DAMshp, AIM, Cre-m, NAI | DMA, TRUSTe | Y | Current |
| | CSF, CSV | RH | cont | off | P | in-h | FTC | no | DPA | Y | Current |
| | CSF, ADV, INF | C | cont | on, off | Y | in-h | FTC | DMA | DMA | N/A | Current |
| | ADV | C | cont | on, off | Y | in-h | FTC | DMA | DMA | no | Current |
| | CVS | HR | cont | on off, HR | PA | in-h | both | no | DPA | Y | Current |
| | ADV, TRN | C | cont | off | Y | in-h | FTC | no | DPA | Y | Current |
| | FNS,GSV,ACT | C | cont | on | NDL | TP | FTC | no | DPA | Y | Current |
| | ADV, CSF, INF | C | cont | on, off | NDL | in-h | FTC | DMA | DMA | no | Current |
| | ADV | C | cont | on, off, MP | NDL | in-h | FTC | DMAshp | DMAshp | N/A | Current |
| | INF | RE | cont | on | NDL | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | GSV | HR, C | cont | on, off | Y | TP | FTC | TRUSTe | TRUSTe | Y | Current |
| | EMP | RE | cont | on, off, MP | Y | in-h | FTC | no | BBB | no | Current |
| | PHT, CPT | C, HR, RE | cont | on, off, HR, MP | Y | in-h | both | BBB | BBB, DPA | Y | Current |
| | APS, ELC, GIR | HR | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | TES | HR | cont | HR | Intranet | in-h | error | N/A | DPA | Y | Current |
| | MED, DRG | HR | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | CSV | C | cont | on, HR | Y | TP | both | no | AAA | Y | Current |
| | CSF, TOY | C, RE | cont | on, HR | Y | TP | both | ESRBPOP | ESRBPOP | Y | Current |
| | GST, ICH, BTC | C | cont | on | No | in-h | FTC | BBB | BBB | Y | Current |
| | EDS, FNS | HR | cont | on, HR | Y | TP | both | TRUSTe | TRUST, DPA | Y | Current |
| | LES, TRN, AUT | C | cont | on | NDL | in-h | FTC | BBB | BBBOnL | Y | Current |
| | CSF, INF, EDS | C | cont | on | Y | in-h | FTC | no | Eftpeb | no | Current |
| | CSF | C | cont | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | ACT, EDS, GSV | C, HR | cont | on, off, HR, MP | Y | in-h | both | BBB | BBB | Y | Current |
| | CSF | C | cont | on | No | in-h | FTC | no | DPA | Y | Current |
| | CPT, CSF, CSV | HR | cont | off, HR, MP | Intranet | in-h | both | no | DPA | Y | Current |
| | CSF | HR | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | CSF, CSV, CST | C, RE | cont | on, off | Y | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | GSV, INF, MCS | HR | cont | on, off, HR, MP | NDL | in-h | both | N/A | DPA | Y | Current |
| | EIP, GST, LAB | HR | cont | HR | Y | in-h | error | no | DPA | Y | Current |
| | CSF, GSV | HR | cont | on, off, HR | Y | in-h | both | N/A | DPA | Y | Current |
| | CSV, INF | C | cont | on, off | Y | in-h | FTC | no | AAA | no | Current |
| | CSV, CSF, INF | HR | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | PVC | HR | cont | on, off, HR, MP | Intranet | in-h | both | no | DPA | Y | Current |
| | CSF | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | FOT, APP, SPT | HR | cont | HR | No | in-h | FTC | no | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | EDS, CSF | C | cont | on, off, MP | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSF, INF, MCS | RE (HR & C | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | MCS, GSV | HR | cont | on, off | Y | in-h | both | AAA | AAA | Y | Current |
| | CPT, CSV | HR, C | cont | on, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | CSV, TRA, INF | C, T, RH | cont | on, off, HR | Y | TP | both | TRUSTe | TRUSTe | Y | Current |
| | GSV, TOY | C | cont | on, off | No | in-h | FTC | no | DPA | Y | Current |
| | AUT, FNS, INS | C | cont | on, off | No | in-h | FTC | no | DPA | Y | Current |
| | GSV, CSV | RE RH | cont | on, HR, MP | No | in-h | both | no | DPA | Y | Current |
| | BTC, GST | RE, M | cont | on, MP | No | in-h | FTC | AABB | DPA | no | Current |
| | CSV, INF | pro | cont | on, off, MP | Y | in-h | FTC | DMA | DMA | no | Current |
| | MCS, CSV | pro | cont | on, off | Y | in-h | FTC | DMAshp | DMAshp | no | Current |
| | EMP | HR | cont | on, off, MP | AUR | in-h | both | no | DPA | Y | Current |
| | INF | RE | cont | on, off, MP | Y | in-h | FTC | no | JAMS | no | Current |
| | INF | H RH | cont | on, off, MP | Y | in-h | both | no | DPA | Y | Current |
| | HCS, MCS | C, M | cont | on, off, MP | Y | in-h | FTC | no | DPA | no | Current |
| | EDS, CPS | C, HR | cont | on, off, HR | Y | in-h | both | no | DPA | Y | Current |
| | CSF | C | cont | on, off, MP | NDL | in-h | FTC | no | DPA | Y | Current |
| | AIR | HR | cont | HR | PA | in-h | error | no | BBB | Y | Current |
| | GSV | RE | cont | on, off, MP | Y | in-h | FTC | TRUSTe | TRUSTe | Y | Current |
| | INF, CSF, CSV | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | INF, CSV, TOY | C RH | cont | on, HR, MP | NDL | in-h | error | no | DPA | Y | Current |
| | INF, CSV | C | cont | on, off, MP | Y | in-h | FTC | no | AAA | no | Current |
| | HCG, GFT, GCG | C | cont | on, off | Y | in-h | FTC | DMA | DMA | no | Current |
| | GSV | RE | cont | on, off, MP | NDL | in-h TI | FTC | TRUSTe | TRUSTe | Y | Current |
| | ADV, CSV, CSF | C | cont | on, off, MP | NDL | in-h | FTC | DMAshp | DMAshp | Y | Current |
| | ICH | HR | cont | HR | Intranet | in-h | error | N/A | DPA | Y | Current |
| | APP, TXF | C | cont | on, off, MP | NDL | in-h | FTC | DMA | DPA | Y | Current |
| | HCS | C, M | cont | on, off | Y | in-h TI | FTC | HON | DPA | no | Current |
| | CPT, CEL, CSF | C, HR | cont | on, off, HR, MP | Y | in-h | both | BBB | BBB, DPA | Y | Current |
| | CSV, TRA, INF | T, RH | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | EMP | HR | cont | HR | Y | in-h | error | TRUSTe | DPA | Y | Current |
| | CSV, EMP | HR | cont | HR | No | in-h | error | SSN | DPA | Y | Current |
| | CSF, CSV | HR | cont | on, off, HR | NDL | in-h | both | no | DPA | Y | Current |
| | CSF, INF | HR | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | INF, CSV | HR | cont | HR | Intranet, | in-h | error | EPON, EPOF, IAPO, SHRM, CLSR | DPA | Y | Current |
| | DRG, BTC | HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | AUV, CPT, CEL | C, HR | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | INF | C | cont | on, HR | NDL | in-h | both | no | no | Y | Current |
| | EDS, INF, EMP | HR | cont | on, HR | NDL | in-h TI | both | TRUSTe | TRUSTe | Y | Current |
| | GSV | RE | cont | on | Y | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | ACE | HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | INF | C, T, RH | cont | off, HR, MP | No | in-h | both | no | CFO, DPA | Y | Current |
| | EDS, CSV | HR | cont | on, HR | Y | in-h | both | no | DPA | Y | Not |
| | CPT, CSF, CEL | C, HR | cont | on, off, HR, MP | Y | in-h | both | BBB | BBB, DPA | Y | Current |
| | INF, GST, BTC | C | cont | off, MP | NDL | in-h | FTC | no | DPA | Y | Current |
| | MCS, INF | HR | cont | on, off, HR, MP | AUR | in-h | both | no | DPA | Y | Current |
| | ACE, ELP, REQ | HR | cont | HR, MP | Intranet | in-h | both | no | DPA | Y | Not |
| | CSF, CSV, ACE | C, RH | cont | on, off, HR, MP | Y | in-h | both | NAITA | TRUST, DPA | Y | Current |
| | CSV, CPT, CSF | C, RE | cont | on | NDL | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | INF, CSV, CSF | C, RH | cont | on | No | in-h | both | no | DPA | Y | Current |
| | CSV, INF | C, RE | cont | on | No | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | INF, MCS | C, HR, RE | cont | on, off | Y | in-h | both | N/A | AAA | Y | Current |
| | EDS | RE | cont | off | NDL | in-h | FTC | N/A | DPA | Y | Current |
| | CSV, ADV | C | pro | on, off, MP | No | in-h | FTC | DMAshp | DMAshp | no | Not |
| | APS, ELP, PCI | C, HR | cont | on, off, HR, MP | No | in-h | both | no | DPA | Y | Current |
| | INF | C | cont | on | Y | in-h | FTC | no | BBB | no | Current |
| | CVS, INF | C, RE | cont | both | NDL | in-h | both | no | AAA | no | Current |
| | EMP | C, HR | cont | on, off, HR | NDL | in-h | both | no | DPA | Y | Current |
| | CSV, INF, EMP | C, HR, RE | cont | on, off, HR | NDL | in-h | both | no | DPA | Y | Current |
| | ACT, CSV, INF | HR | cont | on, off, HR, MP | No | in-h | both | no | DPA | Y | Current |
| | GSV | C | cont | off | No | in-h | FTC | N/A | DPA | Y | Not |
| | GSV | , | cont | on, off | No | in-h | FTC | no | CASRO | no | Current |
| | EMP, INF | C, RE | cont | on, off, HR, MP | No | in-h | both | no | TRUSTe, DPA | Y | Not |
| | EMP | C, RE | cont | on, off | Y | in-h | FTC | no | BBB | no | Current |
| | CSV, INF | C | cont | on, off | NDL | in-h | FTC | no | DMA | no | Current |
| | TES, CSV, CSF | C, HR | cont | on, off, HR, MP | Y | in-h | both | PAB, TPC | DPA | Y | Current |
| | CSF, CSV | C, HR | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | CPT, CEL | C, RH | cont | on, HR | Y | in-h | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | MCS, EDS | HR | cont | on, off, HR, MP | Y | TP | both | no | BBB, DPA | Y | Current |
| | INF, EDS, CSV | C | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | CSF | C, RH | cont | on, off, HR, MP | Y | TP | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | MCS, EDS | C, RE | cont | on off | No | in-h | FTC | no | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | GSV | RE | cont | on, off, MP | Y | in-h | FTC | CASRO | DPA | Y | Current |
| | INF, ADV, TEL | RE | cont | on, off | Y | in-h | FTC | CASRO, MRA | DPA | Y | Current |
| | TRA | C | cont | on, off | Y | in-h | FTC | no | DMA | no | Current |
| | TRA | C | cont | on, off | Y | in-h | FTC | no | DMA | no | Current |
| | CSV | C | cont | on | No | in-h | FTC | no | DPA | Y | Current |
| | CSV, TES | C | cont | on, off, MP | AUR | in-h | FTC | no | DPA | Y | Current |
| | DRG, CSF | C, HR | cont | on, HR | NDL | TP | both | PAB, IOPO, EPON | DPA | Y | Current |
| | HCS | C | cont | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | GSV | RE, RH | cont | on, off, MP | Y | in-h | both | CASRO | DPA | Y | Not |
| | DRG | RE | cont | on, off, MP | NDL | in-h | FTC | no | DPA | Y | Current |
| | DRG, BTC | C, HR, RE | cont | on, off, HR, MP | Y | in-h | both | No | DPA | Y | Current |
| | CSF | C, RH | cont | on, off, MP | NDL | in-h | both | no | DPA | Y | Current |
| | ADV, HCS, INF | C, RE | cont | on, off, MP | NDL | in-h | FTC | DMAgui, HIPPA, COPPA | DMA | no | Current |
| | CSF, INF | C, HR | cont | on, off, HR, MP | Y | in-h TI | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | EMP, CSV, CSF | HR, RE | cont | on, off, HR, MP | No | in-h | both | no | DPA | Y | Current |
| | GSV | RE | cont | on, off | NDL | in-h | FTC | CASRO, ESOMAR, MRA | DPA | Y | Current |
| | FNS | C, RH | cont | on, MP | NDL | in-h | both | no | AAA | Y | Current |
| | DRG, BTC, MED | C, RH | cont | on, HR, MP | No | TP | both | TRUSTe | TRUSTe | Y | Current |
| | BTC, GST, PCI | C, RE, RH | cont | off, MP | Y | in-h | both | no | DPA | Y | Current |
| | AIR, ELC | HR | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | CSV | C, RH | cont | on | NDL | in-h | both | no | DPA | Y | Not |
| | MCS | RE | cont | on, off, MP | Y | in-h | FTC | CASRO | DPA | Y | Current |
| | TRA | HR, T | cont | on, off, MP | Y | in-h | both | no | DPA | Y | Current |
| | CSV | C | cont | on, off, MP | Y | in-h | FTC | no | DPA | Y | Current |
| | CSV | C, pro | pro | on | Y | in-h | FTC | no | DPA | Y | Current |
| | EDF, CSV | C, HR | cont | on, off, HR | NDL | TP | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | ADV, CSV, CSF | RE, RH | cont | on, off, HR | NDL | in-h | both | DMAshp | DMAshp, DPA | Y | Current |
| | INF, MCS, CSV | RE | cont | on | NDL | in-h | FTC | no | DPA | no | Current |
| | TES | C, RH | cont | on | No | in-h | both | no | DPA | Y | Current |
| | GSV | RE | cont | on, off, MP | No | in-h | FTC | CASRO | DPA | Y | Current |
| | GSV | RE | cont | on, off, MP | Y | in-h | FTC | CASRO | DPA | Y | Current |
| | GSV | RE | cont | on, off, MP | No | in-h | FTC | CASRO | DPA | Y | Current |
| | DFN, AIR, ELC | C, HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | CSF, CSV, EDS | C, RH | cont | on, off, MP | NDL | in-h | both | no | BBB, DPA | Y | Current |
| | ELC, CSF | HR | cont | on, HR | Intranet | in-h | both | no | DPA | Y | Current |
| | GCG, GSV | C, HR | cont | on, HR | Y | in-h | both | BBB | BBB, DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | DRG | C, HR | cont | on, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | INF | C, HR | cont | HR | Y | in-h | both | no | DPA | Y | Current |
| | ADV | C, RH | cont | on, MP | Y | in-h | both | no | DPA | Y | Current |
| | CSF | C | cont | on | PA | in-h | FTC | HIPPA | DPA | Y | Current |
| | CSF, INF | C, HR | cont | on, HR | Y | TP | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | INF, HCS | C | cont | on, off | NDL | in-h | FTC | no | DPA | Y | Current |
| | DRG | RE, HR | cont | HR | Intranet | in-h | both | no | DPA | Y | Current |
| | MCS | C, HR | cont | HR | No | in-h | both | no | DPA | Y | Current |
| | GSV, MCS, TRA | C, RH | cont | on, off, HR | No | in-h | both | no | DPA | Y | Current |
| | CSF, CSV | C, HR | cont | on, HR | NDL | in-h | both | no | DPA | Y | Current |
| | CSV | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | GCG | C, RH | cont | on, off, HR, MP | NDL | in-h | both | DMA, DPA for HR | DMA, DPA | Y | Not |
| | GCG | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | CSV | C, HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | DRG | HR, RE | cont | on, off, MP | Y | in-h | both | no | DPA | Y | Current |
| | DRG | HR | cont | HR | NDL | in-h | error | IAPO | DPA | Y | Current |
| | DRG | C, HR | cont | on, off, HR, MP | NDL | In-h | both | no | DPA | Y | Current |
| | TES | C | cont | on | NDL | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | CSF, CSV | C | cont | on, off, MP | NDL | in-h | FTC | no | BBB | no | Current |
| | ICH | C, HR | cont | on, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | CSV, CSF, TES | C, HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | ADV, CSV, CSF | C | cont | on, off | NDL | in-h | FTC | BBB, NAI, OPA | BBB, NAI, OPA | Y | Current |
| | APS, BLD, ICH | HR | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | GCG, HCG, CRM | C | cont | on, off, HR, MP | Y | in-h | both | no | DPA | no | Not |
| | DFN, ACE, GSV | RE, HR | cont | HR | NDL | in-h TI | both | ASISP, PIMC | DPA | Y | Current |
| | TRN, INF, MCS | T, RH | cont | off, HR | NDL | in-h | both | no | DPA | Y | Current |
| | BOK | C, HR | cont | on, off, HR, MP | NDL | in-h | both | no | AAA | Y | Current |
| | EMP | HR | cont | on, off, HR | Y | in-h | both | no | DPA | Y | Current |
| | GSV | HR | cont | on, HR | NDL | in-h | both | no | DPA | Y | Not |
| | COS, DRG, HCG | C, HR, RE | cont | on off, HR | Y | in-h | both | DMA, BBB | DMA | Y | Current |
| | CVS | C, HR, pro | pro | on, off | Y | in-h | both | no | BBB | no | Current |
| | INF | HR | cont | on, off, HR | No | in-h | both | no | DPA | Y | Current |
| | BOK, GCG | C | cont | off, MP | NDL | in-h | FTC | DMAshp | DMAshp | no | Current |
| | CSF, CSV, CPT | HR pro | pro | on, HR | Y | in-h | both | no | DPA | Y | Current |
| | DFN, AIR, ELC | HR | cont | HR | No | in-h | both | N/A | DPA | Y | Current |
| | CSF, CSV, INF | C | cont | on | Y | in-h | FTC | DMA | DMAshp | no | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | CSV, CSF | C, RE | cont | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSV, TES | C | cont | on | NDL | in-h | FTC | no | AAA | no | Current |
| | INF, FNS, CSV | C, pro | pro | on off, MP | NDL | in-h | FTC | no | DPA | no | Current |
| | MED, HCS, CSF | C, RE, RH | cont | on, off | Y | in-h | both | P3P, CNIL member, HON | DPA | Y | Current |
| | PMR, GST | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | EMP, GSV | C, HR | cont | on, off, HR | NDL | TP | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | CSV, | C, HR, RE | cont | on, HR | Y | TP | both | no | DPA | Y | Current |
| | CSV, INF | C, RH | cont | on, HR | NDL | in-h | both | TRUSTe | TRUSTe | Y | Current |
| | FNS, INF, CSV | RE, pro | pro | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSV | ? Pro | pro | on, off | Y | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | CSV, ACT, INF | C, HR | cont | on, HR, MP | No | in-h | both | no | DPA | Y | Current |
| | GCG | HR | cont | on, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | GSV | C, RE | cont | on, off, MP | Y | in-h | FTC | CASRO | DPA | Y | Current |
| | ACE, AUT, MTL | HR | cont | on, off, HR | NDL | in-h | both | no | DPA | Y | Current |
| | CSV | C, RH | cont | on, HR | NDL | TP | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | TEL, CPT, GIE | HR | cont | HR | Y | in-h | error | no | DPA | Y | Current |
| | CSF, CSV | RE, pro | pro | on | Y | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | CSV, INF | ? Pro | pro | on, MP | Y | in-h | FTC | DMA Privacy Promise | DMA Privacy Promise | Y | Current |
| | HCS | RE | cont | on, off | No | in-h | FTC | no | DPA | Y | Current |
| | BOK | C | cont | on, off, MP | NDL | in-h | FTC | DMA | DMAshp | no | Current |
| | CPT, ELC, CSF | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | BOK | C | cont | on | NDL | in-h | FTC | no | DPA | no | Not |
| | AIR, ELP, ICH | HR | cont | on, HR, MP | PA | in-h | both | no | DPA | Y | Current |
| | CSV, CSF, INF | RE | cont | on, off, MP | No | in-h TI | FTC | TRUSTe | TRUSTe | Y | Current |
| | MCS | HR | cont | on, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | HCS, CSF, INF | RE, pro | pro | on, off | No | in-h | FTC | no | DPA | Y | Current |
| | CSF, CSV, INF | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | CSV, CSF, INF | C | cont | on, off, MP | Y | TP | FTC | TRUSTe, CAUCE, DMACfRe-mail | TRUSTe | Y | Current |
| | TRA | C, T | cont | on, off, MP | Y | in-h | FTC | no | DPA | Y | Current |
| | GSV | RE, HR | cont | HR | NDL | in-h | both | no | DPA | Y | Current |
| | GSV, GSF, INF | C | cont | on, off, MP | Y | in-h TI | FTC | TRUSTe | TRUSTe | no | Current |
| | GSV, CSV | C, pro | pro | on, off, MP | NDL | in-h | FTC | no | DPA | Y | Current |
| | APS, AIR | HR, pro | pro | HR | No | in-h | error | no | DPA | Y | Current |
| | CSF | C | cont | on, MP | NDL | in-h | FTC | DMA | DPA | Y | Current |
| | MED, HCS, CSF | HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | HCS | C | cont | on | No | in-h | FTC | no | AAA | no | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | BUS, CEL | C | cont | on, off, HR, MP | NDL | in-h | both | no | JAMS, DPA | Y | Current |
| | CPT, ELC, CSV | C, HR | cont | on, off, HR, MP | Intranet | in-h | both | no | DPA | Y | Current |
| | ARW, BOK, FLM | C | cont | on | Y | in-h | FTC | no | DPA | Y | Current |
| | GSV | RE | cont | on off, MP | Y | in-h | FTC | CASRO | DPA | Y | Current |
| | INF, CSV, CSF | C, pro | pro | on, off, HR | Y | in-h | both | no | DPA | Y | Current |
| | ADV, INF | RE | cont | on | NDL | in-h | FTC | UKTPS | AAA | no | Current |
| | CSF, CSV, EDS | C, HR | cont | on, off, HR | Y | TP | both | TRUSTe | DPA | Y | Current |
| | CSF | C | cont | on, MP | Y | in-h | FTC | no | DPA | Y | Not |
| | INF, CSV, EIP | C | cont | on | No | in-h TI | FTC | no | DPA | Y | Not |
| | GSV | HR | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | ADV | C, HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | AIR, FNS, GIE | HR | cont | HR | Y | in-h | error | no | DPA | Y | Current |
| | EMP | HR | cont | on | Y | in-h | FTC | no | DPA | Y | Not |
| | INS | C | cont | on, off | contract | in-h | FTC | no | TRUSTe | no | Current |
| | CSV | pro | pro | MP | NDL | in-h | FTC | no | DMA | no | Current |
| | ADV | C | cont | on | No | in-h | FTC | no | DPA | Y | Current |
| | INF | C | cont | on, off, MP | No | in-h | FTC | BBB | BBB | no | Current |
| | BTC, INF | RE | cont | on, off, MP | NDL | in-h | FTC | CFR, BR, DHHR | DPA | Y | Current |
| | EDS, HCS | RE | cont | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | GSV, ACT | C | cont | on | Y | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | CGC, FOD | C | cont | on, off, MP | NDL | in-h | FTC | no | AAA | no | Current |
| | INF | RE | cont | on, MP | Y | in-h | FTC | no | DPA | Y | Current |
| | INF, GSV, HCS | ? pro | pro | on, off, HR | No | in-h | both | no | USERTRUST, DPA | Y | Current |
| | INF | C | cont | on | Y | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | LAB, INF, GST | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | CSF | C | cont | on, off, HR, MP | Y | in-h | both | no | DPA | Y | Current |
| | BOK | C, pro | pro | on, off | , | in-h | FTC | DMAshp | DMAshp | no | Not |
| | CSV, INF | C | cont | on | NDL | in-h | FTC | TRUSTe | TRUSTe | no | Current |
| | INF, MCS | C | cont | on | Y | in-h | FTC | KPMG, CIDE, CSPSTI | AAA | no | Current |
| | TRA, INS | T | cont | on, off, MP | Y | in-h | FTC | no | DPA | Y | Current |
| | INF | C | cont | on, off | Y | in-h | FTC | BBB | BBBOnL | no | Current |
| | CSV, INF | C | cont | on off | Y | in-h | FTC | no | Eftpeb | no | Current |
| | APS | HR | cont | on, off, HR | Intranet | in-h | both | no | DPA | Y | Current |
| | CSV, TRA | C | cont | on, off, HR | PA | in-h | both | no | DPA | Y | Current |
| | TRA | C, T pro | pro | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSV, TRA | C, T | cont | on, off, HR, MP | AUR | in-h | both | no | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | HCG, COS, FOD | HR | cont | HR | Y | in-h | error | no | DPA | Y | Current |
| | INF, GSV, HCS | ? pro RH | pro | on, off, HR | NDL | TP | both | no | DPA | Y | Current |
| | INF, GSV, HCS | ? | cont | on, off, HR | NDL | TP | both | no | DPA | Y | Current |
| | CSV, CSF | Cn HR, pro | pro | on, HR | NDL | in-h | both | OPA | DPA | Y | Current |
| | EIP, GST, OGS | C, HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | CSV, CSF, AGC | C, pro | pro | on, off, MP | Y | in-h | FTC | no | DPA | Y | Current |
| | FNS, MED, INS | C RH | cont | HR, MP | AUR | in-h | both | no | DPA | Y | Current |
| | ADV | C | cont | on | Y | in-h | FTC | BBB, NAI, OPA | BBB, NAI, OPA | no | Current |
| | MED | C | cont | on | NDL | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | BOK | C | cont | on, off, MP | Y | in-h | FTC | no | BBB | no | Current |
| | OGS | HR | cont | on, off, HR, MP | NDL | in-h | both | no | DPA | Y | Current |
| | GFT, APP, ARW | C | cont | on, off, MP | Y | in-h | FTC | BBB | BBBOnL | no | Current |
| | ELC, BTC | C, HR, RE | cont | on, HR, MP | No | in-h | both | no | DPA | Y | Current |
| | ADV, CSF | C | cont | on | Y | in-h | FTC | TRUSTe, CAUCE | no | Y | Current |
| | ADV, CSF, INF | C, pro | pro | on, off | Y | in-h | FTC | no | DPA | Y | Current |
| | TRA | C | cont | on, off | No | in-h | FTC | no | DMA | no | Current |
| | CSF, CSV | HR | cont | HR | PA | in-h | error | no | DPA | Y | Current |
| | CSV | C, RH | cont | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSF, CSV, GSV | C | cont | on | NDL | in-h TI | FTC | TRUSTe | TRUSTe | no | Current |
| | CSF, INF | C, RE, pro | pro | on, off, MP | NDL | in-h TI | FTC | no | DPA | Y | Current |
| | CSF, CSV | ? | cont | on | Y | in-h TI | FTC | TRUSTe | TRUSTe | no | Current |
| | GSV | RE RH | cont | on, off, HR | Y | TP | both | TRUSTe | TRUSTe | Y | Current |
| | ACT | HR | cont | HR | NDL | in-h | both | DoC | OR | Y | Current |
| | EDS, CSV | C RH | cont | on | Y | in-h | both | TRUSTe | TRUSTe | Y | Current |
| | HCS | C RH, M | cont | on, off, HR | Y | in-h | both | TRUSTe | TRUSTe, DPA | Y | Current |
| | INV, FNS | HR | cont | HR | NDL | in-h | error | no | DPA | Y | Current |
| | GSV | HR | cont | HR, MP | NDL | in-h | error | no | DPA | Y | Current |
| | CON, PAP, PUL | HR | cont | HR | N | in-h | error | GHEI | DPA | Y | Current |
| | EDS, MCS, EMP | C | cont | on | NDL | in-h | FTC | BBB | BBB | no | Current |
| | TES, EDS | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | CSV | C | cont | on | No | TP | FTC | TRUSTe | TRUSTe | no | Not |
| | GCG, FOD | HR | cont | on, off, HR, MP | PA | in-h | both | no | DPA | Y | Current |
| | ADV | C | cont | on, off | NDL | in-h | FTC | no | DMA | no | Current |
| | GSV | RE | cont | on, off, MP | Y | in-h | FTC | no | DPA | Y | Not |
| | TRA | T | cont | on, off, HR | NDL | in-h | FTC | no | WWTS, DPA | Y | Not |
| | TRA | T | cont | on, off, MP | NDL | in-h | FTC | no | DPA | Y | Current |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | GSV, TXP, DRG | HR | cont | HR | Intranet | in-h | error | no | DPA | Y | Current |
| | TRA | HR, T | cont | on, off, HR | AUR | in-h | both | no | DPA | Y | Current |
| | ADV | C, RH | cont | on, HR | NDL | in-h | both | no | DPA | Y | Not |
| | CSV, INF | C, pro | pro | on, off, MP | No | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | INF | C, pro | pro | on, off, MP | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSF, FNS | C, pro | pro | on | Y | in-h | FTC | TRUSTe | TRUSTe | Y | Current |
| | MUS | C | cont | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSV, TES, CSF | C | cont | on | NDL | in-h | FTC | no | DPA | Y | Current |
| | CSV | C | cont | on | Y | TP | FTC | TRUSTe | TRUSTe | no | Current |
| | CSF, CSV | C | cont | on | Y | TP | FTC | BBB | BBB | no | Current |

**Cellule:** B1

**Commentaire:**

Industry Sector:
ACE: Architectural/Construction/Eng Svc
ACR: Air Conditioning & Refrigeration Eq.
ACT: Accounting Services
ADV: Advertising Services
AGC: Agricultural Chemicals
AGM: Agricultural Machinery & Equipment
AIR: Aircraft and Parts
APP: Apparel
APS: Automotive Parts & Service Equipment
ARW: Artwork
AUT: Automoviles & Light Trucks/vans
AUV: Audio/Visual Equipment
AVS: Aviation Services
BOK: Books & Periodicals
BTC: Biotechnology
BUS: Business Equipment (other than computers)
CEL: Consumer Electronics
COL: Coal
CON: Construction Equipment
COS: Cosmetics & Toiletries
CPT: Computer & Peripherals
CRM: Ceramics Fine Advanced
CSF: Computer Software
CSV: Computer Services
DFN: Defense Industry Equipment
DRG: Drugs and Pharmaceuticals
EDS: Education and Training
EIP: Electronic Industry Prod/Test
ELC: Electronic Components
ELP: Electrical Power Systems
EMP: Employment Services
FLM: Films Videos & Other Recording
FNS: Financial Services
FOD: Foods Processed

FOT: Footwear
GCG: General Consumer Goods
GFT: Giftware
GIE: General Industrial Equipment & Supplies
GST: General Science and Technology
GSV: General Services
HCG: Hosehold Consumer Goods
HCS: Health Care Services
ICH: Industrial Chemicals
INF: Information Services
INS: Insurance Services
INV: Investment Services
LAB: Laboratory Scientific Instruments

**Cellule:** I7
**Commentaire:** HON: Healthcare on the Net
and TRUSTe's privacy guidelines

**Cellule:** I15
**Commentaire:** BBBOnLine Privacy Seal Program

**Cellule:** I18
**Commentaire:** CASRO: Council of American Survey Research Organizations

**Cellule:** C20
**Commentaire:** The following note is included in the item "Personal information received from the EU": "Not applicable. We do not process personal information.
Data we work with relates to real state, including location, physical property attributes, and sales prices".

**Cellule:** I21
**Commentaire:** AAA: American Arbitration Association

**Cellule:** I51
**Commentaire:** Special International BNI Task Force for Data Privacy Issues

**Cellule:** I54
**Commentaire:** Greater Boston Chamber of Commerce

**Cellule:** I63
**Commentaire:** DMA Safe Harbour Program, TRUSTe

**Cellule:** C64
**Commentaire:** Assistance with insurance related disputes.

**Cellule:** C93
**Commentaire:** Not clear what is the data received

**Cellule:** I102
**Commentaire:** CASRO, Marketing Reasearch Association, ESOMAR (?), and TRUSTe

**Cellule:** I105
**Commentaire:** TRUSTe, DMA SHP, Association ofr Interactive Marketing Council for Responsinle E-mail, NAI's E-mail Service Provide Coalitin

**Cellule:** I122
**Commentaire:** Entertainment Software Ratings Board Privacy Online Program

**Cellule:** J126
**Commentaire:** "Exception for third party enforcement body".

**Cellule:** I149
**Commentaire:** American Association of Blood Banks (AABB). The DNA accreditation committee in charge of immigration and naturalization.

**Cellule:** C150
**Commentaire:** They do not specify what kind of data they process

**Cellule:** J153
**Commentaire:** Judicial Arbitration and Mediation Service

**Cellule:** I155
**Commentaire:** They said they are working on meeting HIPPA regulations.

**Cellule:** I172
**Commentaire:** Part of the Secure Site Network certified by Verisign, Inc., a licensee of the TRUSTe Privacy Program.

**Cellule:** I175
**Commentaire:** 1)European Privacy Officers Network
2)European Privacy Officers Forum
3)IAPO
4)Society for Human Resources Management
5)Center for Legal and Social Responsibility

**Cellule:** I188
**Commentaire:** North Alabama International Trade Association

**Cellule:** C202
**Commentaire:**
They represent the following: "X does not currently receive personal information from the EU, it has no activities with respect to such information"

**Cellule:** I206
**Commentaire:** Privacy and American Business; The Privacy Council

**Cellule:** I214
**Commentaire:** CASRO & MRA (Marketing Research Association)

**Cellule:** I219
**Commentaire:** Privacy & American Business, International Organization of Privacy Officers, EPON

**Cellule:** I225
**Commentaire:** DMA

**Cellule:** I228
**Commentaire:** CASRO, ESOMAR, MRA

**Cellule:** I264
**Commentaire:** IAPP International Association of Privacy Officers

**Cellule:** I270
**Commentaire:** TRUSTe  Privacy Bot

**Cellule:** I273
**Commentaire:** American Society for Insdustrial Security's Privacy and Personal Information Management Council

**Cellule:** I288
**Commentaire:** "We comply with the P3P… CNIL Member. We registered our privacy policy to the Commission Nationale de l'Informatique et des Libertés. HON Member. We comply with the HON Code of Conduct…"

**Cellule:** I312
**Commentaire:** TRUSTe, CAUCE, and the Direct Marketing Association Council for Responsible E-mail

**Cellule:** I326
**Commentaire:** Montly UK TPS TPS file subscription

**Cellule:** C335
**Commentaire:** Name, address and charitable donation history from a response handling company in the United Kingdom is transmitted to the US and stored as a data base by client.

**Cellule:** I338
**Commentaire:** The Code of Federal Regulations, The Belmont Report, The Department of Health and Human Services Federalwide Assurance Protection for Human Subjects

**Cellule:** I349
**Commentaire:**
Recipient of KPMG Security Seal as a result of regulatory scheduled security audits; member of Chemical Industry Data Exchange (CIDX) Cyber Security Practices, Standards & Technology Initiative

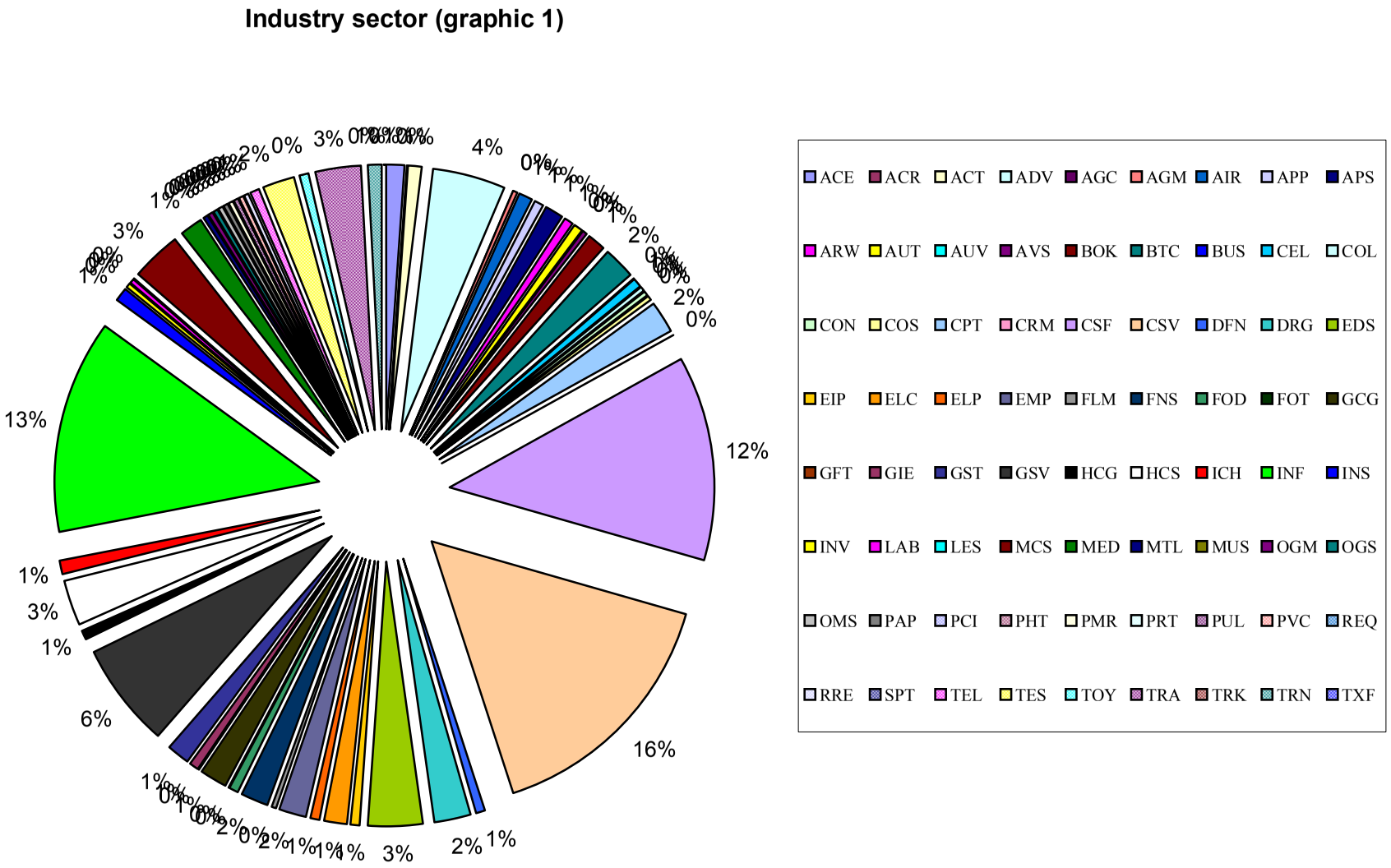
**Cellule:** I360
**Commentaire:** Online Privacy Alliance

**Cellule:** I379
**Commentaire:**
US Department of Commerce Safe Harbour Program

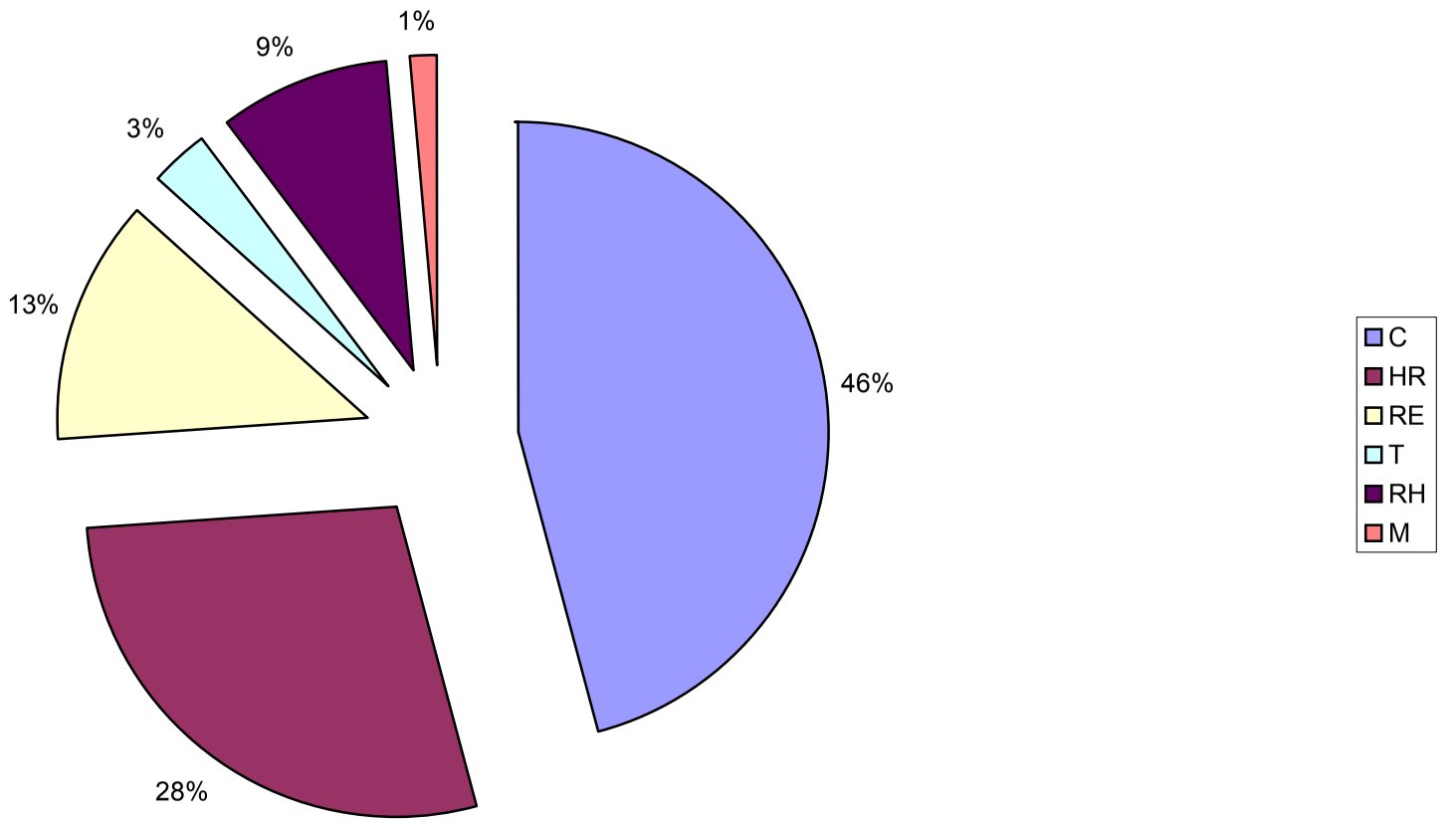
**Cellule:** J379
**Commentaire:** On-Line resolution www.onlineresolution.com

**Cellule:** I384
**Commentaire:** Guidelines for Handling Employee Information.

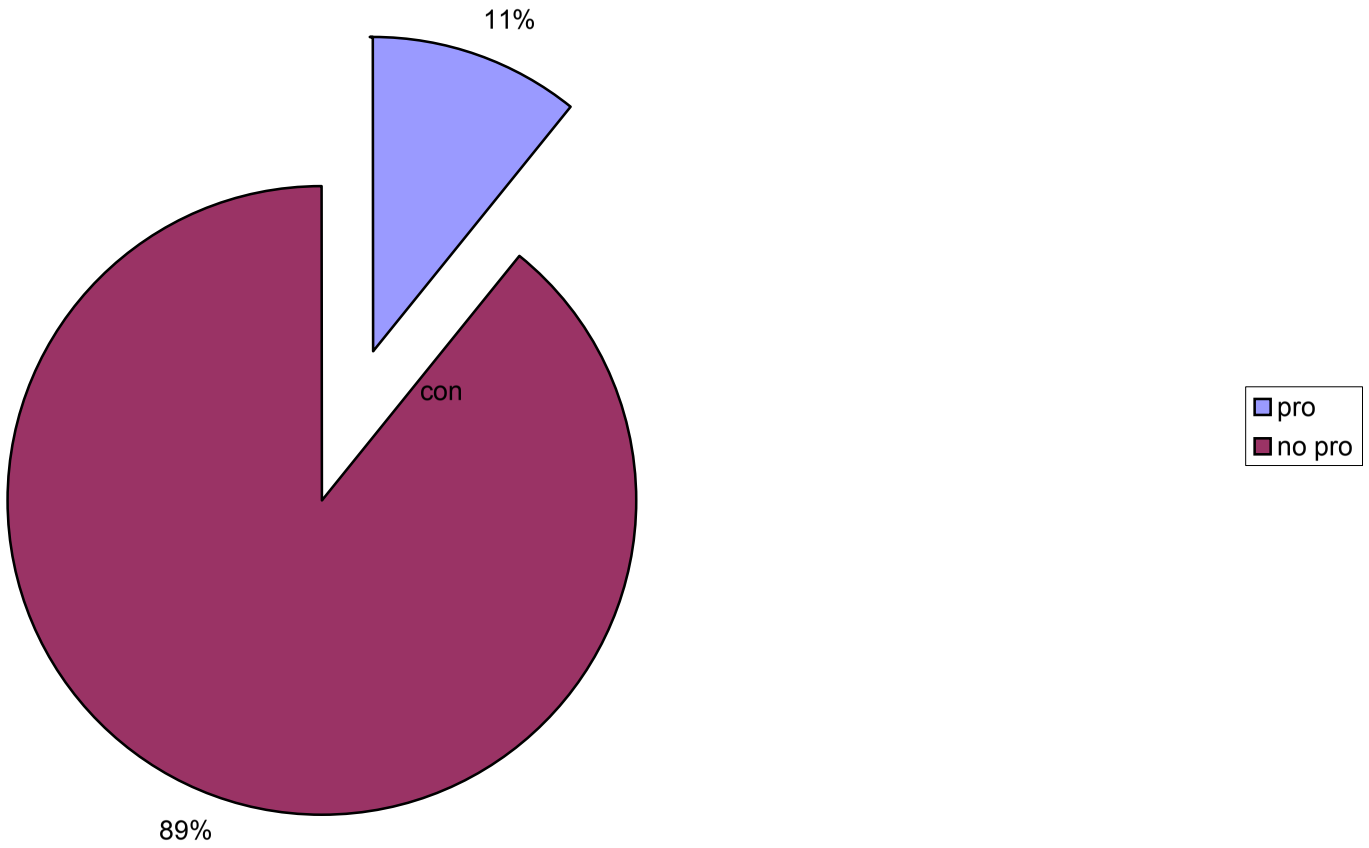
**Cellule:** J391
**Commentaire:** Safe Harbour Team at World Wide Travel Service


Industry sector (graphic 1)
4%
2%
0%
12%
16%
2%
1%
3%
1%
1%
2%
6%
1%
3%
1%
13%
3%
1%
2%
0%
3%
ACE ACR ACT ADV AGC AGM AIR APP APS
ARW AUT AUV AVS BOK BTC BUS CEL COL
CON COS CPT CRM CSF CSV DFN DRG EDS
EIP ELC ELP EMP FLM FNS FOD FOT GCG
GFT GIE GST GSV HCG HCS ICH INF INS
INV LAB LES MCS MED MTL MUS OGM OGS
OMS PAP PCI PHT PMR PRT PUL PVC REQ
RRE SPT TEL TES TOY TRA TRK TRN TXF

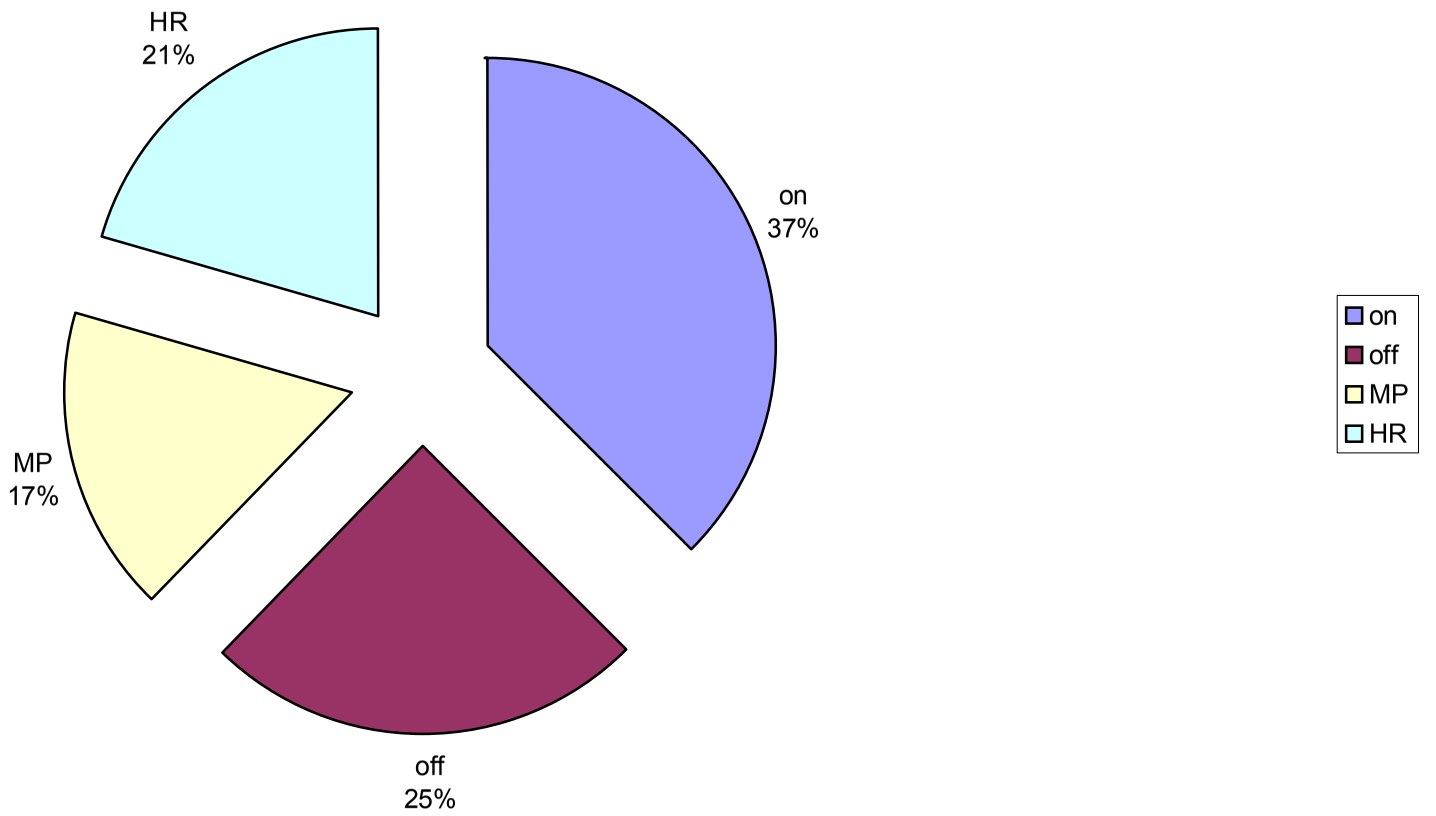
**Data type (graphic 2)**



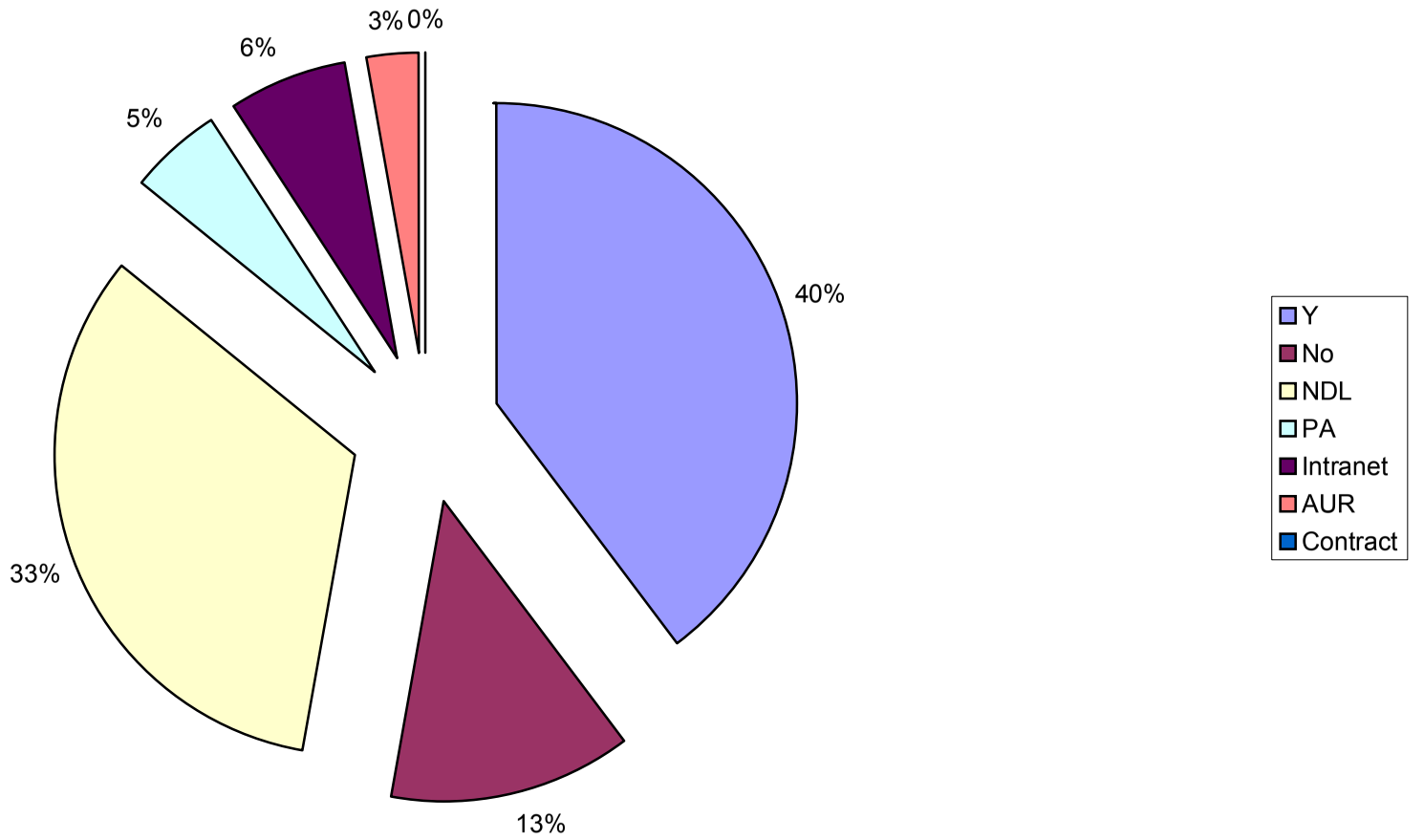
**Processor / Contoller (graphic 3)**



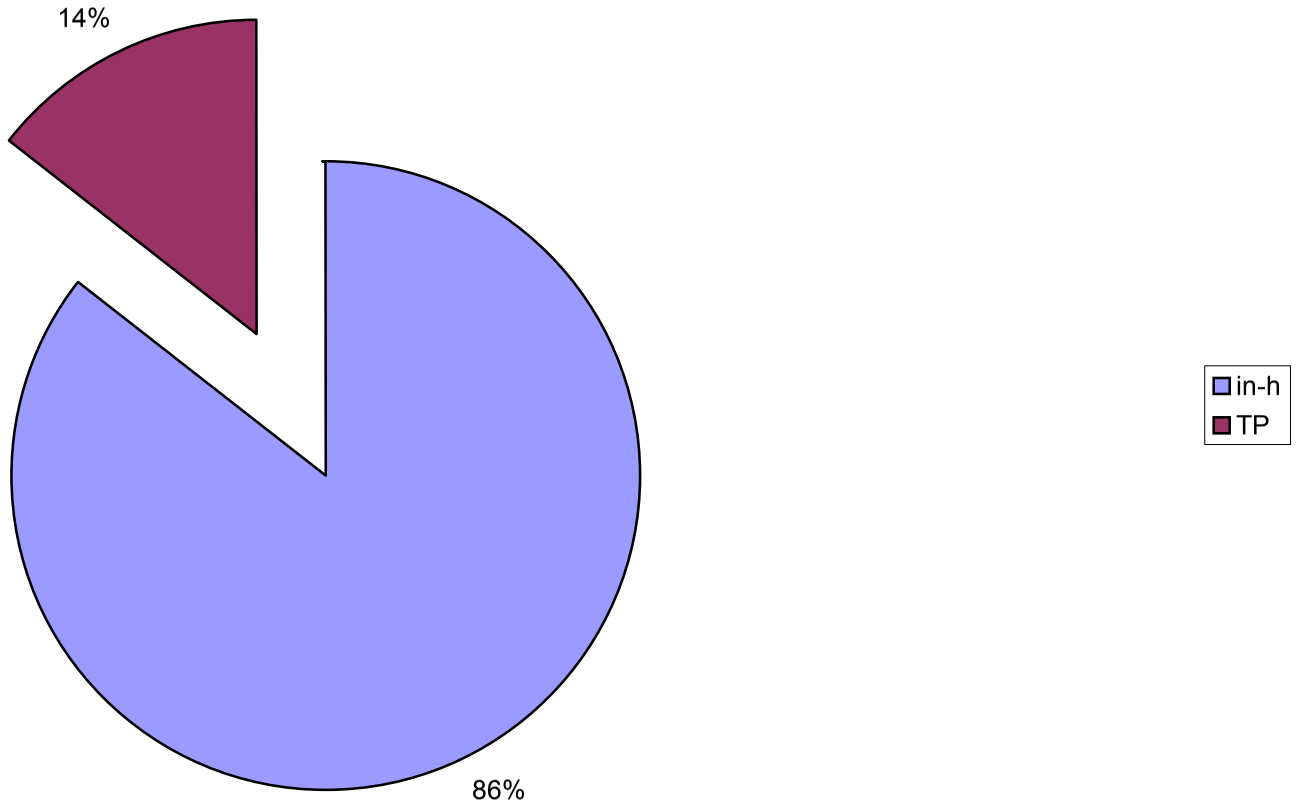
**Personal Data Covered (graphic 4)**



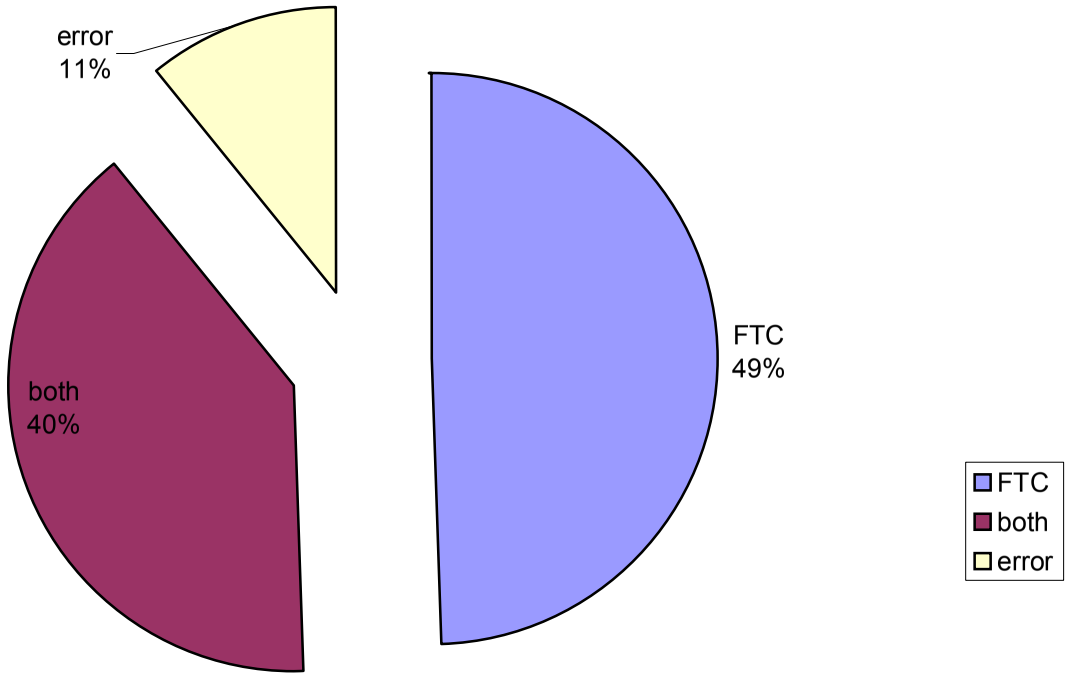
## Accurate Location (graphic 5)



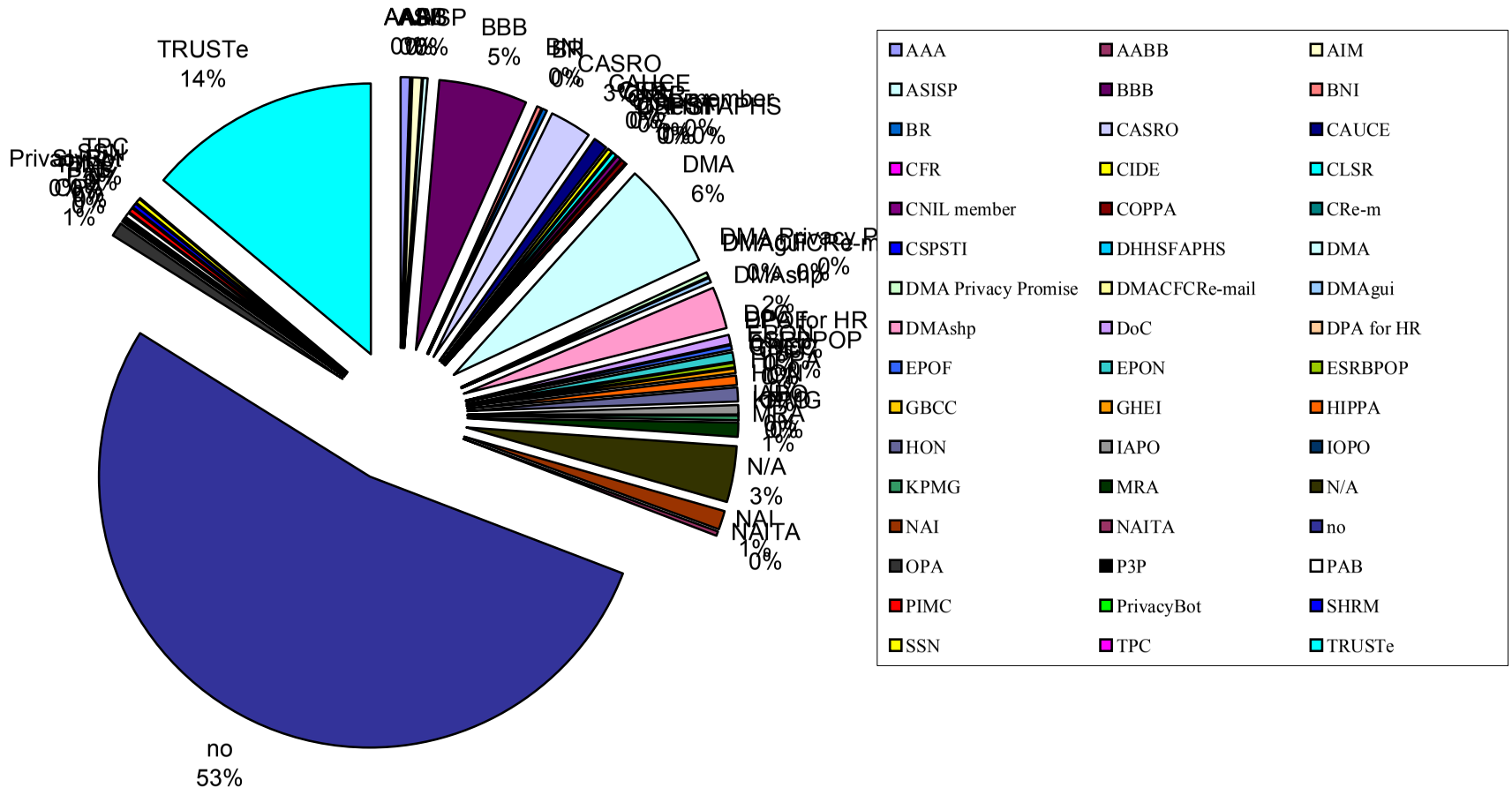
**Verification (graphic 6)**



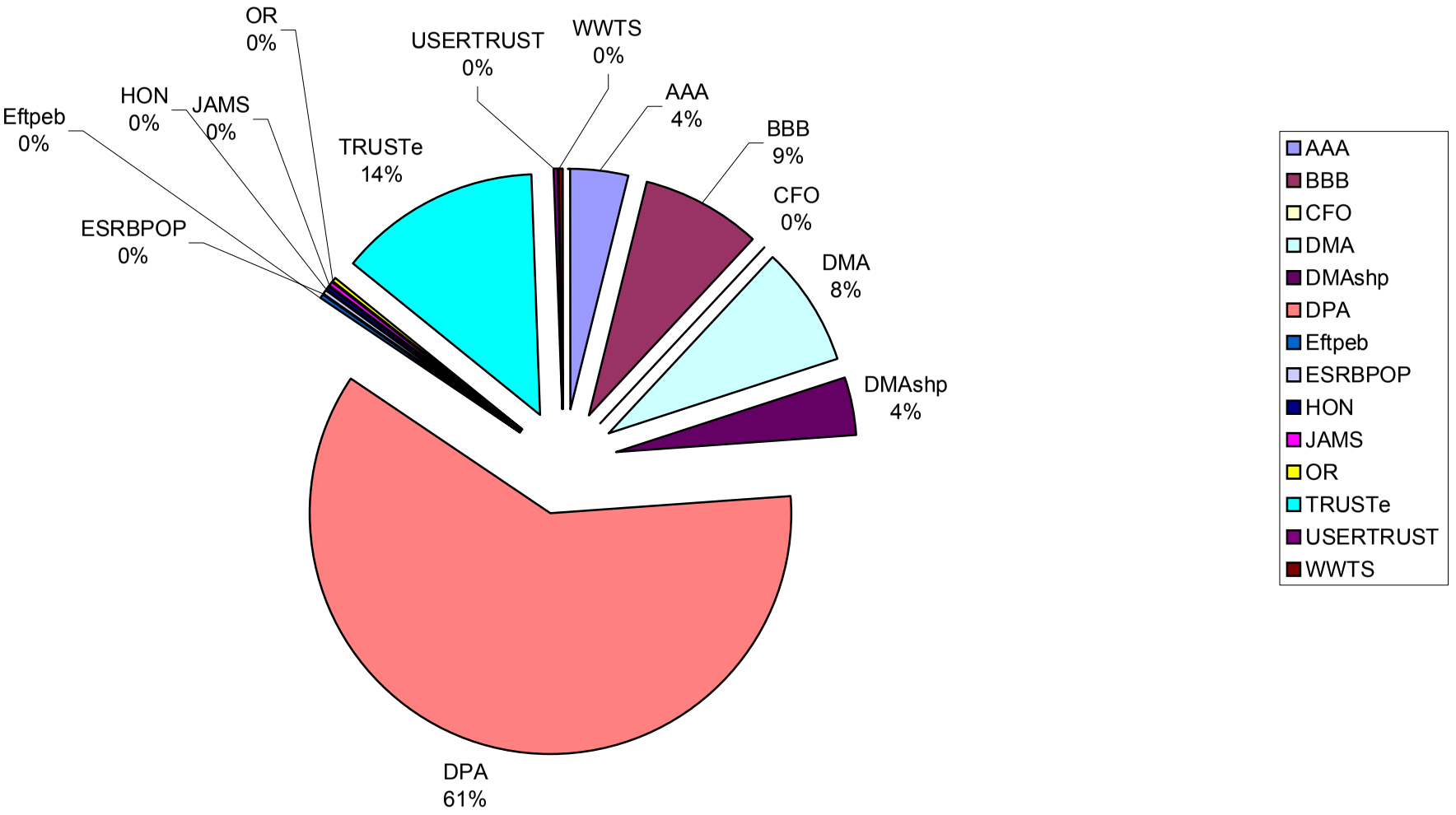
**Regulated by (graphic 7)**



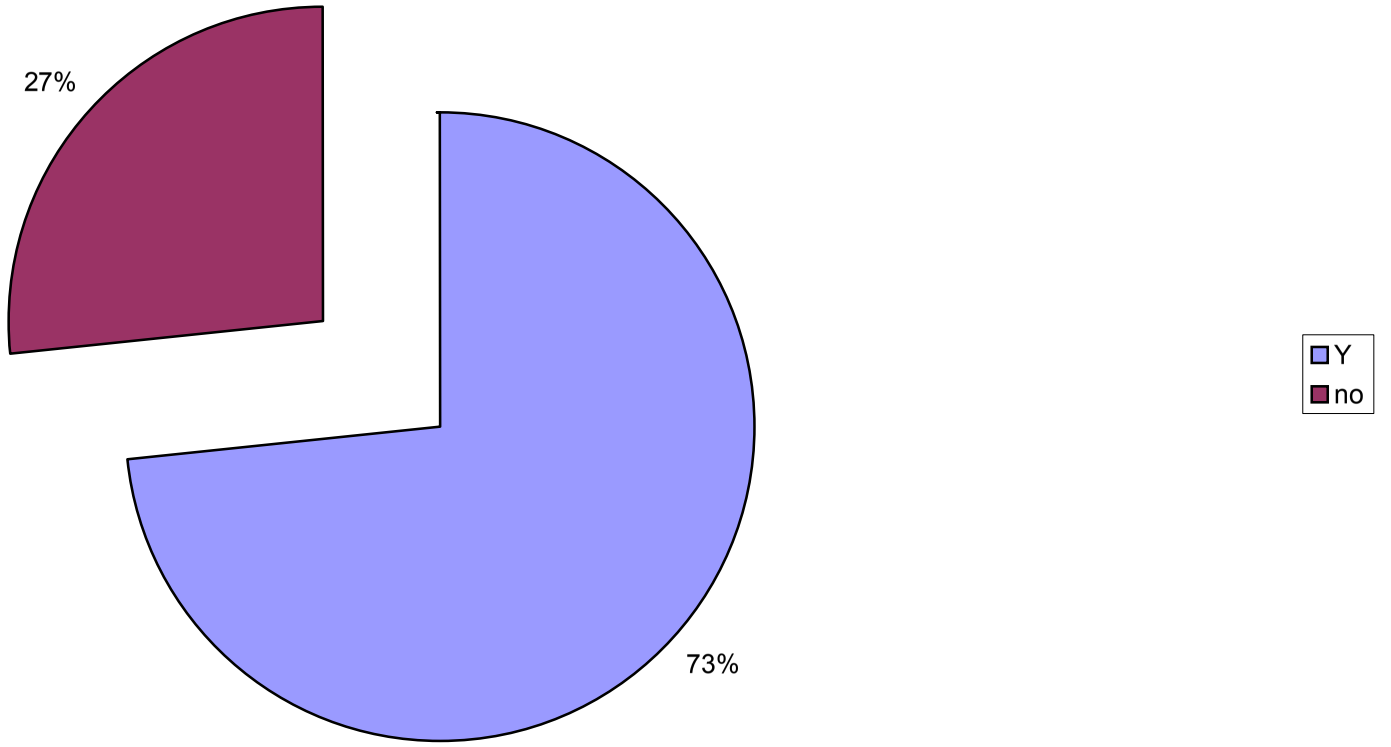
## Personal Data Covered (graphic 8)



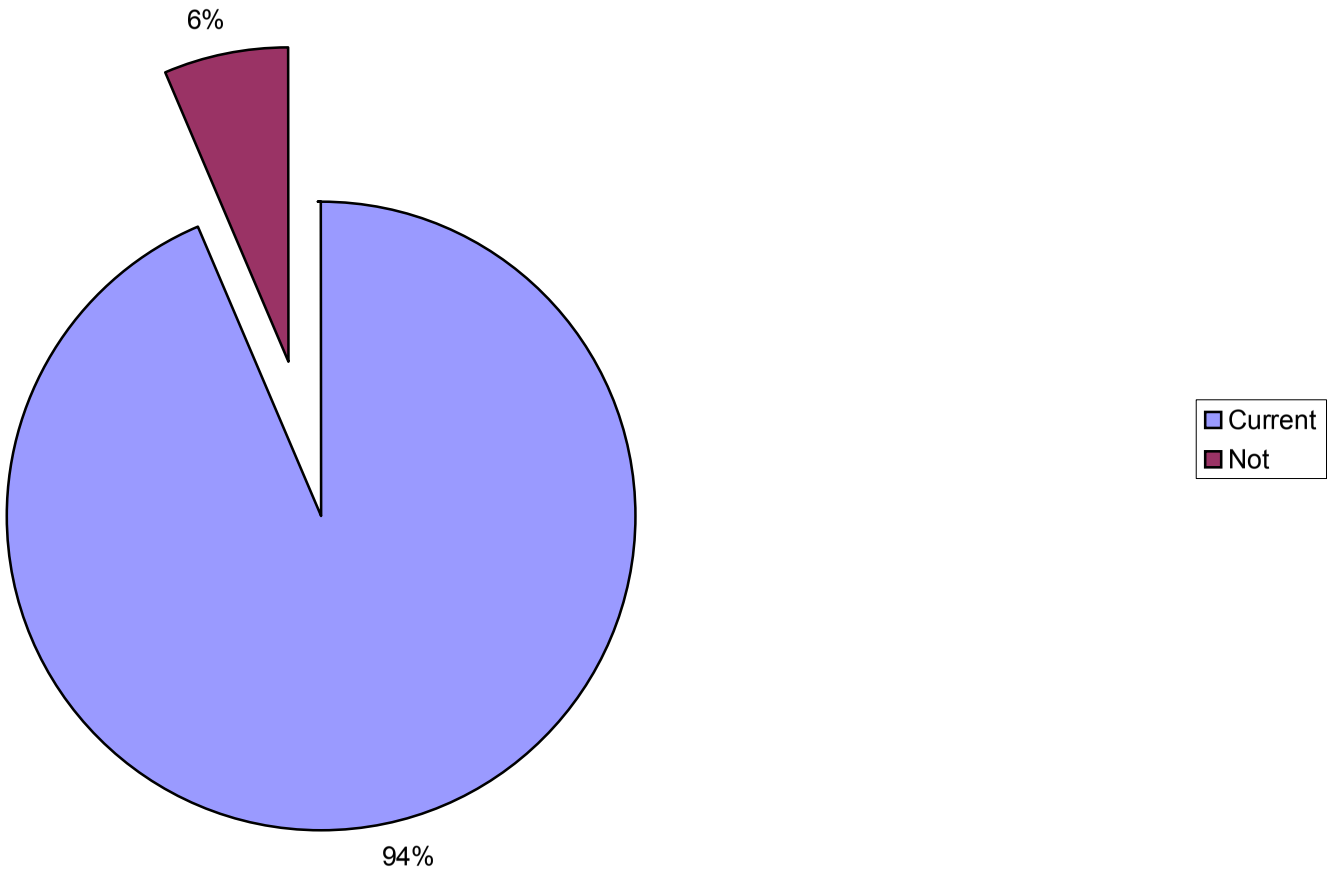
## Dispute Resolution (graphic 9)



**Cooperation DPA (graphic 10)**



**Certification (graphic 11)**



## APPENDIX VI – Data Tables and Graphics of Point 3.1 (Visible compliance/implementation)

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table 1.1: SH Company Eligibility for Safe Harbor (as of November 3, 2003)** | | | | | | | | |
| 2 | *Company* | | *Public Disclosure of Privacy Policy* | *Printable Policy* | *Jurisdiction (FTC/DOT)* | *Coverage* | *Policy Applies to EU Data Indefinitely* | *Policy Signals US Law Preventing Compliance* | *Cont / pro* |
| 3 | 1 | | yes | yes | FTC | Limited no HR | no | no | controller |
| 4 | 2 | | Intranet | unknown | error | Limited - HR | Unknown | Unknown | controller |
| 5 | 3 | | yes | yes | FTC | Limited no HR | no | no | cont/ proc |
| 6 | 4 | | no | unknown | FTC | Limited | Unknown | Unknown | processor |
| 7 | 5 | | Intranet | unknown | error | Limited - HR | Unknown | Unknown | controller |
| 8 | 6 | | yes | yes | FTC | Limited no HR | yes | no | controller |
| 9 | 7 | | yes/no | yes/no | FTC, error | Limited, no off | unknown | unknown | cont/ proc |
| 10 | 8 | | Physical address | unknown | FTC | Limited no HR/on | unknown | unknown | processor |
| 11 | 9 | | yes/no | yes/no | FTC, error | Unlimited | yes | no | controller |
| 12 | 10 | | yes | yes | FTC | Limited - on | no | no | controller |
| 13 | 11 | | yes | yes | FTC | Limited - on | yes | no | controller |
| 14 | 12 | | yes | yes | FTC | Limited - on | no | no | controller |
| 15 | 13 | | yes/no | yes/no | FTC & error | Limited - HR/on | no | no | controller |
| 16 | 14 | | yes/no | yes/no | FTC, error | Unlimited | no | no | controller |
| 17 | 15 | | yes/no | yes/no | FTC | Limited no HR | no | no | controller |
| 18 | 16 | | yes | yes | FTC | Limited no HR | yes | no | processor |
| 19 | 17 | | yes | yes | FTC & error | Limited no off | no | no | controller |
| 20 | 18 | | no | unknown | FTC & error | Limited - HR | Unknown | Unknown | controller |
| 21 | 19 | | Intranet | yes | FTC & error | unclear | no | no | controller |
| 22 | 20 | | yes | yes | FTC | Limited no HR | no | no | controller |
| 23 | 21 | | no | unknown | FTC | Limited no HR | unknown | unknown | processor |
| 24 | 22 | | yes/no | yes/no | FTC, error | Unlimited | no | no | controller |
| 25 | 23 | | no | no | FTC | Limited no HR | no | no | controller |
| 26 | 24 | | yes | yes | FTC | Limited no HR | no | no | controller |
| 27 | 25 | | no | unknown | FTC | Limited no HR | unknown | unknown | controller |
| 28 | 26 | | yes/no | yes/no | FTC, error | Unlimited | no | no | controller |
| 29 | 27 | | Intranet | yes | error | Limited - HR | no | no | controller |
| 30 | 28 | | phsysical address | unknown | error | Limited - HR | unknown | unknown | controller |
| 31 | 29 | | no | unknown | FTC | Limited no HR | unknown | no | controller |
| 32 | 30 | | yes | yes | error | Limited - HR | no | no | controller |
| 33 | 31 | | yes | yes | error | Limited - HR | no | no | controller |
| 34 | 32 | | Intranet | unknown | FTC | Limited - no HR | unknown | unknown | processor |
| 35 | 33 | | yes | yes | FTC | Limited - no HR | yes | no | processor |
| 36 | 34 | | physical address | yes | error | Limited - HR | yes | no | controller |
| 37 | 35 | | yes | yes | FTC | Limited - no HR | no | no | controller |
| 38 | 36 | | yes | yes | FTC | Limited - no HR | no | no | controller |
| 39 | 37 | | yes | yes | FTC, error | Unlimited | yes | no | processor |
| 40 | 38 | | yes | yes | FTC | Limited - no HR | no | no | controller |
| 41 | 39 | | yes | yes | error | Limited - HR | no | no | controller |
| 42 | 40 | | yes | yes | FTC | Limited - no HR | yes | no | controller |
| 43 | 41 | | yes | yes | FTC | Limited - no HR | no | no | controller |

**Cellule:** C2
**Commentaire:** Recital 5; Art. 2(a). If a policy is not publicly disclosed, there is not likely to be any basis for a deceptive practice that would trigger the FTC's jurisdiction.

**Cellule:** D2
**Commentaire:** This is necessary for data subjects, data exporters and DPAs to be able to evaluate a privacy policy at a specific moment in time.

**Cellule:** E2
**Commentaire:** SH Art. 1(2)(b). For the FTC to have jurisdiction, a company must publicly post a privacy policy.

**Cellule:** F2
**Commentaire:** Organizations may subscribe to the Safe Harbor for the treatment of all their EU-origin data or for only some of their EU-origin data.

**Cellule:** G2
**Commentaire:** FAQ 6 states that "the undertaking to adhere to the SH Principles is not time-limited …. [the] undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them , even if it subsequently leaves SH."

**Cellule:** G3
**Commentaire:** The company reserves the right to change the policy

**Cellule:** C4
**Commentaire:**
The privacy Policy covers data collected in the operation of the website, but the personal data covered, as declared in the self-certification formulaire, is only HR data

**Cellule:** D4
**Commentaire:** The privacy Policy covers data collected in the operation of the website, but the personal data covered, as declared in the self-certification formulaire, is only HR data

**Cellule:** E4
**Commentaire:** Error in certification letter, the FTC has no jurisdiction over HR data,

**Cellule:** H5
**Commentaire:** only a general statement concerning disclosure to law enforcement.

**Cellule:** D7
**Commentaire:** Through the homepage it is possible to access to a privacy policy that covers data collected on the Internet, but not HR data

**Cellule:** C9
**Commentaire:**

Yes: the Privacy Policy describes the company as only processor,and they made representations concerning the data they receive as processors.
No: however, in the certification page they represent to cover also HR data, and they do not mention where the privacy policy for HR data is available, they do not publicly disclosed it's location.
In this privacy policy a double analysis should be made. One concerning the processor transfer,where all the SH principles, except the security one should be answered as "not applicable"; and a second one concerning HR data where, considering that we don't have access to the privacy policy all the answers should be "unknown".
However, the company will be scored "unknown" where relevant because the SH concerns, in general, obligations for data controllers.

**Cellule:** C10
**Commentaire:**
Corp. Ofc. Also available via e-mail

**Cellule:** C11
**Commentaire:**
The privacy Policy covers data collected in the operation of the website, but the personal data covered, as declared in the self-certification formulaire, is also HR data, off-line and manually processed.
The analysis is made on the printed privacy policy.

**Cellule:** C16
**Commentaire:**
on-off-MP and HR, however the policy covers only on-line data

**Cellule:** C17
**Commentaire:**
on-off-manually processed. However, the policy covers only on-line data

**Cellule:** C21
**Commentaire:**
The company was contacted in order to ask for the privacy policy since the link given is of an Intranet. The policy reveived by e-mail does not only cover HR data but also consumer's data, so, the availability on an Intranet is not enough.

**Cellule:** F21
**Commentaire:** "personal data covered: all personal data"? Then, the description of the information received from the EU is not clear

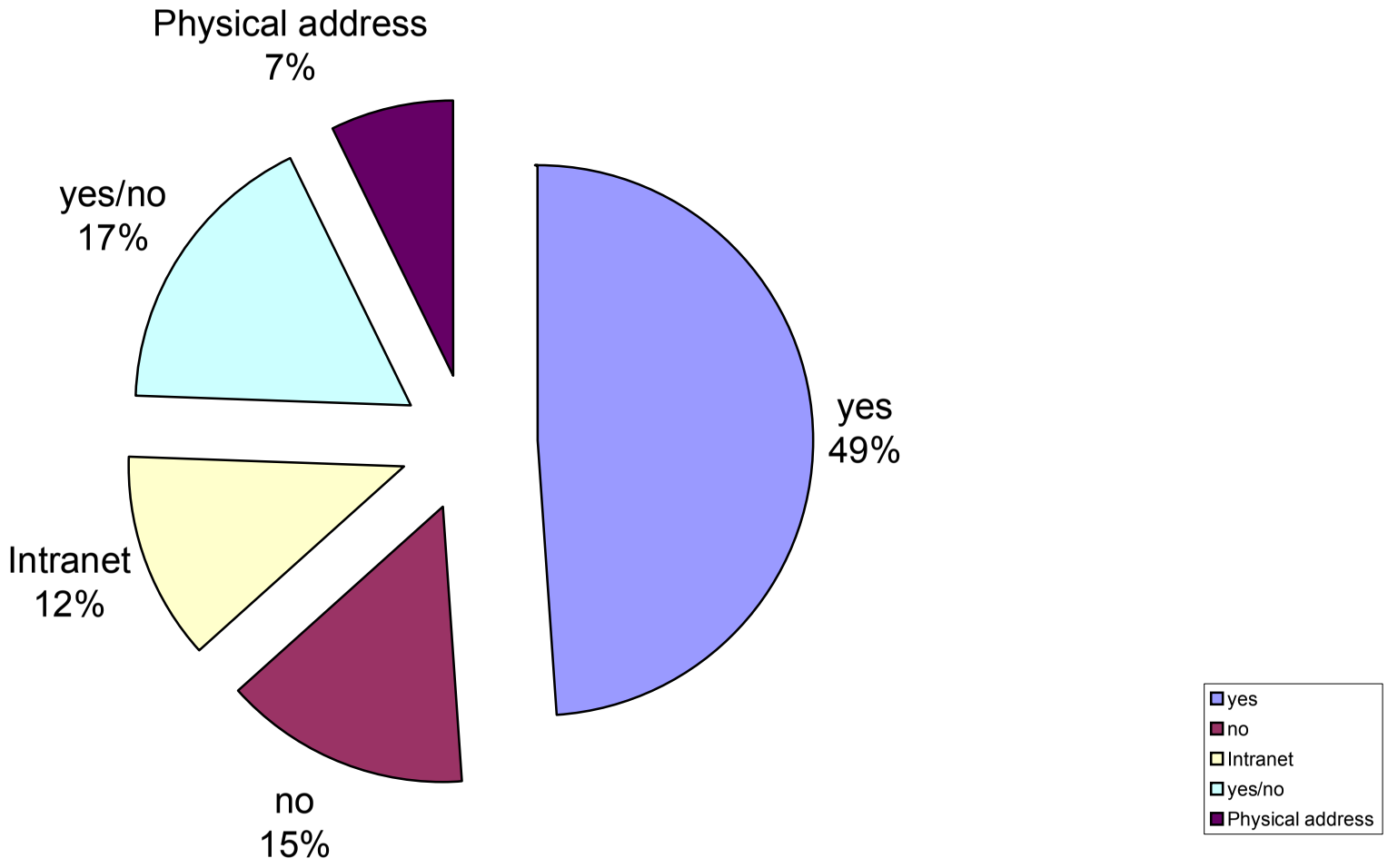
**Cellule:** C24
**Commentaire:** The policy only covers on-line collected data, but the cetification page represents to import also manually processed and human resources data

**Cellule:** C31
**Commentaire:** Certification page says off-line and manually pocessed data, while publicly available policy concerns on-line data.

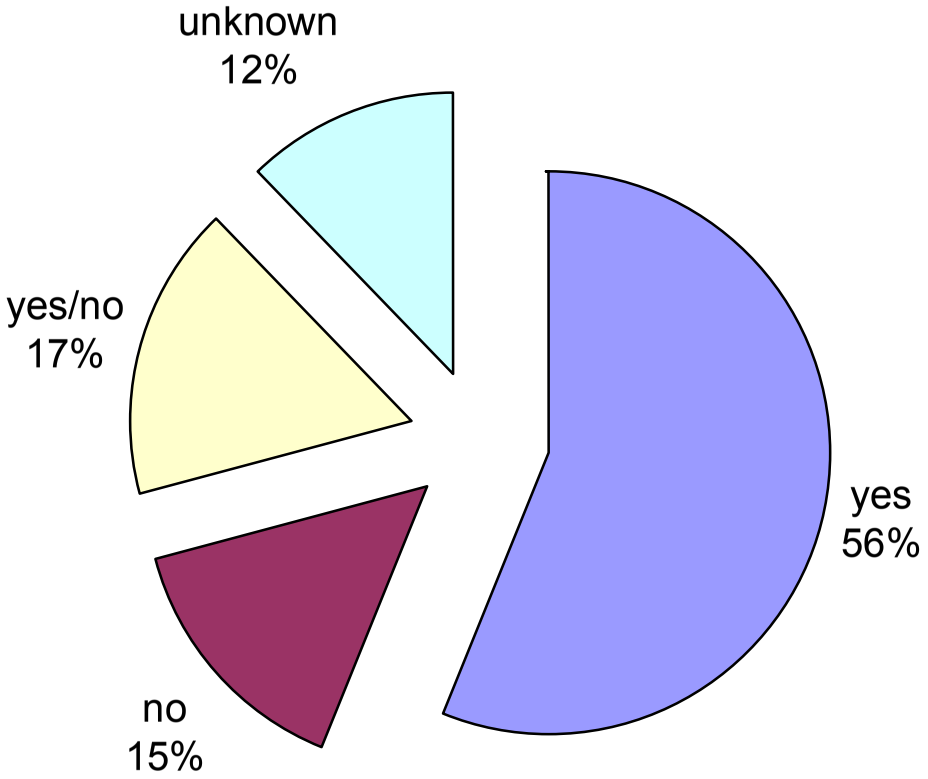
**Cellule:** F35
**Commentaire:** neither the certification page, nor the security policy specify this, we only know that (the company) processes data for health care services purposes

**Cellule:** C36
**Commentaire:** physical address (contact organization)

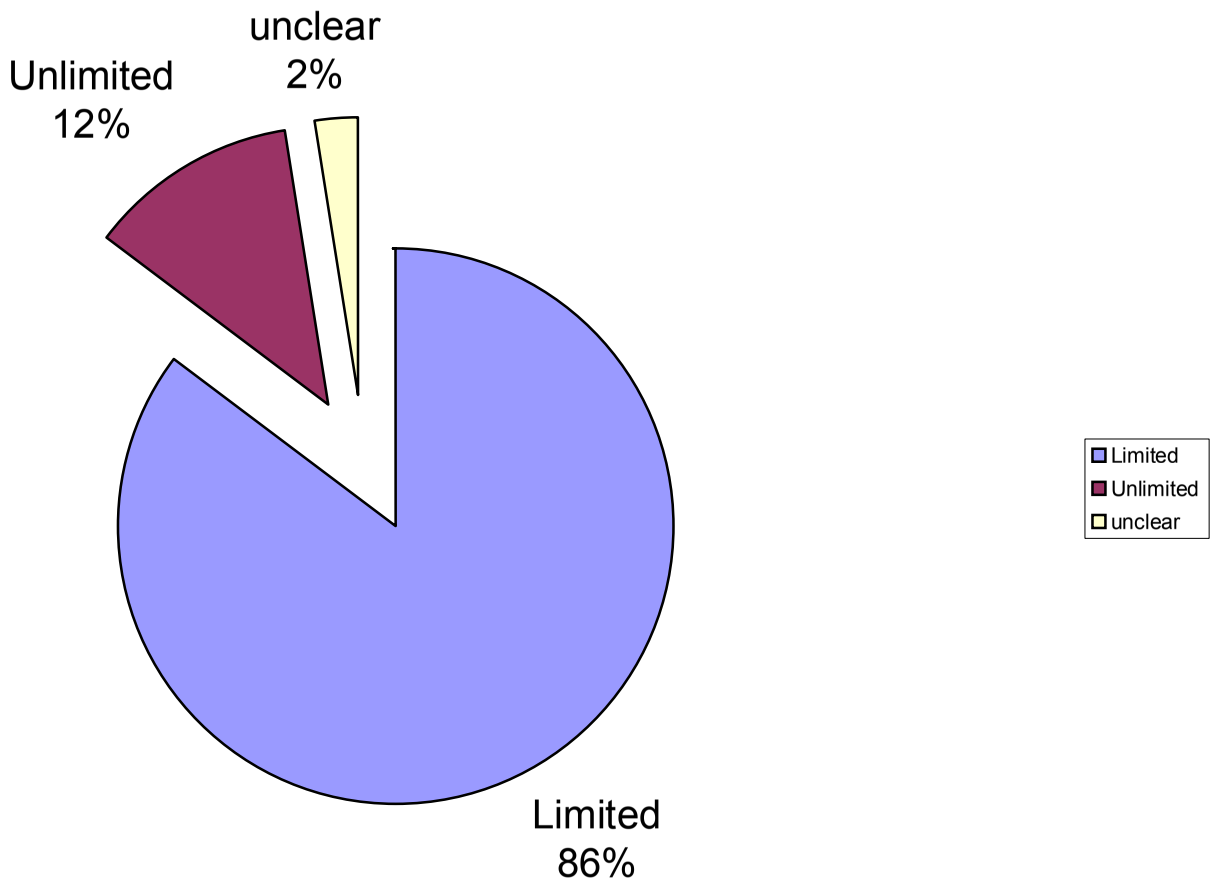
## Public Disclosure of Privacy Policy (Table 1.1, graphic 1)



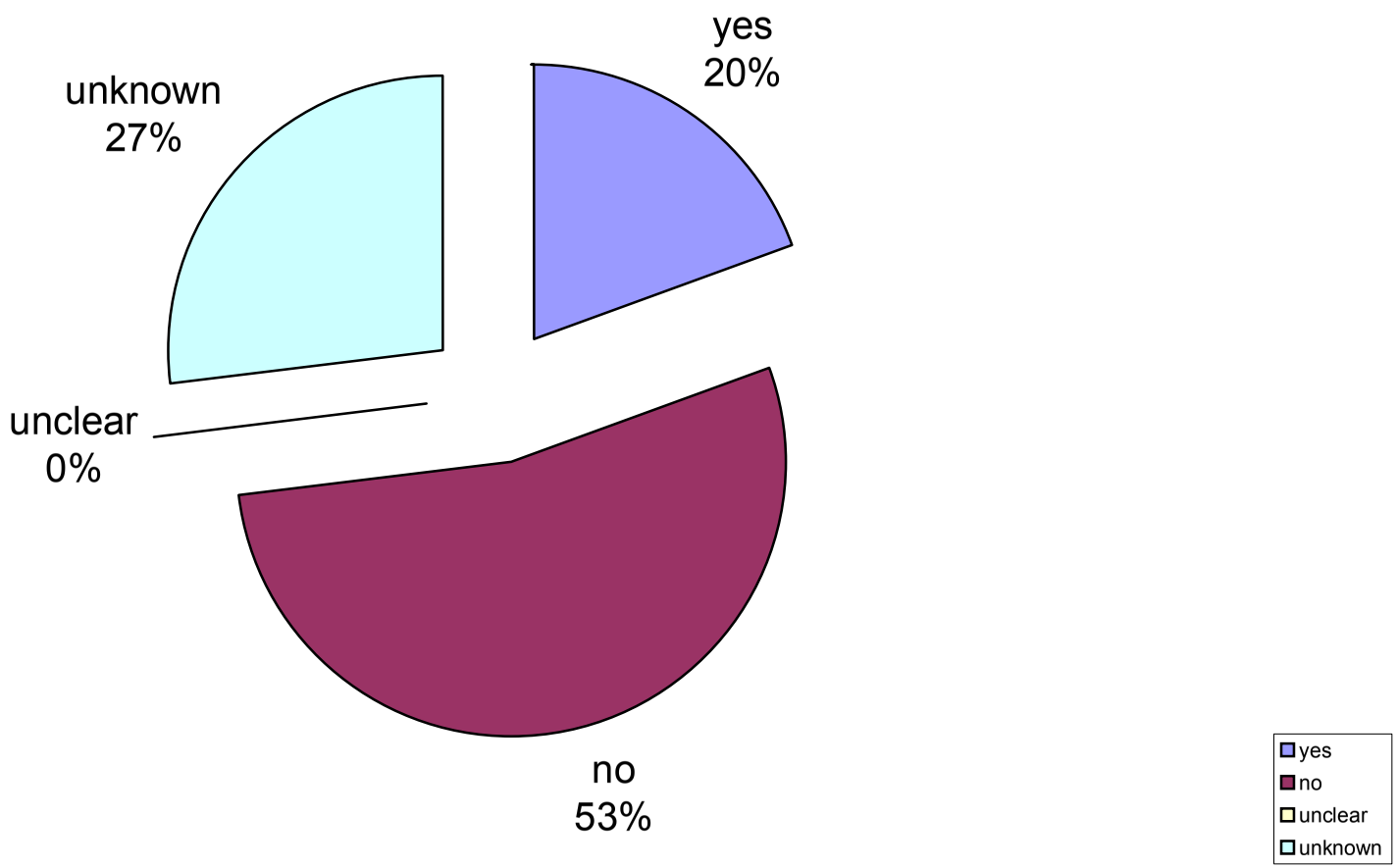
## Printable Policy (Table 1.1, graphic 2)



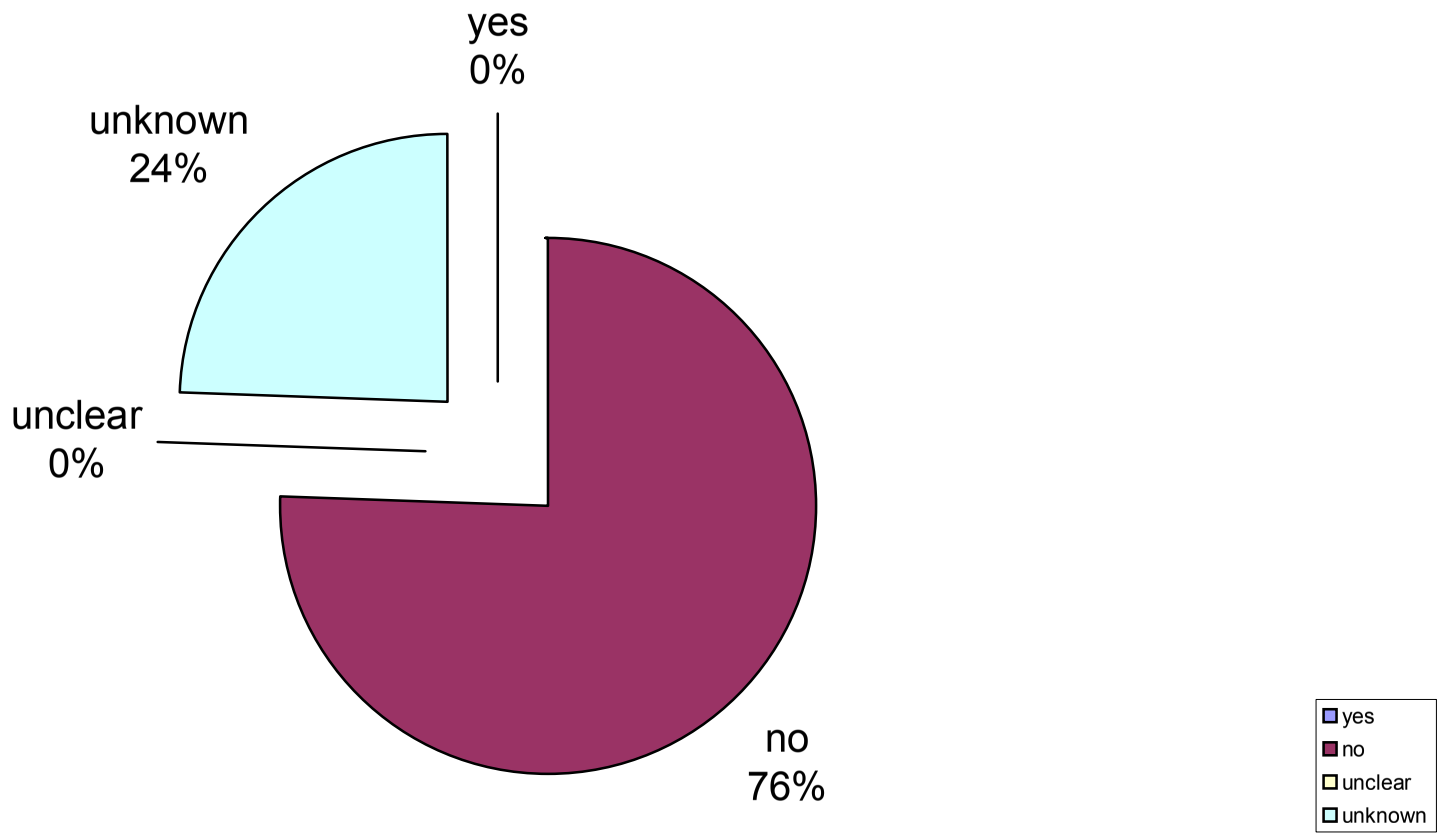
## Coverage (Table 1.1, graphic 3)



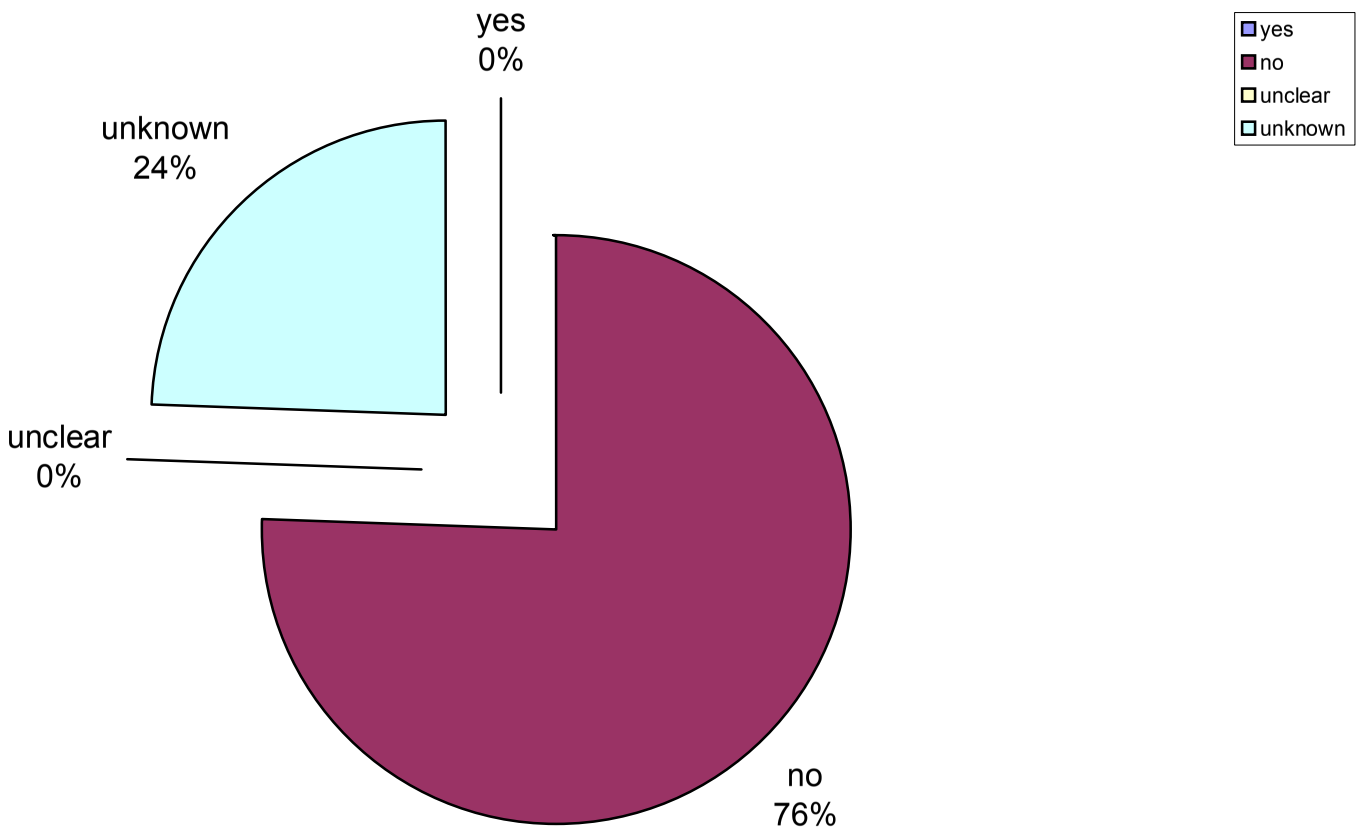
## Policy Applies to EU Data Indefinitely (Table 1.1, graphic 4)



## Policy Signals US Law Preventing Compliance (Table 1.1, graphic 5)



**Controller or Processor (Table 1.1, graphic 6)**



| | A | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table 1.2: SH Company Eligibility for Safe Harbor (FAQ 6 Certification) (as of November 3, 2003)** | | | | | | | | |
| 2 | *Company* | *Name Reported* | *Address Reported* | *Email* | *Tel* | *Fax* | *Description of Types of Processed EU Data* | *Public Location of Policy Provided* | *Accurate Location* |
| 3 | 1 | yes | yes | yes | yes | yes | unclear | yes | yes |
| 4 | 2 | yes | yes | yes | yes | yes | yes | Intranet | Unknown |
| 5 | 3 | yes | yes | yes | yes | yes | unclear | yes | yes |
| 6 | 4 | yes | yes | yes | yes | yes | yes | no | no |
| 7 | 5 | yes | yes | yes | yes | yes | yes | Intranet | Unknown |
| 8 | 6 | yes | yes | yes | yes | yes | yes | yes | yes |
| 9 | 7 | yes | yes | yes | yes | yes | yes | yes/no | yes/no |
| 10 | 8 | yes | yes | yes | yes | yes | no | Physical address | unknown |
| 11 | 9 | yes | yes | yes | yes | yes | yes | yes/no | no |
| 12 | 10 | yes | yes | yes | yes | yes | unclear | yes | no |
| 13 | 11 | yes | yes | yes | yes | yes | yes | yes | yes |
| 14 | 12 | yes | yes | yes | yes | yes | no | yes | no |
| 15 | 13 | yes | yes | yes | yes | yes | yes | yes/no | yes/no |
| 16 | 14 | yes | yes | yes | yes | yes | no | yes/no | no |
| 17 | 15 | yes | yes | yes | yes | yes | no | yes/no | no |
| 18 | 16 | yes | yes | yes | yes | yes | no | yes | yes |
| 19 | 17 | yes | yes | yes | yes | yes | unclear | yes | no |
| 20 | 18 | yes | yes | yes | yes | yes | unclear | no | no |
| 21 | 19 | yes | yes | yes | yes | yes | unclear | Intranet | unknown |
| 22 | 20 | yes | yes | yes | yes | yes | yes | yes | no |
| 23 | 21 | yes | yes | yes | yes | yes | no | no | Unknown |
| 24 | 22 | yes | yes | yes | yes | yes | yes | yes/no | yes/no |
| 25 | 23 | yes | yes | yes | yes | yes | unclear | no | no |
| 26 | 24 | yes | yes | yes | yes | yes | no | yes | yes |
| 27 | 25 | yes | yes | yes | yes | yes | unknown | no | Unknown |
| 28 | 26 | yes | yes | yes | yes | no | no | yes/no | yes/no |
| 29 | 27 | yes | yes | yes | yes | yes | yes | Intranet | unknown |
| 30 | 28 | yes | yes | yes | yes | yes | yes | Physical address | unknown |
| 31 | 29 | yes | yes | yes | yes | yes | yes | no | no |
| 32 | 30 | yes | yes | yes | yes | yes | yes | yes | no |
| 33 | 31 | yes | yes | yes | yes | yes | yes | yes | yes |
| 34 | 32 | yes | yes | yes | yes | yes | unclear | Intranet | unknown |
| 35 | 33 | yes | yes | yes | yes | yes | no | yes | unknown |
| 36 | 34 | yes | yes | yes | yes | yes | yes | Physical address | yes |
| 37 | 35 | yes | yes | yes | yes | yes | no | yes | yes |
| 38 | 36 | yes | yes | yes | yes | yes | no | yes | yes |
| 39 | 37 | yes | yes | yes | yes | yes | yes | yes | no |
| 40 | 38 | yes | yes | yes | yes | yes | no | yes | yes |
| 41 | 39 | yes | yes | yes | yes | yes | no | yes | yes |
| 42 | 40 | yes | yes | yes | yes | yes | no | yes | no |
| 43 | 41 | yes | yes | yes | yes | yes | yes | yes | yes |

**Cellule:** E2
**Commentaire:** This criteria indicates if the Certification lists either a general organizational email address or a specific contact email address for Safe Harbor issues.

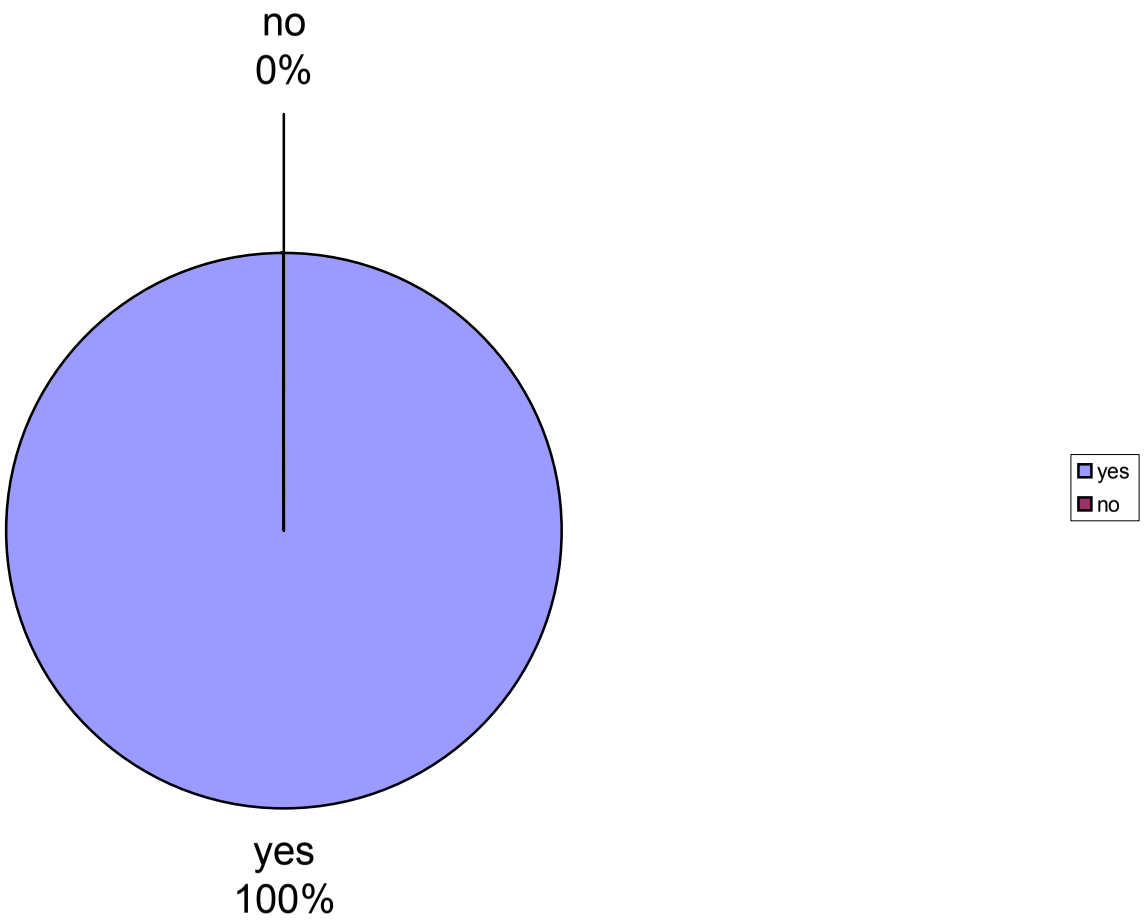
**Cellule:** H2
**Commentaire:** FAQ 6 requires that the certification include a "description of the activities of the organization with respect to personal information received from the EU."

**Cellule:** I2
**Commentaire:** FAQ 6 requires the organization to state "where the privacy policy is available for viewing by the public."

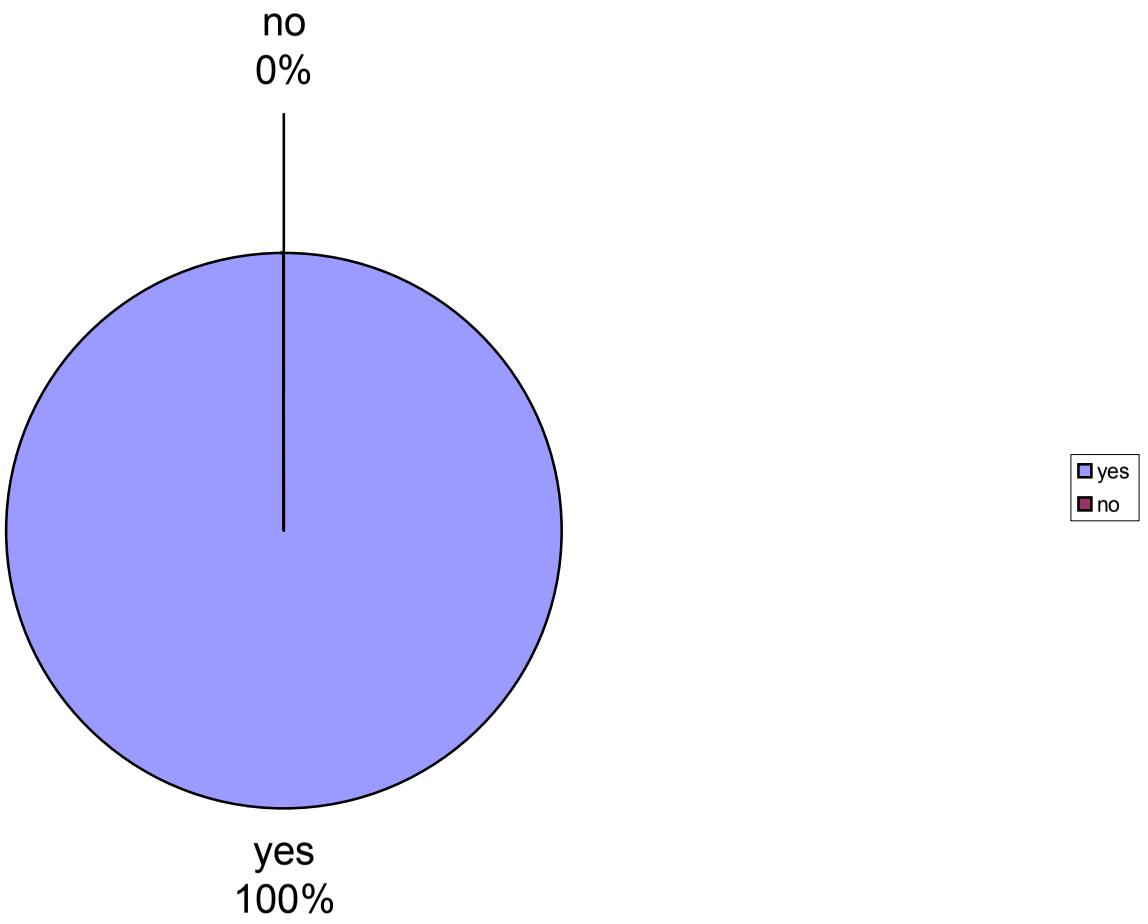
**Cellule:** J2
**Commentaire:** This indicates if the address shown on the Certification is an accurate and precise location for the privacy policy. When the Certification indicates a web site that is not the actual page for the privacy policy, the location will be marked as inaccurate.

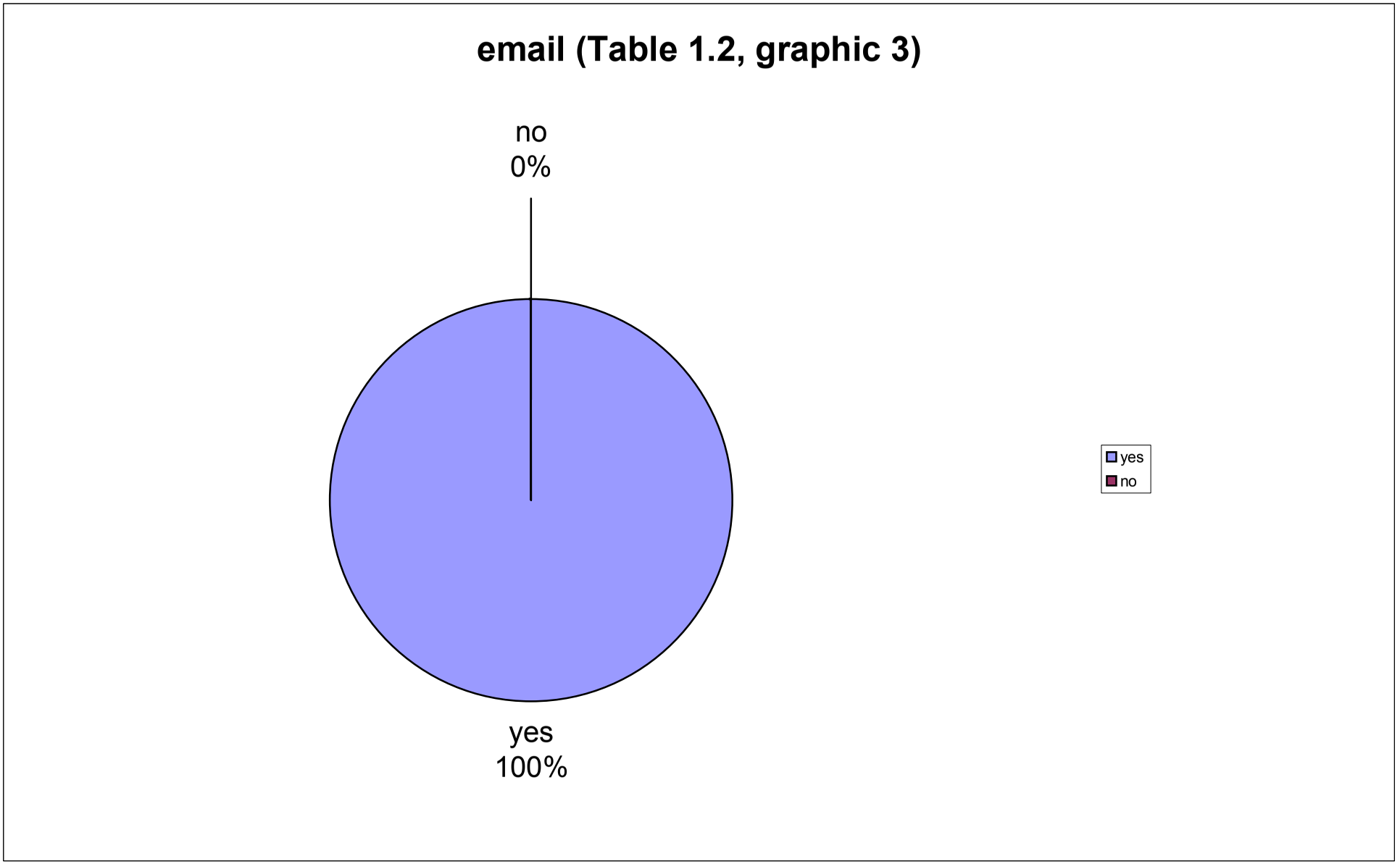
**Cellule:** I5
**Commentaire:** But the Policy is difficult to find if one starts from the Home Page, there's no direct reference to it there

## Name Reported (Table 1.2, graphic 1)

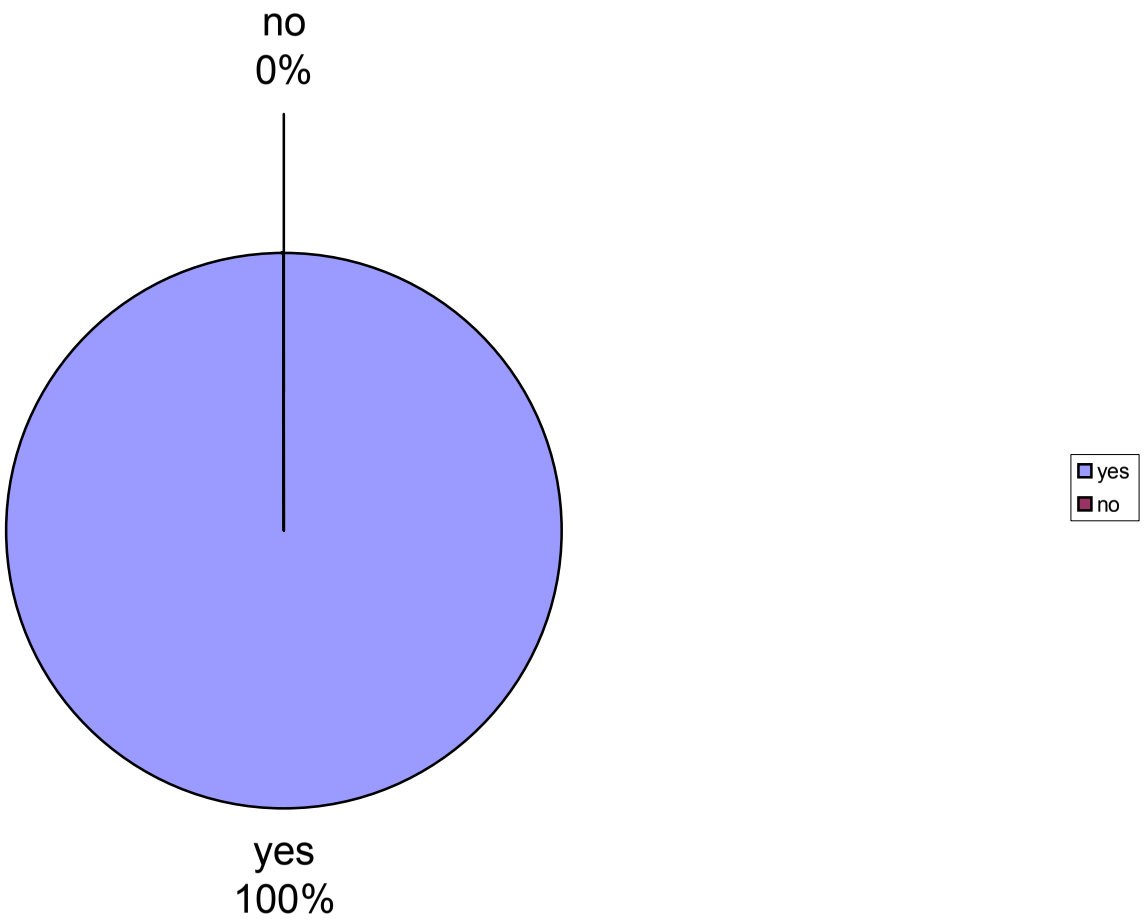


## Address Reported (Table 1.2, graphic 2)

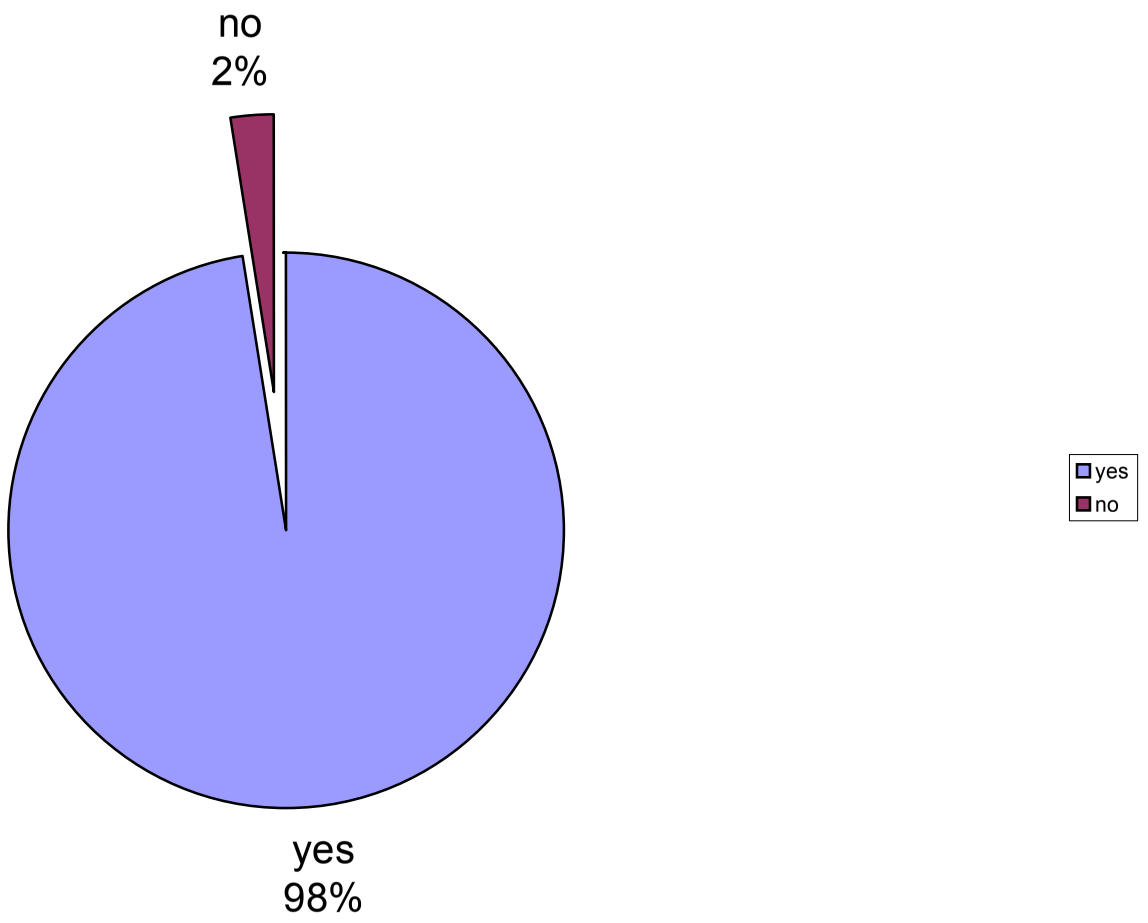



email (Table 1.2, graphic 3)
no
0%
yes
100%
yes
no

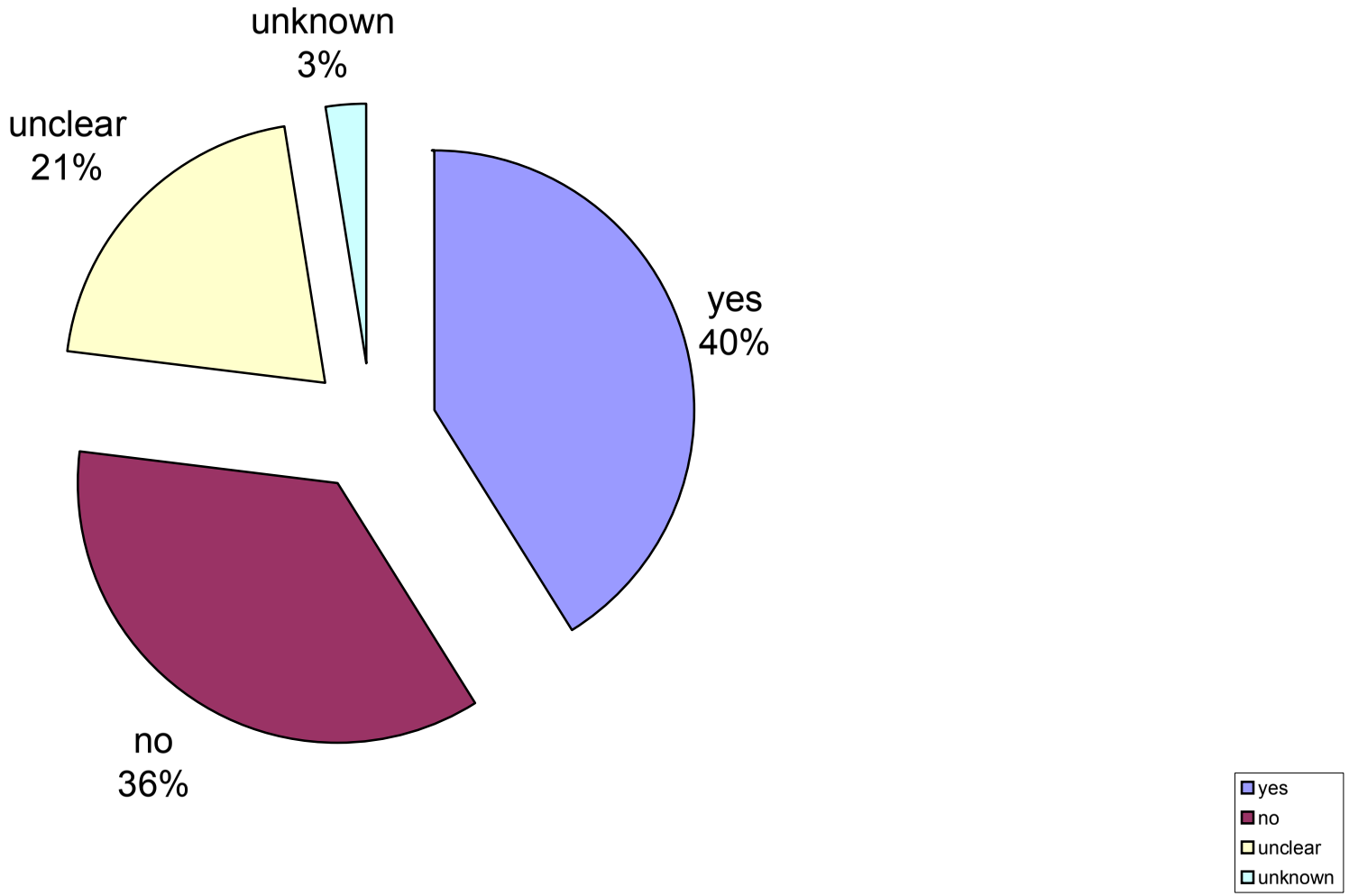
## Telephone (Table 1.2, graphic 4)



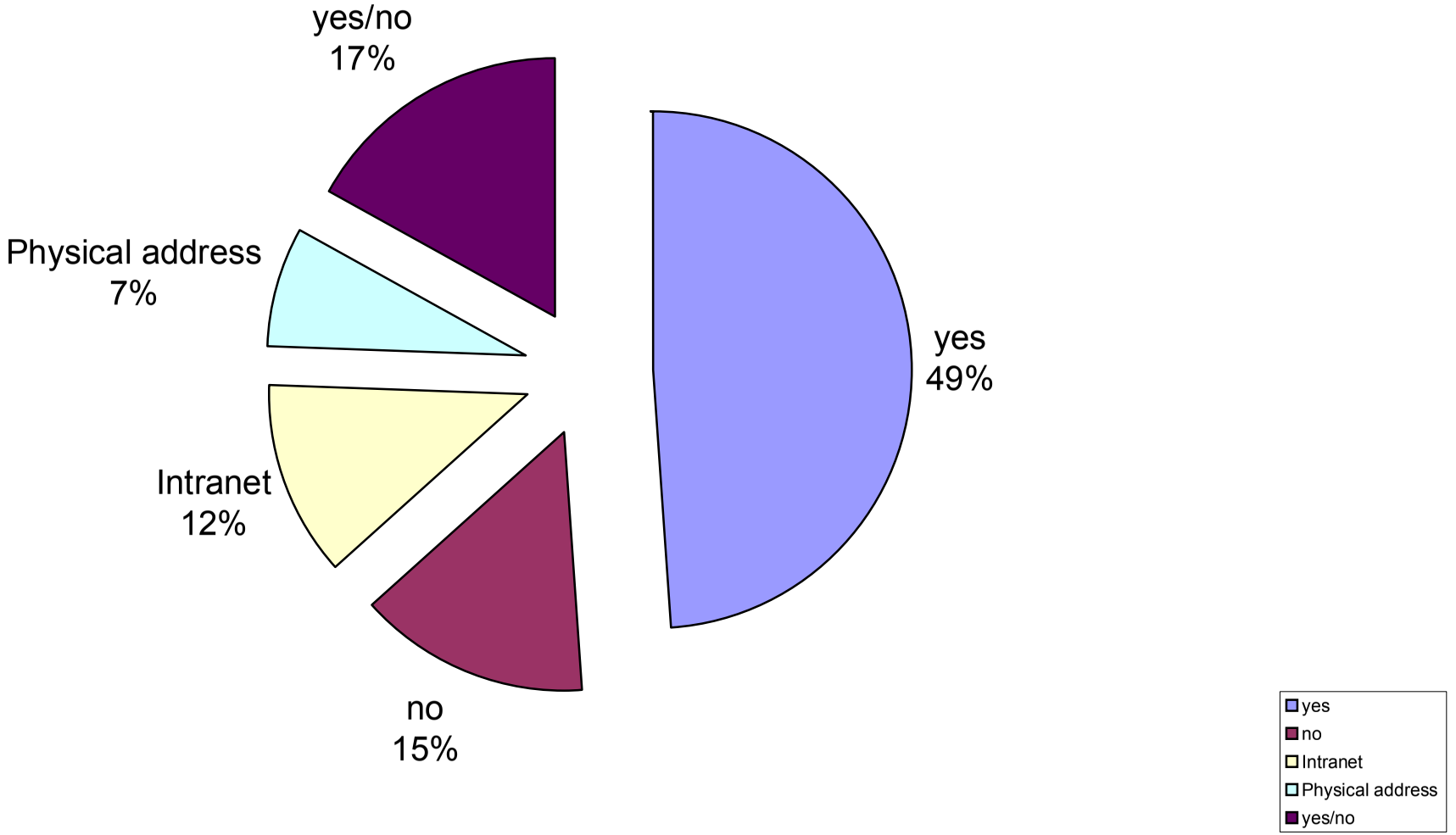
## Fax (Table 1.2, graphic 5)



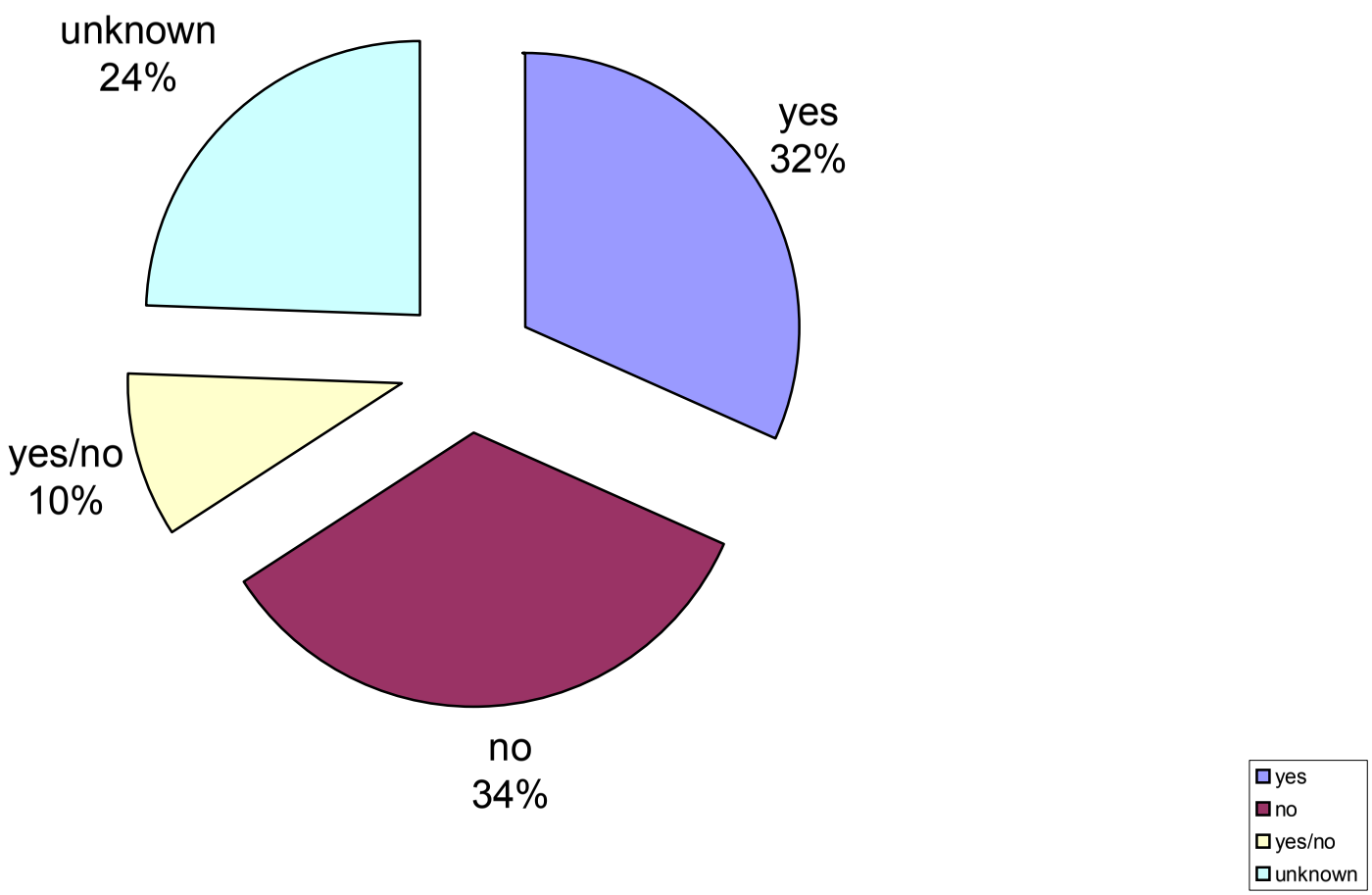
## Description of Types of Processed EU Data (Table 1.2, graphic 6)



## Public Location of Privacy Policy (Table 1.2, graphic 7)



## Accurate location (Table 1.2, graphic 8)



| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table 1.3: SH Company Eligibility for Safe Harbor (FAQ 6 Certification) (as of November 3, 2003)** | | | | | | | | | | |
| 2 | *Company* | | *Date of SH Certification* | *Policy Effective Date* | *Contact Office* | *Regulatory Agency* | *Privacy Program Membership* | *Verification Method* | *Independent Recourse Mechanism* | *HR Data* | *EU DPA Coop* |
| 3 | 1 | | 08/12/2002 | 01/12/2002 | yes | yes | no | In-house | DPA | no | yes |
| 4 | 2 | | 25/02/2002 | 02/01/2002 | yes | no | Unknown | In-house | DPA | yes | yes |
| 5 | 3 | | 18/08/2003 | 19/08/2003 | yes | yes | AAA | In-house | AAA | no | no |
| 6 | 4 | | 27/11/2002 | janv-02 | yes | yes | DMA | In-house | DMAshp | no | no |
| 7 | 5 | | 24/05/2002 | 01/05/2002 | yes | no | no | In-house | DPA | yes | yes |
| 8 | 6 | | 06/03/2002 | March 2002 | yes | yes | no | In-house | DPA | no | yes |
| 9 | 7 | | 27/01/2001 | 02/09/2001 | yes | yes/no | BBB | In-house | BBB & DPA | yes | yes |
| 10 | 8 | | 09/04/2004 | 07/04/2003 | yes | yes | no | in-house | BBB | no | no |
| 11 | 9 | | 20/09/2004 | 07/18/2002 | yes | yes/no | no | in-house | DPA | yes | yes |
| 12 | 10 | | 07/01/2003 | 26/07/2001 | yes | yes | TRUSTe | in-house | TRUSTe & BBB | no | no |
| 13 | 11 | | 03/07/2002 | 01/07/2002 | yes | yes | no | In-house | DPA | no | yes |
| 14 | 12 | | 15/01/2002 | 01/01/2002 | yes | yes | no | TP | DPA | no | yes |
| 15 | 13 | | 06/03/2003 | 12/01/2000 | yes | yes/no | no | in-house | DPA & AAA | yes | yes |
| 16 | 14 | | 15/01/2002 | 02/04/2002 | yes | yes/no | no | in-house | DPA | yes | yes |
| 17 | 15 | | 18/06/2003 | 2001 - | yes | yes | no | In-house | DPA | no | yes |
| 18 | 16 | | 05/09/2001 | 11/01/2000 | yes | yes | DMA | In-house | DMAshp | no | no |
| 19 | 17 | | 27/02/2002 | 28/02/2002_ | yes | yes/no | no | In-house | DPA | yes | yes |
| 20 | 18 | | 04/12/2002 | 01/01/2002 | yes | no | TRUSTe | In-house | TRUSTe DPA | yes | yes |
| 21 | 19 | | 09/10/2003 | 31/12/2002 | yes | no | no | in-house | DPA | yes | yes |
| 22 | 20 | | 20/05/2003 | 14/0/2003 | yes | yes | TRUSTe | in-house | TRUSTe | no | no |
| 23 | 21 | | 06/12/2003 | juin-02 | yes | yes | no | in-house | DPA | no | yes |
| 24 | 22 | | 15/04/2002 | 06/08/2001 | yes | yes/no | TRUSTe | TP | DPA & TRUSTe | yes | yes |
| 25 | 23 | | 03/07/2001 | déc-89 | yes | yes | CASRO | in-house | DPA | no | yes |
| 26 | 24 | | 27/05/2002 | oct-98 | yes | yes | no | in-house | DPA | no | yes |
| 27 | 25 | | 07/02/2002 | 2//7/2004 | yes | yes | no | in-house | DPA | no | yes |
| 28 | 26 | | 08/03/2001 | 20/04/2001 | yes | yes/no | no | in-house | DPA | yes | yes |
| 29 | 27 | | 17/09/2003 | 17/09/2003 | yes | no | no | in-house | DPA | yes | yes |
| 30 | 28 | | 29/11/2003 | 15/06/2001 | yes | no | no | in-house | DPA | yes | yes |
| 31 | 29 | | 28/1/2002 | 07/01/2001 | yes | yes | DMAshp | in-house | DMAshp | no | no |
| 32 | 30 | | 25/06/2002 | 01/05/2002 | yes | no | TRUSTe | TP | DPA & TRUSTe | yes | yes |
| 33 | 31 | | 24/02/2003 | 03/01/2003 | yes | no | no | in-house | DPA | yes | yes |
| 34 | 32 | | 16/05/2003 | 09/01/2002 | yes | yes | no | in-house | DPA | no | yes |
| 35 | 33 | | 28/05/2003 | 01/01/2000 | yes | yes | no | in-house | AAA | no | no |
| 36 | 34 | | 22/03/2002 | 21/03/2002 | yes | no | no | in-house | DPA | yes | yes |
| 37 | 35 | | 03/12/2003 | 13/02/2003 | yes | yes | TRUSTe | TP | TRUSTe | no | no |
| 38 | 36 | | 25/6/2003 | 07/01/2003 | yes | yes | no | in-house | DPA | no | yes |
| 39 | 37 | | 15/03/2001 | 31/01/2000 | yes | yes/no | OPA | in-house | DPA | yes | yes |
| 40 | 38 | | 13/06/2002 | 5/01? | yes | yes | TRUSTe, CAUCE, DMAshp | in-house | DPA | no | yes |
| 41 | 39 | | 23/10/2001 | 20/01/2001 | yes | yes/no | TRUSTe | in-house | DPA & TRUSTe | yes | yes |
| 42 | 40 | | 09/04/2001 | sept-01 | yes | yes | no | in-house | DMA | no | no |
| 43 | 41 | | 29/05/2001 | 26/01/2000 | yes | yes | no | in-house | DPA | no | yes |

**Cellule:** F2
**Commentaire:** FAQ 6 requires that the organization state the specific statutory body that has jurisdiction to hear claims against the organization.

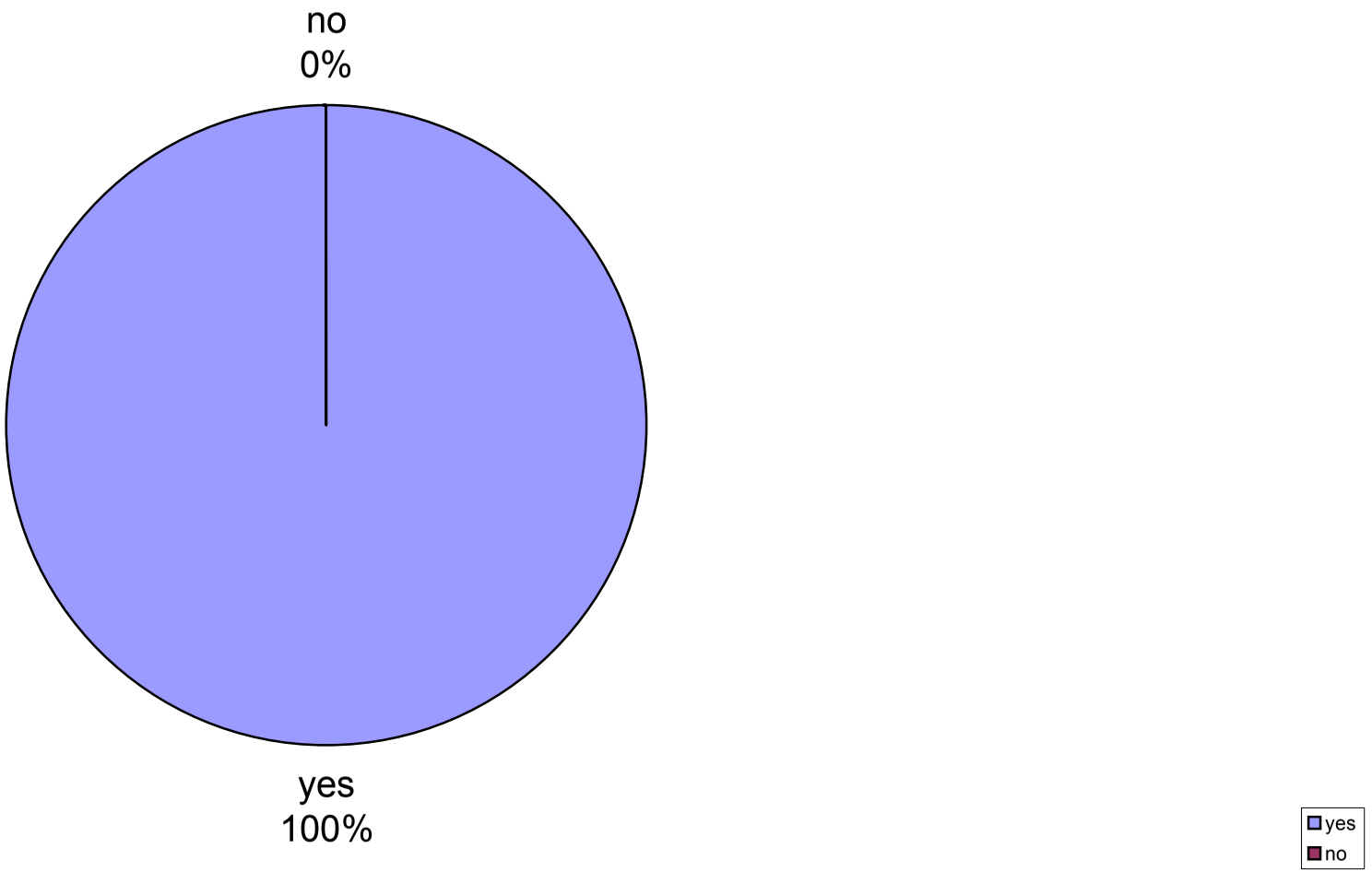
**Cellule:** G2
**Commentaire:** FAQ 6 requires organizations to state the name of any privacy programs to which the organization belongs.

**Cellule:** I2
**Commentaire:** FAQ 6 requires organizations to state the independent recourse mechanism that is available to investigate unresolved complaints.

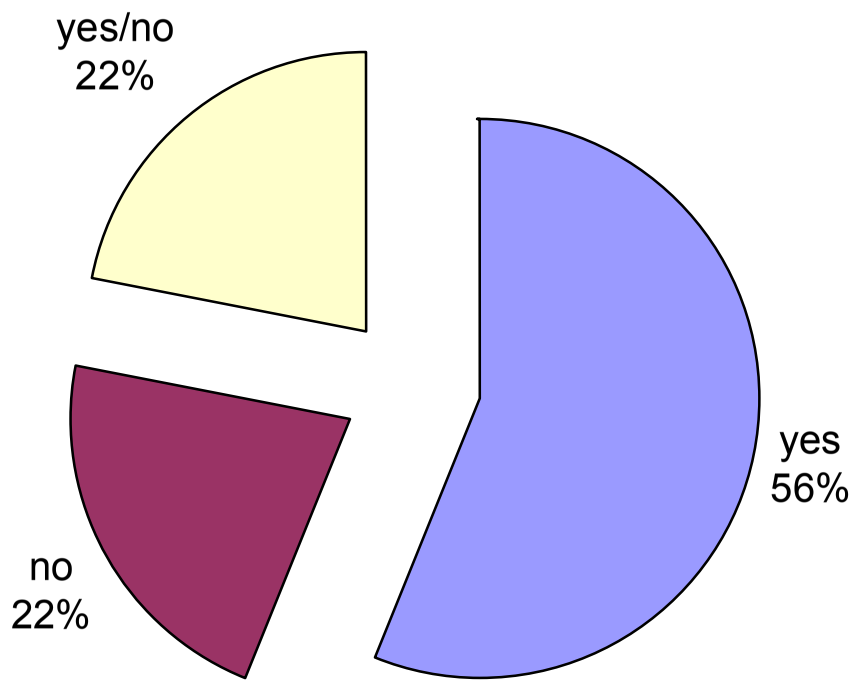
**Cellule:** J2
**Commentaire:** FAQ 6 requires organizations processing human resources data to declare their commitment to cooperate with the DPA and to comply with the advice of such authortiy.

**Cellule:** F4
**Commentaire:** No, letter makes false assertion.

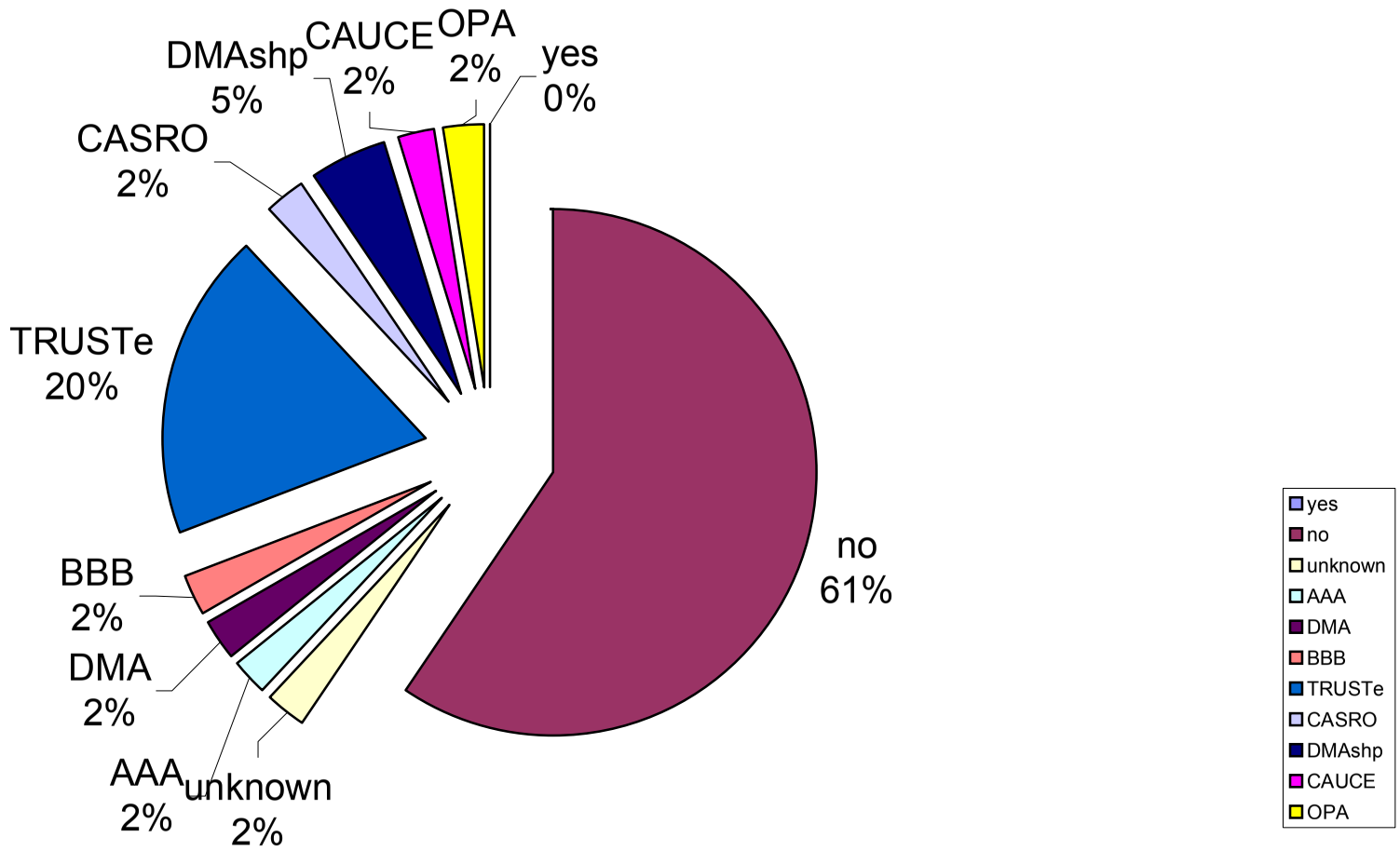
## Contact office (Table 1.3, graphic 1)



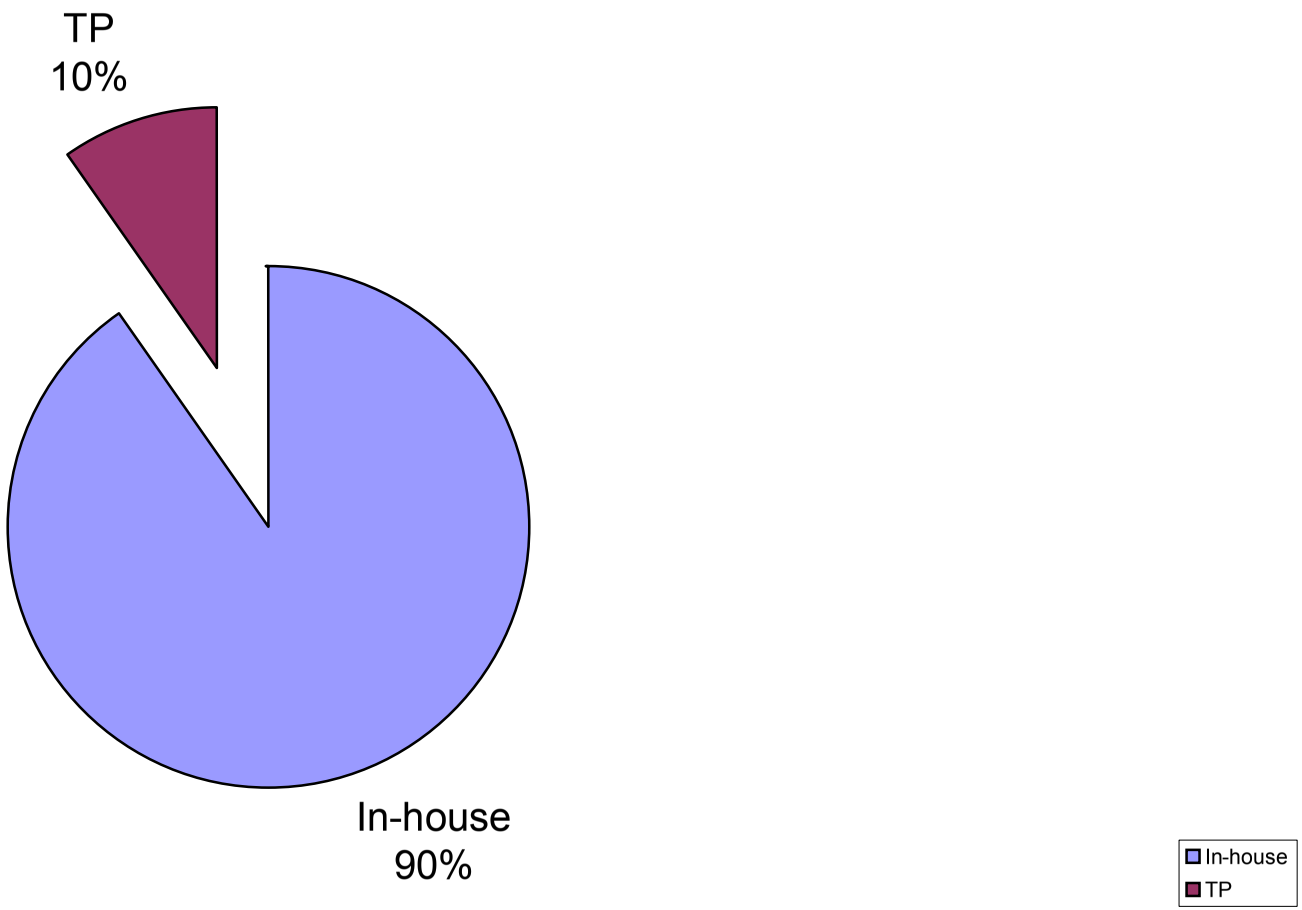
## Regulatory Agency (Table 1.3, graphic 2)



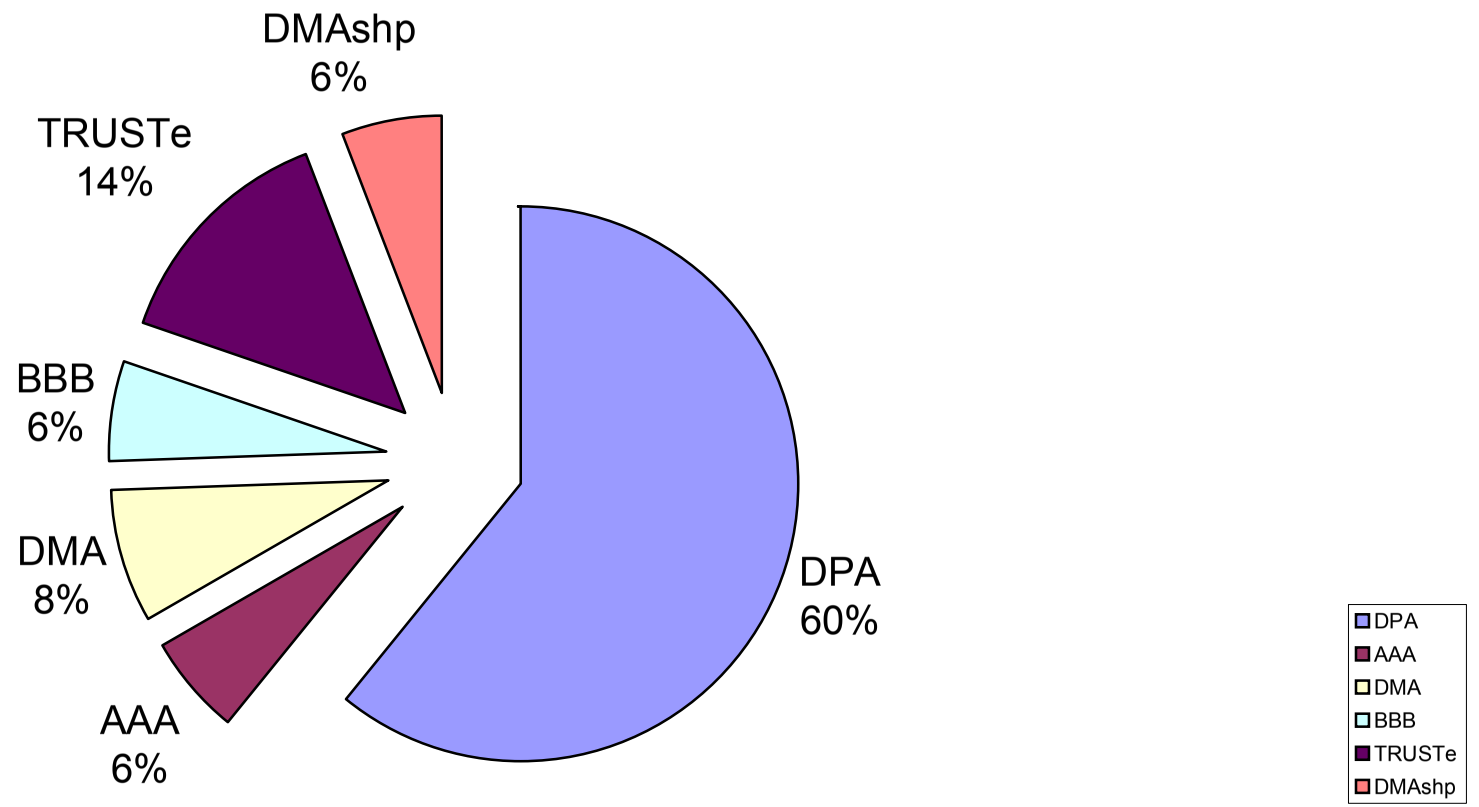
## Privacy Program Membership (Table 1.3, graphic 3)



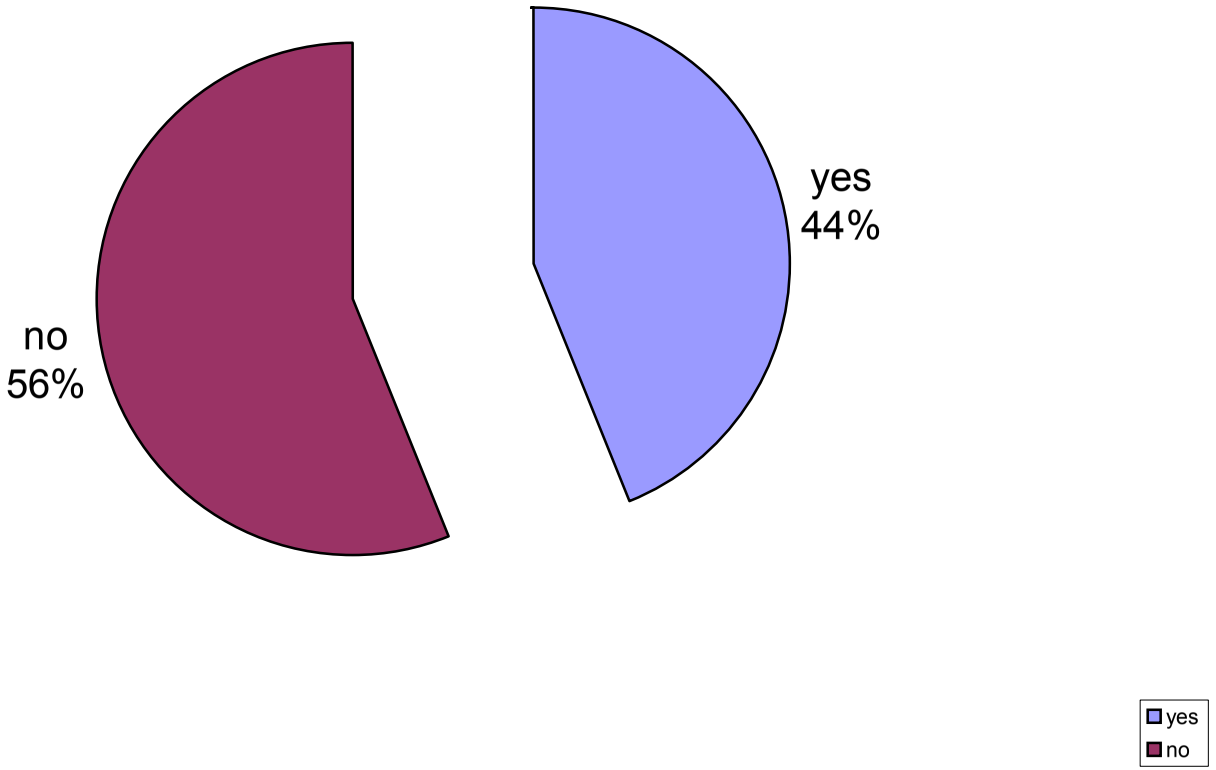
## Verification Method (Table 1.3, graphic 4)



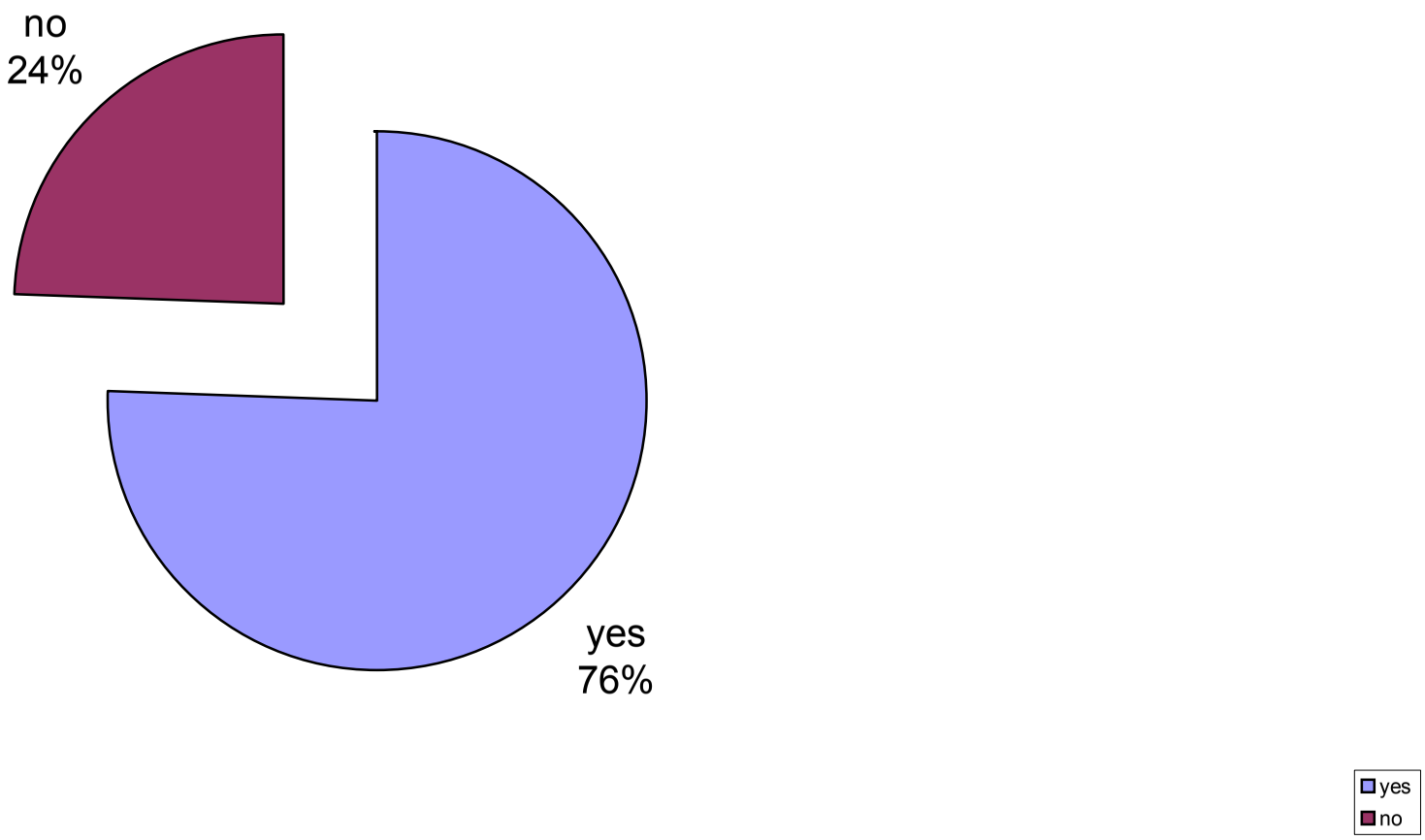
## Independent Recourse Mechanism (Table 1.3, graphic 5)



## HR Data (Table 1.3, graphic 6)

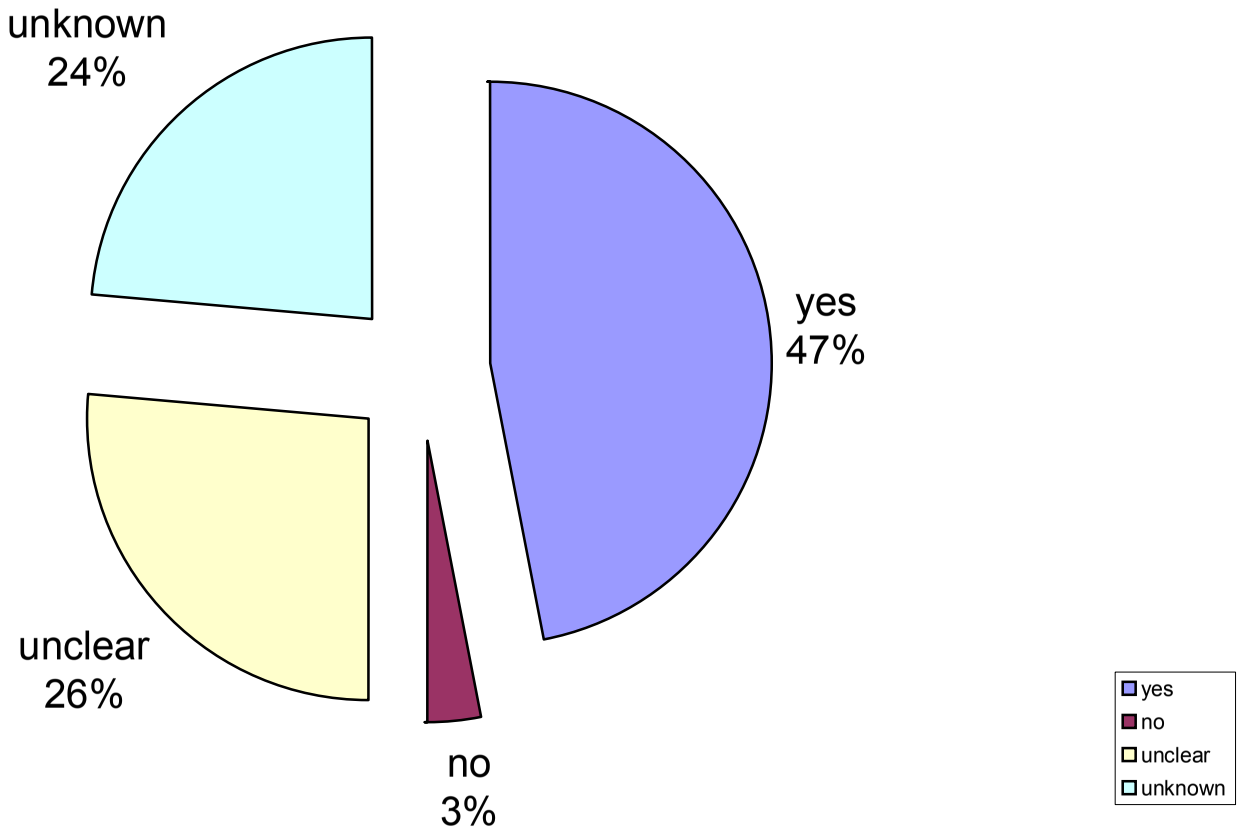


## EU Data Coop (Table 1.3, graphic 7)

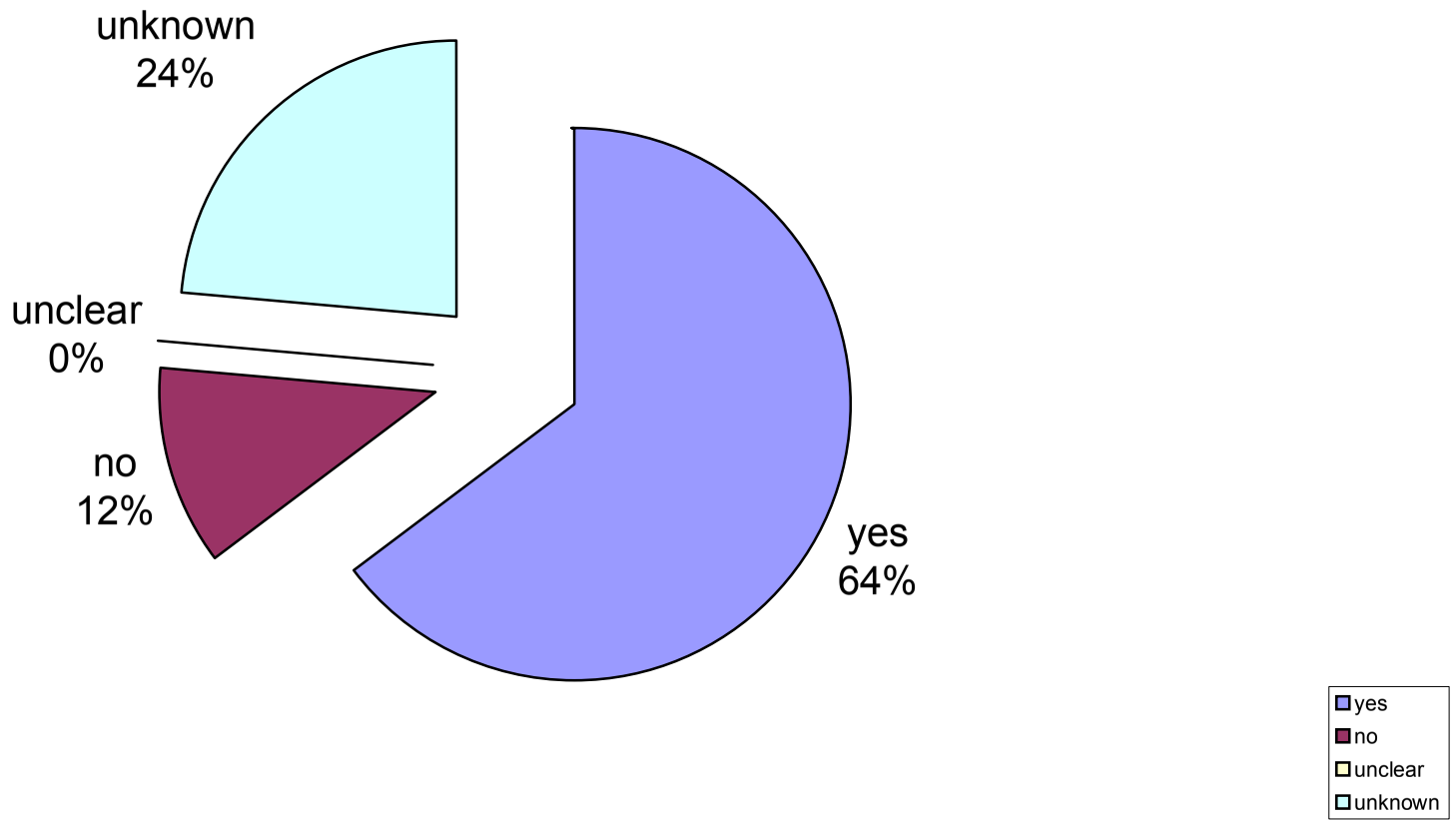


| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table 2.1: SH Company Compliance with Notice Principle (as of November 3, 2003)** | | | | | | | | | | |
| 2 | *Company* | | *Clear* | *Conspicuous* | *Specified Purpose* | *Organization Contacts* | *Notice of secondary use* | *Third Party Disclosures* | *Notice of choice for use* | *Notice of Choice for dissemination* | *Statement of SH Compliance* |
| 3 | 1 | | no | no | unclear | yes | no | yes | napp | no | no |
| 4 | 2 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 5 | 3 | | no | no | unclear | yes | no | unclear | napp | unclear | yes |
| 6 | 4 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 7 | 5 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 8 | 6 | | no | no | no | no | no | unclear | napp | unclear | no |
| 9 | 7 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 10 | 8 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 11 | 9 | | no | no | yes | no | no | yes | napp | yes | no |
| 12 | 10 | | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| 13 | 11 | | yes | yes | yes | yes | no | unclear | napp | unclear | yes |
| 14 | 12 | | no | yes | unclear | yes | yes | yes | yes | no | yes |
| 15 | 13 | | no | no | yes | yes | yes | no | no | napp | yes |
| 16 | 14 | | no | no | unclear | yes | yes | yes | no | no | yes |
| 17 | 15 | | yes | yes | yes | yes | no | no | napp | napp | yes |
| 18 | 16 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 19 | 17 | | yes | yes | yes | no | yes | no | yes | napp | yes |
| 20 | 18 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 21 | 19 | | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| 22 | 20 | | yes | yes | yes | yes | no | unclear | napp | unclear | yes |
| 23 | 21 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 24 | 22 | | yes | no | yes | yes | no | yes | napp | unclear | yes |
| 25 | 23 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 26 | 24 | | yes | yes | yes | no | unclear | unclear | unclear | no | yes |
| 27 | 25 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 28 | 26 | | yes | yes | yes | yes | no | yes | napp | no | yes |
| 29 | 27 | | no | yes | yes | yes | yes | yes | unclear | unclear | yes |
| 30 | 28 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 31 | 29 | | unknown | unknown | unknown | unknown | unknown | unknown | unnown | unknown | unknown |
| 32 | 30 | | yes | yes | yes | yes | no | yes | napp | yes | yes |
| 33 | 31 | | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| 34 | 32 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 35 | 33 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 36 | 34 | | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| 37 | 35 | | yes | yes | unclear | yes | yes | yes | yes | yes | yes |
| 38 | 36 | | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| 39 | 37 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 40 | 38 | | no | yes | no | yes | yes | unclear | yes | no | yes |
| 41 | 39 | | no | yes | unclear | yes | no | unclear | napp | unclear | yes |
| 42 | 40 | | no | no | unclear | yes | no | yes | napp | yes | yes |
| 43 | 41 | | yes | yes | unclear | yes | no | yes | napp | yes | no |
| 44 | | | | | | | | | | | |
| 45 | | | | | | | | | | | |
| 46 | | | | | | | | | | u: | |
| 47 | | | | | | | | | | | |
| 48 | | | | | | | | | | | |
| 49 | | | | | | | | | | | |
| 50 | | | | | | | | | | | |
| 51 | | | | | | | | | | | |
| 52 | | | | | | | | | | | |
| 53 | | | | | | | | | | | |

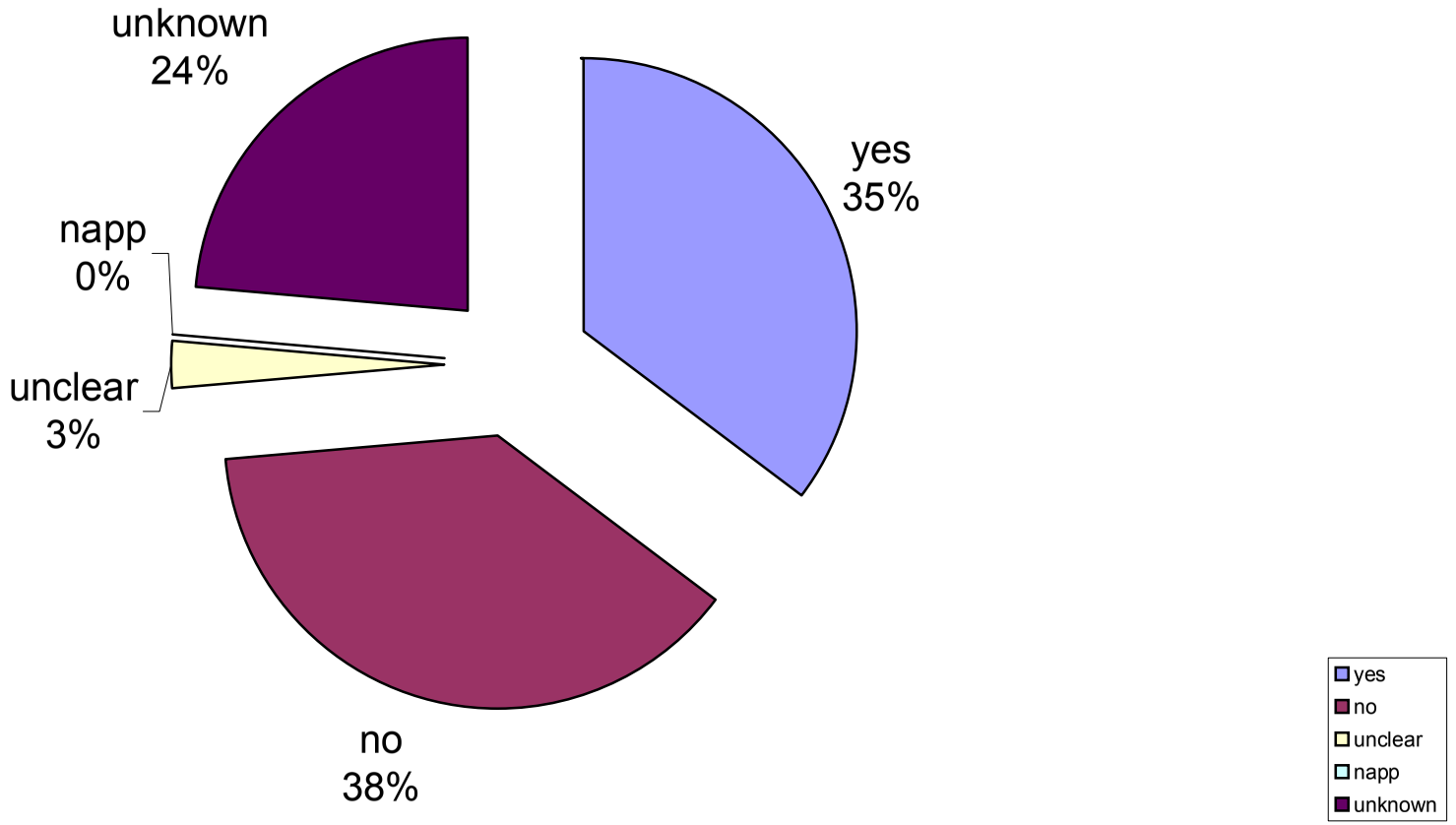
## Specified Purpose (Table 2.1, graphic 1)



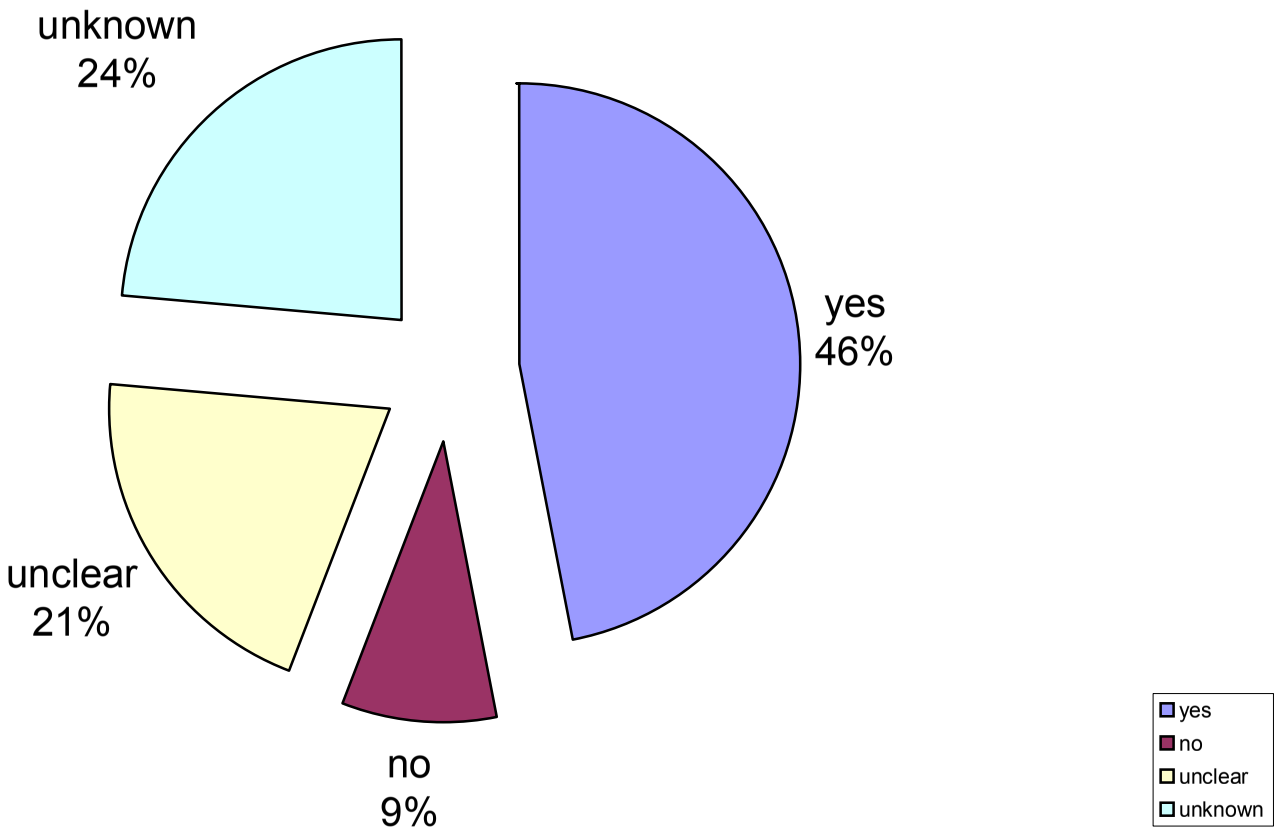
## Organization  Contacts (Table 2.1, graphic 2)



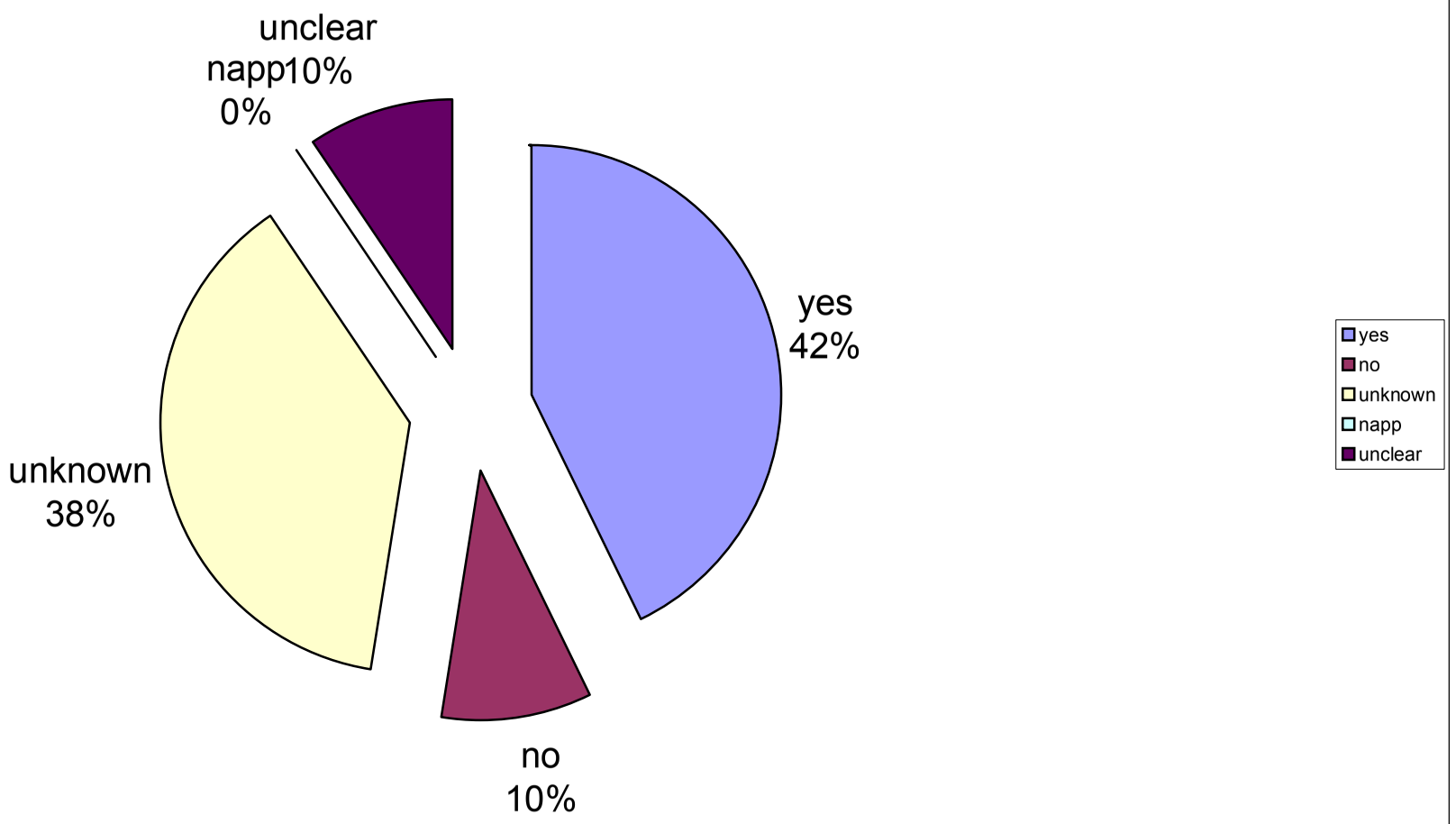
## Notice of secondary use (Table 2.1, graphic 3)



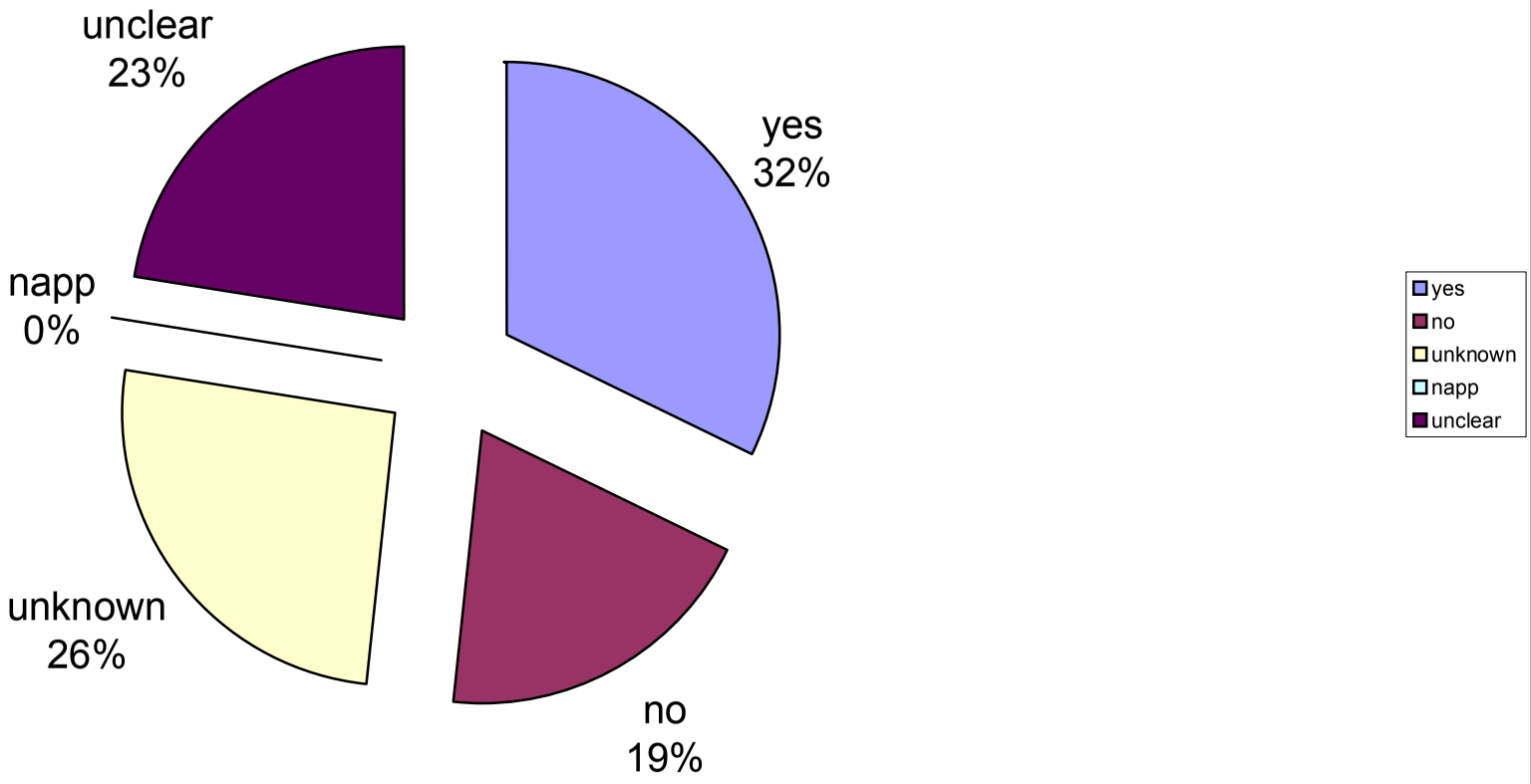
## Third Party Disclosures (Table 2.1, graphic 4)



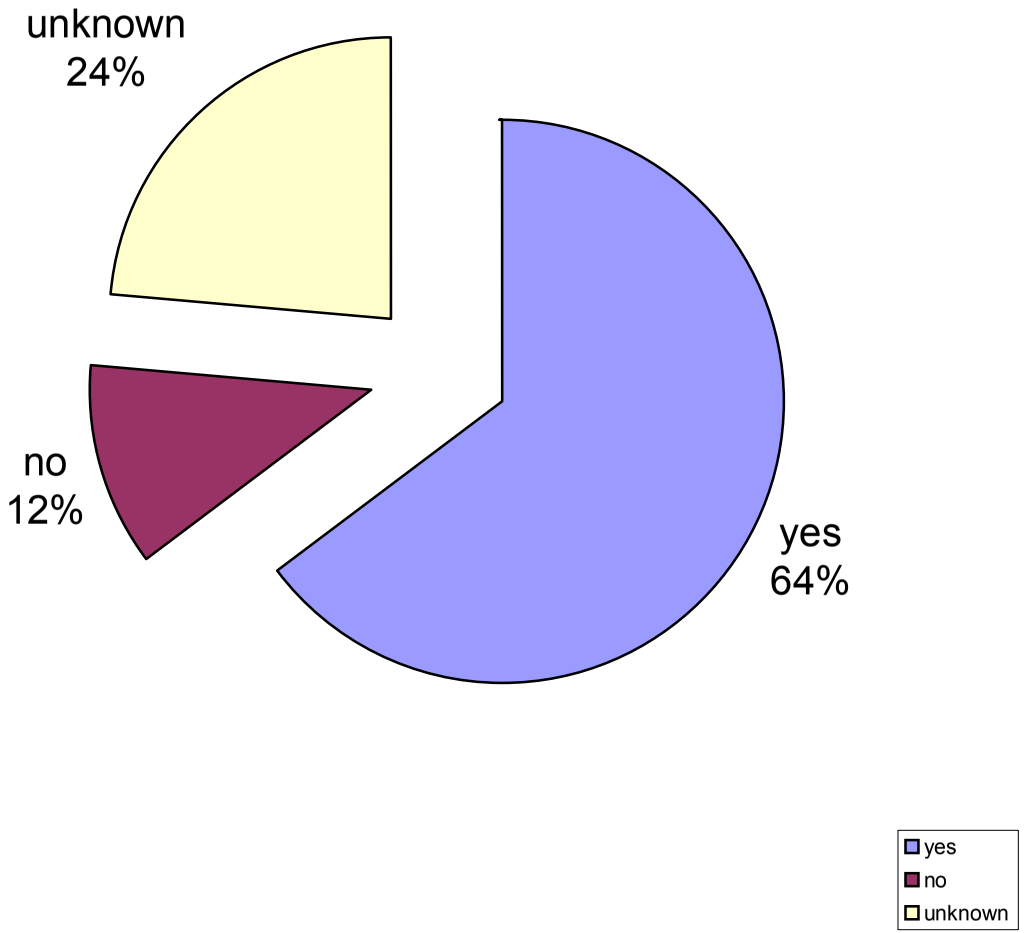
## Notice of choice for use (Table 2.1, graphic 5)



## Notice of choice for dissemination (Table 2.1, graphic 6)



## Statement (Table 2.1, graphic 7)



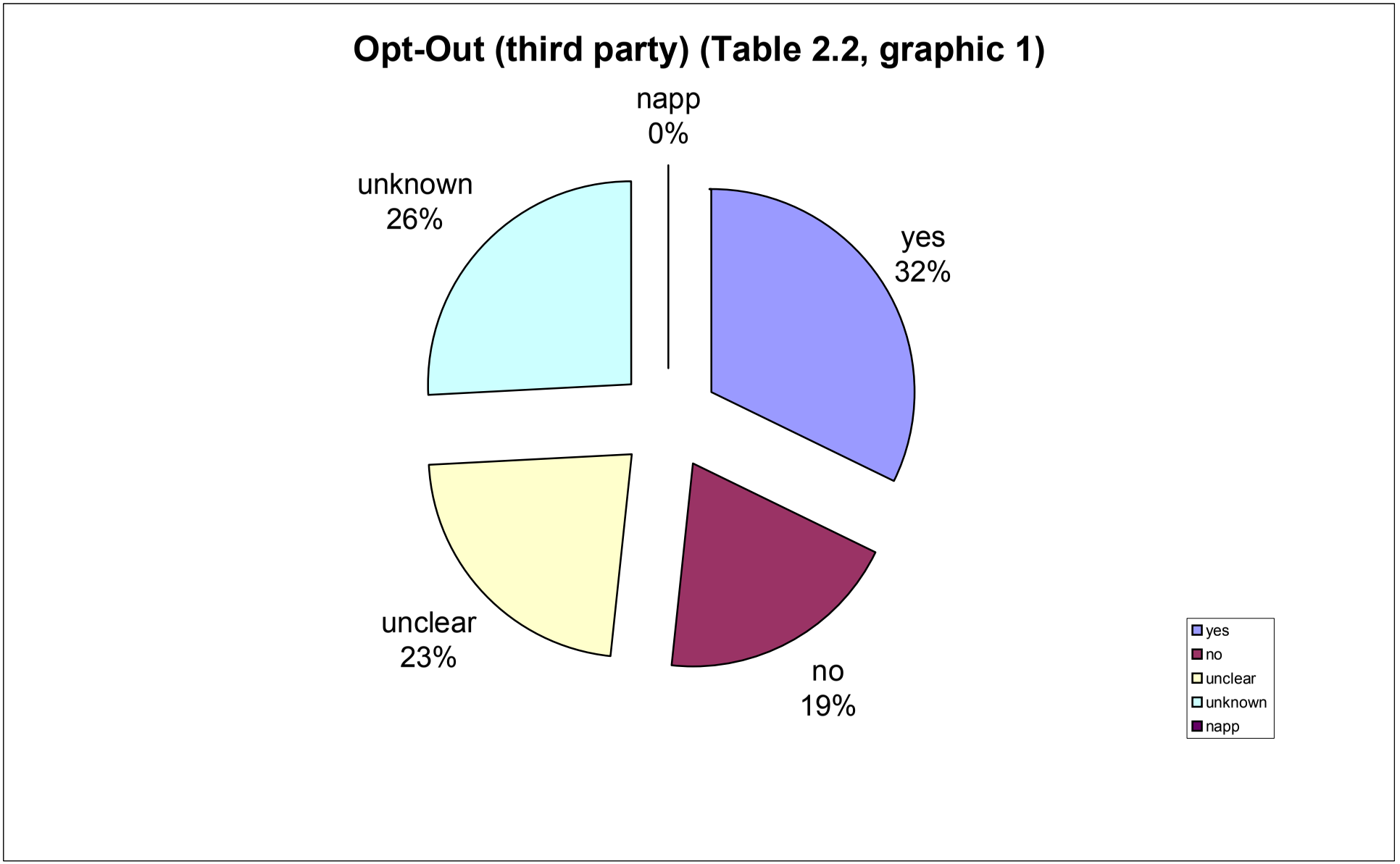
| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table 2.2: Company Compliance with Choice Principle (as of November 3, 2003)** | | | | | | | | |
| 2 | *Company* | | *Opt-out (3rd party)* | *Opt-out (secondary use)* | *Clear* | *Conspicuous* | *Readily Available* | *Affordable* | *Opt-in (Sensitive Data)* |
| 3 | 1 | | no | napp | napp | napp | napp | napp | napp |
| 4 | 2 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 5 | 3 | | unclear | napp | yes | yes | yes | yes | napp |
| 6 | 4 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 7 | 5 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 8 | 6 | | unclear | napp | no | no | no | no | napp |
| 9 | 7 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 10 | 8 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 11 | 9 | | yes | napp | no | no | no | no | napp |
| 12 | 10 | | yes | yes | yes | yes | no | no | napp |
| 13 | 11 | | unclear | napp | no | yes | yes | no | napp |
| 14 | 12 | | no | yes | no | yes | no | no | napp |
| 15 | 13 | | napp | no | napp | napp | napp | napp | napp |
| 16 | 14 | | no | no | napp | napp | napp | napp | napp |
| 17 | 15 | | napp | napp | napp | napp | napp | napp | napp |
| 18 | 16 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 19 | 17 | | napp | yes | no | no | no | no | yes |
| 20 | 18 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 21 | 19 | | yes | yes | yes | yes | yes | unknown | unclear |
| 22 | 20 | | unclear | napp | napp | napp | napp | napp | napp |
| 23 | 21 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 24 | 22 | | unclear | napp | napp | napp | napp | napp | napp |
| 25 | 23 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 26 | 24 | | no | unclear | no | no | no | no | no |
| 27 | 25 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 28 | 26 | | no | napp | no | yes | napp | napp | napp |
| 29 | 27 | | unclear | unclear | no | yes | no | no | unclear |
| 30 | 28 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 31 | 29 | | unknown | unknown | unknown | unknown | unknown | unknown | unknown |
| 32 | 30 | | yes | napp | yes | yes | no | no | yes |
| 33 | 31 | | yes | yes | yes | yes | no | no | yes |
| 34 | 32 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 35 | 33 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 36 | 34 | | yes | yes | yes | yes | no | no | yes |
| 37 | 35 | | yes | yes | no | yes | yes | no | napp |
| 38 | 36 | | yes | yes | yes | yes | no | no | yes |
| 39 | 37 | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 40 | 38 | | no | yes | napp | napp | npp | napp | napp |
| 41 | 39 | | unclear | napp | no | yes | no | no | napp |
| 42 | 40 | | yes | napp | yes | yes | no | no | napp |
| 43 | 41 | | yes | napp | no | no | no | no | napp |

**Cellule:** E2
**Commentaire:** The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."

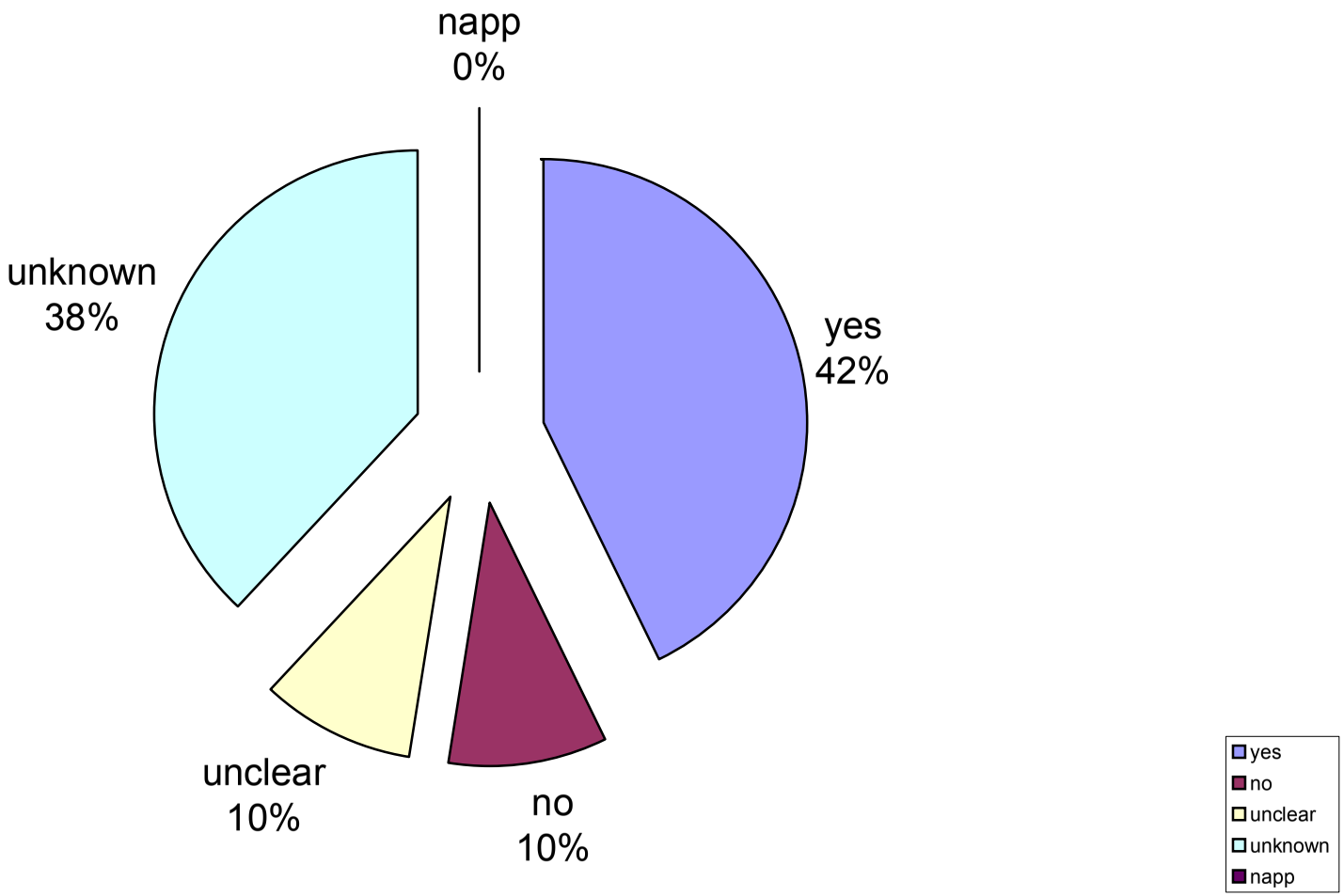
**Cellule:** F2
**Commentaire:** The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."

**Cellule:** G2
**Commentaire:** The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."
"Readily available" means that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out) and that the opt-out mechanism be transparent for data subjects.

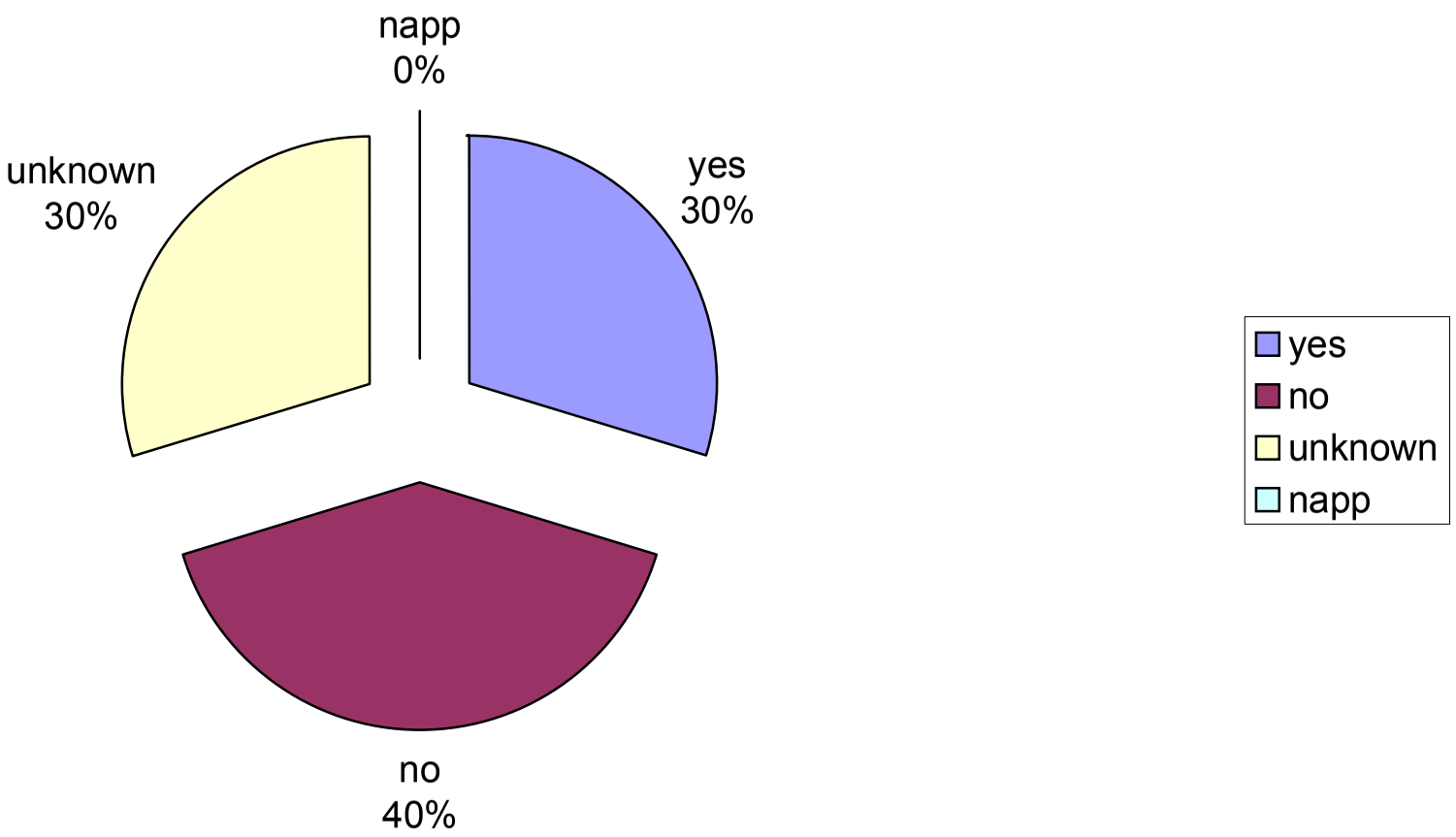
**Cellule:** I21
**Commentaire:** "For sensitive Personal information, the company will give individuals the opportunity to affirmatively and explicitly (opt-in) consent to the disclosure of the information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual."


Opt-Out (third party) (Table 2.2, graphic 1)
napp
0%
unknown
26%
yes
32%
unclear
23%
no
19%
yes
no
unclear
unknown
napp

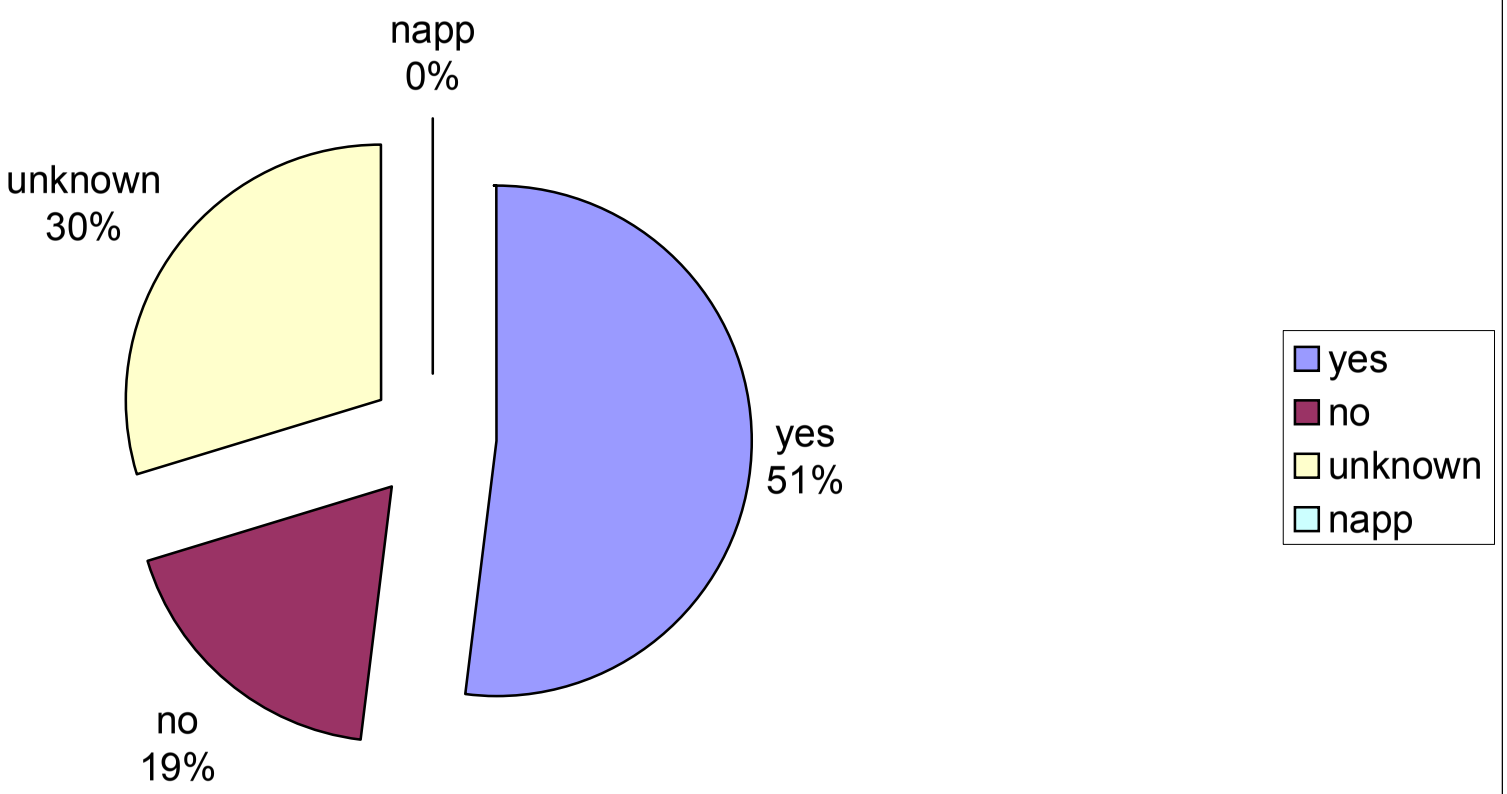
## Opt-Out (secondary use) (Table 2.2, graphic 2)

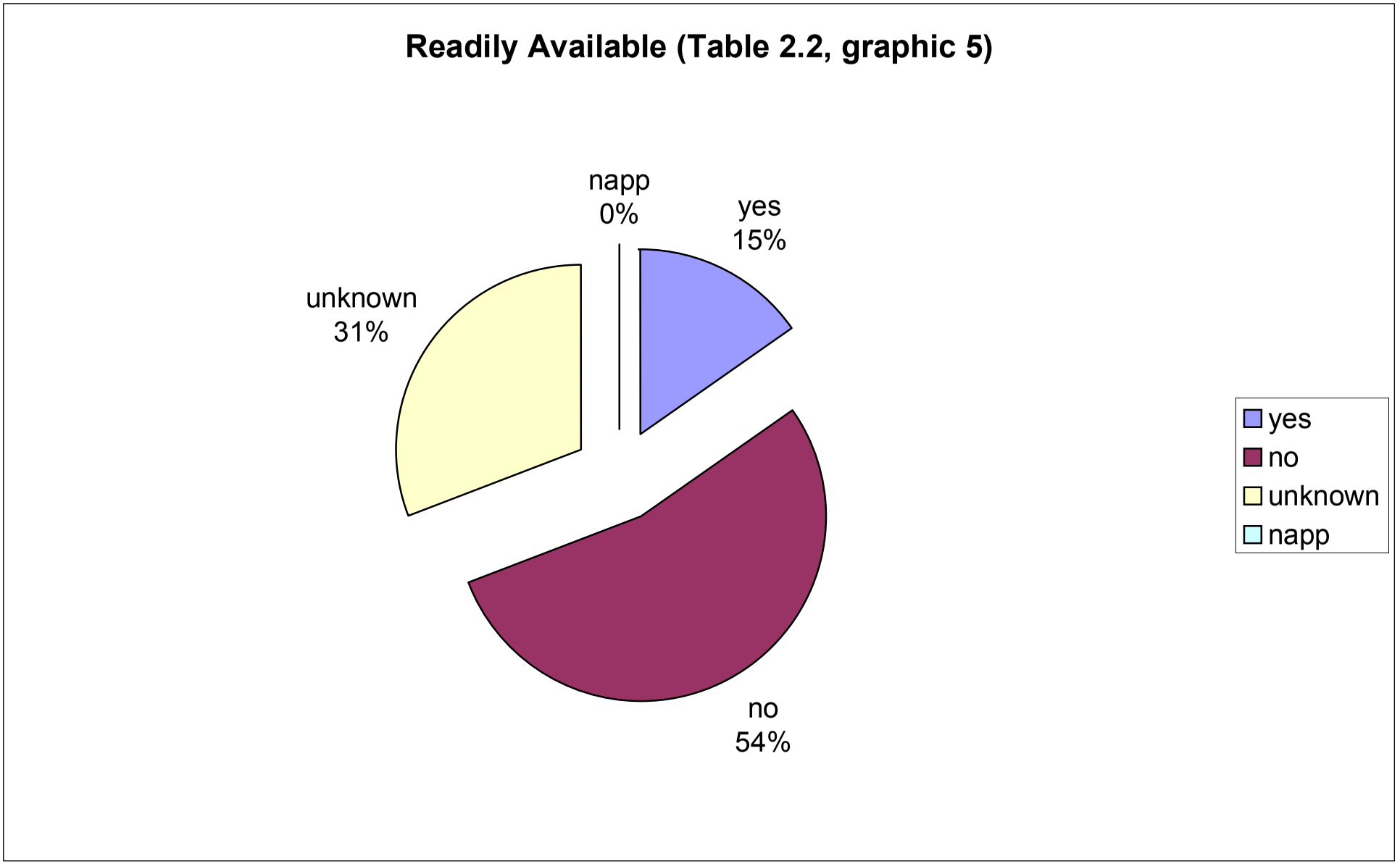


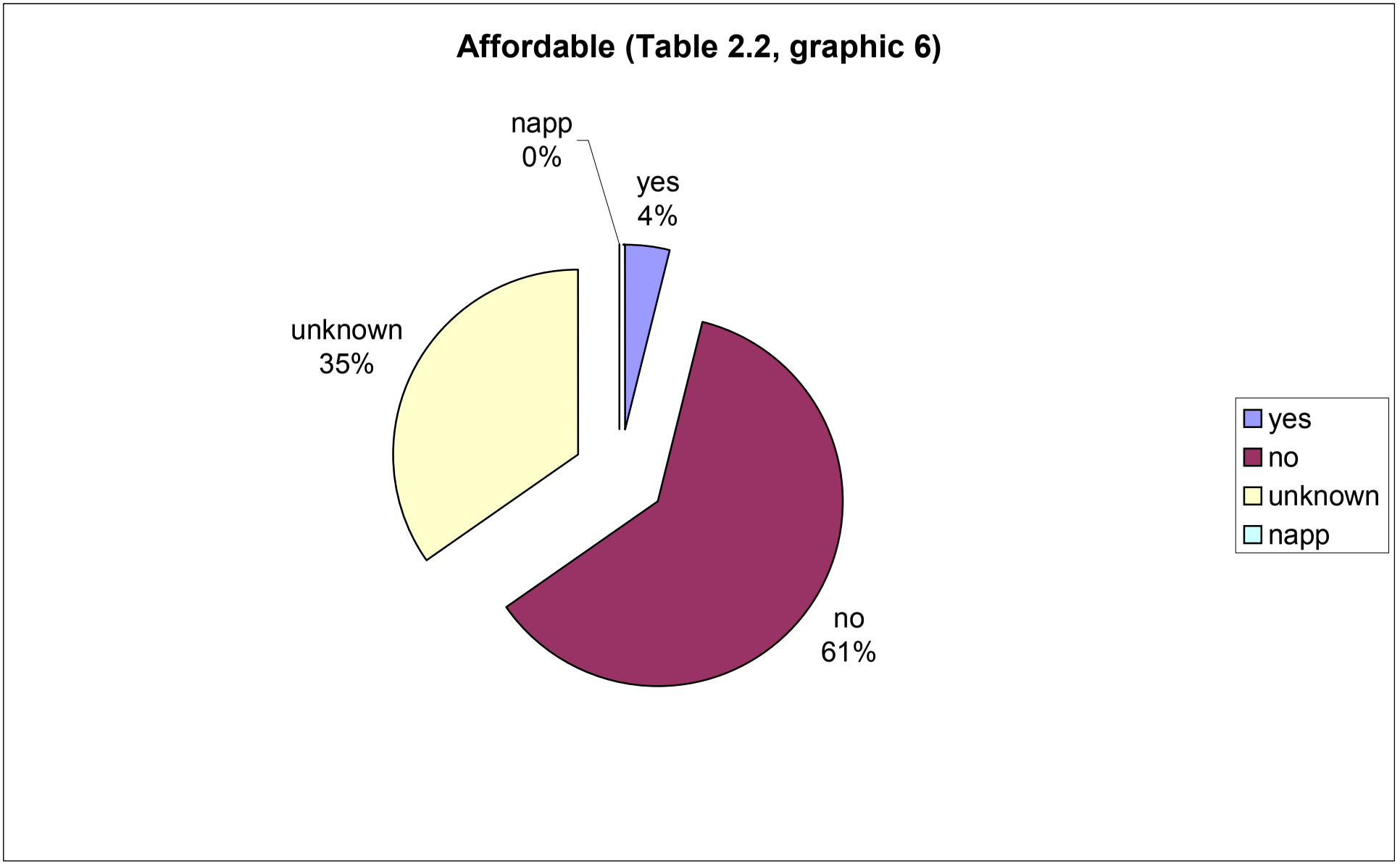
## Clear (Table 2.2, graphic 3)

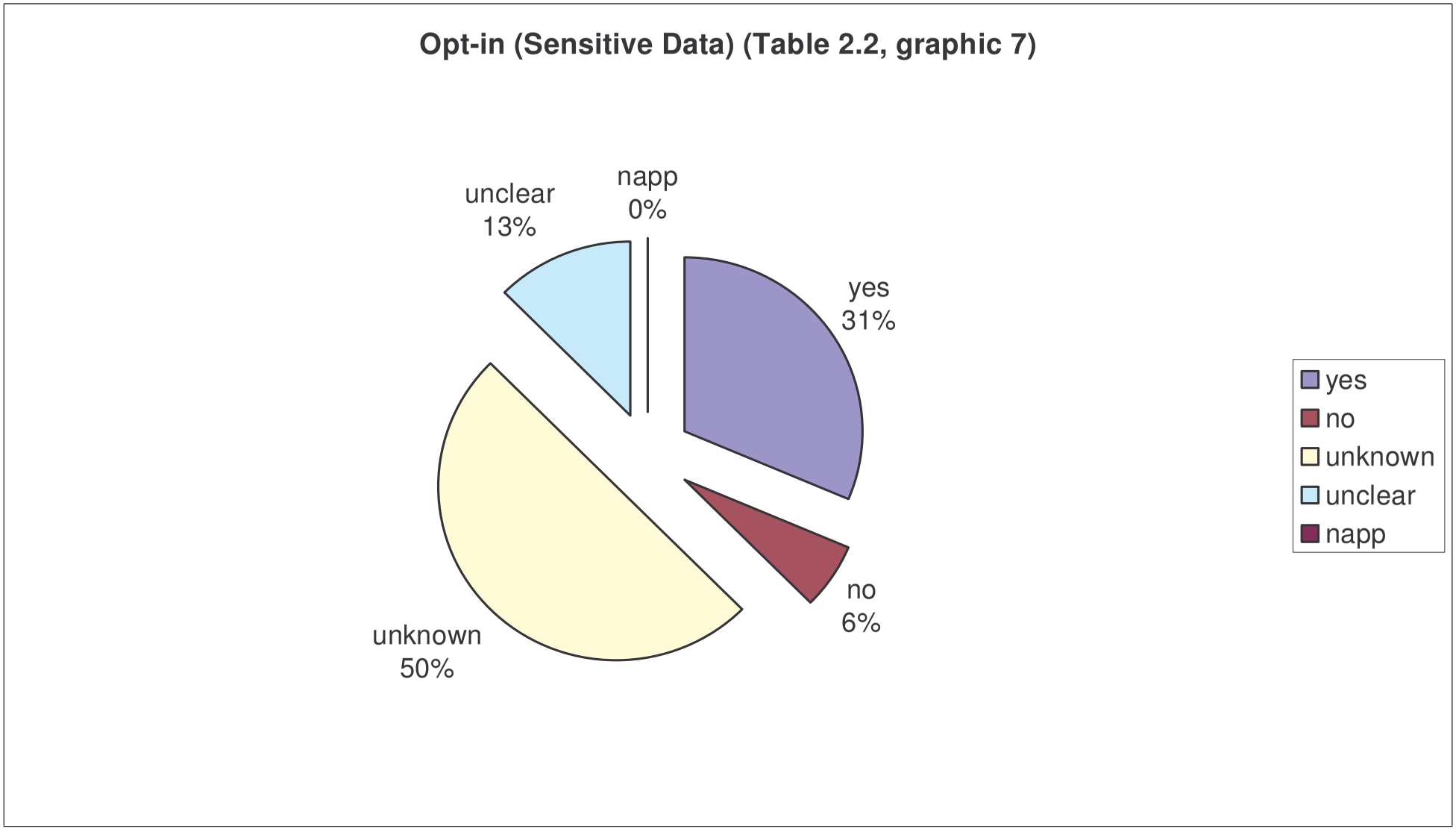


## Conspicuous (Table 2.2, graphic 4)



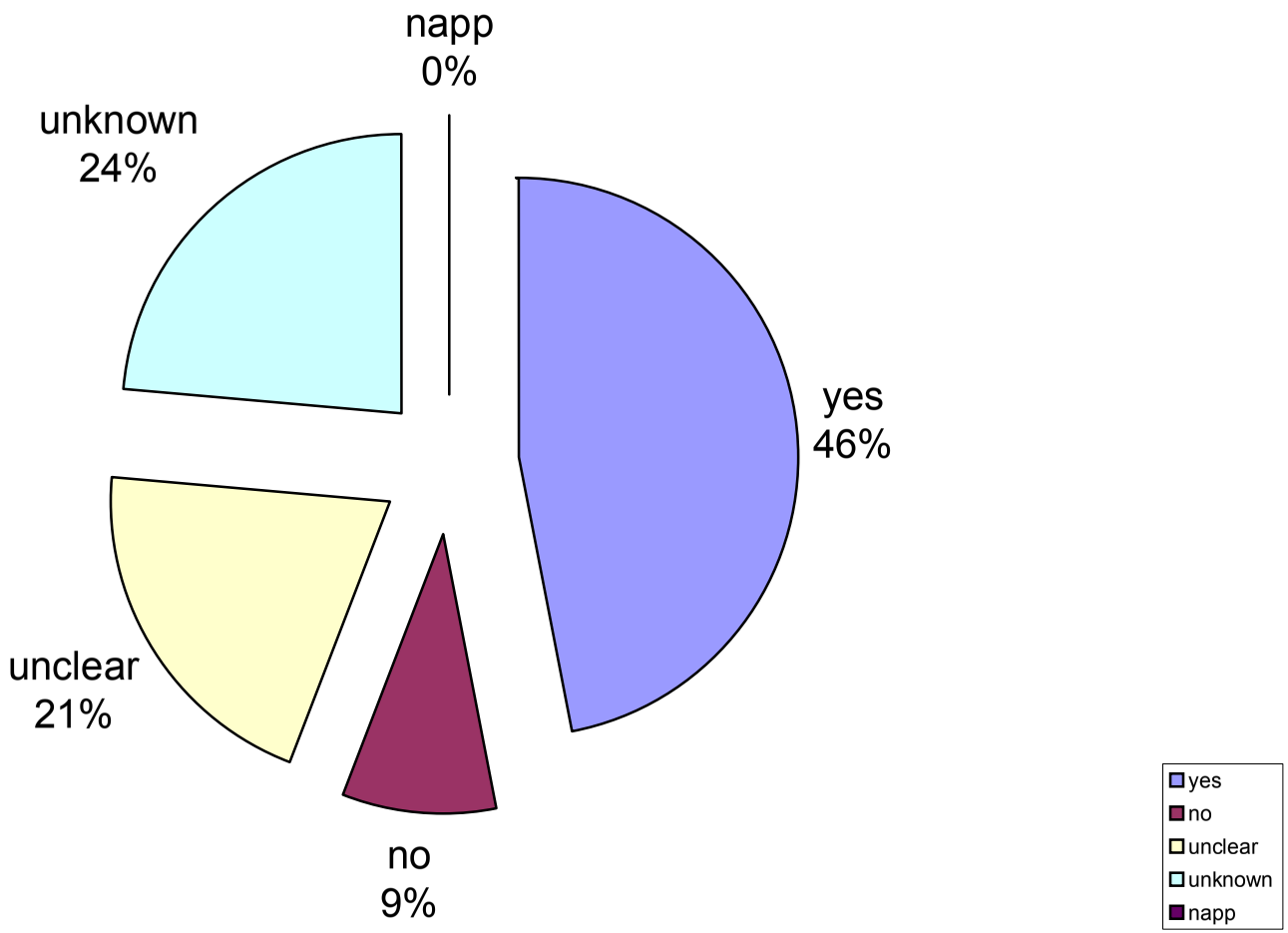

Readily Available (Table 2.2, graphic 5)
napp
0%
yes
15%
unknown
31%
no
54%
yes
no
unknown
napp


Affordable (Table 2.2, graphic 6)
napp
0%
yes
4%
unknown
35%
no
61%
yes
no
unknown
napp

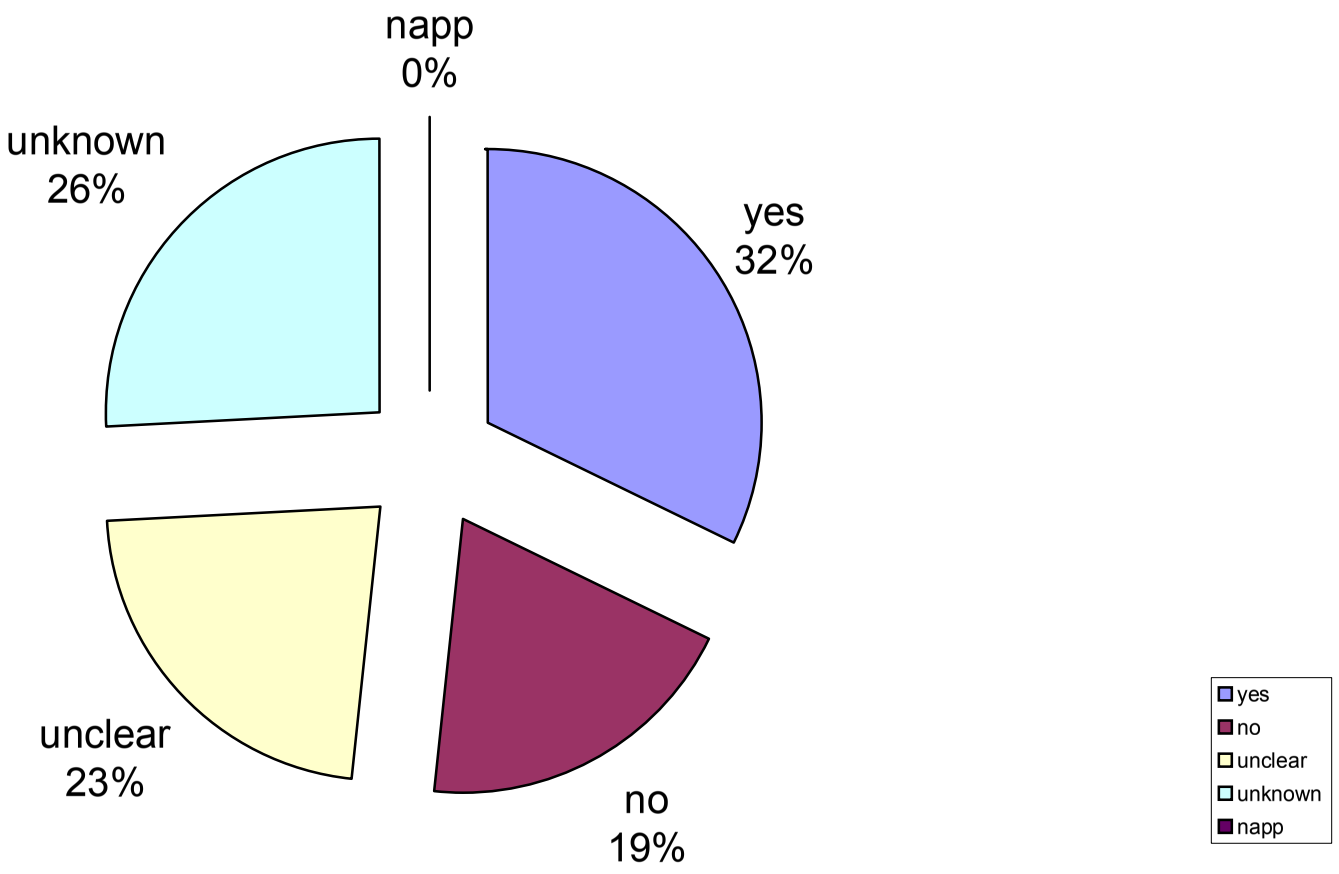

Opt-in (Sensitive Data) (Table 2.2, graphic 7)
napp
0%
unclear
13%
yes
31%
no
6%
unknown
50%
yes
no
unknown
unclear
napp

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table 2.3: Company Compliance with Onward Transfer Principle (as of November 3, 2003)** | | | | | | | | |
| 2 | *Company* | | *Notice of Onward Transfers* | *Choice* | *3rd Party Processor's Commitment to SH* | | | | |
| 3 | 1 | | yes | No | unclear | | | | |
| 4 | 2 | | unknown | unknown | unknown | | | | |
| 5 | 3 | | unclear | unclear | napp | | | | |
| 6 | 4 | | not applicable | Not applicable | not applicable | | | | |
| 7 | 5 | | unknown | unknown | unknown | | | | |
| 8 | 6 | | unclear | unclear | napp | | | | |
| 9 | 7 | | unknown | unknown | unknown | | | | |
| 10 | 8 | | not applicable | not applicable | not applicable | | | | |
| 11 | 9 | | yes | yes | napp | | | | |
| 12 | 10 | | yes | yes | napp | | | | |
| 13 | 11 | | unclear | unclear | napp | | | | |
| 14 | 12 | | yes | no | napp | | | | |
| 15 | 13 | | no | napp | yes | | | | |
| 16 | 14 | | yes | no | napp | | | | |
| 17 | 15 | | no | napp | napp | | | | |
| 18 | 16 | | not applicable | not applicable | not applicable | | | | |
| 19 | 17 | | no | napp | no | | | | |
| 20 | 18 | | unknown | unknown | unknown | | | | |
| 21 | 19 | | yes | yes | yes | | | | |
| 22 | 20 | | unclear | unclear | napp | | | | |
| 23 | 21 | | not applicable | not applicable | no | | | | |
| 24 | 22 | | yes | unclear | no | | | | |
| 25 | 23 | | unknown | unknown | unknown | | | | |
| 26 | 24 | | unclear | no | no | | | | |
| 27 | 25 | | unknown | unknown | unknown | | | | |
| 28 | 26 | | yes | no | no | | | | |
| 29 | 27 | | yes | unclear | unclear | | | | |
| 30 | 28 | | unknown | unknown | unknown | | | | |
| 31 | 29 | | unknown | unknown | unknown | | | | |
| 32 | 30 | | yes | yes | yes | | | | |
| 33 | 31 | | yes | yes | yes | | | | |
| 34 | 32 | | not applicable | not applicable | not applicable | | | | |
| 35 | 33 | | not applicable | not applicable | not applicable | | | | |
| 36 | 34 | | yes | yes | yes | | | | |
| 37 | 35 | | yes | yes | napp | | | | |
| 38 | 36 | | yes | yes | yes | | | | |
| 39 | 37 | | not applicable | not applicable | not applicable | | | | |
| 40 | 38 | | unclear | no | no | | | | |
| 41 | 39 | | unclear | unclear | no | | | | |
| 42 | 40 | | yes | yes | no | | | | |
| 43 | 41 | | yes | yes | no | | | | |

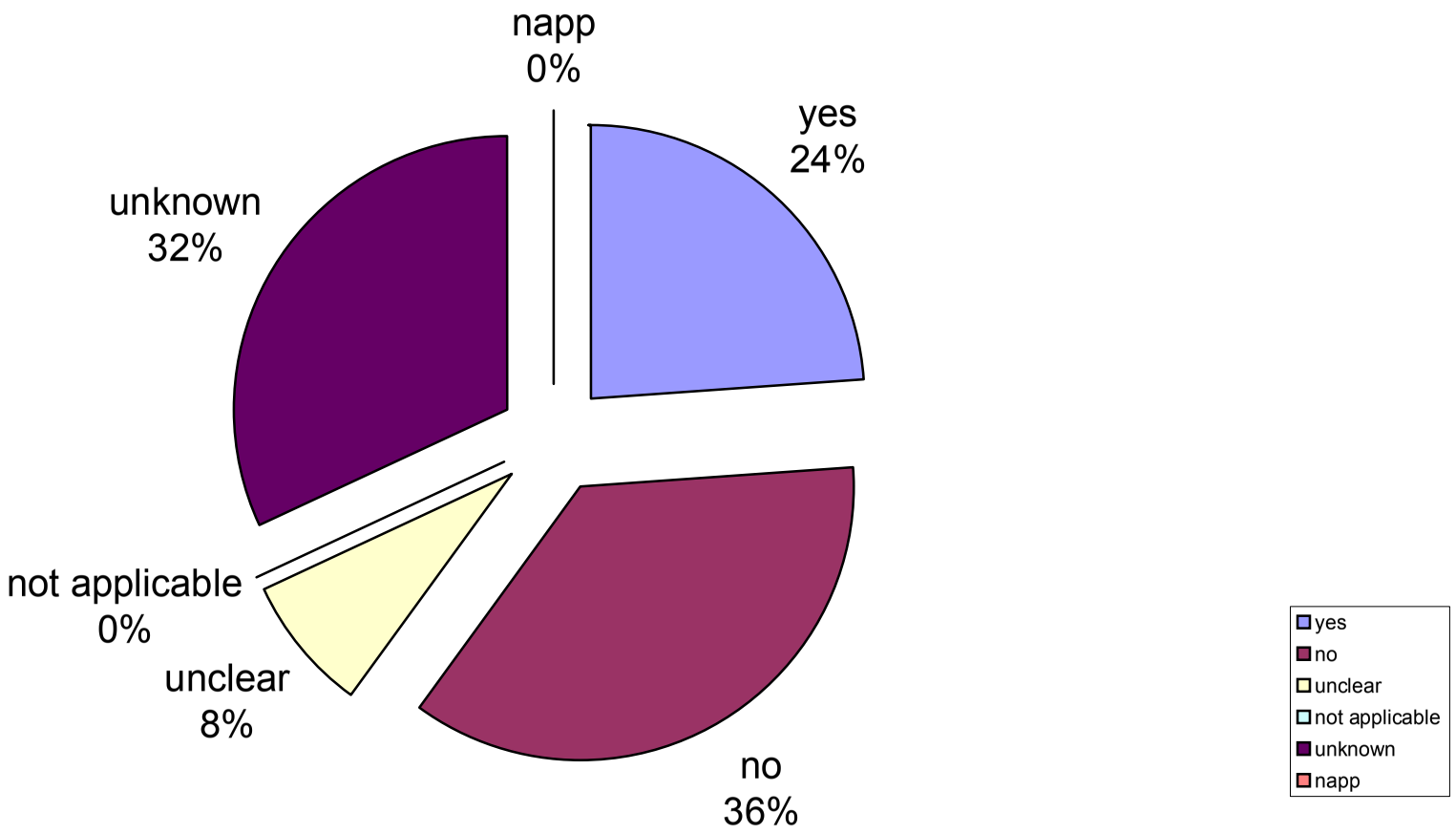
## Notice of Onward Transfers (Table 2.3, graphic 1)



## Choice (Table 2.3, graphic 2)



## Third Party Processor's Commitment to SH
## (Table 2.3, graphic 3)



| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | **Table 2.4: Company Compliance with Security & Integrity Principles (as of November 3, 2003)** | | | | | |
| 2 | *Company* | | *Reasonable Security Precautions* | *Relevance of Data for Specified Purpose* | *Compatible/ Authorized Processing for secondary use* | *Steps to Ensure Reliability for intended use* |
| 3 | 1 | | no | unclear | napp | no |
| 4 | 2 | | unknown | unknown | unknown | unknown |
| 5 | 3 | | yes | unclear | napp | yes |
| 6 | 4 | | unknown | not applicable | not applicable | not applicable |
| 7 | 5 | | unknown | unknown | unknown | unknown |
| 8 | 6 | | no | unclear | napp | no |
| 9 | 7 | | unknown | unknown | unknown | unknown |
| 10 | 8 | | no | not applicable | not applicable | not applicable |
| 11 | 9 | | no | unclear | napp | no |
| 12 | 10 | | yes | no | yes | no |
| 13 | 11 | | yes | yes | napp | yes |
| 14 | 12 | | yes | unclear | yes | yes |
| 15 | 13 | | yes | unclear | no | no |
| 16 | 14 | | no | unclear | no | no |
| 17 | 15 | | no | unclear | napp | no |
| 18 | 16 | | yes | not applicable | not applicable | not applicable |
| 19 | 17 | | yes | unclear | yes | yes |
| 20 | 18 | | unknown | unknown | unknown | unknown |
| 21 | 19 | | yes | unclear | yes | yes |
| 22 | 20 | | yes | unclear | napp | no |
| 23 | 21 | | unknown | not applicable | not applicable | not applicable |
| 24 | 22 | | yes | yes | napp | yes |
| 25 | 23 | | unknown | unknown | unknown | unknown |
| 26 | 24 | | yes | no | unclear | yes |
| 27 | 25 | | unknown | unknown | unknown | unknown |
| 28 | 26 | | yes | unclear | napp | no |
| 29 | 27 | | unclear | unclear | unclear | unclear |
| 30 | 28 | | unknown | unknown | unknown | unknown |
| 31 | 29 | | unknown | unknown | unknown | unknown |
| 32 | 30 | | yes | yes | napp | yes |
| 33 | 31 | | yes | yes | yes | yes |
| 34 | 32 | | unknown | not applicable | not applicable | not applicable |
| 35 | 33 | | yes | not applicable | not applicable | not applicable |
| 36 | 34 | | yes | yes | yes | yes |
| 37 | 35 | | yes | unclear | yes | no |
| 38 | 36 | | yes | unclear | yes | yes |
| 39 | 37 | | unclear | not applicable | not applicable | not applicable |
| 40 | 38 | | yes | unclear | yes | no |
| 41 | 39 | | yes | unclear | napp | no |
| 42 | 40 | | no | unclear | napp | no |
| 43 | 41 | | unclear | unclear | napp | no |

**Cellule:** C2
**Commentaire:** SH Security Principle requires that organizations take "reasonable precautions to protect [data] from loss, misuse and unauthorized access, disclosure, alteration and destruction. " Any site stating that it uses encryption to transmit data will qualify under this SH principle.

**Cellule:** D2
**Commentaire:** SH Data Integrity Principle requires that "personal information must be relevant for the purposes for which it is to be used." The policy must indicate in some way that the data is relevant for the specified purpose.

**Cellule:** E2
**Commentaire:** SH Data Integrity Principle provides "An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual."

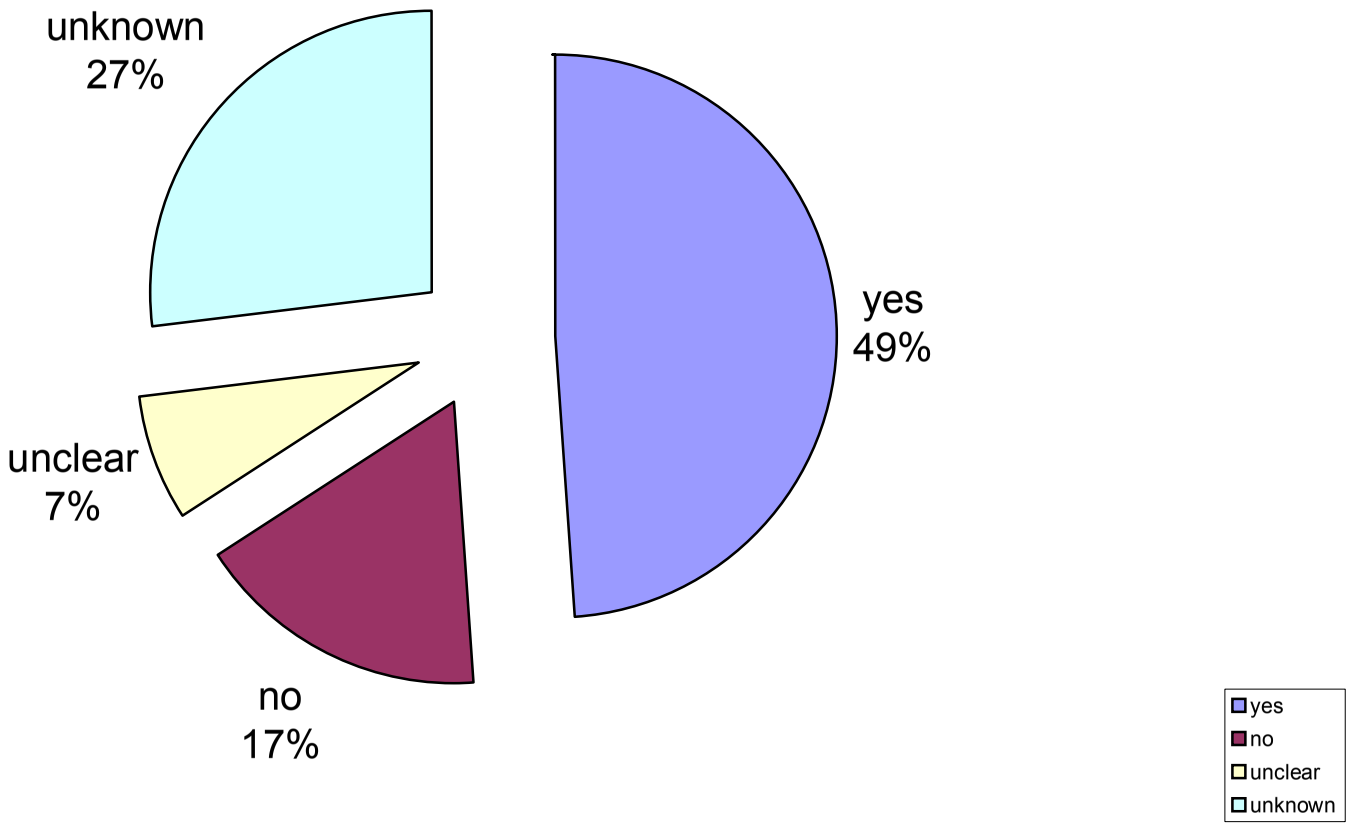
**Cellule:** F2
**Commentaire:** SH Data Integrity Principle requires that "an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current."

**Cellule:** F22
**Commentaire:** no representation made

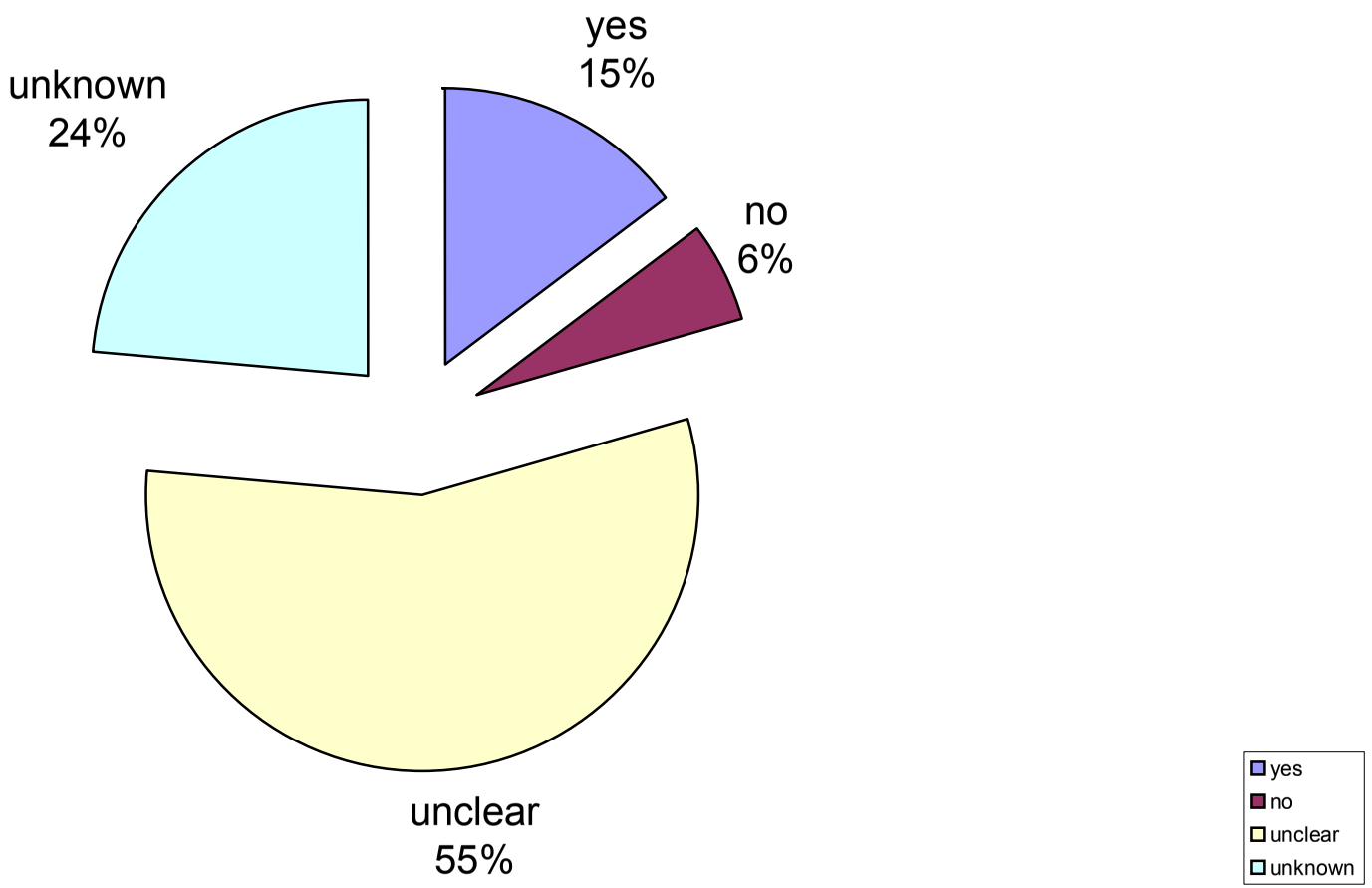
**Cellule:** C39
**Commentaire:** security entry is drafted as an exonoration clause in case X's clients would violate security

**Cellule:** C43
**Commentaire:** only representation about password protection

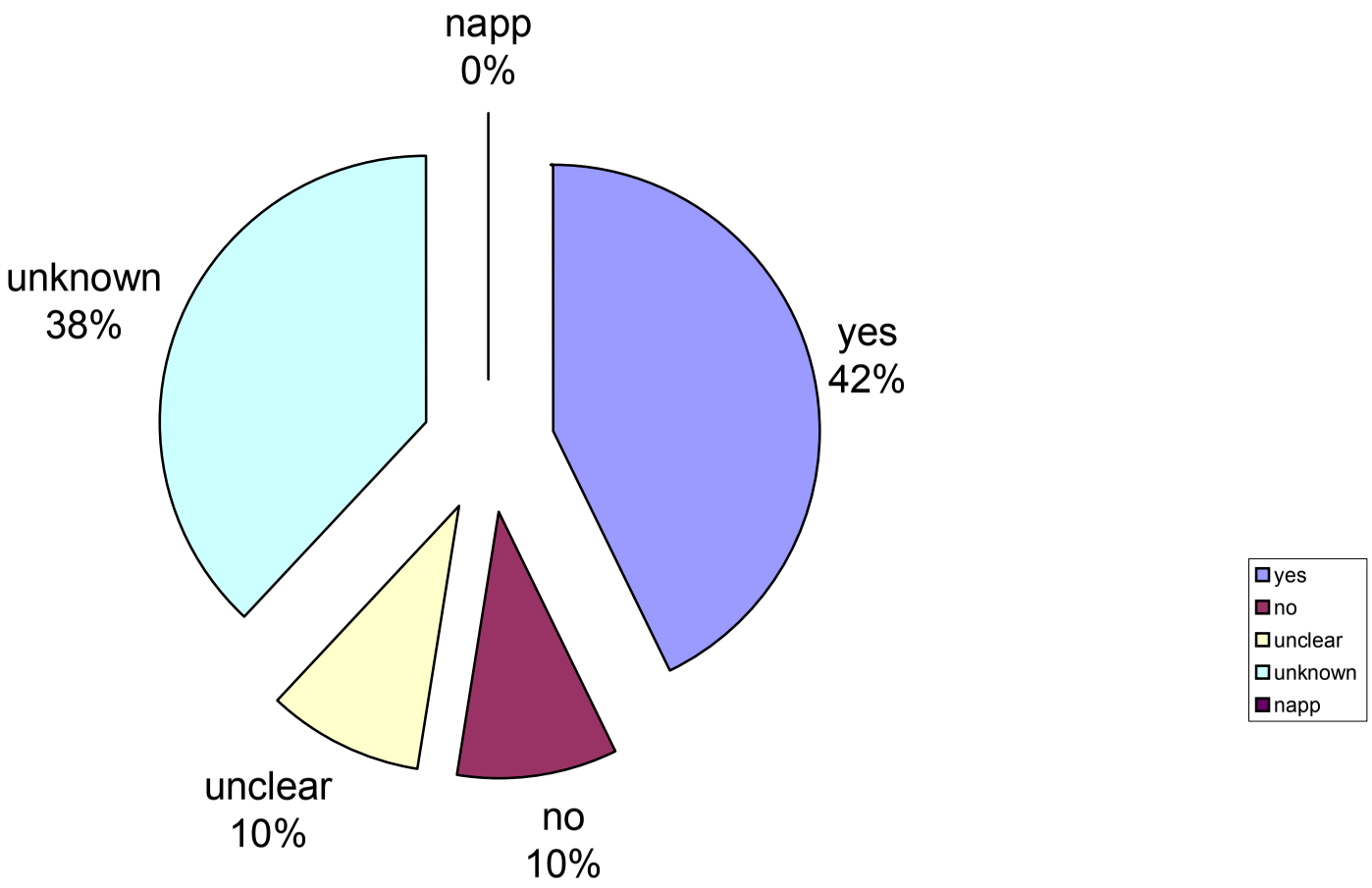
## Reasonable Security Precautions (Table 2.4, graphic 1)



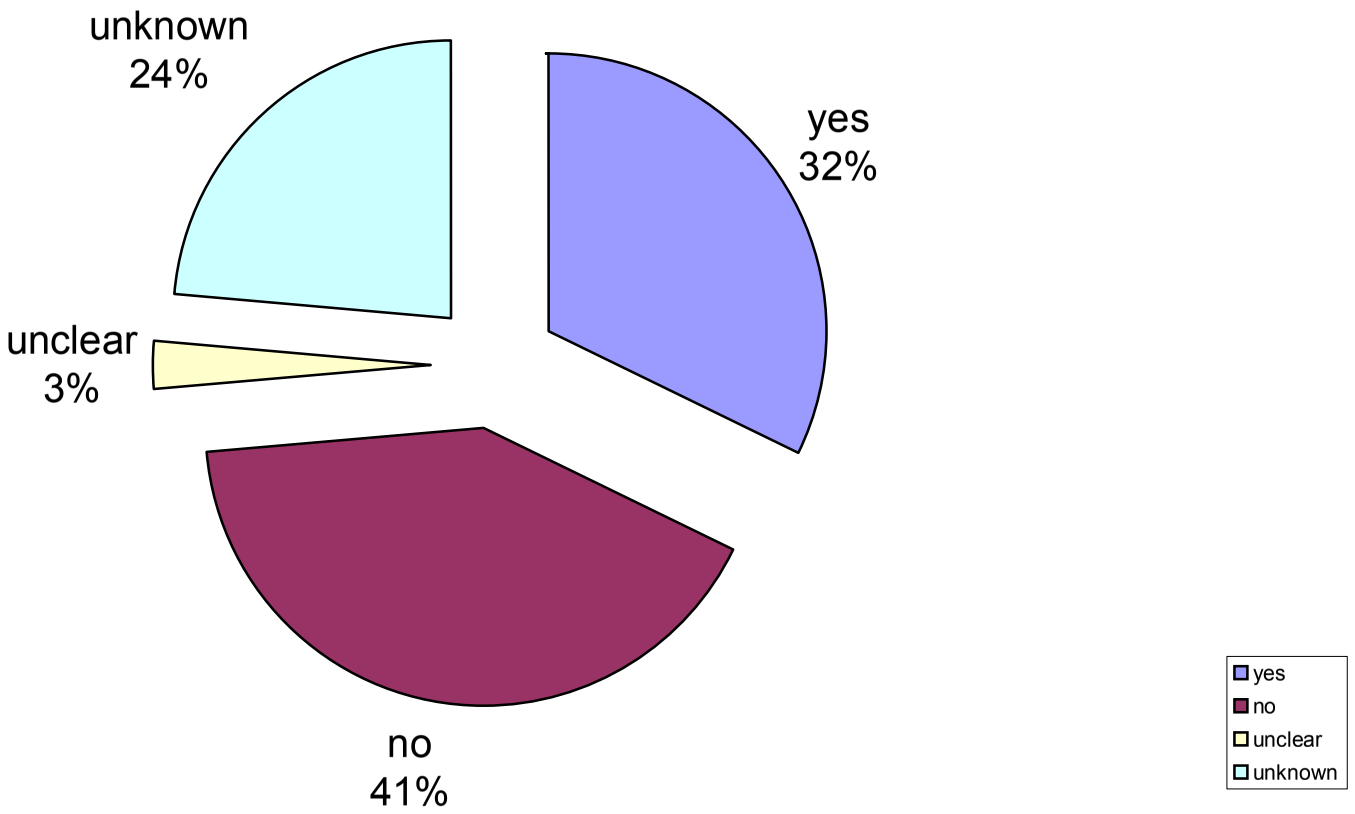
## Relevance of Data for Specified Purpose
## (Table 2.4, graphic 2)



## Compatible/Authorized Processing for Secondary use
## (Table 2.4, graphic 3)



## Steps to Eunsure Reliability for Intended use (Table 2.4, graphic 4)



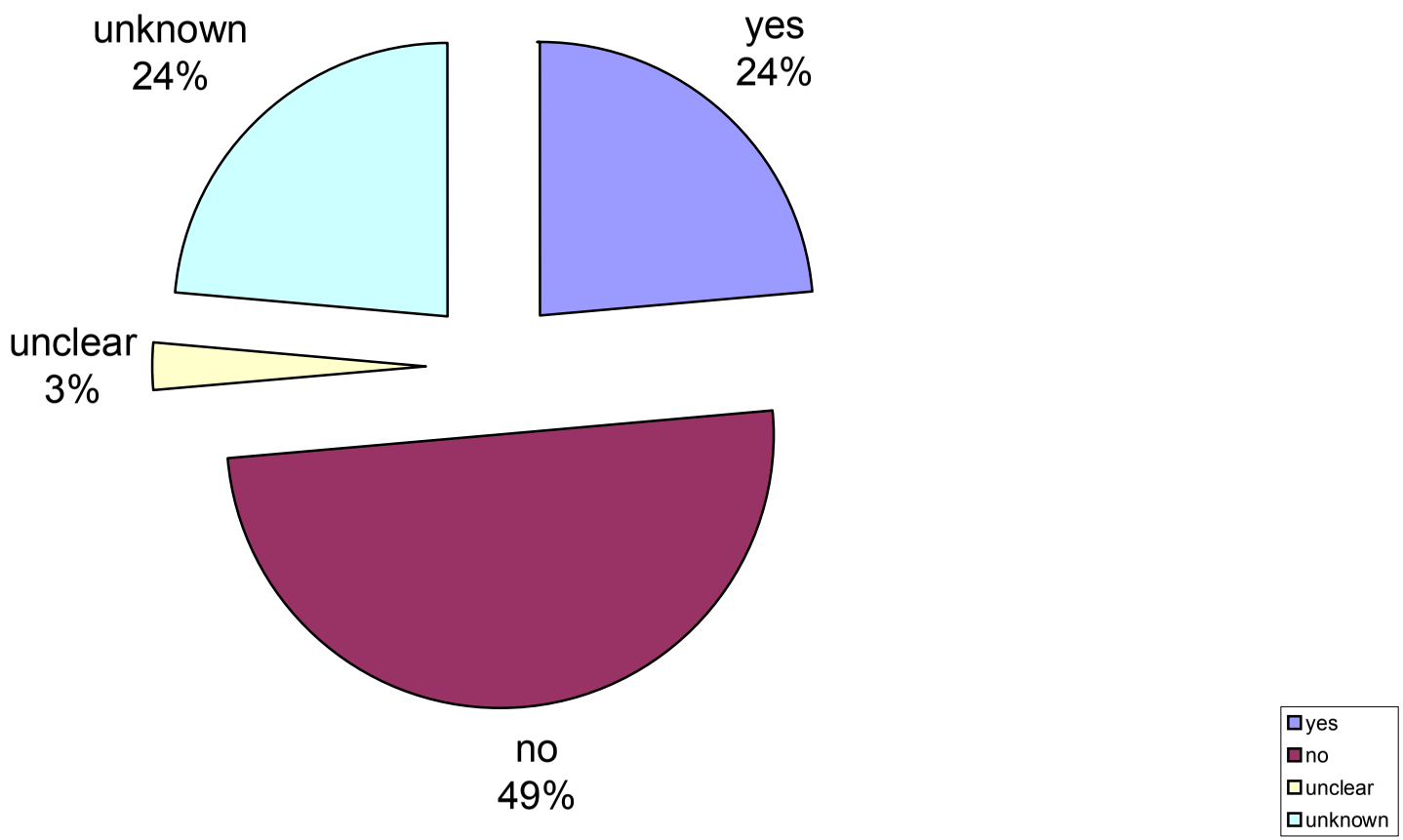
| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | **Table 2.5: Company Compliance with Access Principle (as of November 3, 2003)** | | | | | |
| 2 | *Company* | | *Reasonable Access Provided* | *Reasonable Cost for Access* | *Correction / Amendment of inaccurate data* | *Deletion of inaccurate data* |
| 3 | 1 | | no | napp | no | no |
| 4 | 2 | | unknown | unknown | unknown | unknown |
| 5 | 3 | | no | napp | no | no |
| 6 | 4 | | not applicable | not applicable | not applicable | not applicable |
| 7 | 5 | | unknown | unknown | unknown | unknown |
| 8 | 6 | | no | not app | no | no |
| 9 | 7 | | unknown | unknown | unknown | unknown |
| 10 | 8 | | not applicable | not applicable | not applicable | not applicable |
| 11 | 9 | | no | napp | no | no |
| 12 | 10 | | no | no | yes | no |
| 13 | 11 | | no | no | yes | no |
| 14 | 12 | | no | no | yes | yes |
| 15 | 13 | | no | napp | yes | no |
| 16 | 14 | | no | napp | no | no |
| 17 | 15 | | no | napp | no | no |
| 18 | 16 | | not applicable | not applicable | not applicable | not applicable |
| 19 | 17 | | yes | no | yes | yes |
| 20 | 18 | | unknown | unknown | unknown | unknown |
| 21 | 19 | | unclear | no | yes | yes |
| 22 | 20 | | no | napp | yes | no |
| 23 | 21 | | not applicable | not applicable | not applicable | not applicable |
| 24 | 22 | | no | napp | no | no |
| 25 | 23 | | unknown | unknown | unknown | unknown |
| 26 | 24 | | yes | no | unclear | unclear |
| 27 | 25 | | unknown | unknown | unknown | unknown |
| 28 | 26 | | no | napp | yes | yes |
| 29 | 27 | | yes | no | yes | yes |
| 30 | 28 | | unknown | unknown | unknown | unknown |
| 31 | 29 | | unknown | unknown | unknown | unknown |
| 32 | 30 | | yes | no | yes | no |
| 33 | 31 | | yes | no | yes | yes |
| 34 | 32 | | not applicable | not applicable | not applicable | not applicable |
| 35 | 33 | | not applicable | not applicable | not applicable | not applicable |
| 36 | 34 | | yes | no | yes | yes |
| 37 | 35 | | yes | no | yes | no |
| 38 | 36 | | yes | no | yes | yes |
| 39 | 37 | | not applicable | not applicable | not applicable | not applicable |
| 40 | 38 | | no | napp | yes | no |
| 41 | 39 | | no | napp | yes | no |
| 42 | 40 | | no | napp | no | no |
| 43 | 41 | | no | no | unclear | unclear |

**Cellule:** C12
**Commentaire:** The access is conditioned to specific situations

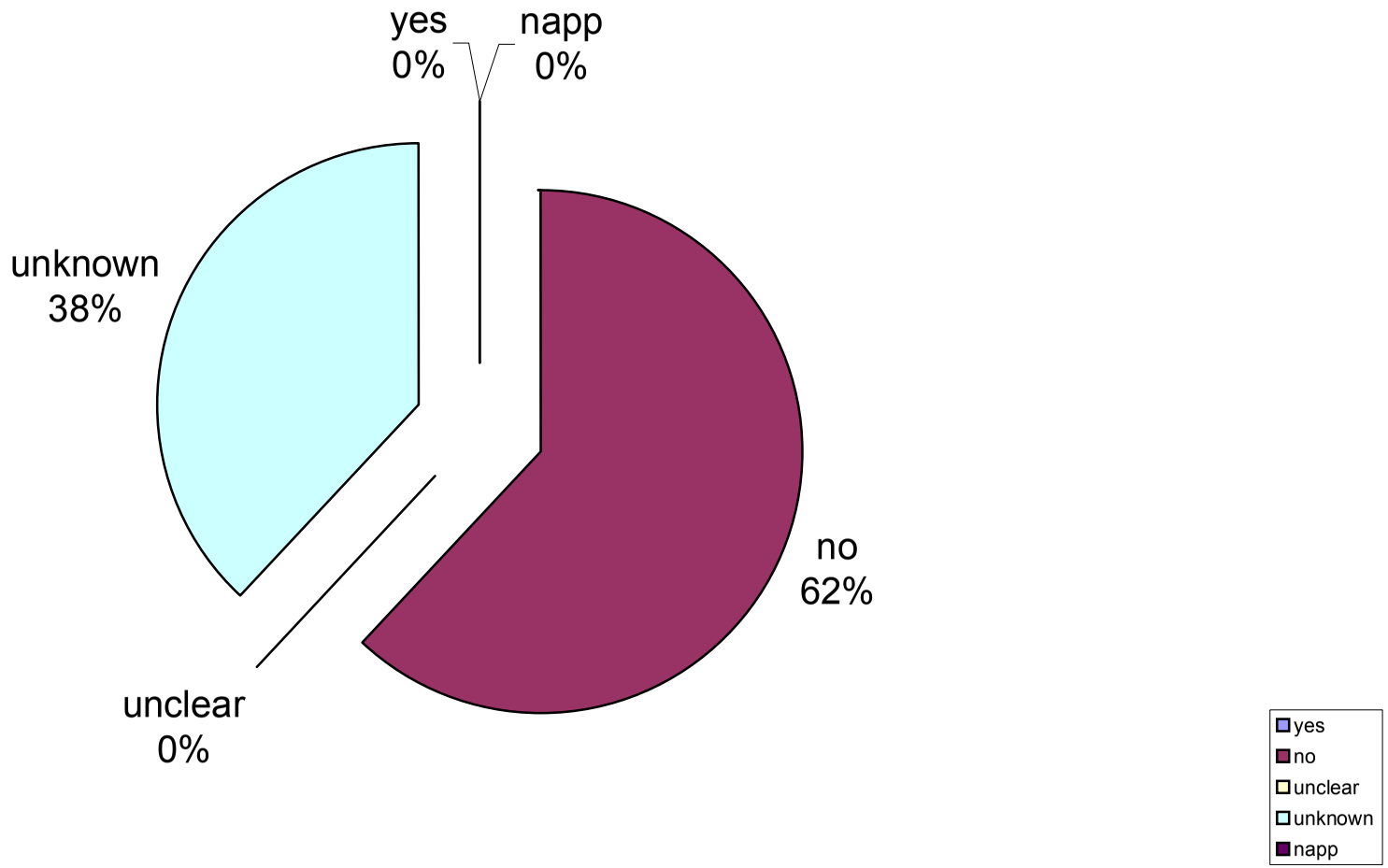
**Cellule:** F13
**Commentaire:** " changing and modifying information previously provided",

**Cellule:** C43
**Commentaire:** access to "my account".  Quid about access to user profiles, etc.

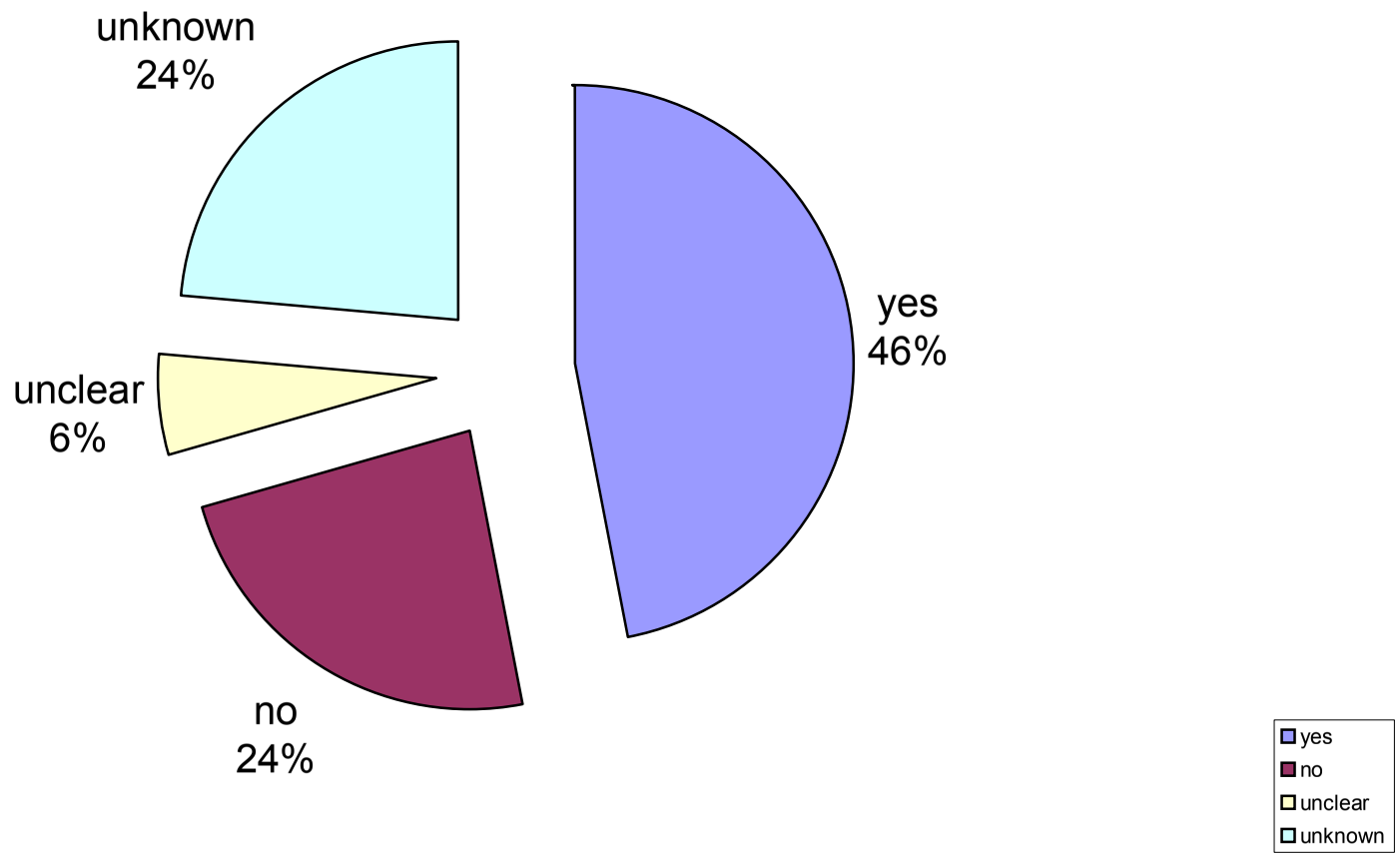
## Reasonable Access Provided (Table 2.5, graphic 1)



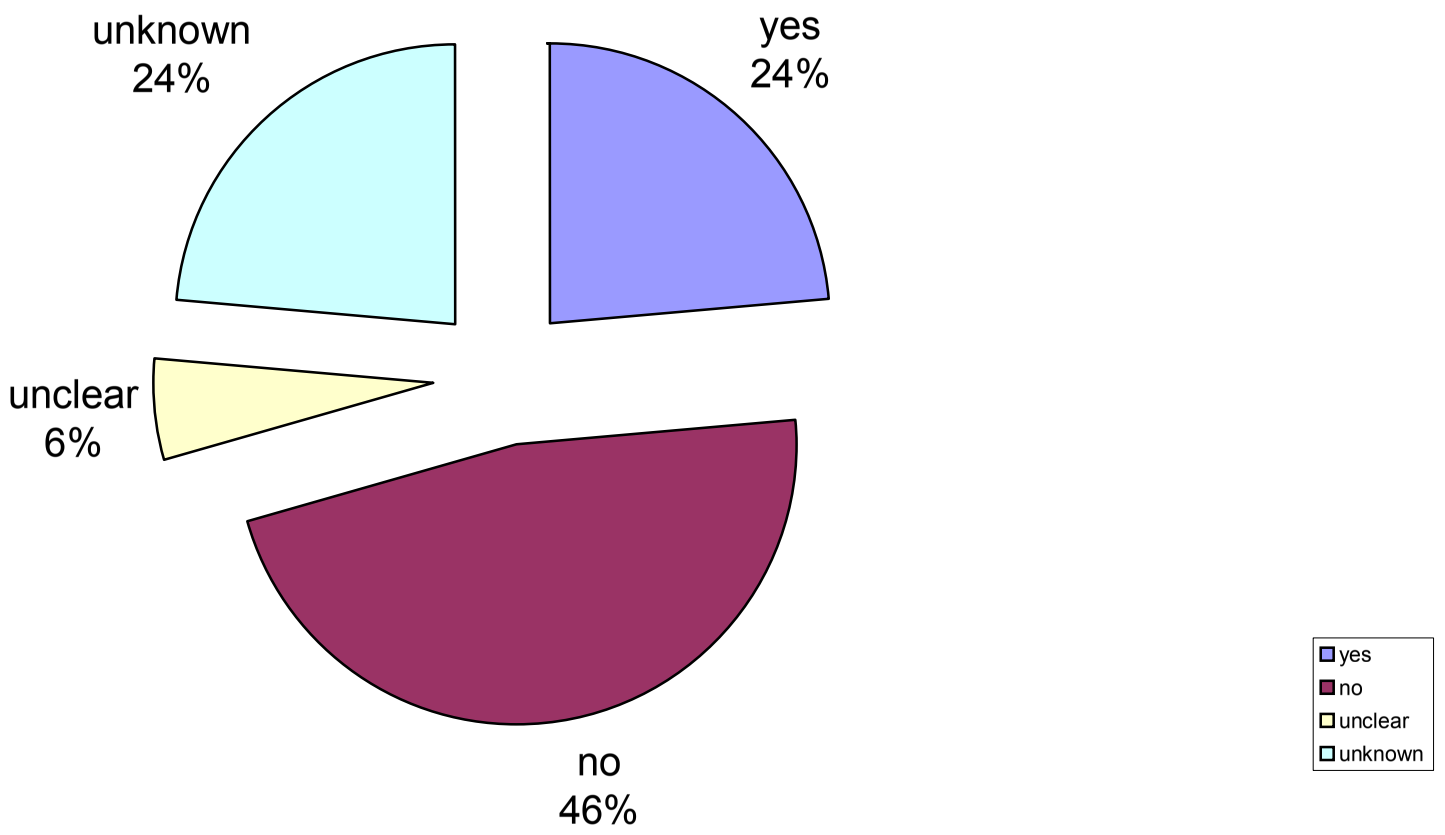
## Reasonable Cost for Access (Table 2.5, graphic 2)



## Correction/Amendment of inaccurate data (Table 2.5, graphic 3)



## Deletion of inaccurate data (Table 2.5, graphic 4)



| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | **Table 3.1: Company Satisfaction of SH Enforcement Principles (as of November 3, 2003)** | | | | | | |
| 2 | *Company* | | *Independent Recourse Mechanisms pursuant to FAQ 5* | *Independent Recourse Mechanisms pursuant to FAQ 11* | *Verification of Policy Statements/ Implementation* | *Obligation to remedy problem* | *Sanctions for Violations* |
| 3 | 1 | | yes | DPA | 08/12/2004 | no | no |
| 4 | 2 | | yes | DPA | 25/02/2004 | unknown | unknown |
| 5 | 3 | | no | AAA | 19/08/2004 | unclear | no |
| 6 | 4 | | no | DMAshp | 27/11/2003 | not applicable | not applicable |
| 7 | 5 | | yes | DPA | 24/05/2004 | unknown | unknown |
| 8 | 6 | | yes | DPA | 06/03/2004 | no | no |
| 9 | 7 | | yes | BBB & DPA | 27/01/2004 | no | no |
| 10 | 8 | | no | BBB | 09/04/2004 | not applicable | not applicable |
| 11 | 9 | | yes | DPA | 20/09/2004 | no | no |
| 12 | 10 | | no | TRUSTe & BBB | 07/01/2004 | unclear | unclear |
| 13 | 11 | | yes | DPA | 03/07/2004 | yes | yes |
| 14 | 12 | | yes | DPA & TRUSTe | 15/01/2004 | unclear | unclear |
| 15 | 13 | | yes | DPA & AAA | 06/03/2003 | no | no |
| 16 | 14 | | yes | DPA | 15/11/2003 | no | no |
| 17 | 15 | | yes | DPA | 18/06/2003 | no | no |
| 18 | 16 | | no | DMAshp | 05/09/2004 | not applicable | not applicable |
| 19 | 17 | | yes | DPA | 27/02/2004 | yes | yes |
| 20 | 18 | | yes | TRUSTe DPA | 04/12/2003 | unclear | unclear |
| 21 | 19 | | yes | DPA | 09/10/2004 | no | no |
| 22 | 20 | | no | TRUSTe | 20/05/2004 | unclear | unclear |
| 23 | 21 | | yes | DPA | 06/12/2003 | not applicable | not applicable |
| 24 | 22 | | yes | DPA & TRUSTe | 15/04/2002 | unclear | unclear |
| 25 | 23 | | yes | DPA | 03/07/2003 | unknown | Unknown |
| 26 | 24 | | yes | DPA | 27/05/2004 | no | no |
| 27 | 25 | | yes | DPA | 07/02/2004 | unknown | unknown |
| 28 | 26 | | yes | DPA | 08/03/2003 | no | no |
| 29 | 27 | | yes | DPA | 17/9/2004 | no | no |
| 30 | 28 | | yes | DPA | 07/12/2004 | unknown | unknown |
| 31 | 29 | | no | DMAshp | 28/01/2004 | unclear | yes |
| 32 | 30 | | yes | DPA & TRUSTe | 25/06/2004 | unclear | unclear |
| 33 | 31 | | yes | DPA | 24/02/2004 | no | no |
| 34 | 32 | | yes | DPA | 16/05/2004 | not applicable | not applicable |
| 35 | 33 | | no | AAA | 2805/2004 | not applicable | not applicable |
| 36 | 34 | | yes | DPA | 22/03/2004 | yes | yes |
| 37 | 35 | | no | TRUSTe | 03/12/2004 | unclear | unclear |
| 38 | 36 | | yes | DPA | 07/01/2003 | no | no |
| 39 | 37 | | yes | DPA | 15/03/2004 | not applicable | not applicable |
| 40 | 38 | | yes | DPA | 13/06/2004 | no | no |
| 41 | 39 | | yes | DPA & TRUSTe | 23/10/2004 | unclear | unclear |
| 42 | 40 | | no | DMA | 04/09/2004 | no | no |
| 43 | 41 | | yes | DPA | 29/05/2001 | no | yes |

**Cellule:** D2
**Commentaire:** SH Enforcement Principle requires "readily available and affordable independent recourse mechanisms." This element of the SH may be satisfied pursuant to FAQ5 or FAQ 11.

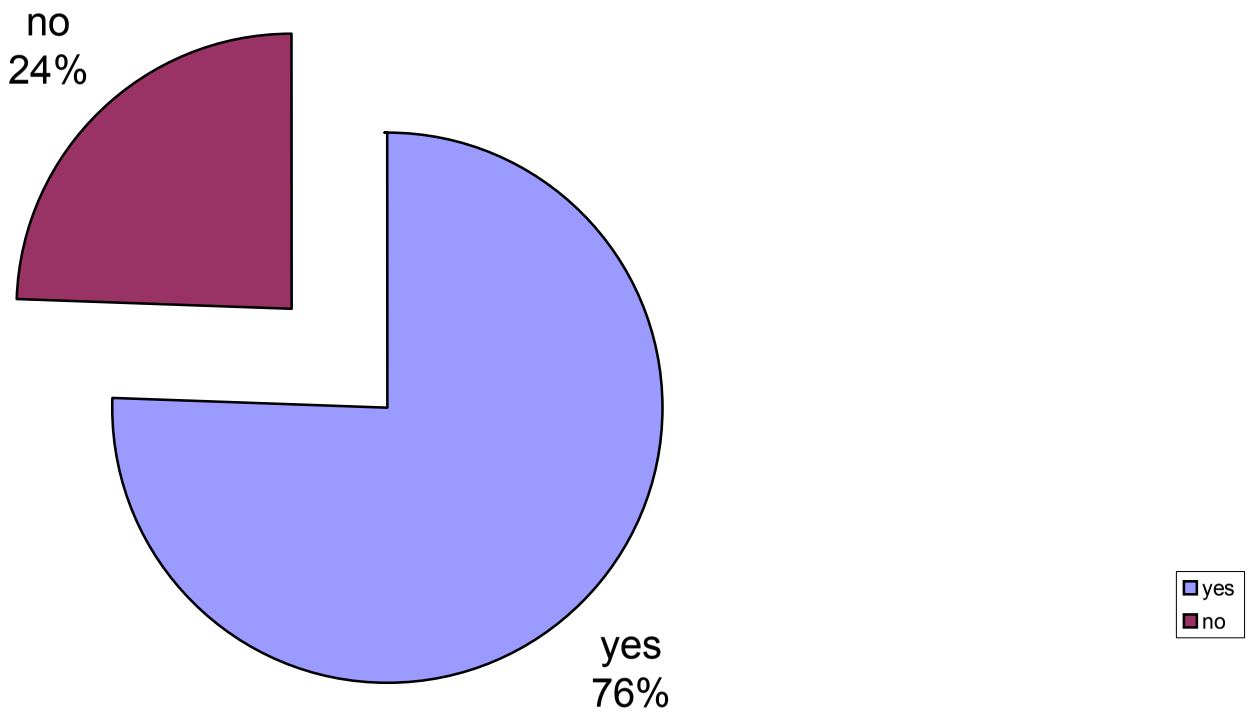
**Cellule:** E2
**Commentaire:** SH Enforcement Principles requires that organizations verify the statements made in their policy certifications and the implementation of their policies at least once a year. This column shows the deadline for the first verification.

**Cellule:** F2
**Commentaire:** SH Enforcement Principle states that enforcement must include "obligations to remedy problems arising out of failure to comply with the Principles."

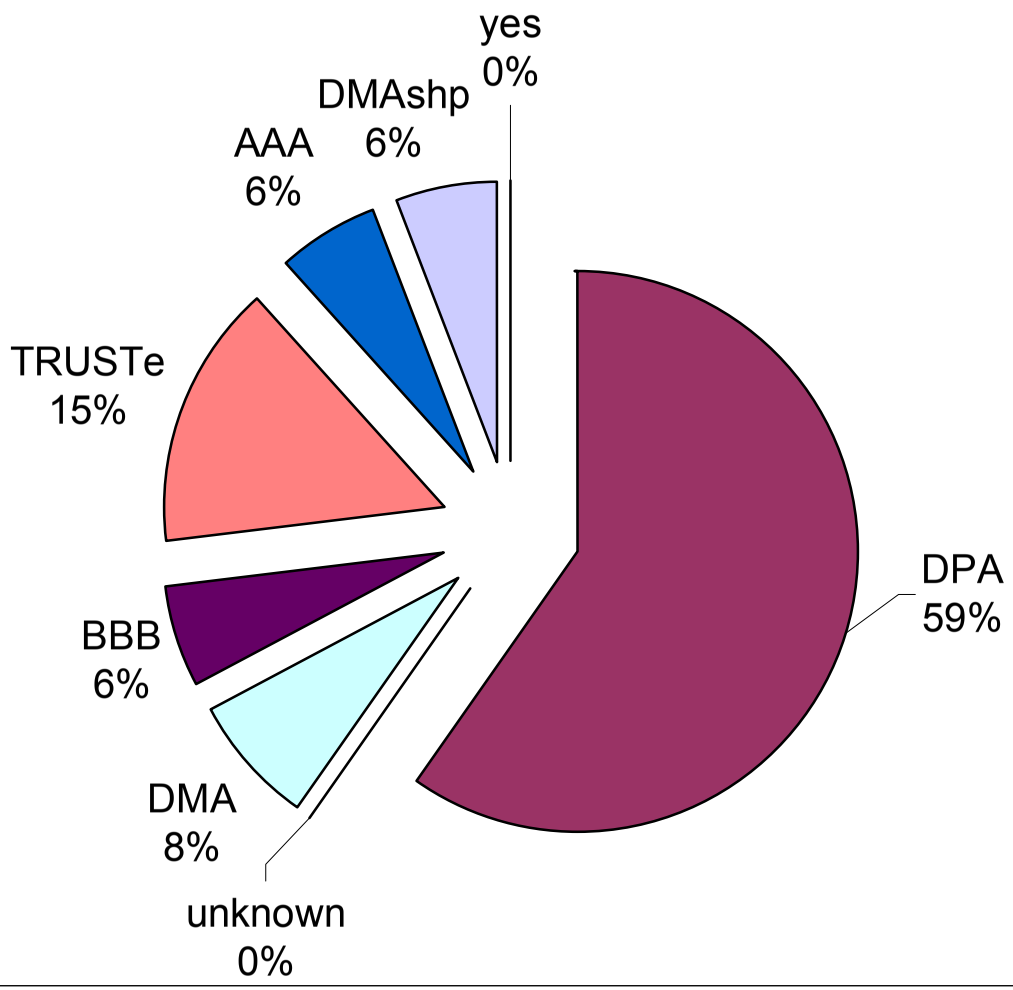
**Cellule:** G2
**Commentaire:** SH Enforcement Principle requires that "sanctions must be sufficiently rigorous to ensure compliance by organizations." Any company that has elected DPA as a recourse mechanism, but that does not fully satisfy FAQ 5, cannot satisfy the sanctions requirement.

**Cellule:** G9
**Commentaire:** Even if BBB foresees sanctions, the company only adheres to BBB for the data it receives as processor, then, where there's no a real obligation of enforcement. However, in the privacy policy dealing with HR data nothing is represented in this regard.

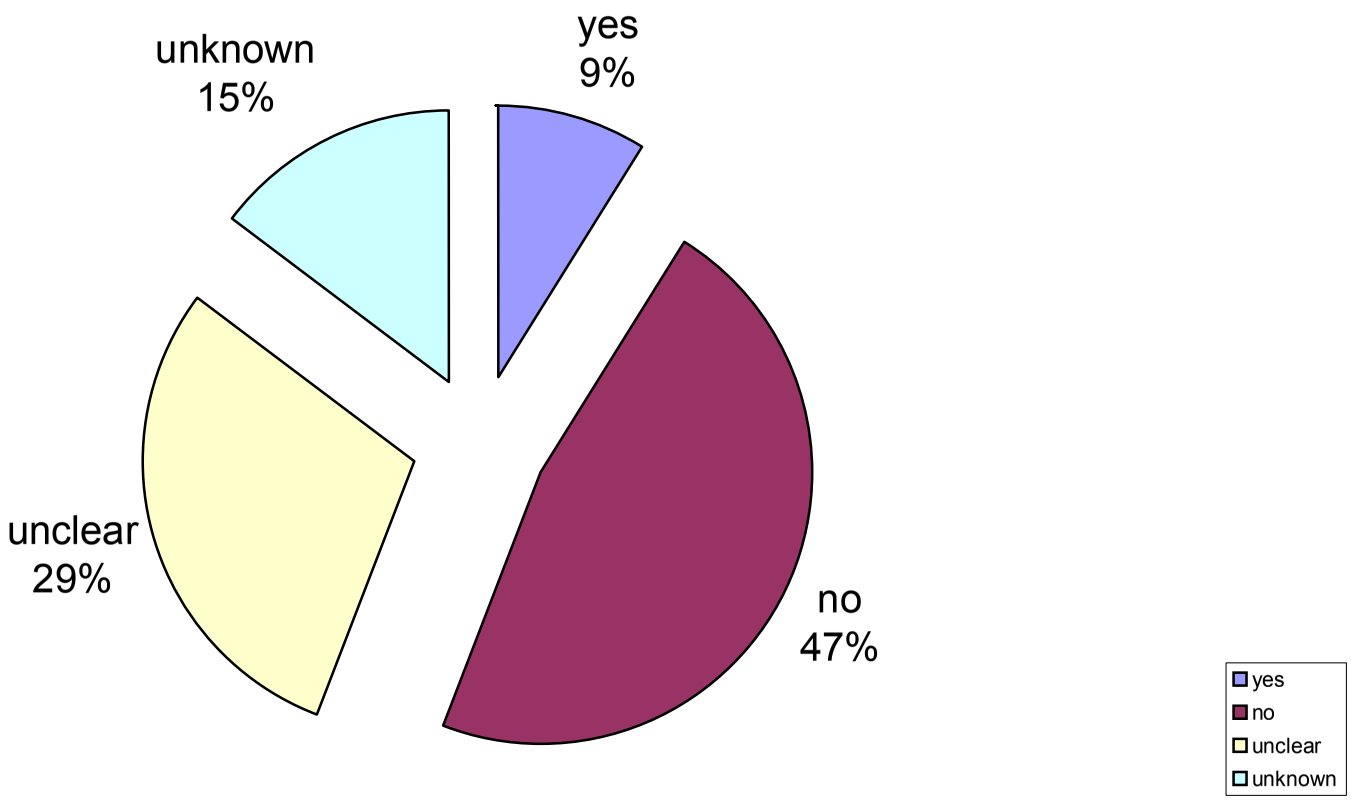
## Independent Recourse Mechanisms pursuant to FAQ 5
## (Table 3.1, graphic 1)



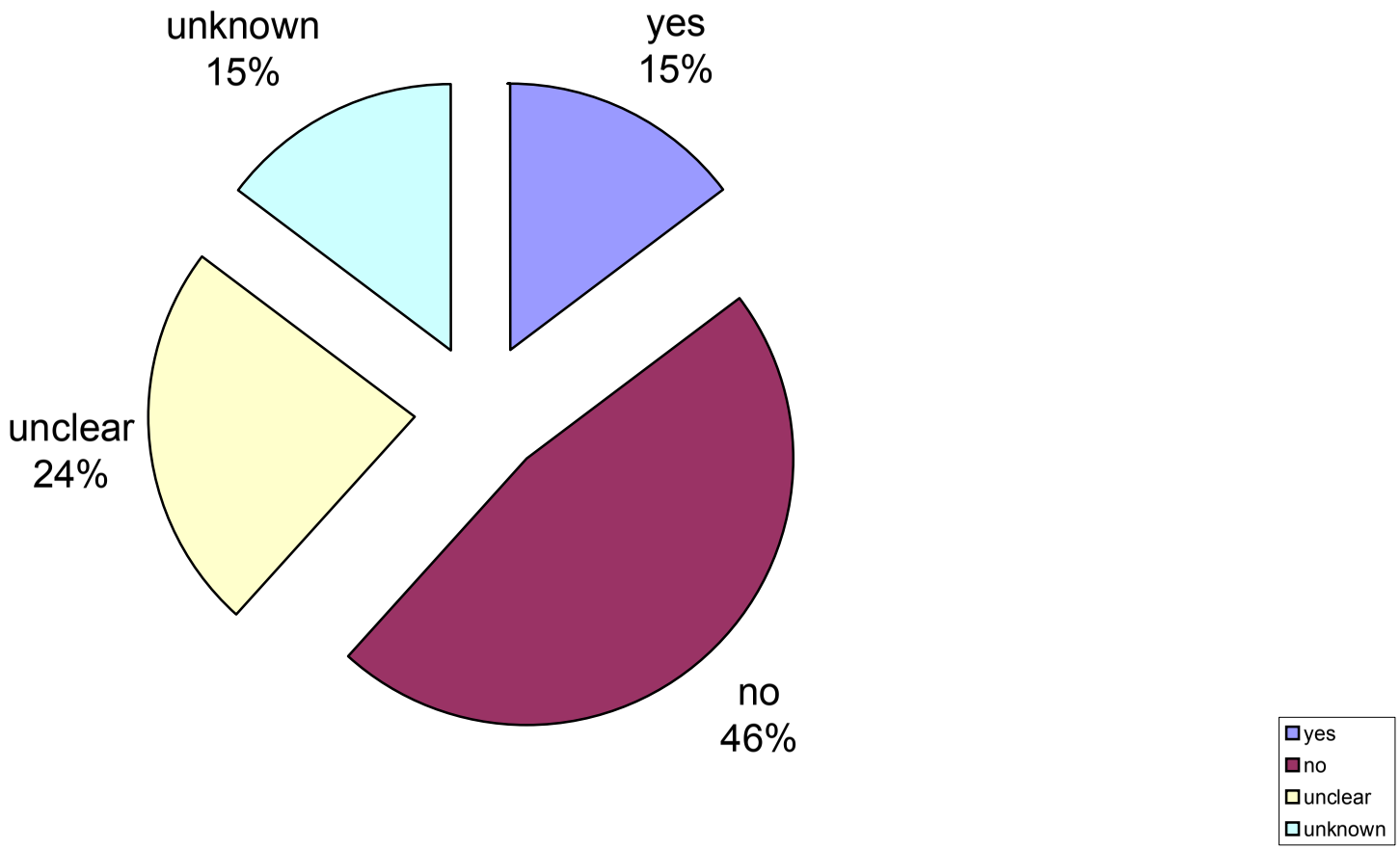
## Independent Recourse Mechanisms pursuant to FAQ 11 (Table 3.1, graphic 2)



## Obligation to Remedy problem
## (Table 3.1, graphic 3)



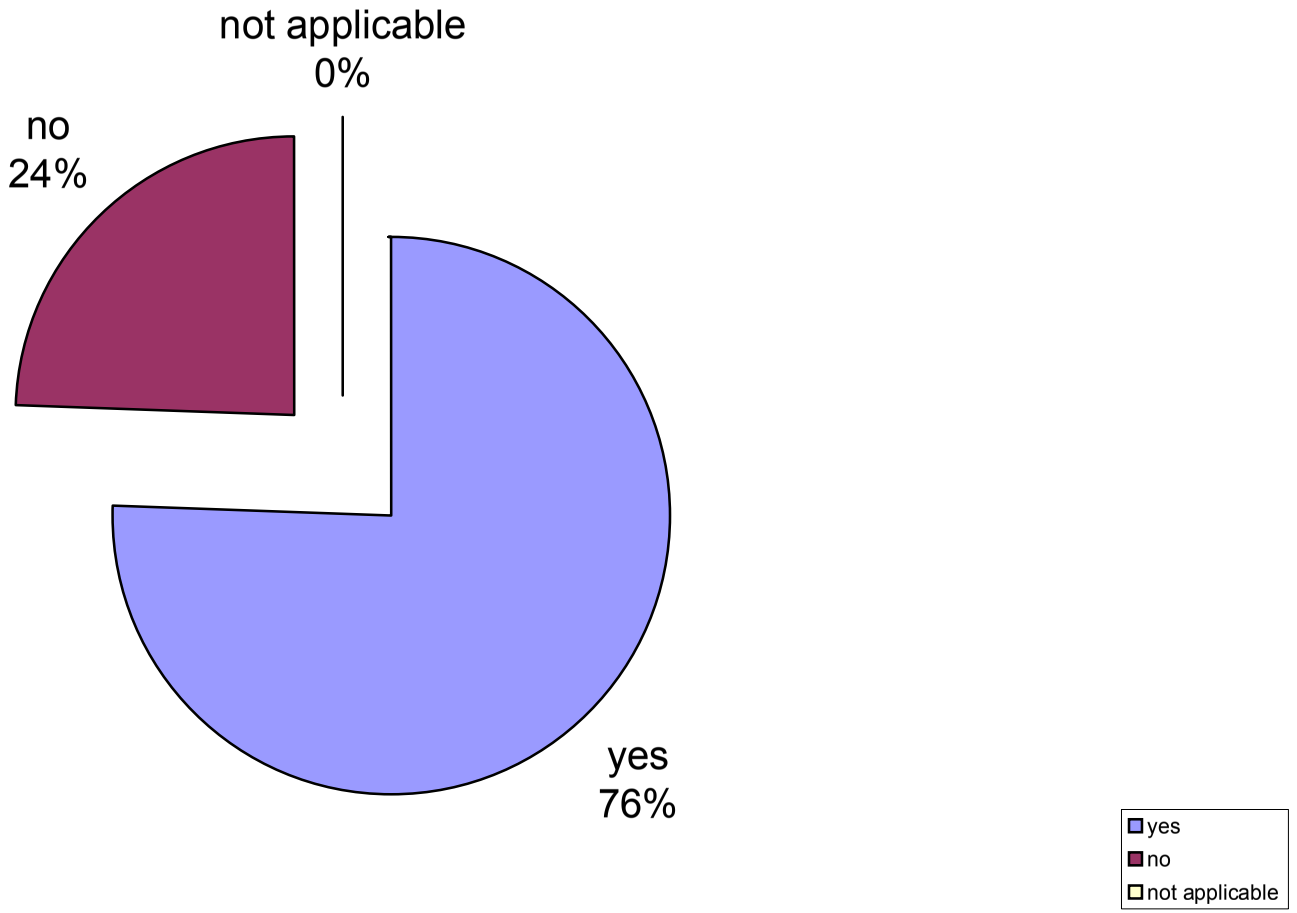
## Sanctions for Violations
## (Table 3.1, graphic 4)



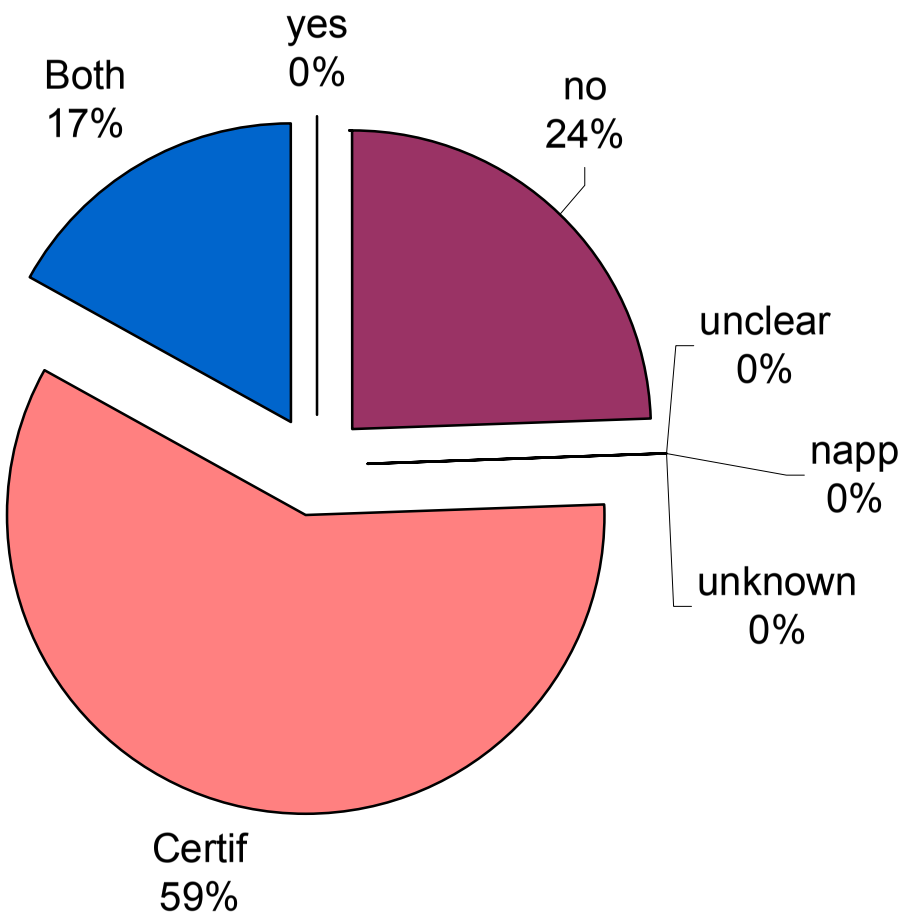
| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | **Table 3.2: Company Conformity to FAQ 5 (as of November 3, 2003)** | | | | |
| 2 | *Company* | | *Elects DPA enforcement* | *Co-operates with DPAs* | *Agrees to comply with DPA advice* |
| 3 | 1 | | yes | Certif | no |
| 4 | 2 | | yes | Certif | unknown |
| 5 | 3 | | no | no | napp |
| 6 | 4 | | no | no | napp |
| 7 | 5 | | yes | Certif | unknown |
| 8 | 6 | | yes | Both | no |
| 9 | 7 | | yes | Both | unknown |
| 10 | 8 | | no | no | napp |
| 11 | 9 | | yes | Certif | no |
| 12 | 10 | | no | no | napp |
| 13 | 11 | | yes | Both | no |
| 14 | 12 | | yes | Certif | no |
| 15 | 13 | | yes | Certif | no |
| 16 | 14 | | yes | Certif | no |
| 17 | 15 | | yes | Certif | no |
| 18 | 16 | | no | no | napp |
| 19 | 17 | | yes | Both | yes |
| 20 | 18 | | yes | Certif | unknown |
| 21 | 19 | | yes | Both | no |
| 22 | 20 | | no | no | napp |
| 23 | 21 | | yes | Certif | napp |
| 24 | 22 | | yes | Certif | no |
| 25 | 23 | | yes | Certif | no |
| 26 | 24 | | yes | Certif | no |
| 27 | 25 | | yes | Certif | unknown |
| 28 | 26 | | yes | Certif | no |
| 29 | 27 | | yes | Both | no |
| 30 | 28 | | yes | Certif | unknown |
| 31 | 29 | | no | no | napp |
| 32 | 30 | | yes | Certif | no |
| 33 | 31 | | yes | Certif | no |
| 34 | 32 | | yes | Certif | unknown |
| 35 | 33 | | no | no | napp |
| 36 | 34 | | yes | Both | yes |
| 37 | 35 | | no | no | napp |
| 38 | 36 | | yes | Certif | no |
| 39 | 37 | | yes | Certif | no |
| 40 | 38 | | yes | Certif | no |
| 41 | 39 | | yes | Certif | no |
| 42 | 40 | | no | no | napp |
| 43 | 41 | | yes | Certif | no |

**Cellule:** C2
**Commentaire:** This is also listed in FAQ 11.

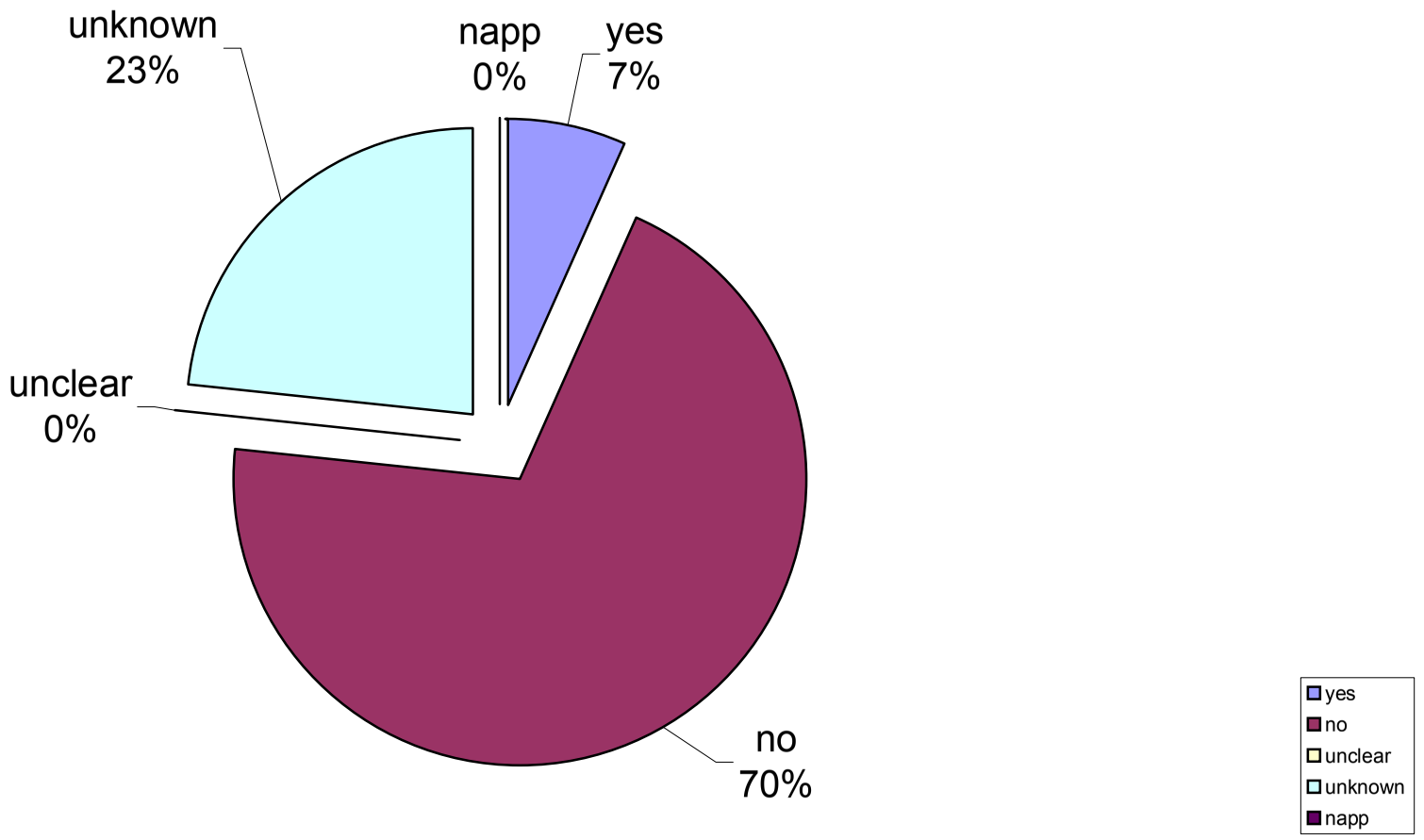
## Elects DPA enforcement (Table 3.2, graphic 1)



## Co-Operates with DPAs (Table 3.2, graphic 2)



## Agrees to comply with DPA advice (Table 3.2, graphic 3)



| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table 3.3: Company Conformity to FAQ 11 (as of November 3, 2003)** | | | | | | | | | | |
| 2 | *Company* | | *US Legal or Regulatory Supervision* | *Independence of recourse mechanism* | *Readily available/affordable recourse* | *Transparency of dispute resolution procedures* | *Company agrees to reverse effects of breach* | *SH Compliant Future Processing* | *Cessation of processing of data for harmed individual* | *Publicity for Findings* | *Sanctions* |
| 3 | 1 | | no | yes | yes | no | no | no | no | no | no |
| 4 | 2 | | no | yes | yes | unknown | unknown | unknown | unknown | unknown | unknown |
| 5 | 3 | | no | yes | yes | yes | unclear | no | unclear | no | no |
| 6 | 4 | | no | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 7 | 5 | | no | yes | yes | unknown | unknown | unknown | unknown | unknown | unknown |
| 8 | 6 | | no | yes | yes | yes | no | no | no | no | no |
| 9 | 7 | | no | yes | yes | yes | unlear | unclear | no | no | unclear |
| 10 | 8 | | no | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 11 | 9 | | no | yes | yes | yes | no | no | no | no | no |
| 12 | 10 | | no | yes | yes | yes | unclear | unclear | unclear | unclear | yes |
| 13 | 11 | | no | yes | yes | yes | yes | yes | no | no | yes |
| 14 | 12 | | no | yes | yes | yes | unclear | unclear | unclear | unclear | yes |
| 15 | 13 | | no | yes | yes | no | unclear | no | unclear | no | no |
| 16 | 14 | | no | yes | yes | no | no | no | no | no | no |
| 17 | 15 | | no | yes | yes | yes | unclear | no | unclear | no | no |
| 18 | 16 | | no | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 19 | 17 | | no | yes | yes | yes | yes | yes | yes | yes | yes |
| 20 | 18 | | no | yes | yes | yes | unclear | unclear | unclear | unclear | yes |
| 21 | 19 | | no | yes | yes | yes | no | no | no | no | no |
| 22 | 20 | | no | yes | yes | yes | unclear | unclear | unclear | unclear | yes |
| 23 | 21 | | no | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 24 | 22 | | no | yes | yes | yes | unclear | unclear | unclear | unclear | yes |
| 25 | 23 | | no | yes | yes | unknown | unknown | unknown | unknown | unknown | unknown |
| 26 | 24 | | no | yes | yes | no | no | no | no | no | no |
| 27 | 25 | | no | yes | yes | unknown | unknown | unknown | unknown | unknown | unknown |
| 28 | 26 | | no | yes | yes | no | no | no | no | no | no |
| 29 | 27 | | no | yes | yes | yes | no | no | no | no | no |
| 30 | 28 | | no | yes | yes | unknown | unknown | unknown | unknown | unknown | unknown |
| 31 | 29 | | no | yes | yes | yes | unclear | yes | unclear | yes | yes |
| 32 | 30 | | no | yes | yes | yes | unclear | unclear | unclear | unclear | yes |
| 33 | 31 | | no | yes | yes | no | no | no | no | no | no |
| 34 | 32 | | no | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 35 | 33 | | no | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 36 | 34 | | no | yes | yes | yes | yes | yes | yes | yes | yes |
| 37 | 35 | | no | yes | yes | yes | unclear | uncear | unclear | unclear | yes |
| 38 | 36 | | no | yes | yes | no | no | no | no | no | no |
| 39 | 37 | | no | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 40 | 38 | | no | yes | yes | no | no | no | no | no | no |
| 41 | 39 | | no | yes | yes | yes | unclear | unclear | unclear | unclear | yes |
| 42 | 40 | | no | yes | yes | yes | unclear | yes | unclear | yes | yes |
| 43 | 41 | | no | yes | yes | no | no | no | no | no | yes |

**Cellule:** C2
**Commentaire:** FAQ 11 allows the Enforcement Principle to be satisfied by "compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution."

**Cellule:** D2
**Commentaire:** FAQ 11 states that "Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record." Under FAQ 11, a company may satisfy this requirement by making a commitment to cooperate with the DPA.

**Cellule:** F2
**Commentaire:** FAQ 11 requires that "recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works." If a company has elected DPA dispute settlement and indicates such mechanism in its privacy policy, then the process will be considered transparent.

**Cellule:** G2
**Commentaire:** FAQ 11 requires that the remedies available in the dispute resolution process include the reversal of the effects of non-compliance.

**Cellule:** H2
**Commentaire:** FAQ 11 requires that the dispute resolution proceeding remedy result in future processing that will be in conformity with the SH Principles.

**Cellule:** I2
**Commentaire:** FAQ 11 requires that the dispute resolution proceeding remedy result in the cessation, when appropriate, of or processing the personal data of the individual who brought the complaint.

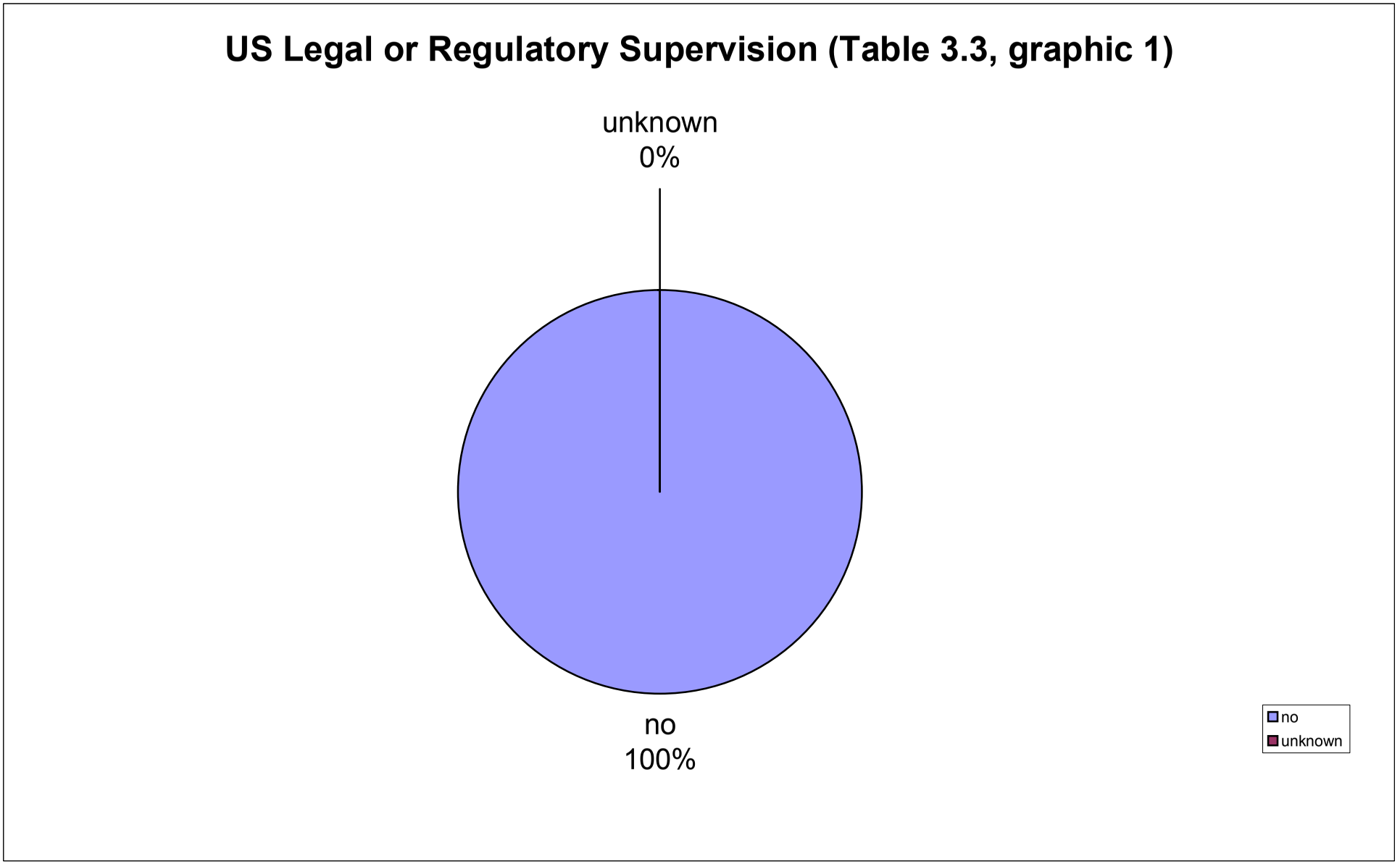
**Cellule:** J2
**Commentaire:** FAQ 11 states that "Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances."

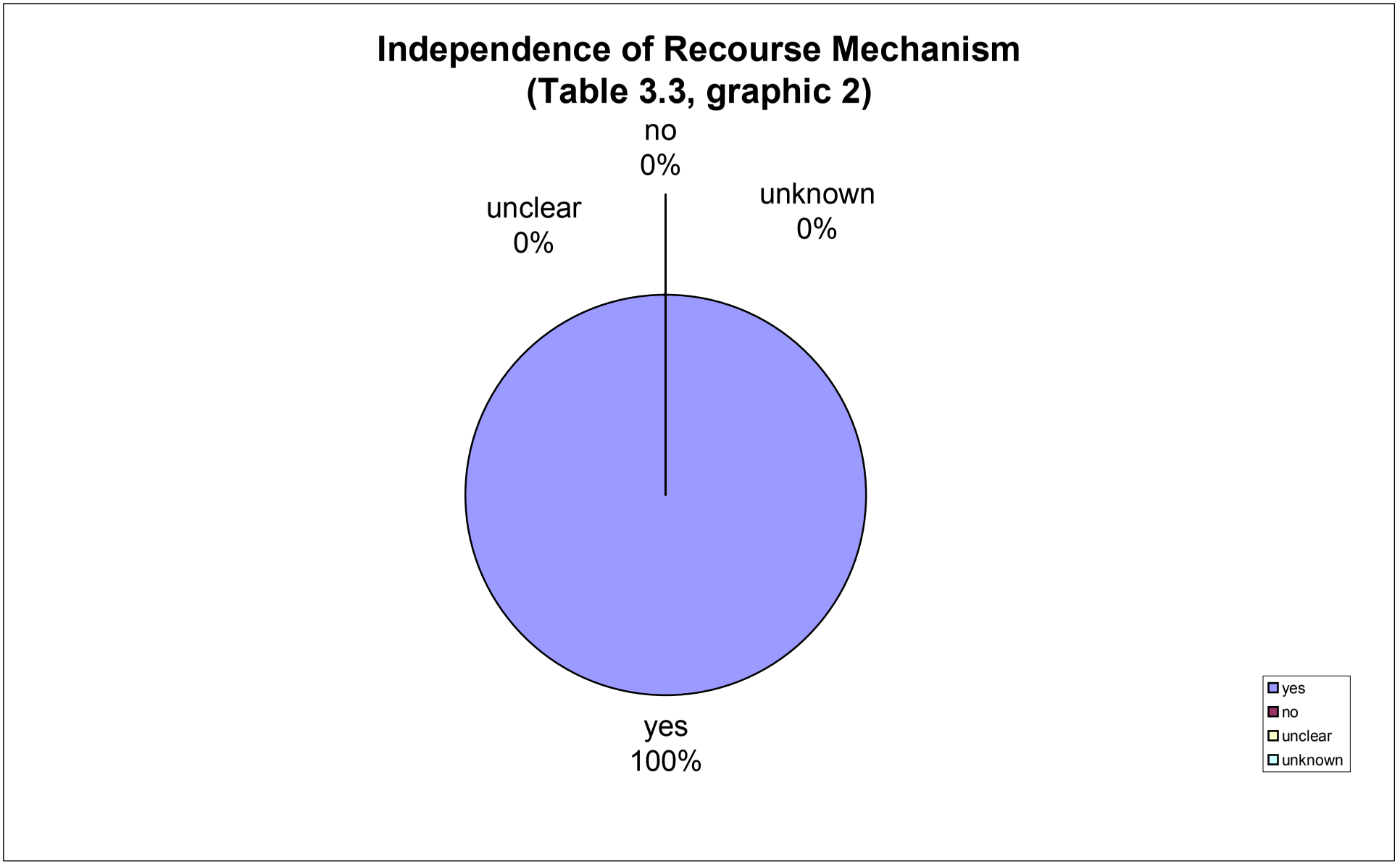
**Cellule:** K2
**Commentaire:** FAQ 11 requires sanctions which "could include suspension and removal of a seal, compensation for individuals for losses … and injuncive orders." In addition, FAQ 11 requires that sanctions include "the requirement to delete data in certain circumstances" depending on the dispute resolution body's interpretation of the data's sensitivity. Any company that has elected enforcement by a DPA, but has not agreed to abide by the DPA decision does not qualify for sanctions.

**Cellule:** I12
**Commentaire:** This company has choosen two ADRs, one does not provide for cessation, the other one is unclear,

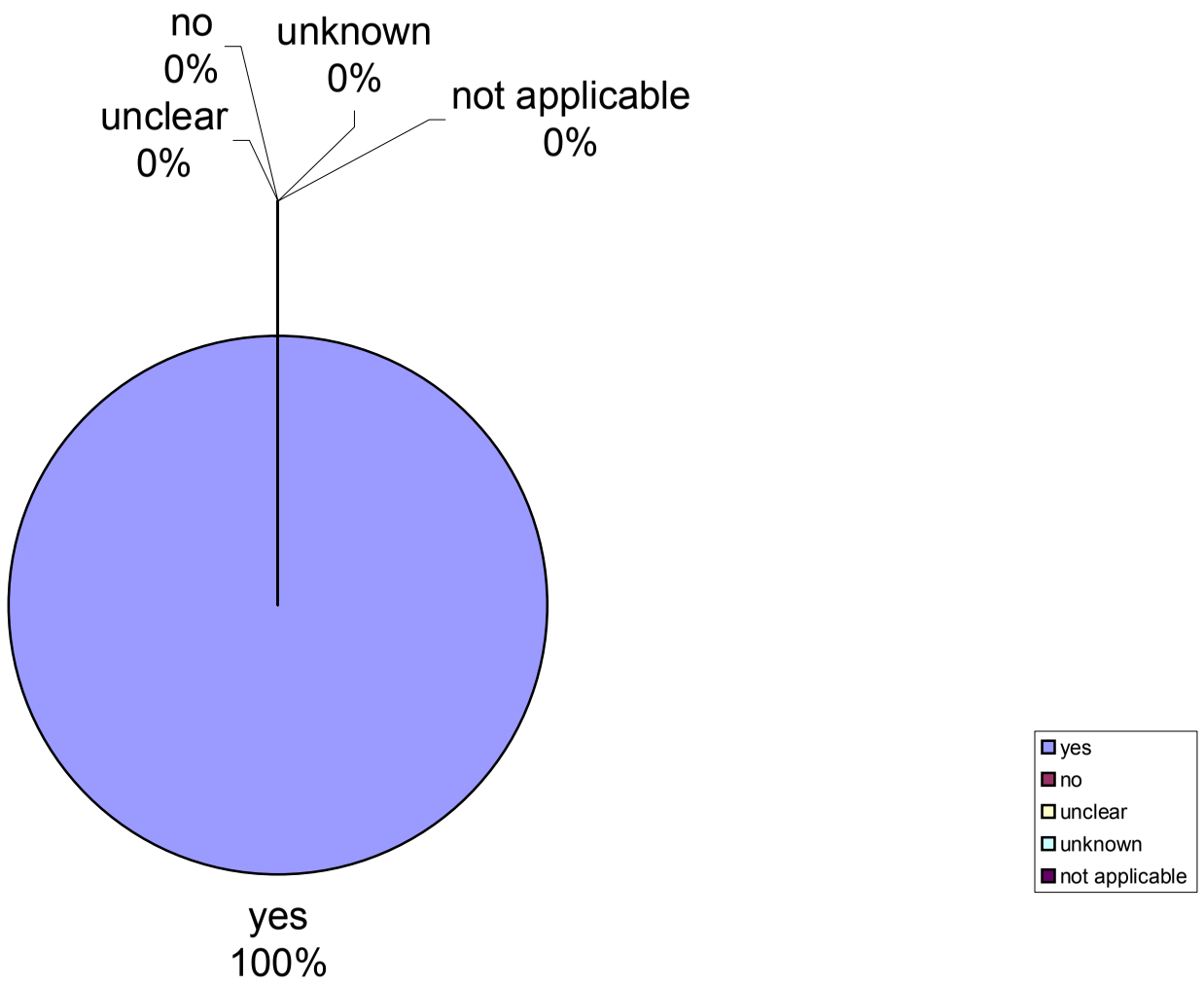
**Cellule:** J12
**Commentaire:** This company has choosen two ADRs, one provides for publication, the other one not.

**Cellule:** K12
**Commentaire:** This company has choosen two ADRs, one provides for sanctions, the other one not.

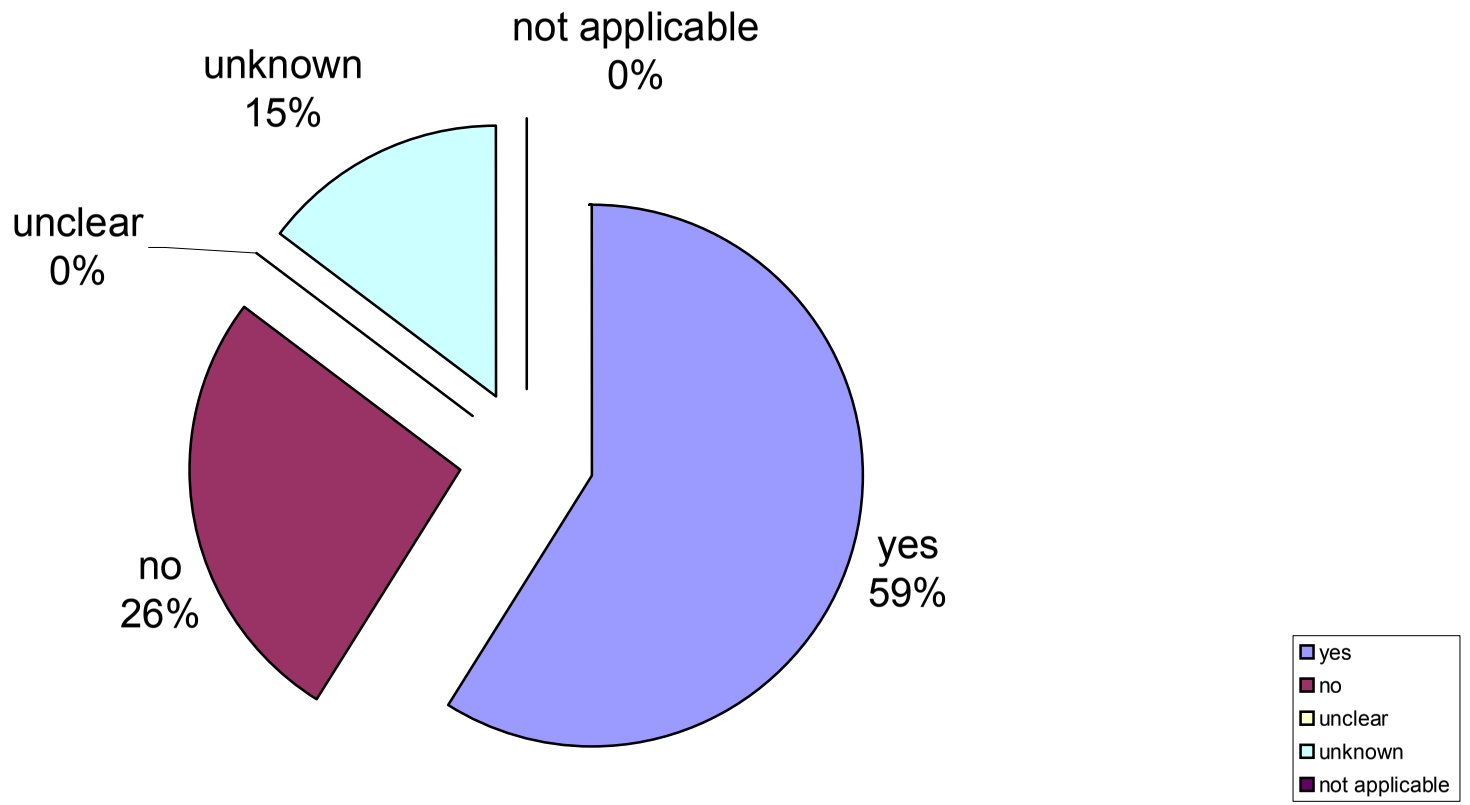

US Legal or Regulatory Supervision (Table 3.3, graphic 1)
unknown
0%
no
100%
no
unknown


Independence of Recourse Mechanism
(Table 3.3, graphic 2)
no
0%
unknown
0%
unclear
0%
yes
100%
yes
no
unclear
unknown

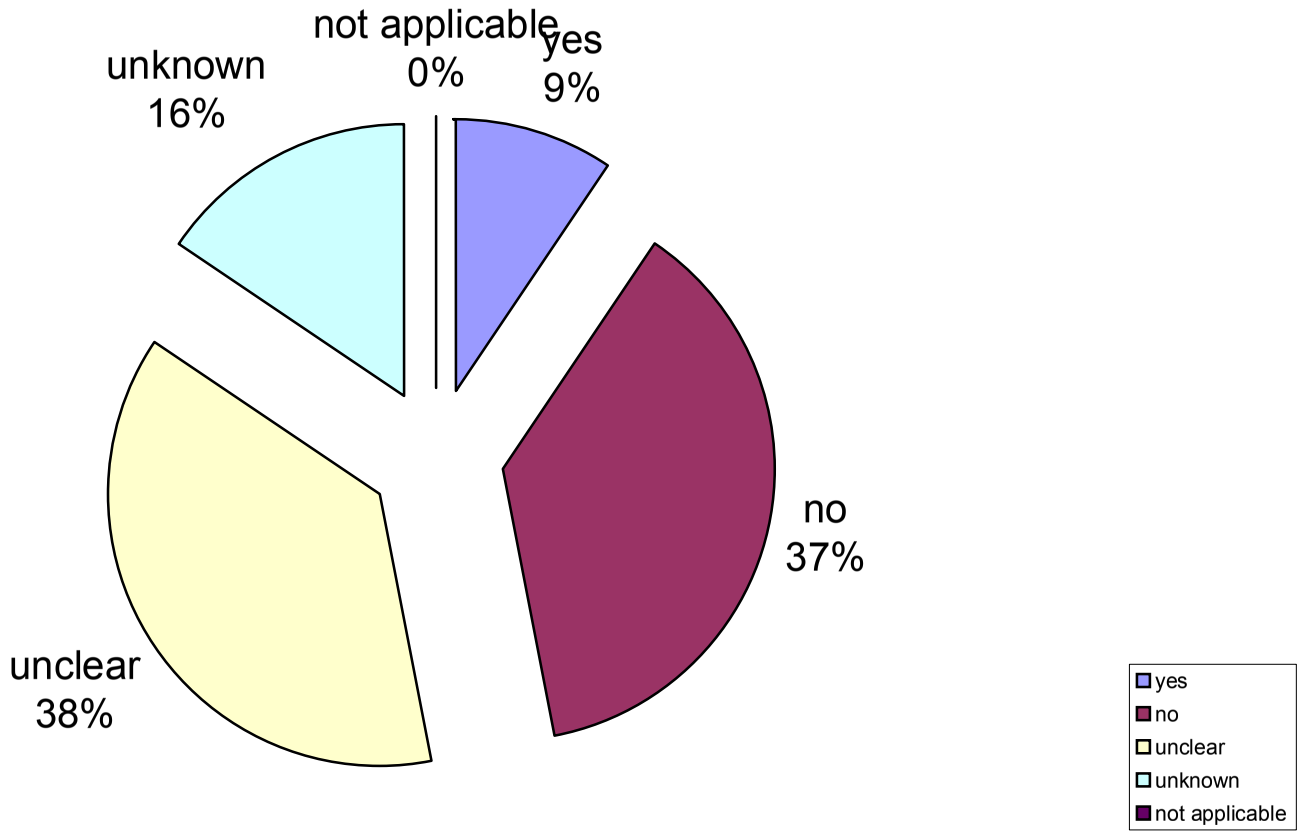
## Readily available/affordable recourse (Table 3.3, graphic 3)



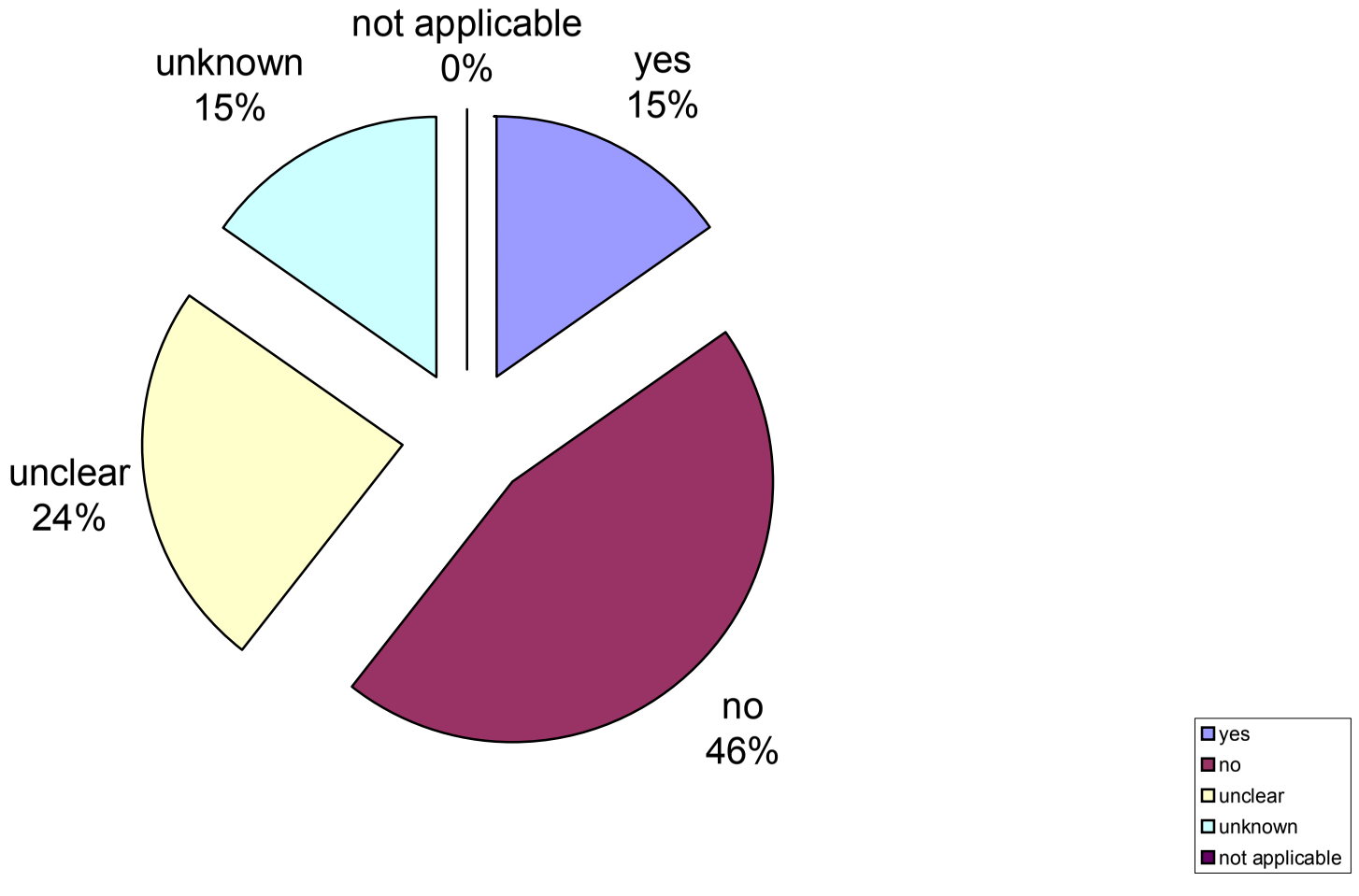
## Transparency of Dispute Resolution Procedures
## (Table 3.3, graphic 4)



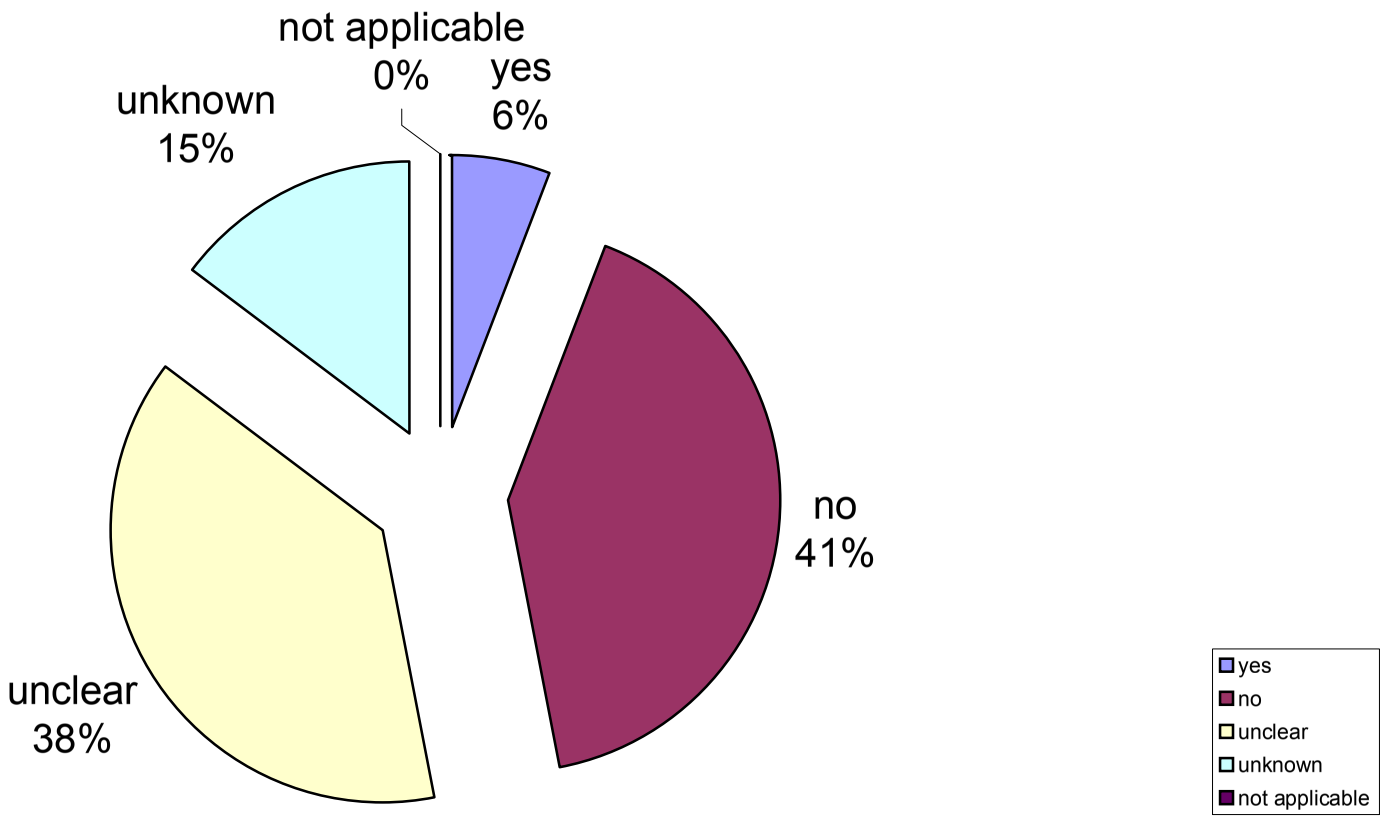
## Company agrees to reverse effects of breach (Table 3.3, graphic 5)



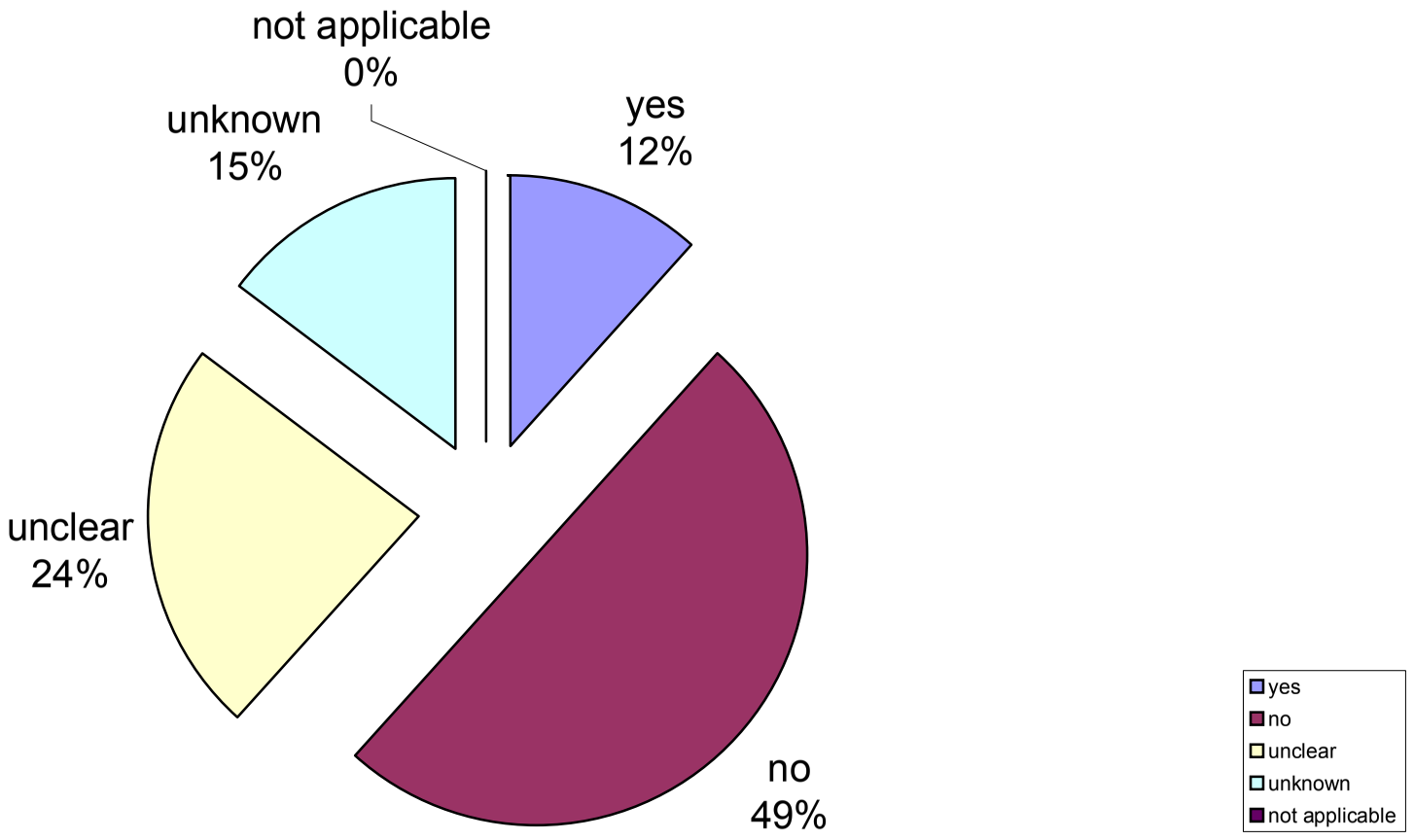
## SH Compliant Future Processing (Table 3.3, graphic 6)



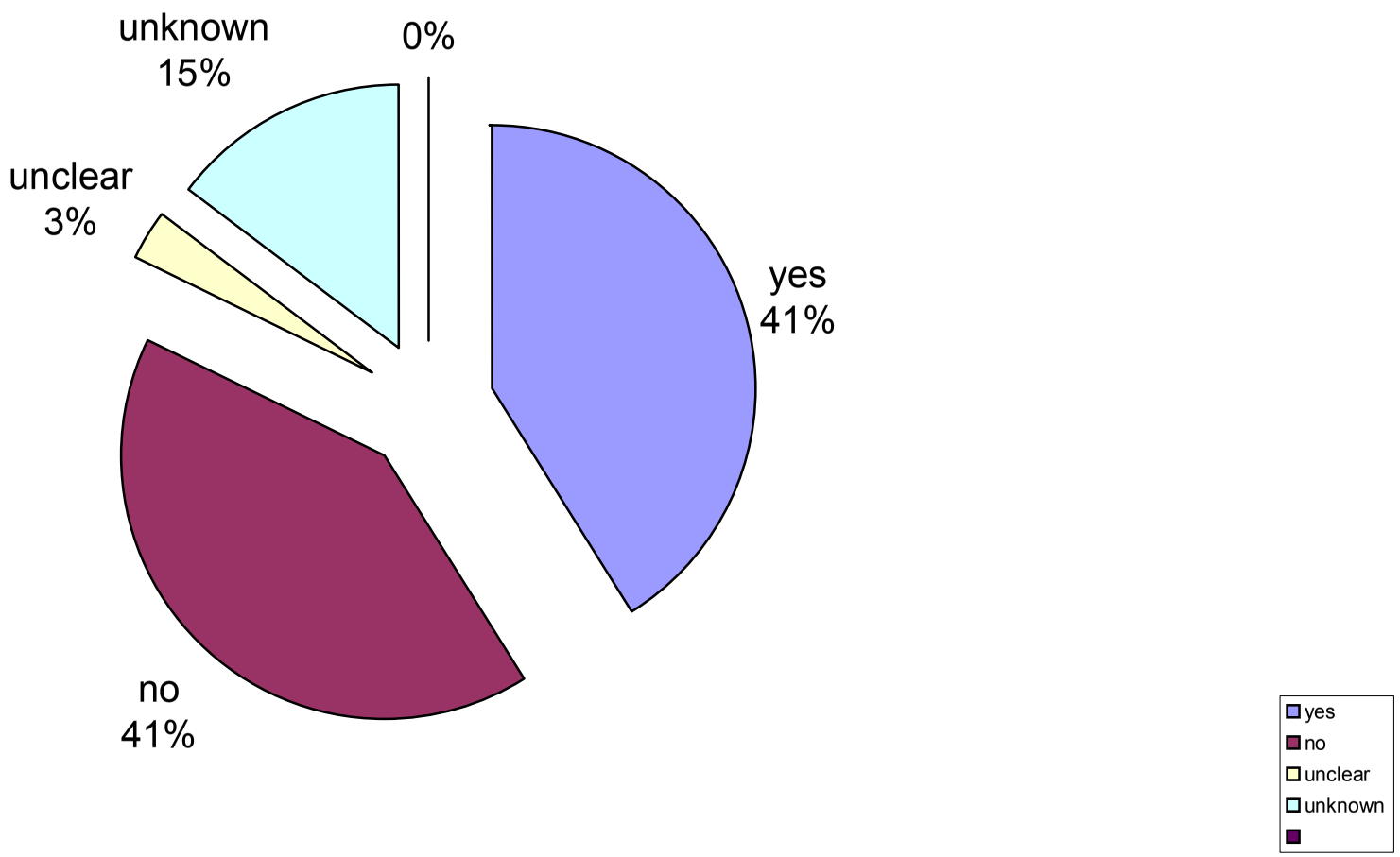
## Cessation of Processing of Data for Harmed Individual (Table 3.3, graphic 7)



## Publicity for Findings (Table 3.3, graphic 8)



## Sanctions (Table 3.3, graphic 9)



| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | **Table A: Incorporation of SH Notice Principles in Privacy Program Rules** | | | | | | | |
| 2 | *Self-Regulatory Privacy Program* | | *Program Contacts* | *Statement of SH Compliance* | *Clear/ Conspicuous Member Policy* | *Members Specify Purposes* | *Members Disclose 3rd Party Recipients* | *Data Subject Choice for use/ dissemination* |
| 3 | AAA | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| 4 | BBB Online | | Yes | No | Yes | Yes | Yes | Yes/No |
| 5 | CASRO | | No | No | No | Yes | No | No |
| 6 | CAUCE | | Not Applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 7 | DMAshp | | Yes | No | Yes | Yes | Yes | Yes |
| 8 | OPA | | No | No | Yes | Unclear | Yes | Yes |
| 9 | TRUSTe | | Yes | Yes | Yes | Yes | Yes | Yes |
| 10 | | | | | | | | |
| 11 | | | | | | | | |
| 12 | | | | | | | | |
| 13 | | | | | | | | |
| 14 | | | | | | | | |
| 15 | | | | | | | | |
| 16 | | | | | | | | |
| 17 | | | | | | | | |
| 18 | | | | | | | | |
| 19 | | | | | | | | |
| 20 | | | | | | | | |
| 21 | | | | | | | | |
| 22 | | | | | | | | |
| 23 | | | | | | | | |
| 24 | | | | | | | | |
| 25 | | | | | | | | |
| 26 | | | | | | | | |
| 27 | | | | | | | | |
| 28 | | | | | | | | |
| 29 | | | | | | | | |
| 30 | | | | | | | | |
| 31 | | | | | | | | |
| 32 | | | | | | | | |
| 33 | | | | | | | | |
| 34 | | | | | | | | |
| 35 | | | | | | | | |
| 36 | | | | | | | | |
| 37 | | | | | | | | |
| 38 | | | | | | | | |
| 39 | | | | | | | | |
| 40 | | | | | | | | |
| 41 | | | | | | | | |
| 42 | | | | | | | | |
| 43 | | | | | | | | |
| 44 | | | | | | | | |
| 45 | | | | | | | | |
| 46 | | | | | | | | |
| 47 | | | | | | | | |
| 48 | | | | | | | | |
| 49 | | | | | | | | |
| 50 | | | | | | | | |
| 51 | | | | | | | | |
| 52 | | | | | | | | |
| 53 | | | | | | | | |
| 54 | | | | | | | | |
| 55 | | | | | | | | |
| 56 | | | | | | | | |
| 57 | | | | | | | | |
| 58 | | | | | | | | |

**Cellule:** H4
**Commentaire:** The "Privacy Program Eligibilty Requirements" only include data subject choice for direct marketing uses of personal information.

**Cellule:** A5
**Commentaire:** The analysis is based on "CASRO Code of Standards and Ethics for Survey Research". However, another webpage states that CASRO has created a Privacy Protection Program (CASRO 3P) "a single service developed to show research companies how to meet the privacy requirements for information collection, storage and dissemination under the following acts and directives: US Safe Harbor, European Union Directive on Data Protection, (...)". The said program is not publicly available on CASRO website.

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | **Table B: Incorporation of SH Choice Principle in Privacy Program Rules** | | | | | | | |
| 2 | *Self-Regulatory Privacy Program* | | *Opt-out (3rd party)* | *Opt-out (secondary use)* | *Clear/ Conspicuous* | *Readily Available* | *Affordable* | *Opt-in (Sensitive Data)* |
| 3 | AAA | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| 4 | BBB Online | | Yes | No | Yes | No | No | No |
| 5 | CASRO | | Unclear | No | No | No | No | No |
| 6 | CAUCE | | not applicable | not applicable | not applicable | not applicable | not applicable | not applicable |
| 7 | DMAshp | | Yes | Yes | Yes | Yes | Yes | Yes |
| 8 | OPA | | Yes | Yes | Yes | No | No | No |
| 9 | TRUSTe | | Yes | Yes | No | No | No | No |
| 10 | | | | | | | | |
| 11 | | | | | | | | |
| 12 | | | | | | | | |
| 13 | | | | | | | | |
| 14 | | | | | | | | |
| 15 | | | | | | | | |
| 16 | | | | | | | | |
| 17 | | | | | | | | |
| 18 | | | | | | | | |
| 19 | | | | | | | | |
| 20 | | | | | | | | |
| 21 | | | | | | | | |
| 22 | | | | | | | | |
| 23 | | | | | | | | |
| 24 | | | | | | | | |
| 25 | | | | | | | | |
| 26 | | | | | | | | |
| 27 | | | | | | | | |
| 28 | | | | | | | | |
| 29 | | | | | | | | |
| 30 | | | | | | | | |
| 31 | | | | | | | | |
| 32 | | | | | | | | |

**Cellule:** F2
**Commentaire:** "Readily available" means that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out.)

**Cellule:** C4
**Commentaire:** The Privacy Program Eligibility Requirements provide an opt-out only to those "outside parties or corporate affiliates operating under a different privacy notice." However, the Privacy Program Assessment Questionnaire states that transfers to outside parties for direct marketing "must provide individuals with the ability to prevent these transfers." Transfers for other uses are not covered by the required opt-out.

**Cellule:** D4
**Commentaire:** The Privacy Program Eligibility Requirements only mandate an opt-out for direct marketing uses.

**Cellule:** D5
**Commentaire:** The opt-out is available for unsolicited email messages. The statement mentions no other opt-out.

**Cellule:** E9
**Commentaire:** The program rules do not explicitly indicate that choice must be offered in a clear and conspicuous manner.

**Cellule:** F9
**Commentaire:** The program rules do not impose any requirements on the means to exercise choice.

| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | **Table C: Incorporation of Onward Transfer Principle in Privacy Program Rules** | | | | |
| 2 | *Self-Regulatory Privacy Program* | | *Notice of Onward Transfers* | *Choice* | *3rd Party Processor's Commitment to SH* |
| 3 | AAA | | Not Applicable | Not Applicable | Not Applicable |
| 4 | BBB Online | | Yes | Yes | No |
| 5 | CASRO | | No | No | No |
| 6 | CAUCE | | Not Applicable | Not Applicable | Not Applicable |
| 7 | DMAshp | | Yes | Yes | Yes |
| 8 | OPA | | Yes | Yes | No |
| 9 | TRUSTe | | Yes | Yes | Unclear |
| 10 | | | | | |
| 11 | | | | | |
| 12 | | | | | |
| 13 | | | | | |
| 14 | | | | | |
| 15 | | | | | |
| 16 | | | | | |
| 17 | | | | | |
| 18 | | | | | |
| 19 | | | | | |
| 20 | | | | | |
| 21 | | | | | |
| 22 | | | | | |
| 23 | | | | | |
| 24 | | | | | |
| 25 | | | | | |
| 26 | | | | | |
| 27 | | | | | |
| 28 | | | | | |
| 29 | | | | | |
| 30 | | | | | |
| 31 | | | | | |
| 32 | | | | | |
| 33 | | | | | |

**Cellule:** E9

**Commentaire:** The Safe Harbor Addendum to the Truste License Agreement 9.0, Program Requirements and Self-Assessment Sheet sets forth the following: "In order for a company to be Safe Harbor compliant it should take steps to ensure certain levels of protection when transferring Personally Identifiable Information to agents or service providers. If you answered no to a.2., what steps has your company taken to review the privacy practices of agents or service providers and to ensure that they abide by your privacy policies or have in place equal policies?

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | **Table D: Incorporation of Security & Integrity Principles in Privacy Program Rules** | | | | | |
| 2 | *Self-Regulatory Privacy Program* | | *Reasonable Security Precautions* | *Relevance of Data* | *Compatible/ Authorized Processing for Secondary Use* | *Steps to Ensure Reliability for Intended Use* |
| 3 | AAA | | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| 4 | BBB Online | | Yes | No | No | No |
| 5 | CASRO | | No | No | Yes | Yes |
| 6 | CAUCE | | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| 7 | DMAshp | | Yes | Yes | Yes | Yes |
| 8 | OPA | | Yes | No | Yes | Yes |
| 9 | TRUSTe | | Yes | No | Yes | Yes |
| 10 | | | | | | |
| 11 | | | | | | |
| 12 | | | | | | |
| 13 | | | | | | |
| 14 | | | | | | |
| 15 | | | | | | |
| 16 | | | | | | |
| 17 | | | | | | |
| 18 | | | | | | |
| 19 | | | | | | |
| 20 | | | | | | |
| 21 | | | | | | |
| 22 | | | | | | |
| 23 | | | | | | |
| 24 | | | | | | |
| 25 | | | | | | |
| 26 | | | | | | |
| 27 | | | | | | |
| 28 | | | | | | |
| 29 | | | | | | |
| 30 | | | | | | |
| 31 | | | | | | |
| 32 | | | | | | |
| 33 | | | | | | |

**Cellule:** C2

**Commentaire:**

Any site stating that it uses encryption to transmit data will qualify under this SH Principle.

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | **Table E: Incorporation of SH Access Principle in Privacy Program Rules** | | | | | | |
| 2 | *Self-Regulatory Privacy Program* | | *Reasonable Access Provided* | *Reasonable Cost for Access* | *Correction of inaccurate data* | *Amendment of inaccurate data* | *Deletion of inaccurate data* |
| 3 | AAA | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| 4 | BBB Online | | Yes | Yes | Yes | No | No |
| 5 | CASRO | | No | Napp | No | No | No |
| 6 | CAUCE | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| 7 | DMAshp | | Yes | No | Yes | Yes | Yes |
| 8 | OPA | | Yes | No | Yes | Yes | No |
| 9 | TRUSTe | | Yes | No | Yes | Yes | Yes |
| 10 | | | | | | | |
| 11 | | | | | | | |
| 12 | | | | | | | |
| 13 | | | | | | | |
| 14 | | | | | | | |
| 15 | | | | | | | |
| 16 | | | | | | | |
| 17 | | | | | | | |
| 18 | | | | | | | |
| 19 | | | | | | | |
| 20 | | | | | | | |
| 21 | | | | | | | |
| 22 | | | | | | | |
| 23 | | | | | | | |
| 24 | | | | | | | |
| 25 | | | | | | | |
| 26 | | | | | | | |
| 27 | | | | | | | |
| 28 | | | | | | | |

**Cellule:** D7
**Commentaire:** Access principle does not set forth that policy needs to mention cost for access.

**Cellule:** C9
**Commentaire:** The program rules contain an access principle that applies only to members who agree to an additional EU policy.

**Cellule:** E9
**Commentaire:** This applies only to members who have signed the additional EU addendum.

**Cellule:** F9
**Commentaire:** This applies only to members who have signed the additional EU addendum.

**Cellule:** G9
**Commentaire:** This applies only to members who have signed the additional EU addendum.

| | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Table F: Incorporation of Enforcement Principles in Dispute Resolution (SH & FAQ 11)** | | | | | | | | | | | | |
| 2 | *Self-Regulatory Privacy Program* | | *Independent Dispute Resolution Body ("DRB")* | *Investigation of each complaint* | *Readily available/ Affordable Recourse* | *Transparency of Recourse Procedures* | *DRB Obtains Reversal of Effects of Breach* | *DRB Obtains SH Compliant Future Processing* | *DRB Obtains Cessation of Processing* | *Compensation for Harm* | *Privacy Program Sanctions* | *Publication of DRB Sanctions* | *Mandatory Referral of DRB Sanctions* |
| 3 | AAA | | Yes | Yes | Yes | Yes | Unclear | No | Unclear | unclear | Napp | No | No |
| 4 | AICPA | | Unknown | Unknown | Unknown | Unknown | Unknown | Unknown | Unknown | Unknown | Unknown | Unknown | Unknown |
| 5 | BBB | | Unclear | Yes | Yes | Yes | Unclear | Unclear | No | No | Unclear | No | Unclear |
| 6 | DMA | | Yes | Yes | Yes | Yes | Unclear | Yes | Unclear | Yes | Yes | Yes | Unclear |
| 7 | ESRB | | No | Unclear | No | No | No | Yes | Yes | Yes | Yes | No | No |
| 8 | JAMS | | Yes | Yes | Yes | No | Unclear | unclear | Unclear | unclear | Napp | No | No |
| 9 | OPA | | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| 10 | TRUSTe | | Yes | Unclear | Yes | Yes | Unclear | Unclear | Unclear | Unclear | Yes | Unclear | No |
| 11 | | | | | | | | | | | | | |
| 12 | | | | | | | | | | | | | |
| 13 | | | | | | | | | | | | | |
| 14 | | | | | | | | | | | | | |
| 15 | | | | | | | | | | | | | |
| 16 | | | | | | | | | | | | | |
| 17 | | | | | | | | | | | | | |
| 18 | | | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | |
| 28 | | | | | | | | | | | | | |
| 29 | | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | |
| 32 | | | | | | | | | | | | | |
| 33 | | | | | | | | | | | | | |
| 34 | | | | | | | | | | | | | |
| 35 | | | | | | | | | | | | | |
| 36 | | | | | | | | | | | | | |
| 37 | | | | | | | | | | | | | |
| 38 | | | | | | | | | | | | | |
| 39 | | | | | | | | | | | | | |
| 40 | | | | | | | | | | | | | |
| 41 | | | | | | | | | | | | | |
| 42 | | | | | | | | | | | | | |
| 43 | | | | | | | | | | | | | |
| 44 | | | | | | | | | | | | | |
| 45 | | | | | | | | | | | | | |
| 46 | | | | | | | | | | | | | |
| 47 | | | | | | | | | | | | | |
| 48 | | | | | | | | | | | | | |
| 49 | | | | | | | | | | | | | |
| 50 | | | | | | | | | | | | | |
| 51 | | | | | | | | | | | | | |
| 52 | | | | | | | | | | | | | |
| 53 | | | | | | | | | | | | | |
| 54 | | | | | | | | | | | | | |
| 55 | | | | | | | | | | | | | |

**Cellule:** I2
**Commentaire:** FAQ 11 requires that the DRB be able to obtain the cessation of processing of data for the harmed individual.

**Cellule:** K2
**Commentaire:** FAQ 11. (e.g. suspension or removal of seal)

**Cellule:** G3
**Commentaire:** "The arbitrator should be empowered to grant whatever relief would be available in court under law or in equity.

**Cellule:** C5
**Commentaire:** It is not clear how the Data Privacy Review Service is integrated, On the contrary, there is a clear description of the integration of Data Privacy Appeals Board,

**Cellule:** F6
**Commentaire:** The recourse procedures are hard to find on the web site and are incomplete.

**Cellule:** C7
**Commentaire:** There's no representation concerning the independence of the body, nor a description of the composition of it.

**Cellule:** D8
**Commentaire:** The arbitration provision must allow for the discovery or exchange of non-privileged information relevant to the dispute

**Cellule:** D10
**Commentaire:** "TRUSTe Website Privacy Seal program. Watchdog Dispute Resolution and Appeal Process" says: TRUSTe makes every effort to hear all complaints; however, TRUSTe is under no obligation to pursue any complaint, which TRUSTe deems to be frivolous or to constitute harassment of TRUSTe or a TRUSTe Licensee.
A complaint is frivolous if it has no factual basis, or if it has no basis in any obligations imposed by the License Agreement. Harassing complaints includes succesive complaints based on allegations previously rejected by TRUSTe, or the filling of multiple complaints with TRUSTe employees other than those designated by TRUSTe to receive complaints,"

The individual, then, is obliged to know the License Agreement to realize what are the obligations imposed by it and as a consequence if he/she is entitled to file a complaint,

**Cellule:** H10
**Commentaire:** The program only mentions "corrective action recommended by TRUSTe."

**Cellule:** I10
**Commentaire:** The program only mentions "corrective action recommended by TRUSTe."

**Cellule:** J10
**Commentaire:** The program only mentions "corrective action recommended by TRUSTe."

**Cellule:** L10
**Commentaire:** Truste may report such disciplinary action publicly on its website, including Licensee's name, the nature of the violation (including a reference to the Section of this Schedule A found to have been violated), and TRUSTe's resulting action.

**Cellule:** M10
**Commentaire:** Truste may refer the Licensee to the Federal Trade Commission or other appropriate government enforcement agency