

Data Protection in the European Union

Data controllers' perceptions

Summary

Fieldwork: January 2008

Report: February 2008

This survey was requested by Directorate-General Justice, Freedom and Security (Unit C5: Data protection) and coordinated by Directorate-General Communication

This document does not represent the point of view of the European Commission.
The interpretations and opinions contained in it are solely those of the authors.

Flash Eurobarometer Series
#226

Data Protection in the European Union

-

Data Controllers' Perceptions

Survey conducted by The Gallup Organization
Hungary upon the request of Directorate-
General Justice, Freedom and Security



Coordinated by Directorate-General
Communication

This document does not reflect the views of the
European Commission.
The interpretations and opinions contained in it
are solely those of the authors.

THE GALLUP ORGANIZATION

Table of Contents

- Table of Contents 3**
- Introduction 4**
- Main findings 6**
- 1. Perceptions about national data protection legislation 8**
 - 1.1 Familiarity with the provisions of the national data protection laws 8
 - 1.2 Data controllers’ assessments of the data protection legislation 8
 - 1.3 Attitudes towards the requirements of the data protection law 9
 - 1.4 Views on the implementation and interpretation of the legislation 10
- 2. In-house practices relating to data protection and personal data transfer 11**
 - 2.1 The usage of privacy enhancing technologies (PETs)..... 11
 - 2.2 Transfer of personal data via Internet and related security measures..... 11
 - 2.3 Transfer of personal data outside the EU 12
- 3. Recent experiences with privacy policy and data protection 14**
 - 3.1 Companies’ experiences with access requests and complaints 14
 - 3.2 Privacy policy notices 15
 - 3.3 Contacts with the national data protection authority 16
- 4. The Future of the legal framework on data protection..... 17**
- 5. Data protection in the light of international terrorism 18**

Introduction

Information relating to individuals, called “personal data”, is collected and used in many aspects of everyday life. An individual provides personal data when he/she, for example, signs up for gym membership, opens a bank account, books a flight or registers on a website. Personal data can be any data that identifies an individual (a “data subject”), such as name or telephone number. As personal data is now collected and exchanged more frequently, additional regulation on data transfers has become necessary.

National laws on data protection demand good data management practices on the part of the entities that process data: the “data controllers”. These include the obligation to process data fairly and in a secure manner, and to use personal data for well-defined and legitimate purposes. National laws also guarantee a series of rights for data subjects, such as

- the right to be informed when personal data is processed
- the reason for such data processing
- the right to access the data and
- (if necessary) the right to have the data amended or deleted.

Over the last two decades, data protection in the EU has faced new challenges and has undergone important changes. For example, the introduction and expansion of the Single Market, and of the so-called “Information Society”, has increased the amount of personal data that flows between EU Member States. Although national laws on data protection have aimed to guarantee the same level of protection and the same rights, some differences exist. These variations could create potential obstacles to the free flow of information and additional burdens for economic operators and citizens. In order to remove these obstacles and burdens, without diminishing the protection of citizens’ personal data, Directive 95/46/EC (“*European Data Protection Directive*”)¹ was developed to harmonise provisions in this field.

This Flash Eurobarometer survey on *Data Protection in the EU* (N° 226) measures perceptions about data protection among data controllers in the 27 EU Member States. The topics covered in the current survey were:

- Perceptions about national data protection legislation
- In-house practices relating to data protection and personal data transfer
- Recent experiences with privacy policy and data protection
- The future of the legal framework on data protection
- Data protection in the light of international terrorism

The survey sample was selected randomly but disproportionately, according to two criteria: country and company size (20-49, 50-249, 250+). All private and non private organisations in the NACE sectors C-Q were eligible (agriculture and fishing excluded).

The targeted number of main interviews varied by the population size of the respective country; in the most populous Member States at least 300, in the medium sized ones at least 200, and in the smallest at least 100 organisations were interviewed

The survey’s fieldwork was carried out between the 8th and 16th of January, 2008. We interviewed over 4,835 randomly-selected “data controllers” throughout the 27 EU Member States. The views expressed in this document were provided by the individuals identified as responsible for data

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

protection within the participating organisations. The survey targeted the following persons within the organisations, in the following order of preference: data protection officer, IT manager, human resources manager, marketing manager – and if an enterprise did not have any of those positions, the general manager. The interview was carried out with the manager, who was identified by other and/or self-identified as the one dealing with data protection within the organisation.

Post-stratification weights were used to restore the artificially-distorted proportions according to company size and industry sector. When we are discussing EU-wide or other supra-national summary estimates, interviews are weighted to correct for the disproportional selection of countries in the starting sample.

This analytical report presents average results from the 27 EU Member States, as well as results for each separate country and results by company category (e.g., company size and sector of activity) and respondents' characteristics (e.g. position in the company). Whenever the same, or an equivalent, question was posed in the previous Eurobarometer survey on Data Protection (*Flash EB 147*), a comparison for the relevant countries has been provided.

A technical note indicating the manner in which the Gallup partner institutes conducted the survey can be found at the end of the analytical report. It provides further detail on interviewing methods, sampling and the statistical margins of error.

Main findings

Perceptions about the current data protection legislation

- A majority of people responsible for data protection issues within companies (56%) said they were somewhat *familiar with the provisions of the data protection law*. However, only 13% claimed to be *very familiar* with this law.
- An equally large proportion of respondents (56%) considered the *protection level offered to citizens by their respective national data protection laws* as ‘medium’. Twenty-eight percent said the protection level was ‘high’ and only 11% indicated that it was ‘low’.
- Half of the respondents in the EU believed that *legislation could not cope with the increasing amount of personal information being exchanged*. Only 5% of respondents thought that the existing legislation concerning data protection was very well suited.
- Individuals responsible for data protection issues generally made a *positive evaluation of the requirements of the data protection laws*: 91% rather agreed that the requirements of the data protection law were necessary in order to guarantee a high level of protection for consumers and the fundamental rights of citizens, only 35% thought that the requirements of the data protection law were too strict and 28% believed that the requirements of the data protection law were unnecessary except for certain sectors of activity.
- Concerning the *implementation and interpretation of the national data protection laws across the EU*, opinions were divided: 38% agreed there was sufficient harmonisation of data protection laws – across Member States – to allow personal data to be freely exchanged within the EU, compared to 33% who did not agree; a third (33%) thought that the data protection law was interpreted and applied more rigorously in their country than in other Member States, while a quarter (25%) said the opposite.
- A significant group of respondents were not able to judge if Member States’ data protection laws were adequately harmonised (29%) or found it extremely difficult to assess whether their national data protection laws had been introduced more rigorously than in other Member States (42%).

In-house practices relating to data protection and personal data transfer

The usage of privacy enhancing technologies (PETs)

- More or less half of the data controllers interviewed throughout the EU (52%) stated that they used Privacy Enhancing Technologies (PETs) in their company. Fourteen percent said that PETs were not used because they had never heard of them.

Transfer of personal data via the Internet

- Two-thirds of respondents throughout the EU (65%) indicated that their company transferred personal data via the Internet. One in three respondents (32%) admitted that their company did not take any security measures when transferring personal data over the Internet.

Transfer of personal data to countries outside of the EU

- Only a minority of respondents indicated that their company transferred personal data to countries outside of the EU (10%).
- Among companies that transferred personal data to non-EU countries, almost half of respondents (46%) indicated that this data mostly concerned clients’ or consumers’ data for commercial purposes, and 27% said it was human resources data for HR purposes.

- Emails were by far the most preferred channel for the transfer of personal data to countries outside of the EU; 78% of respondents said that in their company, personal data was transferred via email.
- Only one in three respondents, who had indicated that their company transferred data to non-EU countries, were familiar with the expression – “standard contractual clauses” (34%).

Recent experiences with privacy policy and data protection

Companies’ experiences with access requests and complaints

- Almost half of the interviewees (46%) indicated that their company had received requests for access to personal data last year, but only a minority of them said that their company had received more than 50 such requests.
- Only 3% of respondents answered that their company had received complaints from individuals whose data was currently being processed.

Privacy policy notices

- Four out of 10 respondents in the EU (41%) answered that their company maintained and updated a privacy policy notice and 17% of interviewees said that their company monitored how frequently their privacy policy notice was examined by the public.

Contacts with the national data protection authority

- At the EU27 level, 13% of interviewees said they were in regular contact with the national data protection authority in their country.
- The largest groups of respondents said they were either looking for advice when contacting their national data protection authority (60%) or that they had made contact in regard to notifications (56%).

The future of the legal framework on data protection

- Four out of ten respondents (38%) approved each of the five listed actions to improve and simplify the implementation of the data protection legal framework. Only 9% of respondents said they were only in favour of one proposed action, or none at all.
- The action most favoured in order to improve and simplify the implementation of the legal framework on data protection was the call for *more harmonised rules on security measures* (84% of respondents were in favour of this), while the least favoured action (56%) was the introduction of *data protection legislation specific to each sector of activity*.

Data protection in the light of international terrorism

- In the eyes of most respondents, the fight against international terrorism was an acceptable reason to restrict data protection rights. A majority of respondents agreed that it should be possible to monitor passenger flight details (80%), telephone calls (70%) and Internet and credit card usage (73% and 69%, respectively) if these actions served to combat terrorism.
- However, there was suspicion about any provisions that would allow the authorities to relax data protection laws. Most respondents, in favour of some relaxation (of the kinds mentioned above), said this should be within clearly-defined limits: around 30% of respondents stressed that only suspects should be monitored, while between 19% and 30% of respondents wanted even stricter safeguards, e.g. monitoring supervised by the judiciary.

1. Perceptions about national data protection legislation

1.1 Familiarity with the provisions of the national data protection laws

When asking those individuals identified as being responsible for data protection issues within the organisations interviewed, to rate their familiarity with the provisions of the respective national data protection laws, a majority (56%) said they were somewhat familiar with the provisions of the data protection legislation. However, only 13% claimed to be very familiar with the law. Furthermore, three out of 10 respondents admitted they were not really familiar with the provisions of the law.

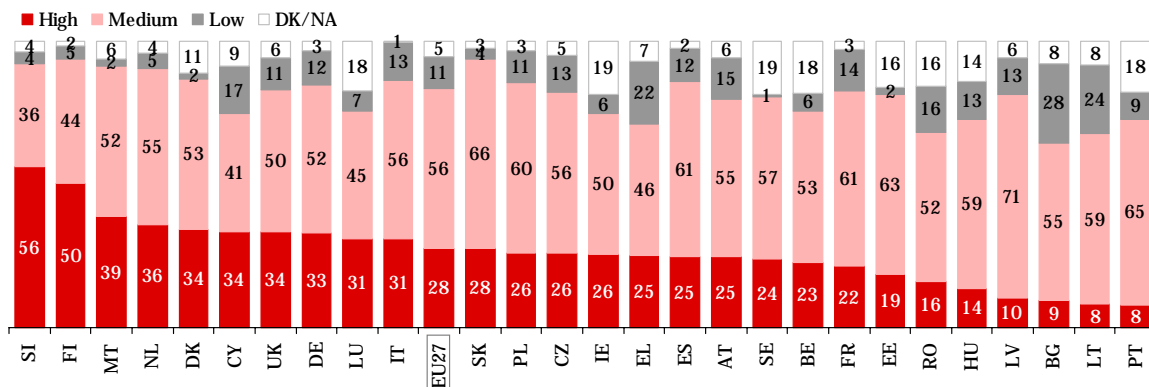
1.2 Data controllers' assessments of the data protection legislation

More than half of respondents (56%) considered the **protection level offered to citizens by their respective national data protection laws** as 'medium'. Twenty-eight percent said the protection level was 'high' and only 11% indicated that it was 'low'.

Results by country showed important disparities between Member States. In Slovenia and Finland, a majority of respondents indicated that the level of protection offered to citizens by national data protection laws was high (56% and 50%, respectively). Furthermore, 36% of Slovenian, and 44% of Finnish, respondents believed there was a medium level of protection.

Portugal and Lithuania (both 8%) were the countries with the lowest numbers of interviewees thinking that the level of protection was high. Bulgaria and Latvia followed, with proportions of 9% and 10%, respectively, sharing this opinion. Respondents in the latter country were also the most likely to have indicated that the level of protection offered by the national data protection laws was medium (71%), while Bulgarian respondents were most likely to have stated that the protection level was low (28%).

Level of protection offered by the data protection law



Q1. Would you say that the level of protection offered by the (NATIONALITY) Data Protection Law for citizens is ...?
%, Base: all respondents, by country

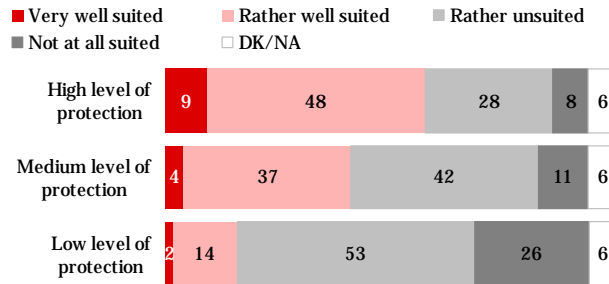
Half of the respondents in the EU believed that the **legislation was unsuited to cope with the increasing amount of personal information being exchanged**, e.g. being transferred over the Internet (38% rather unsuited and 12% not suited at all). Only 5% of respondents thought that the existing legislation on data protection was very well suited to cope with the increase in electronic data exchange and 37% believed it to be rather well suited.

Results per country showed that only in six Member States did a majority of interviewees indicate that the existing legislation on data protection was very well, or rather well, suited to cope with the increasing volumes of personal information being exchanged over the Internet. Among these, Slovenia had the highest rate, with a total of 59%. Denmark (55%), Estonia (54%), Malta and Greece (both 52%) and Austria (50%) also had a majority of respondents who believed that the existing legislation was suitable.

A comparative analysis of data controllers’ opinions showed a **relatively strong correspondence between opinions** about the protection offered by the current data protection laws and the ability of those laws to cope with the increasing amount of personal data exchange. A majority of respondents who rated the protection level of their respective data law as ‘high’ also believed that this legislation could cope with the increasing volumes of personal information being exchanged; 48% believed that the legislation was rather well suited and 9% thought that the legislation was very well suited.

By comparison, those who responded that the level of their national data protection law was ‘low’ were most likely to state that the legislation was unsuitable. More than half of respondents (53%) said that the legislation was rather unsuitable for coping with increased traffic volumes and an additional quarter of respondents (26%) saying that the legislation was not suitable at all.

The existing legislation and the increasing amount of personal data being exchanged
by level of protection offered by the data protection law

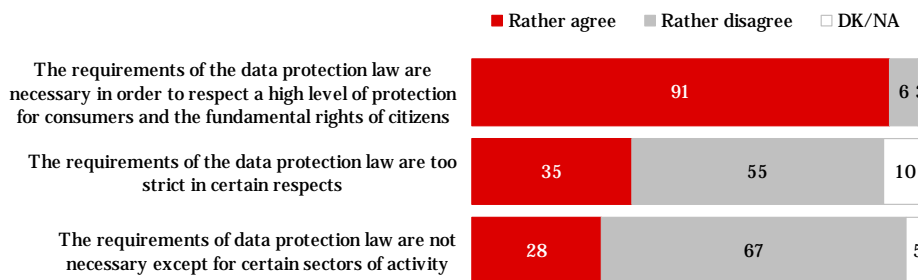


Q1. Would you say that the level of protection offered by the Data Protection Law for citizens is ...?; Q4. In your opinion, do you think that the existing legislation on data protection is suited or not to cope with the increasing amount of personal information being exchanged? %, Base: all respondents

1.3 Attitudes towards the requirements of the data protection law

Individuals responsible for data protection issues generally made a positive evaluation of the requirements of the data protection laws. Ninety-one percent rather agreed that the **requirements of the data protection law were necessary** in order to guarantee a high level of protection for consumers and the fundamental rights of citizens. Only 35% of respondents thought that the **requirements of the data protection law were too strict** and 28% believed that the **requirements of the data protection law were unnecessary** except for certain sectors of activity. These positive assessments showed that those responsible for data protection issues were not opposed to such legislation. On the contrary, they seemed to give strong support to its implementation.

Opinions about the requirements of the data protection law



Q2. From your business perspective and in general terms, would you rather agree or rather disagree with each of the statements concerning the requirements of the data protection law? %, Base: all respondents

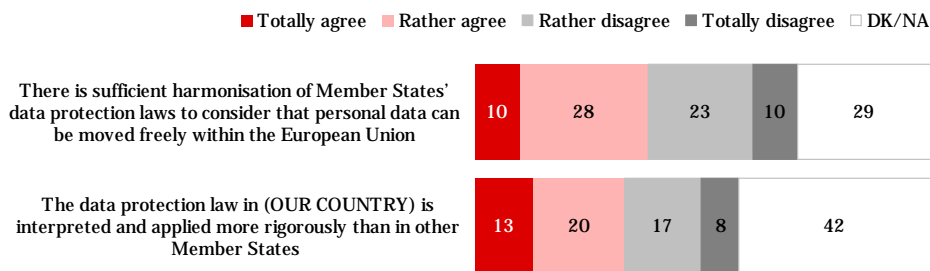
1.4 Views on the implementation and interpretation of the legislation

Concerning the implementation and interpretation of the national data protection laws across the EU, opinions were divided. Thirty-eight percent of respondents agreed there **data protection laws were sufficiently harmonised** across Member States so that personal data could move freely within the EU, compared to 33% who did not agree. Looking at the EU15, the proportion of respondents agreeing that the data protection laws were sufficiently harmonised (to allow the free movement of personal data within the EU) slightly increased between 2003 and 2008 (46% in 2003 vs. 50% in 2008; +4 percentage points).

When asked about the interpretation and application of data protection laws across Member States, 33% reasoned that the **data protection law was interpreted and applied more rigorously** in their country than in other Member States, while a lower proportion of 25% said the opposite. The proportion of respondents who agreed increased slightly between 2003 and the current survey (62% in 2003, 65% in 2008) in this question as well.

A significant group of respondents were not able to judge if Member States' data protection laws were adequately harmonised (29%) or found it extremely difficult to assess whether their national data protection laws had been introduced more rigorously than in other Member States (42%).

Opinions about the implementation of the data protection law



Q3. For each of the following propositions, please tell me if you totally agree, rather agree, rather disagree or totally disagree with it?
%, Base: all respondents

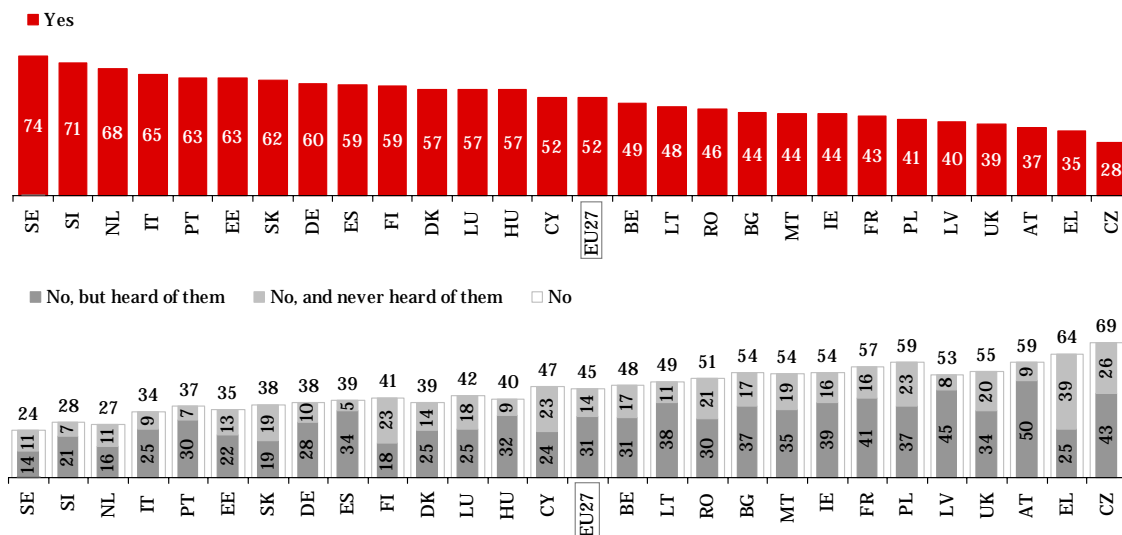
2. In-house practices relating to data protection and personal data transfer

2.1 The usage of privacy enhancing technologies (PETs)

More or less half of data controllers interviewed throughout the EU (52%) stated that they used technology or software that enhanced privacy protection of databases in their company (i.e. Privacy Enhancing Technologies (PETs)). Three out of 10 respondents (31%) said they did not use such technologies in their company, however, they did know that such technology existed, while 14% said that PET was not used because they had never heard of it. In comparison with the usage of PETs in 2003, the proportion of companies that used such technology has increased substantially in the EU15 Member States (from 32% to 55%).

The individual country results again showed significant variation; while three-quarters of Swedish companies used PETs (74%), only slightly more than a quarter of Czech companies did so (28%). Focusing on the percentages of respondents who said that PETs were not used in their company, we found that half of Austrian respondents said they did not use such technology although they had heard of the existence (and maybe also of the benefits) of such software and technology. Greek respondents, on the other hand, were the most likely not to use PETs because they had not heard of them (39%).

Usage of ‘Privacy Enhancing Technology’



Q5. Do you use any technology or software products that enhance privacy protection of databases in your company (for example, cookie cutters, encryption tools, automatic anonymisation software, Platform for Privacy Preferences (P3P)), also called ‘Privacy Enhancing Technologies’?

%, Base: all respondents, by country

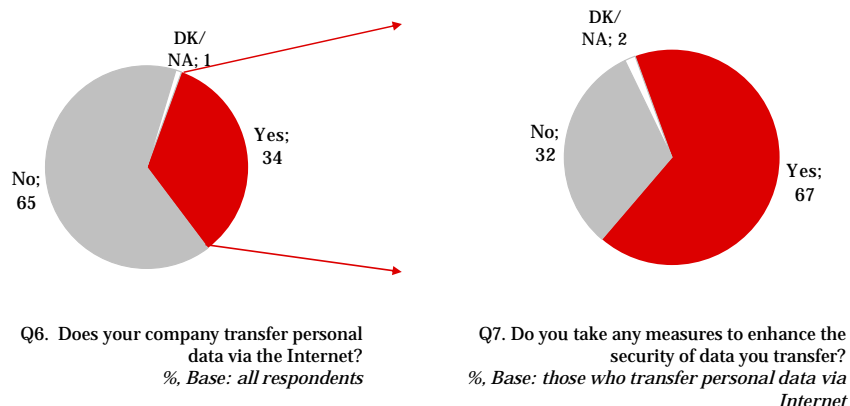
Respondents working in the service sector were more likely than respondents working in other activity sectors to use technology PETs. Fifty-nine percent of respondents in the service sector said they used PETs, compared to, for example, 47% of respondents in the trade sector. Results by size of the company showed that usage of PETs was more widespread in large companies, with over 250 employees (70%). 47% of respondents in the smallest companies and 58% in the medium-sized companies reported using such technology.

2.2 Transfer of personal data via Internet and related security measures

Two-thirds of respondents throughout the EU (65%) indicated that their company transferred personal data via the Internet. Two-thirds of companies that transferred data via the Internet (67%) also took some measures to enhance the security of the data that was transferred. Nevertheless, 32% of

respondents admitted that their company did not take any security measures when transferring personal data via the Internet.

Transfer of personal data via the Internet and related security measures



The proportion of companies that transferred personal data via the Internet ranged from 13% in Germany to 59% in Slovakia. Looking at the other countries at the top and the bottom of the ranking, it was noted that in Bulgaria (14%), Luxembourg (22%) and the Netherlands (23%) less than one in four respondents said that their company transferred personal information via the Internet, compared to a majority of respondents in Portugal (58%), Denmark (56%) and Austria (50%).

Companies in the construction and industry/manufacturing sectors (38% and 37%, respectively) were more likely to have transferred personal data via the Internet than companies in the service and trade sectors (33% and 30%, respectively). But, when companies in the service sector transferred data via the Internet, they were more likely (than other sectors) to have taken measures to keep the data secure (73% compared to 63% in the industry sector, and 64% in the construction and trade sectors).

Although larger companies made only slightly more transfers of personal data via the Internet, they took more steps to keep the data secure. Thirty-seven percent of respondents in large companies said that personal data was transferred via the Internet, and 86% of them also indicated that measures were taken to enhance data security. By comparison, 33% of respondents in small companies said that data was transferred via the Internet and 61% of them also said that security measures were taken.

2.3 Transfer of personal data outside the EU

A principle of the European *Data Protection Directive* is that personal data can only be transferred to countries outside the EU that guarantee an *adequate* level of protection. Only a minority of EU respondents in charge of data protection issues indicated that their company transferred personal data to countries outside the EU (10%) against 89% who indicated that no such transfers occurred.

The *industry and service sectors* were more inclined to transfer personal data to non-EU countries, with 13% and 10%, respectively, of respondents saying that their company made such transfers. By comparison, 5% of respondents in the construction sector and 6% of respondents in the trade sector answered that such data was transferred outside of the EU.

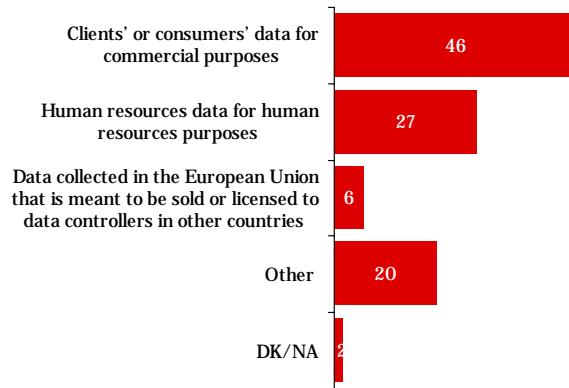
Results by the *size of the company* revealed that the largest companies had the highest rate of respondents answering that personal data was transferred outside the EU (15% vs. 9% of small companies, and 11% of medium-sized companies). The more international perspective of large companies compared to that of SMEs may well explain this result.

Respondents, who indicated that their company transferred personal data to non-EU countries, were also asked: a) what type of personal data they most frequently transferred and b) which channels were used to transfer the data. As a last step, respondents were asked if they were aware of the expression “standard contractual clauses”.

Type of personal data transferred to countries outside the EU

Among companies that transferred personal data to non-EU countries, almost half of respondents (46%) indicated that this data mostly concerned clients’ or consumers’ data for commercial purposes, and 27% said it was human resources data for HR purposes. 6% said that their company mostly transferred EU data that was meant to be sold or licensed to data controllers in other countries. Finally, one in five respondents answered that the data their company transferred was mostly data of another type than those listed so far.

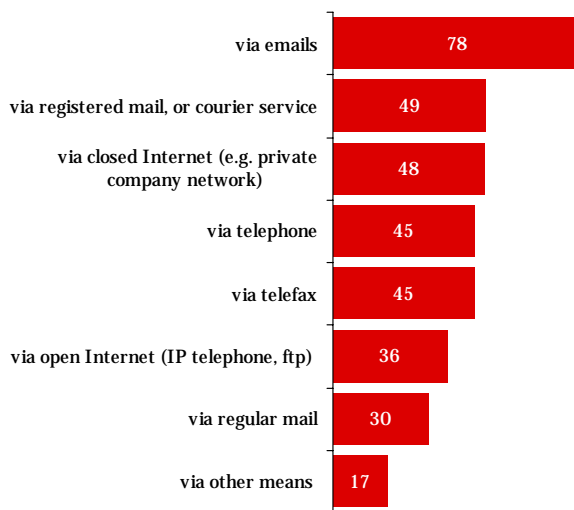
Type of data transferred to non-EU countries



Q9. What type of data does your company transfer to such countries, mostly?
 % Base: those who transfer personal data outside the EU

Channels used to transfer personal data to countries outside the EU

Ways to transfer personal data outside the EU



Q10. How does your company transfer personal data to other countries? Do you use each of the tools I will read out? Do you transfer personal data ...
 % Base: those who transfer personal data outside the EU

Personal data are predominantly transferred using electronic means. Four-fifths of respondents (78%) said that in their company personal data was transferred to countries outside the EU using emails. More or less equal proportions of respondents mentioned that such transfer happened via registered mail or a courier service (49%), via ‘closed’ internet (e.g. a company network) (48%), by telephone or fax (both 45%). A smaller proportion of respondents answered that their company transferred personal data to non-EU countries via ‘open’ internet (IP telephone or ftp server) (36%) or regular mail (30%). Finally, 17% of interviewees indicated that other channels, than those mentioned so far, were used to make such transfers

Awareness of the expression “standard contractual clauses”

The European *Data Protection Directive* requires Member States to permit transfers of personal data to countries outside the EU only where there is adequate protection for such data. The European Commission approved “standard contractual clauses” which companies transferring data to non-EU countries could use to fulfil the requirements set down by the Data Protection Directive. Respondents, who had indicated that their company transferred data to non-EU countries, were asked if they had even heard of the expression “standard contractual clauses”. Only one in three respondents (34%) were familiar with this expression and two-thirds (65%) said they had never heard of it.

3. Recent experiences with privacy policy and data protection

3.1 Companies' experiences with access requests and complaints

“Subject Access” is a data subject’s right to see personal data held about them by an organisation. If it is proven that personal information held about a data subject is incorrect or misleading, steps can be taken to have this rectified or destroyed. In extreme cases, compensation can be claimed if damage and distress have been caused. In order to analyse the experiences of EU companies with subject access requests and complaints filed by data subjects, respondents were asked:

- how many **access requests** their company had received last year, and
- if they had ever received **complaints** from individuals whose data was currently being processed.

Almost half of the interviewed individuals responsible for data protection issues in their company (46%) indicated that their company had received requests for access to personal data during the previous year.

Slightly less than four out of 10 respondents (37%) reported that their company did not receive any access requests in the same period. Finally, seventeen percent of respondents could not tell / were not aware if their company received any access requests.

Those who were requested to provide access to personal data held by their organisation were most likely to report only a few such requests: 28 percent of respondents said that their company received less than 10, and 14% indicated that their company had received between 10 and 50 requests. Only 6% of interviewees answered that their company had received more than 50 requests during the last year.

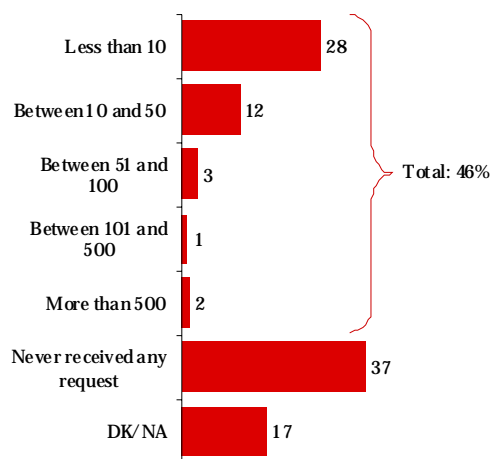
Overall, **only 3% of respondents answered that their company had received complaints** from individuals whose data was currently being processed.

Results by *company characteristics* showed that individuals responsible for data protection issues in companies with more than 250 employees were those receiving the most access requests and complaints. Not surprisingly, respondents in the bigger companies reported receiving a large number of access requests (13%, over 50 requests) – while only 5% and 6%, respectively, of respondents in small and medium-sized companies said that they received more than 50 requests.

Similarly, the percentage of respondents who reported that their company had received *complaints* from individuals, whose data was being processed, was 14% in the largest companies, compared to 3% in medium-sized companies and 2% in the smallest companies.

Compared to 2003, the number of complaints received remained stable in the EU15 countries (4% in 2003 vs. 3% in 2008), but the access requests decreased sharply (from 71% to 46%).

Access requests to personal data held by the organisation



Q14. Could you indicate the approximate number of requests for access to personal data received by our company during last year?
%, Base: all respondents

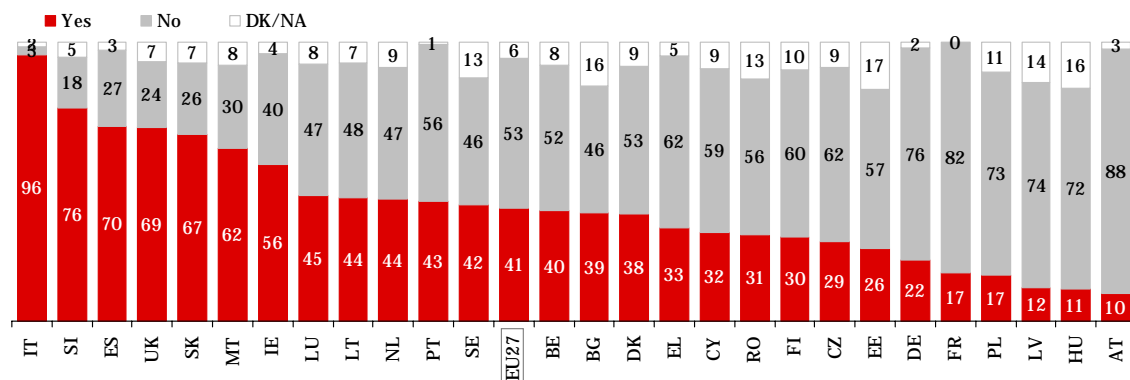
3.2 Privacy policy notices

A “*privacy policy*” notice describes how a data controller collects personal information about data subjects; for example, it mentions what personal information is collected, how the data may be used, with whom they may share it, what choices data subjects have regarding its use, and how the data is protected. A data controller may update the privacy policy notice when changes are made in the privacy practices, because of changes in relevant and applicable legal or regulatory requirements, the business or business practices.

Four out of 10 respondents throughout the EU (41%) answered that their company **maintained and updated a privacy police notice**, while slightly more than half of respondents said that this did not happen (53%). A minority of 6% did not know if their company updated these policy notices.

The individual country results showed that almost all respondents in Italy claimed that their company maintained and updated a privacy policy notice (96%). Slovenia (76%), Spain (70%), the UK (69%), Slovakia (67%), Malta (62%) and Ireland (56%) also had a majority of respondents who answered that their company updated such notices. Austrian companies, on the other hand, were the ones that least frequently said they maintained and updated privacy policy notices (10% of respondents answered “yes”), followed by companies in Hungary (11%) and Latvia (12%).

Maintaining and updating privacy policy notices



Q13a. Does your company maintain and update privacy policy notices?
%, Base: all respondents, by country

Seventeen percent of interviewees in the EU27 answered that their **company monitored how frequently their privacy policy notice was examined by the public**, and three-quarters (74%) said that their company did not monitor such practices. Furthermore, 9% of respondents did not know if such monitoring took place.

Italian companies were the ones that not only most often maintained and updated a privacy policy notice, but they were also the most likely to say that public examination of that notice was monitored (65% said this occurred in Italy). The proportion of companies that monitored how frequently the notices were examined by the public was significantly lower in all other Member States.

Companies in the service sector, more often than companies in other *activity sectors*, said they updated and maintained privacy policy notices and monitored how frequently such notices were examined by the public. While half of respondents in the service sector (49%) answered that their company updated privacy policy notices, compared to, for example, only 33% in the construction sector. Similarly, one in five respondents working in the service sector (19%) answered that their company monitored the review of policy notices by the public compared to, for example, 12% in the trade sector.

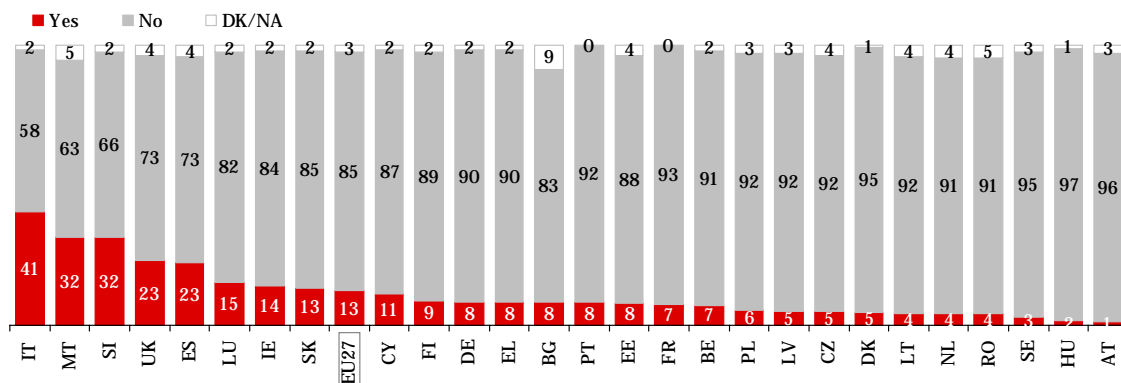
Results by *company size* showed that those with fewer employees were less likely than larger companies to maintain and update privacy policy notices or to monitor how frequently these notices were examined by the public. Thirty-six percent of respondents in companies with less than 50 employees said that their company updated privacy policy notices, and 15% said that they monitored if

these notices are reviewed by the public. The corresponding percentages for respondents in companies with more than 250 employees were 62% and 27%.

3.3 Contacts with the national data protection authority

At the EU27 level, 13% of interviewees reported that they were in regular contact with the national data protection authority in their country, while 85% claimed the opposite. Results showed large variations between countries in the regularity of contacts with data protection authorities. Regular contact with the authority was most likely for Italian companies (41%). There was also a high level of respondents who were in regular contact with the national data protection authorities in Malta and Sweden (both 32%). However, regular contacts with data protection authorities practically never occurred in Austria (only 1% of respondents said they were in regular contact with the authority), Hungary (2%) and Sweden (3%).

Contacts with the national data protection authority



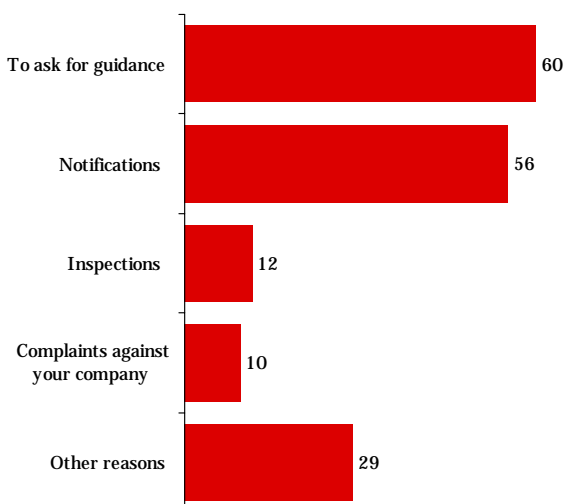
Q12a. Are you in regular contact with the national data protection authority of (OUR COUNTRY)?
%, Base: all respondents, by country

Results by *activity sector* showed that data controllers in the service sector were more likely than those working in other sectors to be in regular contact with the national data protection authority (18% vs. 10% in the industry sector and 8% in the construction and trade sectors). The likelihood that a company had regular contacts with the national data protection authority increased with *company size*. Respondents working in a large company were three times more likely, than respondents in the smallest companies, to say they had regular contact with the data protection authority (31% vs. 10%).

Respondents were also asked why they had been in contact with the national data protection authority. They could select several reasons from a pre-defined list.

The largest group of respondents (60%) said they were looking for advice. More than half of respondents (56%) had contacted this authority concerning notifications. Smaller proportions of respondents said that they contacted the authorities concerning inspections (12%) or complaints against their company (10%). Finally, three out of 10 respondents (29%) said they had been in touch with their national data protection authority for other reasons than those specified in the survey.

Reasons for contacting the national data protection authority



Q12b. Were you in contact with national data protection authority concerning ...
%, Base: those who were in contact with the national data protection authority

4. The future of the legal framework on data protection

In this chapter we analyse the actions that companies would favour in order to improve and simplify the implementation of the legal framework on data protection. The respondents were presented with a list of five actions and were asked to indicate for each one if they were in favour or not.

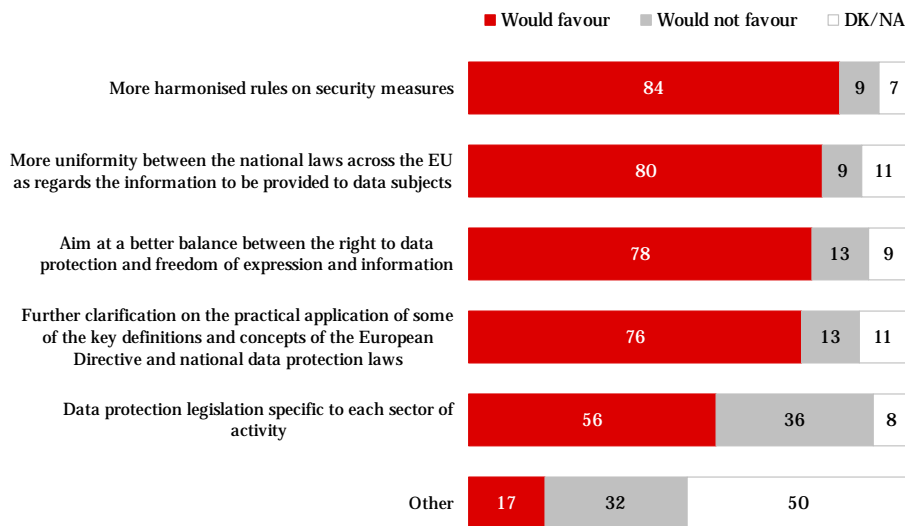
The most favoured action in order to improve and simplify the implementation of the legal framework on data protection was **greater harmonisation of the rules on security measures** (84% of interviewees were in favour of this action), while the least favoured action was the development of data **protection legislation specific to each sector of activity** (56% of interviewees favoured this action).

In line with the desire for more harmonisation, a similar proportion of respondents supported the other actions listed in the survey:

- Eight out of 10 respondents were in favour of **making national laws, with respect to information provided to data subjects, more uniform across the EU.**
- Seventy-eight percent agreed with the **aim of having a better balance between the right to have your data protected, and freedom of expression and information.**
- A slightly lower proportion of 76% would welcome **further clarification on the practical application of some of the key definitions and concepts of the European Directive and national data protection laws.**

Finally, 17% of respondents favoured an action other than those listed in the survey, while 32% did not favour any additional actions to improve and simplify the implementation of the legal framework on data protection.

Favoured actions to improve and simplify the implementation of the legal framework on data protection



Q16. Please indicate which of the following actions would you favour to improve and simplify the implementation of the legal framework on data protection?
 %, Base: all respondents

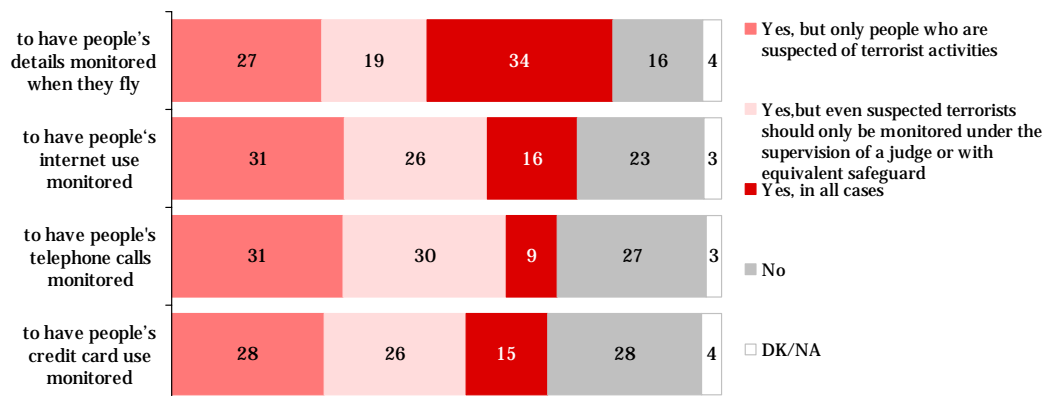
5. Data protection in the light of international terrorism

Towards the end of the survey, the data controllers' attitudes were explored in respect of any restriction of individuals' data protection rights, because of monitoring actions taken in the fight against terrorism. Respondents were asked whether in light of international terrorism, it should be possible to have people's actions monitored, e.g. their telephone calls, use of the Internet, credit card transactions or their personal flight details.

The results indicated that most interviewees were ready to accept restrictions of data protection rights where this benefited the fight against international terrorism. A majority of respondents answered positively that it should be possible to monitor the different actions listed in the survey (a conditional or unconditional yes answer was given by 69%-80% of respondents, depending on the activity), while only a minority dismissed this idea completely (16%-28%).

However, respondents were still suspicious about any provisions that would allow authorities to restrict data protection rights, even if this assisted the authorities in the fight against terrorism. Most respondents who were in favour of monitoring telephone calls, Internet and credit card usage or passenger flight details, emphasised that the restrictions of the data protection laws should have clearly defined limits. Around 30% of respondents stressed that only suspects should be monitored and between 19% and 30% wanted to see even stricter rules applied, i.e. monitoring of activities of suspects should only be possible when it was carried out under the supervision of a judge.

Monitoring of people's phone calls, Internet usage, credit card usage and personal details when flying



Q17. In light of the fight against international terrorism, do you think that, in certain circumstances, it should be possible:
%, Base: all respondents

Over three-quarters (80%) of respondents agreed that people's personal flight details should be monitored, and a third (34%) felt that this could be done unconditionally (i.e. should be possible *in all cases*) – this action received the most 'unconditional' support.

Most respondents agreed with the public authorities' assessment that the Internet was an efficient and dangerous tool for the preparation of terrorist attacks and that it should be monitored. After people's flight details, respondents were the most likely to agree to the monitoring of Internet usage (73%), with just a quarter (23%) dismissing this possibility.

Respondents were more reluctant to agree to the monitoring of telephone calls and credit card transactions. While a majority still agreed that this could be done (70% and 69%, respectively, but in most cases conditionally), more than a quarter of respondents were opposed to the idea of such checks (27% and 28%, respectively). Particularly in regard to telephone calls, respondents feared that the authorities were prying too much into people's private lives as a by-product in the fight against terrorism. In this case, respondents were the least likely to say that monitoring should be possible in all cases (9%) and most likely to say that it should only be applied to suspects (31%) or that even suspected terrorists should only be monitored under the supervision of a judge (30%).