EUROPEAN DATA PROTECTION SUPERVISOR

Measuring compliance with Regulation (EC) 45/2001 in EU institutions and bodies ("Spring 2007")

General Report

Brussels, 14 May 2008

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

Introduction

According to Article 41, paragraph 2 of Regulation (EC) 45/2001, the European Data Protection Supervisor is responsible for monitoring and ensuring the application of the Regulation. In March 2007, the EDPS launched a procedure known as "Spring 2007" as part of an effort to measure compliance with the Regulation in the various institutions and agencies and to take stock of the progress made so far.

I. Methodology

The first part of the operation took the form of letters addressed to the heads of institutions and agencies in their role as persons responsible for ensuring compliance with the Regulation.

When proceeding to make requests to the institutions/agencies, the EDPS made a distinction between different categories of institutions/agencies, based on the period since the appointment of a Data Protection Officer (DPO). The idea behind this was that the appointment of a DPO gave an indication on when compliance with the Regulation had been initiated within the institution/agency which is an important factor to take into account when measuring compliance.

Category 1

"Category 1" agencies were all those agencies where at the time of the launching of the "Spring 2007" exercise, no DPO had yet been appointed (March 2007). This was the case for 10 out of the 36 operational agencies.

The first action concerning these agencies was launched in the beginning of March 2007[1] when letters were sent out to the directors of the agencies concerned, informing them of their obligation to appoint a DPO (Article 24 of the Regulation) and to notify the appointment to the EDPS by mid May 2007. Copies of those letters were also sent to the responsible DGs at the Commission to underline the necessity to provide the DPO with adequate resources to be able to perform his/her duties.

Replies to these letters were received informing the EDPS of the appointment of a DPO. When necessary the EDPS made further requests concerning these appointments notably to ensure that an adequate term of mandate had been set and that there were no conflicts of interest between the duty as DPO and other official duties, in particular in relation to the provisions of the Regulation.

A second action took place in July 2007 in the form of letters sent to the agencies concerned requesting:
- Information on the available resources provided to the DPO to carry out his/her duties;
- An inventory of all processing operations involving personal data in the agency.

[1] Two letters were sent on 15 May (ECDC, EASA) with deadline to reply to EDPS by mid-July 2007

Replies to these letters were requested by December 2007 and an analysis of the information was carried out.

Category 2

"Category 2" agencies and institutions were all those institutions/agencies where at the time of the launching of the "Spring 2007" operation, a DPO had been in office for under 2 years. This category concerned 10 institutions/agencies.

Letters were sent on 19 April 2007 in which four groups of questions were raised:

1. Concerning the DPO:
- Whether adequate resources have been allocated to the DPO for him/her to be able to carry out his/her functions effectively.
- An explanation of the available resources for the DPO (e.g. secretary, assistant, training, potential time allocated for his/her function as a DPO).

2. Inventory and notifications of processing
- Whether an inventory of processing operations involving personal data has been made in the institution/body and to receive a clear explanation as to its results.
- To what extent the institution/body has complied with the obligation to notify processing operations to the DPO.

3. Prior checking of processing operations
- A recent inventory of those processing operations in the institution/body which fall under the scope of Article 27 of Regulation 45/2001 and should therefore be submitted to the EDPS for prior checking was requested.
- A clear explanation on the latest status of all cases mentioned in this inventory.

4. Further implementation
Full implementation of the Regulation has many other aspects including, for example, the adoption of further implementing rules (Article 24.8 of the Regulation) and raising awareness on data protection issues among staff members. The EDPS therefore requested to receive models of privacy statements used by the agency and information on how data subjects can exercise their rights.

The EDPS, as an institution, must also comply with Regulation (EC) 45/2001. A specific note was therefore sent to the Head of Administration of the EDPS requesting information on the inventory of processing operations; the inventory of processing operations subject to prior checking and further implementation of the Regulation.

Replies to all category 2 agencies and institutions were requested by mid-September 2007.

The answers have been analysed and, where necessary further clarifications were requested at the beginning of January (with an answer requested by end of February).

Category 3

"Category 3" agencies and institutions were all those institutions/agencies where at the time of the launching of the "Spring 2007" operation, a DPO had been in office for more than 2 years. This category covered 16 institutions/agencies.

Letters were sent on 20 April 2007 in which the same four groups of questions were raised as for category 2 (see above) adding a question relating to areas in the work of prior checking which were initially qualified by the EDPS as "priority areas" (medical files, staff appraisal, disciplinary procedures, social services and e-monitoring).

Where relevant a question was raised on:

- Why the EDPS has not received notification of some of these areas.
- A clear explanation why the responses to the EDPS are pending for so long in certain specifically mentioned case files.

All institutions/agencies replied.

Following the replies to these letters, when necessary, further clarifications were requested in order to have an accurate picture of the situation.

The division of institutions and agencies into different categories proved useful in order to raise the relevant questions according to the situation of the agency/institution. In the analysis of the replies, however, a distinction between agencies and institutions proved more relevant. Indeed, letters were sent out to 4 agencies which were grouped in category 3 because they had a DPO since a number of years (OHIM, CPVO, EMEA, FRA/ex EUMC[2]). However, the situation of agencies must be singled out: they do not always have the same means to dedicate to data protection and hence a certain margin of manoeuvre was allowed. In the assessment of progress made, this specificity has been taken into account.

II. Results of the reporting exercise

1. Data Protection Officers

a) Appointment of a DPO

As mentioned above at the time of the launching of the "Spring 2007" exercise, all institutions had appointed a DPO. However, out of the 36 operational agencies, 10 had not yet done so. The letters sent out by the EDPS to the directors of the agencies concerned reminding them of their obligation to appoint a DPO, resulted in the appointment of a DPO in all agencies. Subsequently however, due to departure of the person acting as DPO, in one agency a definite replacement has not yet been found. The EDPS has urged this agency to resolve the situation.

In November 2007, the EDPS was also informed of the appointment of a DPO at the European Investment Fund (EIF), a function which had been previously performed by the DPO of the EIB.

[2] Please see annex at end of report for list of abbreviations

b) Adequacy of resources provided to the DPO

According to Article 24(6) of the Regulation, the DPO must be provided with the staff and the resources necessary to carry out his or her duties. Although when gathering information, the EDPS did not make a distinction between institutions and agencies, this distinction is relevant as concerns the resources allocated to the DPOs, since the size and nature of agencies have to be taken into account in this assessment.

Agencies

In nearly all the agencies the DPO exercises his function of DPO on a part time basis and exercises other functions in parallel, such as legal adviser or contact officer. According to the EDPS, providing sufficient staff resources for the DPO function notably implies that sufficient time must be allocated to the DPO to enable him or her to perform the duties assigned to him or her. This is especially true at the start of the setting up of a DPO function where numerous tasks are to be undertaken such as awareness raising, setting up a register of processing operations, providing necessary tools to enable controllers to notify processing operations to DPO in accordance with Article 25 (notification forms, instructions, bilateral meetings), and the notification of processing operations subject to prior checking to the EDPS. The EDPS has noted that, particularly in the agencies, the fact that DPOs also have other duties often hinders their availability for DPO functions.

In some agencies a limited percentage of working time has been allocated for DPO duties (10% or 20%). In one agency the DPO was appointed full time for a set period of time to enable him to perform his duties. These measures are welcomed by the EDPS, if only because they also contribute to ensuring the independence of the DPO function[3]. Some agencies have also assigned trainees to help the DPOs in the performance of their duties.

In many agencies, the DPO has the support of other services such as the legal service, or the IT services. One agency (EMEA) has also appointed a "data controller" whose responsibilities are to "assist the DPO and the EDPS in the performance of their duties, to implement technical and organisational measures intended for the lawful processing of personal data of EMEA staff members, and to notify the DPO of any data processing operation before undertaking it, in accordance with Article 25 of the Regulation".

As concerns training possibilities for DPOs in agencies, in general, the DPOs are able to attend the DPO network meetings and the training for new DPOs organised by the EDPS.

Institutions

The three main institutions (Commission, Council, EP) have a full time DPO. The European Court of Auditors also has a full time DPO. The other DPOs are part time

[3] See EDPS Position paper on the role of the DPOs in ensuring effective compliance with Regulation (EC) 45/2001, Brussels, November 2005

with no clear cut time allocated for DPO tasks. Their other functions are notably legal adviser, managerial adviser, head of IT, or finance officer.

The bigger institutions have also appointed an assistant DPO. In most cases the assistant is full time.

Some institutions have also appointed data protection coordinators (DPCs) or contact persons. The biggest network is that of the Commission with a DPC in each DG. The Council has a smaller network of contact persons in the field of data protection (7 persons). The ECB has appointed record management specialists as data protection coordinators for the business areas of their portfolio. Their role is to assist the DPO in various ways, including identifying the relevant controllers and promulgating the DPO's advice.

As for budget, only one institution (ECB) has mentioned an allocated budget for the DPO. Some institutions underline that they have never refused a budgetary commitment (Council, ECA). The DPOs of the institutions often benefit from the support of other services such as the legal or IT service.

Some institutions mention training for the DPO mostly in the form of participation in the DPO network meetings. The EDPS considers this as a very minimum to enable DPOs to carry out their duties and to be aware of developments in the field of data protection.

2. Notification to the DPO in accordance with Article 25

Article 25 of the Regulation provides that the DPO should receive a notification of processing operations involving personal data. Although not mandatory, the EDPS has underlined the usefulness of a general inventory of all processing operations involving personal data as a tool to measure compliance with this obligation and requested that the agencies and institutions send this inventory to the EDPS.

Agencies:

Out of the 10 agencies with a recently appointed DPO (category 1), 5 have not yet set up an inventory of processing operations. This is largely due to the fact that these agencies were recently set up or because the DPO function is new. In most agencies, it has therefore been difficult for the EDPS to assess the level of notifications to the DPO.

In order to assist the controllers in their notification work some DPOs (at EACA, EFSA, FRONTEX, EACI, PHEA, for example) have developed specific tools such as information sessions, bilateral meeting with controllers, comments on the main provisions of the Regulation and guides with examples of how to fill in a notification form. Despite these instruments and the fact that notification of processing operations to the DPOs is a legal obligation, notification has been generally very low in most agencies.

The reasons for this low level of notification differ according to the categories of agencies:

In the most recently set up agencies or those with a more recent DPO, only in two agencies have the DPOs received all notification forms duly filled in (FRONTEX, FRA). In the other agencies notifications to the DPO have not yet started. This can be explained by the fact that the DPOs have so far concentrated on awareness raising, identifying processing operations and drafting a notification form. The EDPS has therefore encouraged those agencies to proceed with notifications to the DPO in accordance with Article 25.

In other agencies where DPOs have been appointed for a longer period of time and in which an inventory has been established, either no information on the notifications to the DPO has been provided, or the level of processing operations notified is fairly low. This low level of notification is more worrying than in recently set up agencies and could be a result of the inadequate means that the DPO has to obtain compliance from data controllers or of the limited time allocated to the DPO to enable him/her to perform his/her duties. The EDPS has therefore, where necessary, underlined the responsibility of the management of agencies in ensuring compliance with this legal obligation and set a specific target.

Institutions

Out of the 11 EU institutions and bodies with a DPO since more than two years, three do not have an inventory of processing operations. In two of these bodies, the setting up of such an inventory is in progress whereas in one case, the institution does not intend to set up such an inventory as it is not considered as a legal obligation. As mentioned above, the EDPS considers that, although not a legal obligation, the inventory is a useful tool to measure compliance notably with Article 25.

Other institutions presented positive progress and good results as to how many of the listed operations are entered in DPO register. When considering the results, the EDPS has taken into account the size of the institution/body. Indeed in the larger institutions, full compliance is often harder to achieve. In two bodies, the EDPS was informed that all the listed processing operations had been notified to the DPO (EO, OLAF). In the other institutions/bodies, the level of listed processing operations notified to the DPO ranges around 85%. The EDPS is satisfied with this level of notification, but underlines that full compliance should be achieved in all institutions. In some institutions/bodies, where the level of compliance is relatively low, the EDPS has highlighted the need for closer cooperation from controllers and set a specific target.

3. Prior checking of processing operations

In his letter to agencies which had already appointed a DPO at the start of the "Spring 2007" exercise (category 2 and 3), the EDPS requested an overview of the state of compliance in the field of prior checking notifications in accordance with Article 27 of the Regulation. In the category 3 institutions/agencies the EDPS also requested an update on the status of the cases falling in the priority areas and which had not yet been submitted to the EDPS (medical files, staff appraisal, disciplinary procedures, social services and e-monitoring). An explanation was required as to why notification of these cases had not yet been made to the EDPS. In some cases an explanation was

also requested as to why responses to questions raised by the EDPS in pending prior checking cases had taken so long.

Agencies

Within agencies, in general, prior checking notifications to the EDPS have been relatively low as DPOs have been busy with the task of first obtaining notifications from controllers in accordance with Article 25 and identifying cases subject to prior checking (see above). In at least 4 agencies, no inventory of cases subject to prior checking has yet been established.

The EDPS has encouraged the notification of ex post processing operations to the EDPS, but is considering establishing a procedure for those processing operations based on a standard procedure common to all agencies. As for true prior checking for procedures common to all agencies, the EDPS is also considering being consulted at an early stage of the procedure by the Heads of Agencies so as to integrate data protection aspects.

In the identification of processing operations subject to prior checking, agencies have sometimes identified procedures involving the processing of personal data which the EDPS has considered as not subject to prior checking (e.g. personal files of staff). In the replies sent to the agencies, the EDPS has therefore invited the DPOs to refer to previous positions taken by the EDPS on similar cases.

Institutions

As for notification of cases subject to prior checking in the institutions, four institutions have so far notified to the EDPS all of the processing operations subject to prior checking (EO, OLAF, ECB, EIB). In these cases, the backlog of ex post prior checking cases has therefore been absorbed.

As for the other institutions, on average about 50% of identified prior checking cases have been submitted to the EDPS for prior checking. This can be explained in general by the lack of notification to the DPO as seen above (point II.2 Notification to the DPO in accordance with Article 25). The EDPS will continue to encourage further notifications of ex post processing operations in order to reach full compliance as early as possible and has set specific targets, where necessary.

In one institution, only two cases have been submitted. The EDPS will be closely monitoring this institution.

4. Further implementation

The full implementation of the Regulation has many other aspects, including for example the adoption of further implementing rules (Article 24(8) of the Regulation) and raising awareness on data protection among staff members. The EDPS as the European Guardian of personal data puts special emphasis on the rights of data subjects. In this context, in his letter of April 2007, the EDPS invited institutions and those agencies with a DPO to submit models of privacy statements and to provide some feedback on the general practice on how data subjects can exercise their rights.

a) Raising Awareness

Raising awareness on data protection issues is one of the tasks assigned to the DPO (Article 24(1)a), but must also be seen as a task for the institution/body itself in view of ensuring compliance with the Regulation.

In many institutions and agencies, information is given through specific intranet websites (for example, Council, EMEA, OHIM, European Commission (several DPCs have their own website in intranet), OLAF, ECJ, CDT, EIB, EP). Some institutions have also designed a specific internet website. Institutions/bodies have also published information brochures on data protection (Council, CDT, EP) or intervene regularly in general newsletters or articles for internal publication. At OLAF, whenever new opinions or instructions are issued they are prominently displayed on the home page of OLAF intranet for a period of several days, EDPS opinions and decisions are put on this website along with the OLAF DPO quarterly reports. The PHEA has also developed an intranet section including guidelines, practical tips, privacy statements and notification forms.

Training or coaching by the DPO or by others is also a useful tool to raise awareness on data protection and has been promoted by a number of institutions and bodies. For example, at the Council the DPO unit ensures regular internal conferences organised for newly recruited officials. At the Commission, in addition to information and training by DPCs in their DGs, a general and specialised training session is organised by DG ADMIN in cooperation with a professional training organisation. The EP has also developed training on data protection by the Professional Training Unit. Some of the DPOs of agencies have also provided lectures to staff and management and used this occasion to distribute useful materials to staff (FRONTEX and ECDC, for example). The European Ombudsman has invited the EDPS to give a speech in view, notably, of raising awareness of staff on data protection issues.

b) Implementing rules

Article 24.8 of Regulation (EC) 45/2001 provides that further implementing rules concerning the Data Protection Officer shall be adopted by each institution or body. These rules shall in particular concern the tasks, duties and powers of the DPO. At the time of the sending of the letters to institutions and bodies, only 6 had adopted implementing rules in accordance with the Regulation. The "Spring 2007" exercise encouraged 7 other institutions and bodies to adopt such rules in 2007 and beginning of 2008. Six institutions and bodies are presently in the course of working on the adoption of such rules. The EDPS can therefore be satisfied with the progress made in this field, but encourages those institutions and bodies which have not yet done so to adopt such rules.

c) Data protection statement

The EDPS requested institution/bodies to submit examples of privacy statements. The aim in this exercise was not to evaluate each and every data protection clause or privacy notice under the Regulation, but rather to spot shortages and good practices as to content and means of conveying the information.

Many institutions and agencies with an existing DPO at the time of launching the Spring 2007 exercise submitted examples of data protection statements. As concerns the content of these statements, some listed each and every item in Articles 11 and 12 (e.g. CdT, Council, CPVO, COM), whereas others were general privacy statements which cover several processing operations at the same time. The EDPS considers that specific information for a particular processing operation is to be preferred to general statements covering various operations which often tend to be too vague or general. Although not a mandatory item, some statements include a general description of security measures. The EDPS considers that this inclusion may be reassuring for data subjects.

As to the means used to provide the information, in most cases the privacy statement is published on Intranet or Internet. Other good practices include putting it on the wall where people come and go (ECA), or including data protection information or requirements in other documents (for example in contracts, invitations to an interview or invitations to a medical visit). The Council has developed a practice whereby information required under Articles 11 and 12 is sent on personalised Staff Notes to all staff by the e-distribution service. The ECB has developed standard clauses for contracts entered into by the ECB, and publishes a privacy statement on its website

d) Exercise of rights of data subjects

In general, data subjects are informed of their rights on the DPO website, in a privacy statement accessible by intranet, and in documents or information notices submitted to them. Typical procedures to exercise their rights include contacting the controller, a generic mailbox, or the DPO. Some institutions/bodies have developed a specific form for data subjects to exercise their rights (published on Intranet).

Institutions and bodies have underlined the various ways of exercising the right to rectification depending on context. In some cases the rectification of data is done by the data subjects themselves, for example, by updating certain information in online application forms (e.g. change of address) and in other cases only after validation by the controller or by attaching documents to the file (e.g. disciplinary file).

III. Conclusions and further steps

The "Spring 2007" exercise has helped boost compliance with Regulation (EC) 45/2001, if only because it has encouraged the appointment of a DPO in every institution and operational agency. It has also encouraged most institutions and agencies to draft an inventory of processing operations involving personal data in view of measuring compliance with the Regulation more particularly as concerns notification to the DPO in accordance with Article 25 and subsequent notification of those operations falling under Article 27 for prior checking by the EDPS.

In the area of notification to the DPO, the EDPS is concerned about the low level of notification in most of the agencies and has therefore encouraged further compliance in this field. As for institutions, the progress made in this area is generally satisfactory, although the EDPS considers that full compliance should have been

achieved. The need for support for DPOs in order to obtain notifications from controllers will be signalled to the management of the institutions and bodies. As for notification of processing operations to the EDPS for prior checking, the level of notifications received from agencies is generally fairly low. This can be explained in most cases by the fact that the DPOs have been busy first obtaining notifications from the controllers. The EDPS acknowledges this, but has encouraged further progress in this field and set a specific target in some cases. As for institutions, only four institutions have managed to notify all ex post processing operations to the EDPS. In the other cases, the EDPS has underlined the need to scale up the level of notifications so as to absorb the backlog of ex post cases and in some cases set a specific target.

The "Spring 2007" exercise must be seen as a first step in ongoing work by the EDPS to monitor and ensure the application of the Regulation. Individual letters have been sent in reply to all letters received from the institutions and bodies with particular emphasis according to the specifics of the case. The EDPS will also proceed with on the spot inspections in some institutions or bodies in view of checking the reality. Finally, further requests to measure compliance with the Regulation will also be sent at a later stage in order to assess further progress made.

Annex

List of abbreviations

Institutions and agencies subject to "Spring 2007" exercise

CdT	Translation Centre for the Bodies of the European Union
Cedefop	European Centre for the Development of Vocational Training
CFCA	Community Fisheries Control Agency
COM	European Commission
CoR	Committee of the Regions
CPVO	Community Plant Variety Office
Council	Council of the European Union
EACEA	Education, Audiovisual and Culture Executive Agency
EACI	Executive Agency for Competitiveness and Innovation
EASA	European Aviation Safety Agency
EAR	European Agency for Reconstruction
ECA	European Court of Auditors
ECB	European Central Bank
ECDC	European Centre for Disease Prevention and Control
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EEA	European Environment Agency
EESC	European Economic and Social Committee
EFSA	European Food Safety Authority
EIB	European Investment Bank
EIF	European Investment Fund
EMEA	European Medicines Agency
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
EO	European Ombudsman
EP	European Parliament
ERA	European Railway Agency
ETF	European Training Foundation
EUMC	European Monitoring Centre on Racism and Xenophobia
EU-OSHA	European Agency for Safety and Health at Work
Eurofound	European Foundation for the Improvement of Living and Working Conditions
FRA	European Union Agency for Fundamental Rights (to replace EUMC)
Frontex	European Agency for the Management of Operational Cooperation at the External Border
GSA	European GNSS Supervisory Authority
OHIM	Office of Harmonisation of the Internal Market
OLAF	European Antifraud Office
PHEA	Executive Agency for the Public Health Programme