EUROPEAN COURT OF AUDITORS

Data Protection Officer

Luxembourg, 22 March 2017

SG1090732EN02-17PP-CA018-17FIN-ORAN.doc

ACTIVITY REPORT FOR 2016

Introduction

1. Regulation No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data has been applicable at the ECA since 2002.
2. Article 24 of the Regulation requires each Community institution or body to appoint at least one Data Protection Officer (DPO). Since June 2010, Johan Van Damme has been the Court's Data Protection Officer and his mandate was renewed in June 2015.
3. The Court's implementing rules, which were updated in 2012, require the DPO to produce an annual activity report.

Notification of processing of personal data

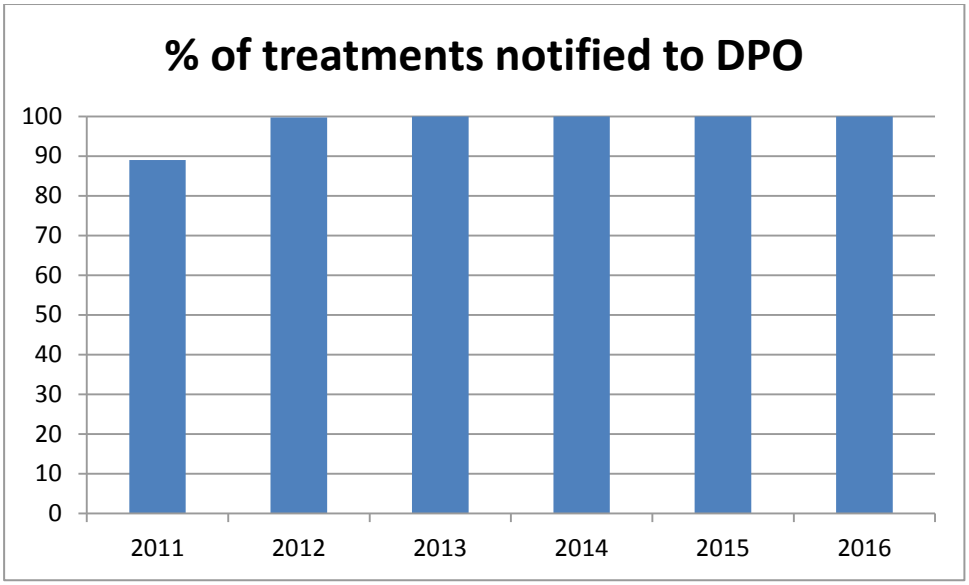
4. Article 25 of Regulation No 45/2001 requires controllers to notify the DPO of any data processing operation. The controllers are the Secretary-General, directors, some principal managers, the DPO, some committees, the panel for financial irregularities and, in the case of audits, the Members.
5. In 2016, all new personal data processing operations were reported to the DPO before processing started. The initiative taken by the Principal Manager of the Audit Quality Control Committee to verify any audit programme that did not notify the DPO of the processing of personal data largely contributed to this success. It is a legal obligation to notify the DPO of any processing of personal data by the Court and it is recommended that the person responsible for processing (the data controller) should notify the DPO from the planning phase onwards. For one Information System built in 2016, there was no notification during the planning phase: the system was discovered during a security audit and went live without taking the DPO's opinion into consideration.

12, rue Alcide De Gasperi - L-1615 Luxembourg
T +352 4398 47777 **E** ECA-data-protection@eca.europa.eu **eca.europa.eu**

The DPO's Register

6. All data processing operations reported by the controllers are recorded in the DPO's Register, which is available on the ECA's Intranet/website.
7. In 2016, 34 new notifications were received and entered in the DPO's Register; no notifications were deleted as no processing ended in 2016. One notification was updated in line with one of the new obligations that came into force under the Staff Regulations in May 2014. The total number of notifications thus increased to 200, with a modification rate of 21%, i.e. the highest number of modifications in the last six years.
8. This was the third year in a row since the Data Protection Regulation was introduced in 2001 that all personal data processing operations had been notified to the DPO.
9. Key Performance Indicator 1: The number of DPO notifications was set at 100% and this was achieved for the first time in 2013.
10. In 2011, the notification rate was 89%; in 2012, 99.7%; and since 2013, 100%.

Graph 1 – Percentage (%) of treatments notified to the DPO

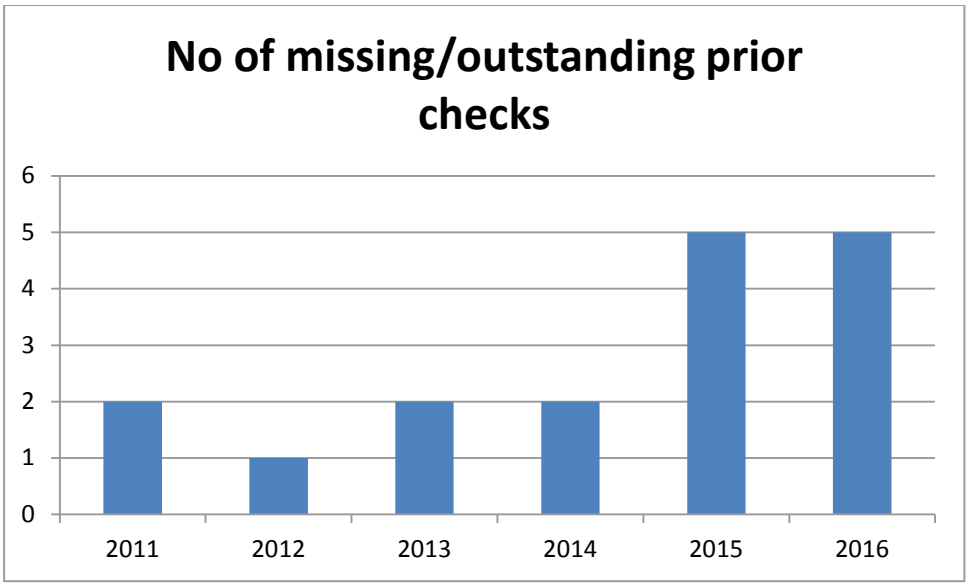


Prior checks

11. Article 27 of Regulation No 45/2001 requires that 'processing operations concerning personal data likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purpose shall be subject to prior checking by the European Data Protection Supervisor (EDPS)'.
12. In 2016, the five outstanding prior checks carried over from 2015 remained.

13. These prior checks were not carried out due to a review of the current procedures and the reform process launched at the Court. However, all necessary precautions were taken to comply with the Data Protection Regulation, including notification of the DPO.
14. Key Performance Indicator 2: The number of missing/outstanding prior checks was set at 0. In 2016, the number of outstanding prior checks was 5.
15. In 2011, 2013 and 2014, the number of missing prior notifications was 2; in 2013, it was 1; and in 2015, the figure was also 5.

Graph 2 – Number of missing/outstanding prior checks

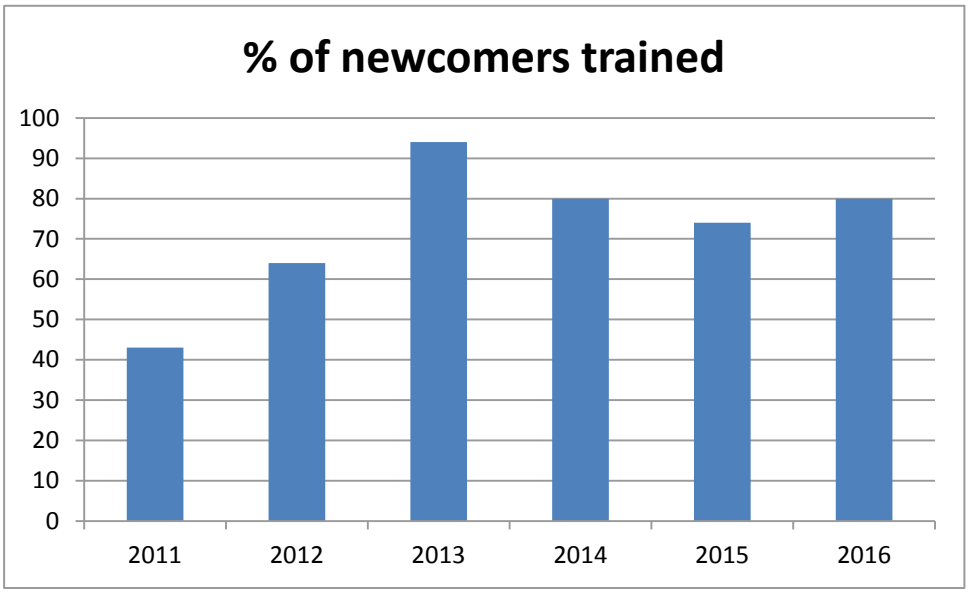


Data protection awareness

16. The information issued to staff since 2002 on the processing of personal data, which explains the key elements of Regulation No 45/2001, including rights and obligations, is still valid and is available on the DPO's page on the ECA's Intranet.
17. The DPO's page was used to disseminate awareness campaigns, best practices, guidelines and general information on data protection matters, including videos used by data protection authorities during their national data protection awareness campaigns.
18. Newly recruited staff are briefed about the Data Protection Regulation applicable at the EU Institutions at a mandatory e-learning session organised by the ECA's Professional Training unit.
19. Key Performance Indicator 3: The number of newcomers to be trained within three months of recruitment was set at 100%.
20. The penalty introduced in 2016 of suspending internet access for newcomers who have not received training within three months of being recruited was not systematically applied. Despite this new measure and the fact that multiple reminders were issued, the participation rate remained insufficient.

21. In 2016, 84 newcomers were trained, i.e. a training rate of 80% for all staff invited to participate in the e-learning session.
22. The rate for trained staff was 43% in 2011, 64% in 2012, 94% in 2013, 80% in 2014 and 74% in 2015.

Graph 3 – Percentage of newcomers trained



23. An extensive awareness campaign for auditors was organised with the aim of minimising the use of personal data in audit reports. The publication of a Good Practice note, combined with workshops and bilateral meetings with certain audit teams, had an immediate and positive impact on clearing letters issued in 2016.

Meetings with controllers, inspections and audits

24. The DPO continued to visit certain controllers at regular intervals to discuss specific and general data protection issues, mainly relating to Human Resources, the Legal Service and audit. Ad hoc informal meetings were held with Court staff upon request.
25. In 2016, the DPO paid special attention to newly launched audits, the publication of audit results, requests to use cloud services and the treatment of personal data by the ECA's credit card company.
26. The DPO assisted the archives team in establishing the retention period for every type of document processed at the ECA, especially for the Private Offices, potential fraud cases, the Internal Panel on Financial Irregularities, the harassment procedure and audit entities.
27. Dumpster-diving carried out at regular intervals found very few documents containing personal data in the ordinary wastepaper bins. The increased use of secure bins, coupled with an awareness campaign, helped to obtain this excellent result.

28. The DPO carried out several security audits of information systems which store and process personal data.

Cooperation between DPOs and the EDPS

29. The DPOs of the EU institutions/bodies met twice during 2015 to exchange experiences and best practices and to discuss data protection issues of mutual concern; they were also informed about the review of data protection legislation.
30. The EDPS visited the Court and had a meeting with the President and the Secretary-General to discuss the accountability principle introduced by the General Data Protection Regulation. This accountability principle will also be applicable to all EU Institutions and Agencies from 2018 onwards.
31. An inter-institutional project was set up to configure Windows10 devices in such a way that they protect the privacy of EU staff.

Opinions and comments

32. In 2015, the number of opinions delivered on data protection issues in response to requests from various sources increased to 55 (an increase of 27% compared with 2015). The main opinions that were delivered concerned access to documents, the use of cloud services, access rights to personal data on auditees' premises, the use of mobile devices, troubleshooting of translation tools, surveys, the use of CCTV cameras, and the right to be forgotten.

Complaints and data breaches

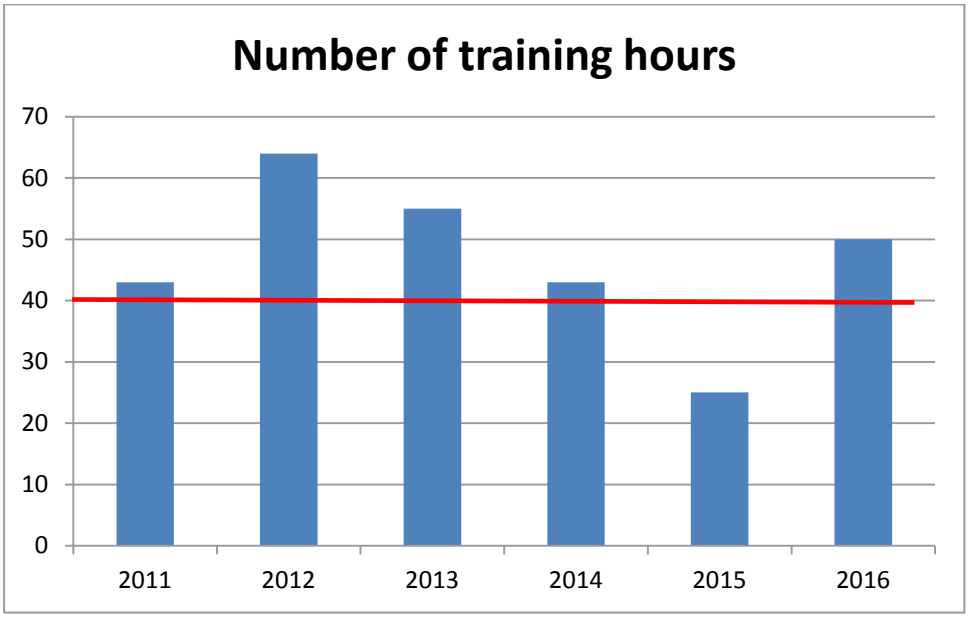
33. A complaint was received from a staff member who asked for some personal data to be removed from the accounting system at the European Commission or for access rights to be reduced. As a result, the European Commission will considerably reduce access rights to some specific personal data stored in the system.
34. One complaint received from an audited organisation accused the auditors of having collected an excessive amount of personal data. The complaint turned out to be unfounded as the auditors' actions were fully in line with international audit standards, were covered by the Court's mandate and complied fully with the Data Protection Regulation.
35. Three investigations were launched to establish whether a data breach had occurred. In one case, personal data filed in a medical form were found on the Intranet and were removed immediately. The second case concerned audit information about pension rights that had become accessible to all auditors even though only the audit team should have had access. In this case, access rights were limited immediately. The third case concerned pictures that were made available on a public cloud service which was hosted outside the EU and lacked the

necessary data protection measures. The pictures were removed immediately when the data controller was informed.

Training

36. Key Performance Indicator 4: To keep up with new technologies, case law, standards and best practices, the DPO should update its knowledge. At least five training days, covering data protection and information security topics and equivalent to 40 continuing professional education (CPE) hours, should be taken every year, or 120 hours over a three-year period. This is equivalent to what international professional audit organisations require for their members in order to maintain certification.
37. In 2016, this objective was fully met with 50 training hours. For the first time, the DPO's assistants also obtained 24 hours' specific data protection training in preparation for the new Data Protection Regulation.
38. In 2011, the number of hours was 43; in 2012, 64; in 2013, 55; in 2014, 43 and in 2015, 25.

Graph 4 - Number of training hours



DPO resources

39. A half-time administrator is assigned to the DPO function, supported by a half-time assistant. In November 2015, the Legal Service transferred an assistant to the DPO function to enable it to cope with its increased workload, especially archive cleaning, handling new notifications, reviewing the content of the DPO's Register and updating the Court's Intranet and website. Current resources are deemed sufficient to comply with the requirement of Regulation No 45/2001 to 'provide him or her with the staff and resources to carry out his or her duties'.

Conclusions

40. 2016 was a challenging year for the DPO due to increases in the number of personal data processing operations, requests from the public about the ECA's processing of their personal data, and requests for advice by data controllers and data processors, especially in the field of cloud computing.

41. Interest appears to have increased as a result of continuous awareness-raising by the DPO but also because the Audit Quality Control Committee systematically checks data protection compliance for each newly planned audit. The adoption of the General Data Protection Regulation by the European Parliament in April 2016 made it clear that the European Union had attained a new level of personal data protection. Awareness campaigns in all Member States in newspapers and magazines and on Internet news portals gave data protection permanent visibility throughout 2016.

42. In December 2016, the European Commission published a proposal for a new Data Protection Regulation applicable to all EU Institutions and Agencies with effect from 25 May 2018. Preparations to ensure compliance with this new regulation started in 2016 and will result in an action plan to bridge the gap between the current regulation and the new one that will hopefully be adopted by the European Parliament as soon as possible. 2017 is a transitional period that will require considerable efforts to be made by all EU Institutions and Agencies.

Johan Van Damme