EUROPEAN COURT OF AUDITORS

Data Protection Officer

Luxembourg, 9 February 2018
SG1100289EN01-18PP-CA020-18-OR.docx

ACTIVITY REPORT FOR 2017

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). Johan Van Damme has been the Court's Data Protection Officer since June 2010, 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

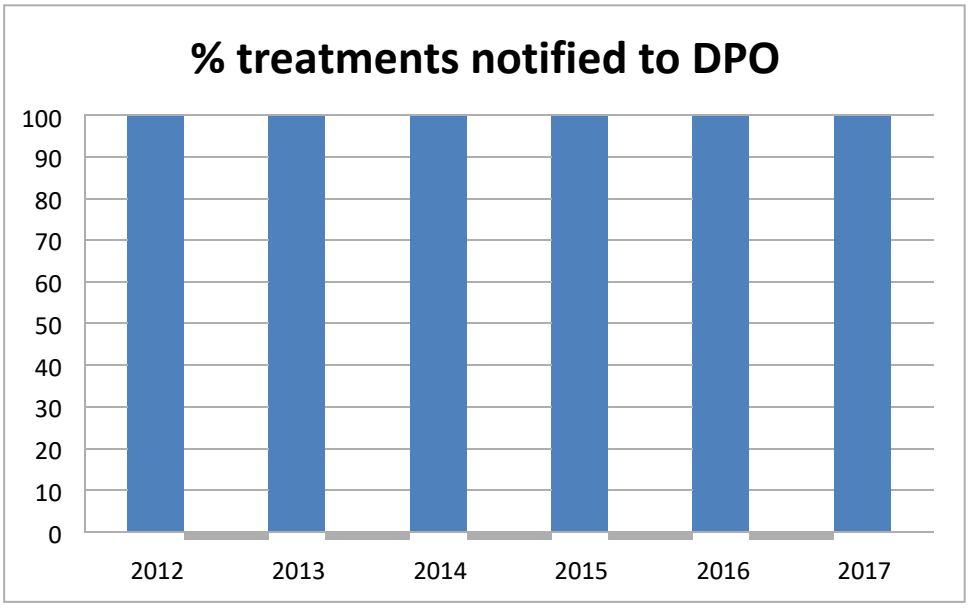
4. Article 25 of Regulation No 45/2001 requires controllers (responsible for the processing of personal data) to notify the DPO of any data processing operation. The controllers are the Secretary-General, the directors, some principal managers, the DPO, some committees, the panel for financial irregularities and, for audits, the Members.
5. In 2017, 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 block 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. The Information System set up in 2016 was not notified during the planning phase and went live without taking the DPO's opinion into consideration. This problem was discovered during a security audit and the system was phased out in 2017.

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 2017, 26 new notifications were received and entered in the DPO's Register; eight notifications were deleted as their processing ended in 2017. The total number of notifications thus increased to 218, with an increase of 17%.
8. This was the fourth year in a row that all personal data processing operations had been notified to the DPO since the Data Protection Regulation had been introduced in 2001.
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 2012, 99.7%; and since 2013, 100%.

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



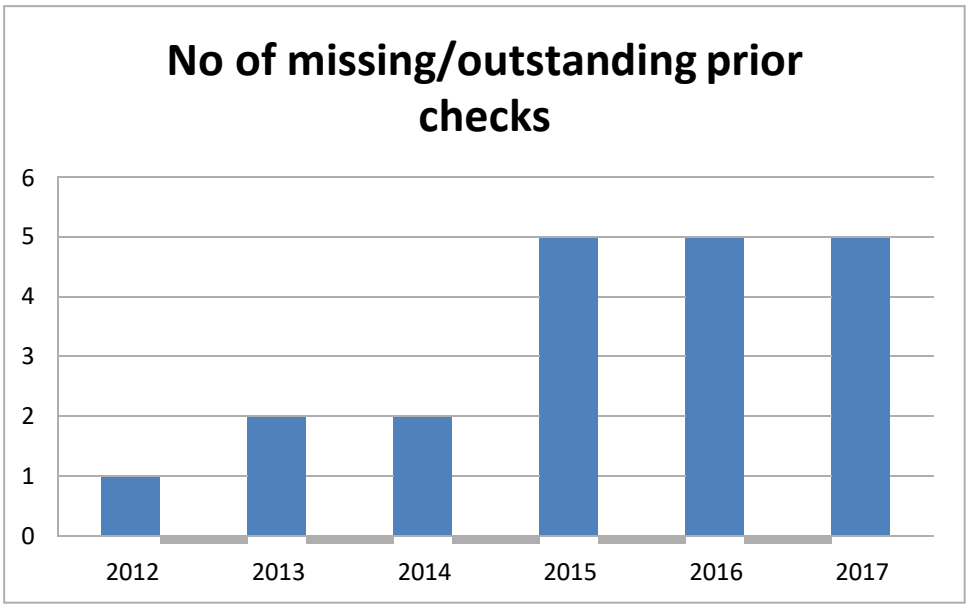
Prior checks

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 2017, the five outstanding prior checks carried over since 2015 remained.
13. These prior checks were not carried out due to a review of the data protection regulation that no longer requires a prior notification, because current procedures are being reviewed or

because no processing took place. 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 2017, the number of outstanding prior checks was 5.
15. In 2012, the number of missing prior notifications was 1, in 2013 and 2014 it was 2; and since 2015, the figure has also been 5.

Graph 2 – Number of missing/outstanding prior checks



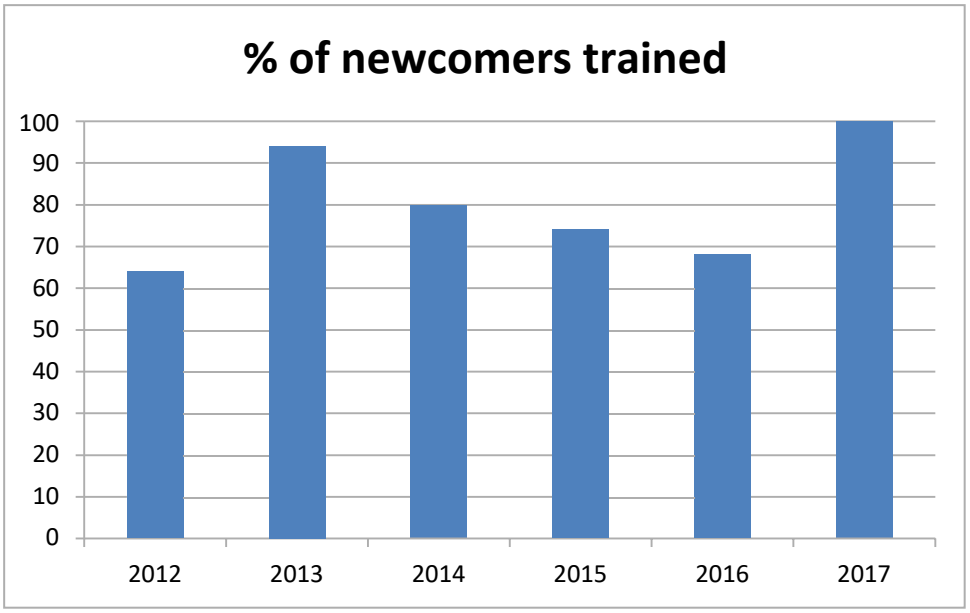
Data protection awareness

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. During the year, this e-learning module was updated and supplemented with a mandatory in-class presentation.
20. Key Performance Indicator 3: The number of newcomers to be trained within three months of recruitment was set at 100%.
21. The penalty introduced in 2016 of suspending internet access for newcomers who have not received training within three months of being recruited was systematically applied. Thanks to

this measure, introduced in 2016, the participation rate reached its target value and even surpassed it, as four staff recruited in 2016 participated in a 2017 training.

22. In 2017, 124 newcomers were trained, i.e. a training rate of 103% for all staff invited to participate in the e-learning session.
23. The rate for trained staff was 64% in 2012, 94% in 2013, 80% in 2014, 74% in 2015, and 68% in 2016.

Graph 3 – Percentage of newcomers trained



24. An extensive awareness campaign for auditors was organised during the year with the aim of minimising the collection of personal data, their secure transfer from the auditees to the ECA and the publication of a minimum of personal data in audit reports.
25. During the Court's Training Day a presentation was held on the new data protection regulation that will come into force on the 25th of May 2018, explaining the impact on the Court, EU citizens and clients.

Meetings with controllers, inspections and audits

26. The DPO continued to visit certain controllers at regular intervals to discuss specific and general data protection issues, mainly relating to Translation, Human Resources, the Legal Service and audit. Ad hoc informal meetings were held with Court's staff upon request.
27. In 2017, the DPO paid special attention to the destruction of personal data after their retention period, newly launched audits, the transfer or personal data from auditees and the use of several potential cloud services.
28. The DPO worked in close cooperation with the archives team in setting up a procedure to transfer digital data from certain information systems to the archives, and the deletion of data

outside the defined retention period. In addition, a start was made on establishing retention periods, archiving and deletion rules for collaborative digital working spaces.

29. Dumpster-diving carried out at regular intervals found no 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.
30. The DPO carried out several security audits of information systems which store and process personal data.

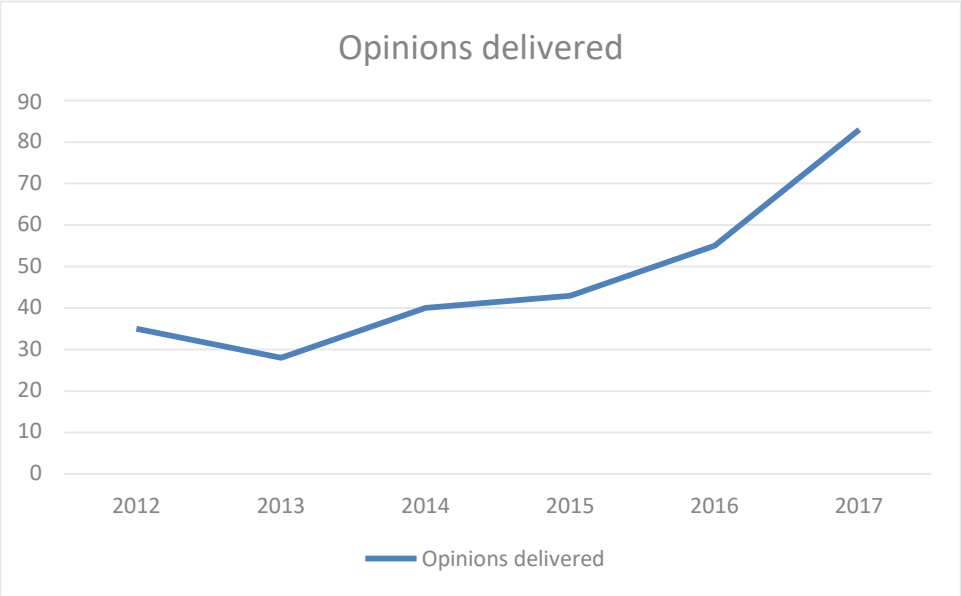
Cooperation between DPOs and EDPS

31. The DPOs of the EU institutions/bodies met twice during 2017 to exchange experiences and best practices and to discuss data protection issues of mutual concern that were largely focussed on the review of the data protection legislation and the implications it will have on the EU Institutions, the role of the DPO and the new rights given to the persons concerned.
32. The EDPS organised several workshops, in which the ECA's DPO participated, regarding new obligations, the role of the DPO, new data protection principles like accountability, privacy by design and default and privacy impact assessment.
33. The inter-institutional project set up in 2016 to implement privacy settings in Windows 10 devices was delivered to the network.
34. The GAP analysis was made regarding the current regulation and the Commission's proposal for a new data protection regulation for EU Institutions. On the basis of this analysis, an action plan for the Court was set up and shared with the DPO network. At the end of the year, the implementation of the action plan was on track and did not show any delays.

Opinions and comments

35. In 2017, the number of opinions delivered on data protection issues in response to requests from various sources increased to 83 (an increase of 50% compared with 2016). The main opinions that were delivered concerned access to documents, recruitment procedures, the use of cloud services, access rights to personal data on auditees' premises, the use of mobile devices, translation tools, surveys, retention of data, the use of CCTV cameras, transfer of data to other organisations, and the right to be forgotten.

Graph 4 - Number of Opinions delivered



Complaints and data breaches

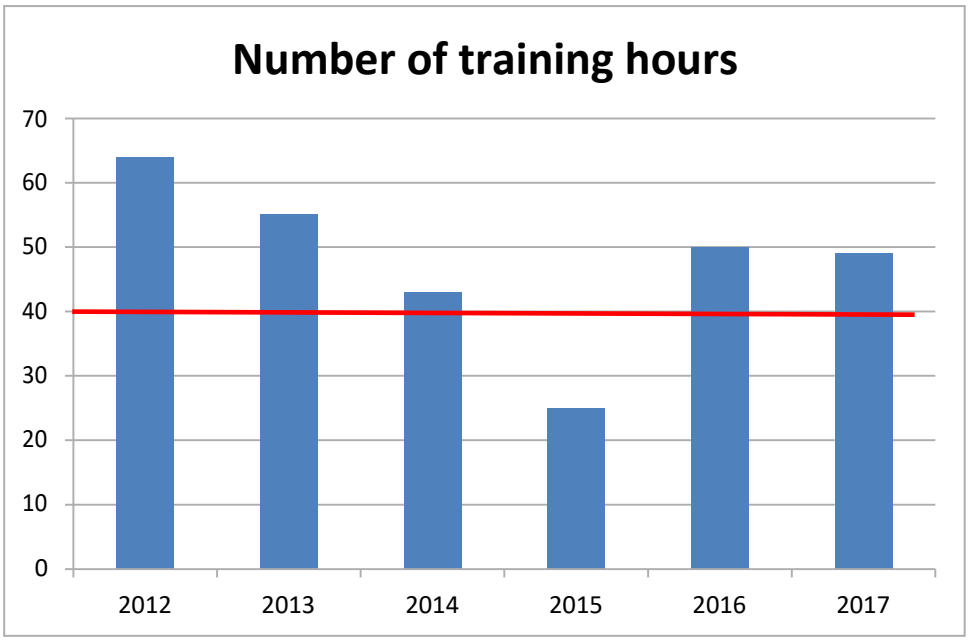
36. A complaint made in 2016 was reopened as the promised corrective measures were considered insufficient by the complainer. As a result the personal data concerned, which were stored in the accounting system at the European Commission, were deleted to the complainant's satisfaction.
37. Three investigations were launched to establish whether a data breach had occurred. In one case, where personal data was unlawfully transferred to an external expert, it was promptly destroyed at the DPO's request. For the second case, the investigation is still on-going and should clarify whether a particular category of personal data regarding a small number of people (3-5) was unlawfully processed. The third case concerned audit documents that were accessible to a larger group of auditors. The access rights in the information system were promptly reduced.

Training

38. Key Performance Indicator 4: In order to keep up with new technologies, case law, standards and best practices, the DPO needs to update his/her knowledge. At least five training days covering data protection and information security topics need to be taken every year, equivalent to 40 continuing professional education (CPE) hours, 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.
39. In 2017, this objective was fully met with 49 training hours. The DPO's assistants also obtained 74 hours' specific data protection training especially in preparation for the new Data Protection Regulation.

40. In 2012, 64; in 2013, 55; in 2014, 43 and in 2015, 25.

Graph 5 - Number of training hours



Data protection reform

41. In 2016, the European Parliament adopted a new data protection regulation, which, however, did not include the EU Institutions. However, on the 17th of January 2017, the Commission proposed a similar regulation covering the EU Institutions, Agencies and Bodies. The preparation for the new regulation already started in 2016, but from the publication of the proposal, the DPO was able officially to start its preparations to make sure that the Court would be ready to comply with this regulation by the 25th of May 2018.
42. A GAP analysis was made between the existing and proposed regulations. Based on the result of this analysis, an action plan was set up and its implementation started without delay.
43. At the end of the year, the action plan was on track and did not show any delays.

DPO resources

44. A half-time administrator is assigned to the DPO function, supported by two half-time assistants. 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' and also to prepare the Court to comply with the new data protection legislation that will come into force on the 25th of May 2018.

Conclusions

45. 2017 was a challenging year for the DPO due to increases in the number of personal data processing operations, the considerable increase in requests from the persons concerned, the people responsible and staff processing personal data. This is an excellent indicator that the

culture on the treatment of data protection had changed, insofar as all those concerned took their roles seriously and wanted to comply with the legal obligations relating to data protection principles.

46. In December 2017, the European legislator (European Parliament, Council and Commission) had not yet agreed on a final text for the new Data Protection Regulation that is to come into in force on the 25 May 2018. Preparations to ensure compliance with this new regulation started in 2016, continued in 2017 and will probably result in some adjustments to the action plan. In 2018, the PO team will have to make considerable efforts to get the Court ready for the new regulation.

Johan Van Damme