EUROPEAN DATA PROTECTION SUPERVISOR

REPORT
Survey 2015

Measuring compliance with data protection rules in EU institutions

21 January 2016

TABLE OF CONTENTS

I. Foreword

The European Data Protection Supervisor (EDPS) is the independent supervisory authority responsible[1] for monitoring and ensuring compliance with Regulation (EC) No. 45/2001 (the Regulation)[2], the relevant data protection law applying to EU institutions, bodies, offices and agencies ("EU institutions") processing personal information.

When it comes to collecting, using and storing personal data both in their day-to-day work and in their core business activities, the EDPS aims at supporting EU institutions in moving beyond a purely compliance based approach to one that is also based on accountability[3] in close cooperation with the Data Protection Officer (DPO) appointed in each EU institution. EU institutions need to not only comply with the Regulation, they need to be able to *demonstrate* such compliance.

With a view to becoming increasingly effective and because we strive for even better interaction with the EU institutions we monitor, every second year, the EDPS performs a **general stocktaking exercise**, focussing on aspects that indicate progress made in the implementation of the Regulation in the EU institutions. This report is the result of the fifth consecutive exercise; it is based on the responses received from **61 EU institutions** by September 2015[4].

In line with the EDPS enforcement policy[5], this report is published with the intention to encourage greater accountability for compliance with data protection by EU institutions. The report is part of our efforts to train and guide EU institutions on how best to respect in practice data protection rules, whilst focusing on types of processing which present high risks to individuals. The report thus emphasises **progress** made in comparison to previous Surveys, but also underlines **shortcomings**. It also evaluates the results of the **visits** to a number of EU institutions carried out based on the results of the previous Survey.

The responses received and previous compliance visits confirm that the implementation of the Regulation is not only a matter of time and resources, but also of organisational will. This report thus does not evaluate the individual performance of the DPO appointed in each EU institution. Rather, it looks at the overall performance of each EU institution bearing responsibility for protecting the right of individuals to privacy when processing of personal data. Ensuring compliance is indeed a process that requires the **commitment** and **support** of the management in each EU institution.

The EDPS will take the results of this Survey into account in planning further supervision and enforcement activities. However, in our supervision of EU institutions, we will act through education, persuasion and example, preserving our powers of enforcement as a last resort. Our activities will combine **guidance** to EU institutions, **enforcement actions** and other measures to promote **accountability**. In particular, compliance visits triggered by a manifest lack of commitment by an institution or body will be planned on the basis of the results of this Survey.

---

[1] In accordance with Article 41 (2) of the Regulation.
[2] Regulation (EC) 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.
[3] See the EDPS Strategy 2015-2019 published on 2 March 2015, available on the EDPS website: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26_Strategy_2015_2019_EN.pdf.
[4] Several bodies and agencies replied after this date. Where possible, their replies were still incorporated in this report.
[5] See the EDPS Policy Paper of 13 December 2010 on "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001", p. 8.

II. Executive Summary

This Survey gives a global state of play regarding the compliance of EU institutions with data protection rules and thus illustrates the EDPS' role as independent supervisory authority.

Although the Survey is technical in nature and focusses on formalities, it delivers valuable signals to assess trends, promotes transparency vis-à-vis stakeholders and it feeds into the choices the EDPS makes as regards supervision and enforcement activities. Its publication marks a moment for determining EDPS activities for the upcoming year 2016.

In general, the results show steady progress in implementing data protection rules throughout all EU institutions. The Survey thus confirms a generally positive trend amongst very heterogenic EU institutions, which vary significantly in scope and complexity of their processing operations.

The well-established and mature institutions now need to focus on maintaining their achievements in terms of maintaining proper inventories and keeping up notification rates to their data protection officers and the EDPS.

Less mature institutions have made up ground, with several agencies reporting perfect notification scores. Where progress has slowed down, notably on notifications to the EDPS, we will provide the necessary support to ensure that data protection becomes a reflex.

III. Main Report

1. Introduction

As public administrations, EU institutions process personal data, both in their core business activities and in their administrative tasks.

It is the responsibility of EU institutions to protect fundamental rights and freedoms of natural persons with respect to the processing of personal data and to put in place appropriate and effective measures to ensure that the principles and obligations set out in Regulation (EC) 45/2001 (the Regulation) are complied with and to be able to demonstrate this.

It is the duty and task of the European Data Protection Supervisor (EDPS) to monitor and ensure that individuals' rights are respected in accordance with the Regulation[6].

In his Policy Paper adopted in December 2010[7] the EDPS announced that "*he will continue to conduct periodic 'surveys' in order to ensure that he has a representative view of data protection compliance within EU institutions/bodies, and to enable him to set appropriate internal objectives to address his findings*".

End April 2015, the EDPS undertook the fifth stock-taking exercise, a continuation of the exercises conducted every second year since 2007 and thus allowing for charting compliance trends over time.

The exercise had a wide scope, involving all relevant 61 EU institutions, and focussed on aspects that give a good indication of the progress made in the implementation of the Regulation by them. Apart from the usual questions on the state of the inventory and the register, this edition of the survey additionally included questions on transfers under Article 9 of the Regulation, information security, measures taken to ensure effective deletion of personal data at the end of their retention period and the involvement of the DPO in designing new processing operations.

This report is based on the responses received from 61 EU institutions (including certain former second and third pillar bodies) to EDPS letters raising specific questions. The EDPS received replies from all EU institutions concerned except the SESAR JU. The EDPS will address this issue separately.

The EDPS will take the results of this exercise into account when planning future supervision and enforcement action programmes. Such programmes will combine guidance to EU institutions, enforcement actions and other measures to promote accountability.

The report is organised as follows: section 2 contains a comparative analysis of the replies received in response to our letters, question by question, each including a short explanation why this question was relevant; section 3 follows up on the visits launched as a consequence of the 2011 Survey; where possible, the results achieved in terms of compliance before and after the visits are compared to analyse their impact; section 5 concludes and summarises.

[6] In accordance with Article 41 (2) of the Regulation.

[7] See the EDPS Policy Paper of 13 December 2010 on "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001", p. 8.

2. Comparative results of the survey

2.1. Inventory and Register of Processing Operations. State of play on notifications to the EDPS

Unlike in previous exercises, the EDPS did not request copies of the actual inventory or register, but only the relevant *numbers* of processing operations (1) identified in inventory, (2) those notified to the DPO and included in the register, (3) those identified as subject to Article 27 and (4) those already notified to the EDPS under Article 27. Where such information was also available on a more granular basis, such as per Directorate-General, institutions were invited to provide such information as well.

A **large majority** of EU institutions keep –as recommended by the EDPS– **both an inventory and a register**. Those EU institutions who do not keep a separate inventory sometimes add a section on future processing operations to the register, effectively integrating the two documents in one (e.g. the EP).

*Article 25 of the Regulation provides that the DPO shall receive a notification of all processing operations involving personal data. According to Article 26 of the Regulation, these are to be kept in a **Register**, whose minimum content is defined in that Article. Processing operations considered as "risky" under Article 27 of the Regulation also have to be notified to the EDPS for prior checking. Additionally, an "**inventory**" of processing operations planned or already happening, but not yet notified to the DPO, is an invaluable planning tool for the institutions. The EDPS recommends that such an inventory contain at least the following fields: name of the processing operation, brief description of the processing operation (including purposes), Article 25 notification (done or not), Article 27 notification (whether required and whether done or not) as well as a contact person (controller "in practice").*

Compared to the last general survey in 2013, **notification rates have risen in general**. The tables below provide an overview of the rates in the current survey and changes compared to the 2013 survey. The column "Article 25" refers to all processing operations. This also includes those which additionally have to be notified to the EDPS under Article 27 of the Regulation. The column "Article 27" provides separate information on these processing operations.

In some cases, rates have declined. This usually concerns EU institutions with a high compliance rate in cases where updates of the inventory have led to DPOs becoming aware of additional processing operations. This can lead to fluctuations in the 90% to 100% range and is not as such a cause for concern. Given that new processing operations are constantly developed, it is difficult to achieve a notification rate of 100% for Article 25, especially for large institutions. For Article 27 notifications, even one or two new processing operations that have not yet been notified can cause what might seem to be a noticeable drop in notification rates. The reason is that the number of such processing operations per institution tends to be quite low[8].

The purpose of these benchmarks is to compare EU institutions to the performance of their peers. It would not be fair to compare a well-established institution like the Council or the Commission with a recently established Agency which is still in the process of growing and

[8] The average number of processing operations falling under Article 27 is 20 if excluding the Commission, which has more than 200.

setting up. For this reasons, institutions are compared to others of similar maturity in terms of their data protection functions, resulting in four groups (A to D)[9].

Institution/body	% Art 25 notifications	% Art 27 Notification	Art. 25 rate compared to 2013 survey	Art 27 rate compared to 2013 survey
ECA	100%	90%	+/- 0	- 10
EC	97%	91%	+ 1	- 9
Council	98%	100%	+ 4	+/- 0
ECB	100%	83%	+/- 0	+/- 0
ECJ	95%	97%	- 2	+4
COR	100%	100%	+ 2	+/- 0
EESC	93%	100%	- 6	+ 5
EIB	92%	84%	- 8	-13
EP	91%	92%	- 2	-8
OLAF	94%	100%	- 6	+/- 0
OMBUDSMAN	81%	100%	- 19	+/- 0
CDT	72%	93%	- 3	+ 1
Group average	**96%**	**93%**	**-3**	**-3**

Table 1: Notification rates for institutions in group A

Institutions in group A show on average quite high notification rates, mostly in the 90% range. As mentioned earlier, starting from such a high level limits the room for improvement and some institutions have reported lower levels compared to the 2013 survey. If such fluctuations occur on a high level, this is not necessarily a cause for concern. It does however highlight that the register is a living document - new processing operations are added, old ones sometimes removed, existing ones updated. In fact, several replies referred to reviews of the register, often resulting in updates of notifications. This means that the work is not done once a register is completed for the first time.

That being said, some of the drops are noticeable. The drop of Article 27 notification rates at the EIB is due to the identification of new additional processing operations subject to prior checking.

The Ombudsman has also identified additional processing operations that need to be notified, resulting in a temporary drop of the Article 25 notification rate.

Institution/body	% Art 25 notifications	% Art 27 Notification	Art. 25 rate compared to 2013 survey	Art 27 rate compared to 2013 survey
CEDEFOP	98%	100%	+ 8	+ 7
CPVO	87%	86%	- 4	- 4
EASME	100%	100%	+ 10	+ 10
EASA	94%	100%	+ 13	+ 35
EDPS	94%	100%	- 4	+/- 0
EEA	86%	100%	- 9	+/- 0

[9] See annex 3 for an explanation on how the groups were created.

EFSA	94%	100%	+ 16	+ 16
EIF[10]	34%	47%	-	-
EMCDDA	74%	93%	- 2	+/- 0
EMA	96%	91%	- 4	- 3
EMSA	100%	92%	+ 3	+ 7
ECSEL[11]	15%[12]	100%	-	-
ENISA	92%	100%	+ 3	+/- 0
ETF	100%	100%	+/- 0	+/- 0
EUROFOUND	100%	100%	+ 8	+/- 0
FRA	100%	100%	+ 4	+/- 0
OHIM	94%	97%	+ 4	+ 7
OSHA	97%	100%	+ 1	+/- 0
Group average	**90%**	**94%**	**+3**	**+5**

Table 2: Notification rates for institutions in group B

The institutions in group B broadly show solid performance, with FRA, Eurofound, EASME and ETF reporting perfect scores. CEDEFOP and OSHA barely missed perfect scores by one or two notifications.

A special mention also goes to EASA, which used to at the lower end compared to its peer group. Its low performance in the 2011 survey led to a compliance visit in spring 2012, which resulted in a significant improvement in the 2013 survey. The report of that survey noted that while EASA had already come a long way, further actions were still expected. EASA has delivered and has now joined the ranks of good performers.

The EEA has identified several new processing operations and has also undergone a reorganisation, necessitating some updates; these developments have resulted in a temporary drop.

Some numbers are not easily comparable to the last survey.

The EIF partly relies on the EIB for many administrative processing operations. A finding in the 2013 survey was that very few of the EIF's independent processing operations had been notified and that the bulk of the processing operations included in the register were in fact "EIB Group" notifications, for which the EIF relied on the EIB. In the meantime, the EIF has started a review of its inventory and register, finding a significant number of additional processing operations (64 processing operations identified in the inventory, as opposed to 23 EIF-specific processing operations plus 16 EIB group processing operations before). The numbers reflect the state as of EIF's reply to the survey - after the cut-off date, the EIF has made a lot of progress (see also section 3.3 below).ECSEL is the merged successor for ARTEMIS and ENIAC, so the numbers cannot easily be compared to the last survey. While ECSEL has "inherited" some procedures and processing operations from its predecessor organisations (such as those identified for prior checking), a comprehensive review of the inventory and register is ongoing; according to ECSEL's planning, all updated notifications should have been sent to the DPO by end of September.

[10] EIF numbers cannot be usefully compared to the 2013 survey, see below.
[11] ECSEL is the merged successor for ARTEMIS and ENIAC, so the numbers cannot easily be compared to the last survey
[12] See explanation on p. 8 below.

EMCDDA's rate on Article 25 notifications is one of the lowest in this group. Unlike for some other agencies, this appears to really reflect a lack of progress, given that the number of notifications has stagnated. EMCDDA should take steps to close this gap.

Institution/body	% Art 25 notifications	% Art 27 Notification	Art. 25 rate compared to 2013 survey	Art 27 rate compared to 2013 survey
EACEA	98%	96%	+/- 0	+ 1
CHAFEA	82%	100%	+ 30	+/- 0
ECDC	100%	100%	+ 4	+/- 0
EFCA	96%	100%	+ 17	+/- 0
ERA	92%	93%	+ 6	+ 4
FRONTEX[13]	88%	90%	-	-
GSA[14]	52%	54%	-	-
INEA	91%	100%	+ 22	+ 37
Cleansky 2	100%	100%	+ 7	+/- 0
ECHA	100%	100%	+/- 0	+/- 0
ERCEA	90%	100%	- 8	+ 5
F4E	64%	73%	- 2	- 10
FCH JU	100%	100%	+/- 0	+ 33
IMI	75%	100%	- 25	+/- 0
REA	89%	93%	- 7	+ 11
SESAR	-	-	-	-
Group average	**88%**	**93%**	**+3**	**+6**

Table 3: Notification rates for institutions in group C

Group C is no longer lagging behind group B, showing that while bringing the inventory and register into shape takes effort, it can be done. ECHA, FCH-JU, Cleansky and ECDC reported perfect scores; EACEA and EFCA came very close.

Frontex used to be a cause for concern, receiving a compliance visit from the EDPS in late 2012. For the 2013 survey, the visit did not seem to have had much of an effect yet. This year, however, Frontex has shown a solid performance. Cooperation with Frontex has significantly improved, with good cooperation during an inspection carried out in 2014 and a change in Frontex' activities towards more processing of personal data for operational purposes.

F4E's notification rates decreased slightly. However, the percentages mask the fact that the absolute numbers in the inventory and register have increased significantly - for Article 25 from 21 out of 32 done to 38 out of 59 done; for Article 27 from 15 out of 18 to 22 out of 30. The numbers are therefore not a sign of stagnation, but of an uphill race.

At the cut-off date, GSA still underperformed compared to its peers (see also section 3.4 below) and SESAR did not reply to the survey on substance (see section 2.6 below).

[13] Frontex only provided a copy of its register for the 2013 survey, not the inventory, so no useful comparison can be made.
[14] GSA did not reply to the 2013 survey on time, so no useful comparison can be made.

Institution/body	% Art 25 notifications	% Art 27 Notification	Art. 25 rate compared to 2013 survey	Art 27 rate compared to 2013 survey
ACER	34%	36%	+ 6	+ 5
BEREC[15]	36%	31%	+ 23	- 2
CEPOL	24%	56%	+ 21	+ 13
EASO	54%	62%	+ 35	+ 37
EBA	100%	29%	+ 86	- 38
EDA	100%	100%	-	-
EEAS	80%	47%	+ 48	- 20
EIGE	50%	86%	- 13	+/-0
EIOPA	13%	44%	+/-0	- 14
EIT	28%	38%	+ 13	- 32
ESMA	32%	29%	- 3	- 32
ESRB[16]	see ECB	see ECB	-	-
EUISS	25%	17%	+ 25	+ 17
eu-LISA	81%	11%	+ 81	+ 11
EUSC	52%	100%	+ 52	+ 100
Group average	**53%**	**47%**	**+29**	**+3**

Table 4: Notification rates for institutions in group D

Group D includes the newest agencies and bodies; thus notification rates are often lower. As these agencies are often still in the process of setting up their business processes, their inventories tend to be less settled as well.

ACER is an example of this: while its Article 25 notification rate only increased slightly, this masks the fact that the number of notifications in the register almost tripled - this gain was offset by a similar increase in the number of processing operations identified in the inventory[17].

Similarly, the increase in Article 25 notifications at the EEAS is in fact bigger than is apparent from the notification percentages. While in 2013, it had identified 65 processing operations in its inventory, this number grew to 118 in 2015, so increasing the notification rate was a win in an uphill race. The decrease on Article 27 is the result of a similar uphill race: 15 out of 32 processing operations are reported as notified, as compared to 10 out 15 in 2013, which results in a lower rate, but nonetheless present a gain in control over its processing operations.

EBA appears to have focused on Article 25 notifications first, showing an impressive improvement, especially taking into account the growth of the inventory from 35 to 58 entries. This identification of new processing operations also uncovered more cases subject to Article 27, resulting in a noticeable drop in the Article 27 notification rate (from 4 out of 6 to 5 out of 17). The next step for EBA will then be to close this gap.

[15] BEREC notified several additional processing operations under Article 27 after the cut-off date for contributions to the survey, so they could not be taken into account for the calculation here.
[16] The ESRB's processing operations are integrated in the ECB's documentation; the ECB DPO is also the ESRB DPO.
[17] In 2013, ACER reported 9 out of 32 Article 25 notifications as done, this time, it reported 31 out of 92 as done.

EASO is an example of agency steadily increasing its performance, moving from below average in its group to slightly above the middle of the field.

EIT shows some improvements on Article 25, but the Article 27 notification rate has decreased due to the identification of additional processing operations that have to be notified.

eu-LISA - whose permanent DPO was appointed only in spring 2014 - has shown very good progress on Article 25 notifications, starting from zero in the 2013 survey. However, it is lagging behind on Article 27 notifications and should take steps to close this gap.

Several of the agencies in this group which had shown a slow start in the preceding surveys have received visits or staff secondments from the EDPS in the meantime, with the aim of boosting compliance:

EUSC has received a staff secondment from the EDPS in autumn 2014 and effectively cleared its Article 27 backlog; on Article 25, it is moving in the right direction.

EIGE was already flagged for a visit following the 2011 survey, which was carried out spring 2013. The 2013 survey already showed results of this, with very respectable scores for an agency of its age. However, the momentum seems to have decreased, EIGE should not rest on its laurels, but continue to increase its compliance.

EIOPA is in a similar uphill race as ACER and the EEAS: the number of entries in the inventory has almost doubled from 2013 to 2015 (70 instead of 40). The decrease in Article 27 notification rates is due to the fact that several future processing operations have already been identified for prior checking in the inventory.

EUISS appointed its first DPO following the 2013 survey. In autumn 2014, a consultancy visit on staff level was carried out. While there is some progress, EUISS should ramp up its compliance activities. This notably requires the business units to provide their Article 25 notifications to the DPO, so the process of prior checking can start where needed.

ESMA's Executive Director and the EDPS met in spring 2013; in summer 2015, a consultancy visit took place. The noticeable decrease in the Article 27 notification rate is due to the identification of many additional processing operations subject to it.

2.2. Transfers in 2013-2014 to recipients not subject to national provisions implementing Directive 95/46/EC

Sounds familiar? Already in the **2013 exercise** (Survey 2013)[18], the EDPS had requested EU institutions to provide information on transfers of personal data to recipients not subject to national legislation implementing Directive 95/46/EC. The EDPS then asked for information on such transfers in an open manner to obtain a general overview, also with a view to adopting guidance.

In 2013, out of a total of 62 EU institutions and bodies, 35 entities stated that they did not carry out such transfers at all; 17 more stated that there were no structural transfers, but that they might occur in single specific cases. Against this background, the EDPS had then concluded (Survey 2013, p. 18) that: "**Article 9 transfers as part of the core business activities of EU institutions are rare**".

[18]See https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24_survey_report_EN.pdf.

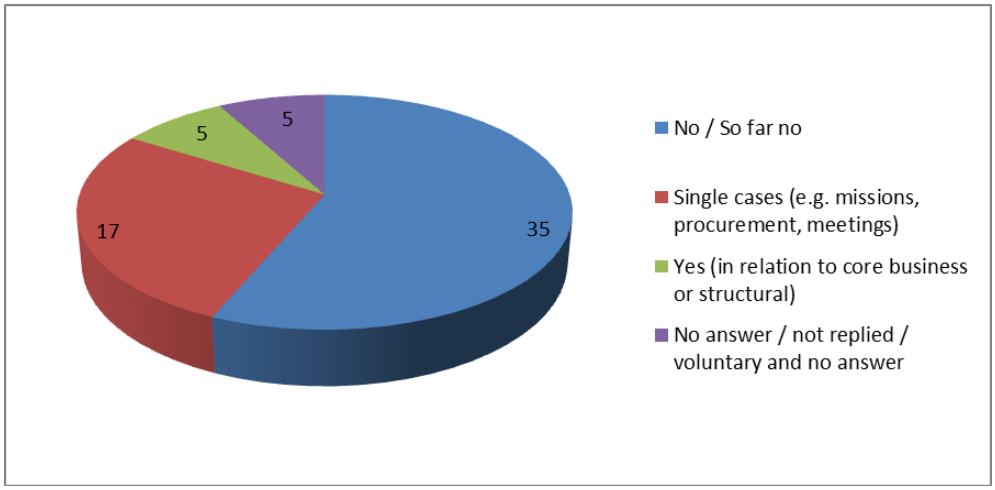

Figure 1: Overview of Article 9 transfers (2013 exercise)

So what's new? In July 2014, the **EDPS published a Position Paper** on "The transfer of personal data to third countries and international organisations by EU institutions and bodies"[19]. Against this background, for the **present exercise**, the EDPS enquired about recent transfers of personal data under Article 9 in the years 2013 and/or 2014. Only 18 out of a total of 61 institutions replied in the affirmative. Article 9 transfers as part of the core business activities of EU institutions are thus still rare[20]. However, because these transfers are associated with **increased risks**, we invited **more detailed information** in the context of the present exercise.

Different types of transfers under Article 9: Where transfers had occurred during this period, EU institutions were invited to indicate separately transfers under Article 9(2) (adequacy assessment), Articles 9(6) or 9(7) (derogations) and those transfers under Article 9 to recipients which are established in EEA countries, but conduct types of activities that are excluded from the application of Directive 95/46/EC (e.g. to judicial authorities).

Article 9 of the Regulation *mainly concerns transfers to third countries and international organisations.*
As transfers to third parties necessarily entail a certain loss of control over personal data, it is important that the recipients be subject to appropriately strict data protection rules. This is not a problem for transfers within or between EU institutions, and also not for transfers to most recipients in the EU. For transfers to other third parties, this can become a problem, as their data protection standards are often weaker than the EU standard. For this reason, Article 9, which regulates such transfers, is more restrictive than the rules for intra-EU transfers. This reflects the ***increased risk associated with such transfers****.*

[19] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf.

[20] The comparative decrease in numbers from the 2013 exercise can be explained by the limitation to a specific time-period (e.g. the CJEU noted that certain processing operations in principle foresee such transfers, but no such transfer had occurred during 2013 or 2014). Other institutions indicated that they did not consider certain transfers under Article 9 as *theirs* (e.g. EDPS for those carried out by third party providers for their own purposes or Cedefop for staff providing their personal data to organizers of meetings / conferences / events in third countries).

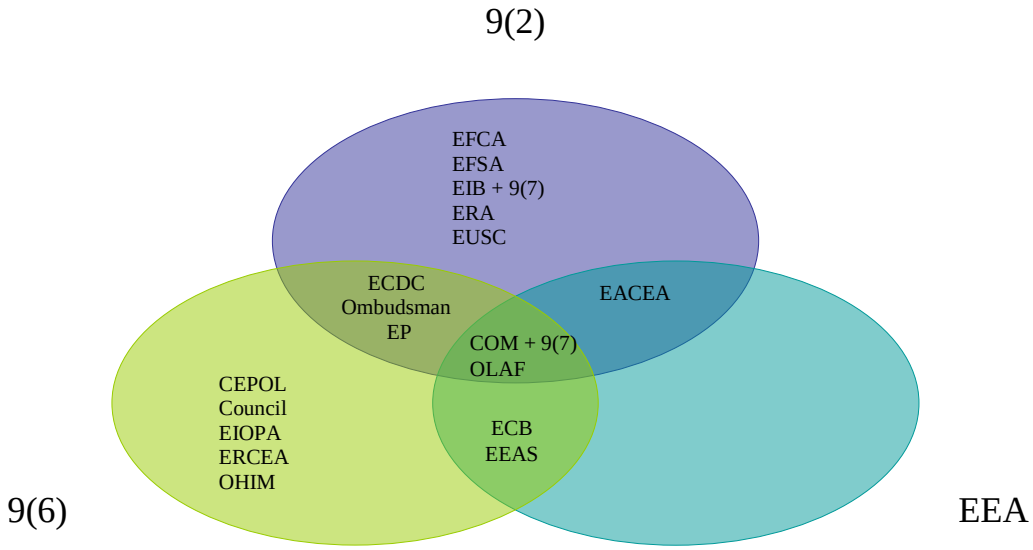

Figure 2: Diagram of types of Article 9 transfers (2015 exercise)

Of those 18 institutions[21] that reported transfers under Article 9 for that period, three (the EFSA, the CJEU and the Ombudsman) explicitly highlighted the **use of social media**: Twitter[22], YouTube, LinkedIn and Flickr pages (EFSA) as well as Google+ (Ombudsman).

- Further specifications of transfers under Article 9 were requested in a table regarding the processing activity (as mentioned in notification Article 25), the recipient, the basis (e.g. adequacy assessment by the data controller), the field (e.g. law enforcement), the "how" of the transfer (e.g. sending data by post, by e-mail, granting access to a data base, etc.), the categories of personal data as well as the frequency of such transfers.
- Additionally, the EDPS wanted to know about any particular difficulties encountered in the above activities and, if possible, their reasons.
- Lastly, the EDPS enquired whether an internal monitoring and registration system of Article 9 transfers exists.

As regards **transfers under Article 9(2)**, 11 institutions[23] indicated transfers during 2013 and/or 2014 regarding very different categories of personal data in a variety of fields and with varying frequency (these elements would not seem to allow for further conclusions beyond the individual processing operation). E.g. the EACEA noted such transfers for the purpose of awarding and implementing grants in the field of education, the EFCA in the context of the

[21] The Commission reported more granularly: 14 out of 41 Directorates-General had transfers under Article 9 for that period. The EMSA noted that "The only data that EMSA would transfer, to actors outside of the EU, usually with an intermediation of the travel agency, would be limited data used for booking travel services for missions of the EMSA staff: transport and hotels. The reality does not justify application of Art. 9".

[22] See https://secure.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Legal_notice/Twitter_policy for the EDPS' Twitter Policy. More guidance should become available by the publication of the EDPS' e-communication guidelines.

[23] The Commission reported that 7 out of 41 Directorates-General had transfers under Article 9(2) for that period.

transmission of inspection reports regarding fishing vessels, the EIB for actuarial calculation of staff pension rights (similarly for pension management: EUSC).

Recipients include international organizations (e.g. OECD for EIB, WHO, FAO and OECD for EFSA), but also regional and national authorities and designated contact points (e.g. for DG EAC and EACEA for educational/vocational programmes, transport authorities in the case of ERA or customs authorities for DG TAXUD).

In the majority of cases, the basis for such transfer is an adequacy assessment conducted by the controller (e.g. DG AGRI for the monitoring of organic farming information). Other possibilities include e.g. an adequacy decision by the European Commission (e.g. DG RTD for proposal evaluation and grant management) or the EU-US Safe Harbor Agreement.

12 institutions[24] reported **transfers under Article 9(6)** during 2013 and/or 2014, again regarding very different categories of personal data in a variety of fields.

Main recipients include travel agencies (CEPOL, ECB, EIOPA[25]); visa agencies/consulates (ECB, EIOPA); diverse regional and international organizations (e.g. in the area of fisheries management for DG MARE or WHO for DG SANTE and ECDC) and customs authorities for DG TAXUD.

Almost all alternatives of Article 9(6) were mentioned in the institutions' replies as legal basis:

- Art. 9(6)(a) is relied upon by DG ESTAT for registering participants in a video-contest and by DG TAXUD for access to a collaborative space in the context of participation in Fiscalis and Customs Programmes;
- Art. 9(6)(c) is cited regarding the management of local staff in EU Delegations and for transfers regarding social security and tax administration by the EEAS;
- Art. 9(6)(d) is the basis for DG MARE in the context of vessel reporting and by DG JUST for their rapid alert system for non-food dangerous products;
- Art. 9(6)(d) + (e) are used by the Council for 3rd country missions and by DG SANTE for their Early Warning and Response System.

Transfers under Article 9(7) are to a destination that does not ensure an adequate level of protection, but for which the controller has adduced adequate safeguards[26]. Such transfers are rare: only two DGs of the Commission (DGs SANTE and TAXUD) and the EIB identified such transfers (although none actually occurred yet for the EIB).

Only four institutions (EACEA, ECB, EEAS and OLAF) noted that they had transferred personal data under Article 9 to recipients which are established in **EEA countries**, but

[24] The Commission reported that 9 out of 41 Directorates-General had transfers under Article 9(6) for that period.
[25] The EMSA noted that "The only data that EMSA would transfer, to actors outside of the EU, usually with an intermediation of the travel agency, would be limited data used for booking travel services for missions of the EMSA staff: transport and hotels. The reality does not justify application of Art. 9".
[26] See Position Paper p. 14, section 6. See Position Paper, pp. 21/22, section 6.3 for the mandatory involvement of the DPO in the analysis process that takes place before adequate measures are adopted as well as for the three scenarios of EDPS ex-ante involvement.

conduct types of activities that are excluded from the application of Directive 95/46/EC (e.g. to police or judicial authorities[27]).

***

No problems at all? In the light of the reported frequency and sometimes complexity of the above activities, it is surprising that only the EIB indicated **encountered difficulties**, noting that it was hard to establish the **adequacy of third countries**. Indeed, the EDPS has acknowledged in his Position Paper (p. 13, section 5.2) that "...in practice, it will not always be feasible for the controller to conduct a complete assessment of adequacy for a third country or international organisation. In such cases, the controller should assume that the level of adequacy is inadequate and **consider other options**...".

Where the controller decides nonetheless to conduct an **adequacy assessment**[28], the EDPS noted in the Position Paper (pp. 13+14, sections 5.2 and 5.3) that "In the light of the accountability principle, the data controller should where relevant thoroughly **document the steps taken to ensure adequacy**, and to conduct a suitable risk assessment." In addition, "Any analysis conducted by the controller should be...made available to the EDPS upon request".

As also noted in the EDPS Position Paper (p. 14, section 5.3), "In the light of the policy on consultations in the field of supervision and enforcement, the **DPO** of the EU institution or body should always be consulted and involved in the analysis. Furthermore, data controllers are encouraged to submit a consultation to the **EDPS** when the matter presents: (a) a certain novelty or complexity (where the DPO or the institution has a genuine doubt), or (b) a clear impact on data subjects' rights (either due to the processing activities' risks etc.)".

***

Regarding the existence of an **internal monitoring and registration system** of Article 9 transfers, only six institutions indicated the existence of such a system. One institution announced that such a system will be created soon, whereas another larger institution envisages the centralization of its existing system(s).

The fact that only roughly a quarter of all institutions executing transfers under Article 9 have an internal monitoring and registration system in place is a worrying state of affairs. In the Position Paper (p. 9, section 3.4), the EDPS has noted that such a system is "helpful in supporting internal management of international transfers and in ensuring effective accountability and compliance with the Regulation". The EDPS had consequently recommended the creation of such systems as best practice, highlighting that "This should not only include transfers based on adequacy but also – and more importantly – transfers based on derogations (Article 9(6) and 9(7))".

To **ensure effective accountability and compliance with the Regulation**, the EDPS therefore recommends institutions to create an internal registration system of Article 9 transfers.

[27] See Position Paper, pp. 22/23, section 7. As noted there: "Those exclusions were necessary before the adoption of the Lisbon Treaty, but they are now in principle inconsistent with Article 16 thereof, as well as with Article 8 of the European Union Charter on Fundamental Rights".
[28] See pp. 10 - 12, section 4.2 of the Position Paper on the notion of "adequacy".

Figure 3: Overview replies on transfers (2015 exercise)

Q1 **Transfers under Art. 9**	*Q2* **Art. 9(2)**	*Q3* **Art. 9(6)**	*Q4* **Art. 9(7)**	*Q5* **EEA**	*Q7* **Monitoring / registration system**
CEPOL		CEPOL			
COM (per DG[29])	COM (7 DGs)	COM (9 DGs)	COM (2 DGs)		COM (2 DGs)
Council		Council			
EACEA	EACEA			EACEA	
ECB		ECB		ECB	
ECDC	ECDC	ECDC			ECDC
EEAS		EEAS		EEAS	
EFCA	EFCA				EFCA
EFSA	EFSA				
EIB	EIB		EIB		EIB ("soon")
EIOPA		EIOPA			EIOPA
EP	EP	EP			
ERA	ERA				
ERCEA		ERCEA			ERCEA
EUSC	EUSC				
OHIM		OHIM			
OLAF	OLAF	OLAF		OLAF	OLAF
Ombudsman	Ombudsman	Ombudsman			
18	11	12	2	4	6

The "how" of the transfer. Most transfers happen through three main communication channels: by post (letter, sometimes registered, or "*note verbale*"; 8 cases), by email (in some cases encrypted; 11 cases) or by granting access to a particular database (7 cases) or through a combination of these channels (5 cases). Other possibilities include transfers via a fax, a web-form, by phone or by hand.

2.3. Information security

The EDPS asked whether:

- there is a process specifically dedicated to manage your information security?
- risk assessments are performed for data processing operations? If so, the EDPS asked to provide the proportion (%) of the data processing operations for which a risk assessment has been done in the last two years.
- the institution has a general security policy in place[30]? If so, does the general security policy include a section on information security?
- there is a formal process in place for the handling of security incidents?
- the DPO is notified in case the information security incident involves personal data?

[29] AGRI, EAC, GROW, HR, MARE, RTD, TAXUD for Art. 9(2); EMPL, ESTAT, JUST, MARE, NEAR, PMO, SANTE, TAXUD, TRADE for Art. 9(6).
[30] This question did not regard the application-specific security policies.

All institutions but eight replied that they have a process in place, which is specifically dedicated to manage their information security. Two institutions plan to establish such a process later in 2015. Two institutions explicitly mentioned ISO certification (ECHA / ISO 9001) or implementation (GSA (GNSS); ISO 27001) in this context.

> *Under Article 22(1) of the Regulation, having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational* ***measures to ensure a level of security appropriate to the risks*** *represented by the processing and the nature of the personal data to be protected.*
>
> *Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.*

19 institutions replied that they do not perform risk assessments for their data processing operations, at least not on a regular basis, with one institution noting that such an approach was "not realistic in an institution with limited resources". A majority of institutions (38), however, explicitly confirmed conducting risk assessments for their data processing operations. Out of this majority, 18 institutions provided indications as to the percentage of processing operations covered by such exercise ranging from "negligible" to 100% (the latter for eight institutions), which means that, for institutions conducting risk assessments and providing percentages, on average, two-thirds (66,4%) of their data processing operations have undergone a risk assessment.

16 institutions indicated that they do not have a general security policy in place, two institutions mentioned their intention to establish one later in 2015. For the most part, these general security policies include a section on information security. One institution noted that, whilst it does not have general security policy, it does have an ICT Security Policy.

45 institutions confirmed the existence of a formal process for the handling of security incidents (13 clearly indicated the absence of such a process), two more noted that such process was currently being developed.

REA: "...an online tool is accessible to the whole research family and in case of a security breach involving personal data...the concerned controller will have to use this form so as to signal a data breach..."

Only six institutions indicated that their DPO is not notified in case the information security incident involves personal data[31]; one noted the absence of such notification despite repeated audit recommendations in that respect. For one institution, such notification was identified as being linked to the DPO's primary tasks as IT officer, rather than his DPO function. Several institutions pointed at the hypothetical nature of such notification to the DPO, as no such incidents had occurred.

Ombudsman: "Although there is no standard personal data breach notification procedure, in the past, when a data security incident occurred, the DPO was formally notified of it. In particular, the data controller submitted a report of the incident to the DPO. The report included the following information: (a) a chronology of the events leading up to the unauthorised transferring of the personal data; (b) the amount and nature of the personal data that has been transferred and number of data subjects concerned; (c) the action being taken to mitigate the possible adverse effects of the personal data breach; (d) the action being taken to inform those affected by the incident or reasons for the decision not to do so; and (e) the measures being taken to prevent repetition of the incident in the future."

[31] For one institution, such notification obligation will be included in a formal process, which is currently being developed.

Overall, the EU institutions have recognised that information security needs to be managed as a process i.e. that information security is not an item that is performed once and for all but rather needs to be constantly monitored and re-evaluated. However, it seems that risk assessments have not fully permeated the EU institutions' information security processes (risk assessments are an important tool to deal with the uncertainties related to managing security within an organisation[32]). This raises the question as to how EU institutions decide on the allocation resources and associated efforts to improve their information security.

Furthermore, security incident management[33] seems to be mostly dealt with formally within the EU Institutions, often involving the DPO when personal data is affected. This approach ensures that personal data breaches are handled properly, in line with the potential impact of the data breaches to the data subjects.

2.4. Ensuring effective deletion of personal data

The EDPS enquired about the existence of:

- a **written policy** regulating the effective deletion of personal data at the end of their retention period;
- a **standard procedure** regulating the effective deletion of personal data at the end of their retention period;
- **automated processes** supporting the deletion procedure across all your systems;
- measures to ensure the **erasure** of information **in back-ups**, if any?

*Under Article 4(1)(e) of the Regulation, personal data must be kept in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the data were collected or for which they are further processed. Under Article 4(2) of the Regulation, it is for the controller to ensure that this obligation is complied with.*

Out of 61 institutions, 38 indicated that they have a **written policy regulating the effective deletion** of personal data in place. One institution noted that it was in the process of establishing such a policy. However, certain explanatory statements would indicate that a rather large interpretation of "*policy*" underlies this self-assessment: a number of institutions seemingly count the definition of a retention period in the DPO register "per processing operation" as having a written policy. Two institutions identified the creation of a written policy as a "future" or "ongoing" project, for one institution, such a policy is currently "pending for approval".

The EDPS had asked for a short description of the general policy or, if the policy is specific to each or selected processing operations, a selected **description**. Most institutions replied using processing specific examples, such as the following:

EFCA: "Concerning processing operations in the area of HR,...the HR archives have been structured into eight sub-categories of files containing personnel data. The general policy regarding retention period is laid down in the notifications to EFCA's Data Protection Register. Therefore, a summary table of retention periods for HR files has been extracted. In the HR Roadmap, an annual revision and follow-up of HR activities is included. This prompts the checking of archives and retention periods and the launch of a destruction exercise once a year".

[32] See ISO 27001, ISO 27005, BSI standard 100-3, NIST special publication 800-300, EBIOS, Octave Allegro, MAGERIT.
[33] See ISO 27035, NIST 800-61r2.

EUISS: "The traineeship rules stipulate that at the end of the traineeship programme, only a limited amount of data (last name, first name) will be kept by the Documentation and Research Officer together with a report regarding the activities of the trainee for archiving and record purposes (e.g. letters of reference)."

Regarding the existence of a **standard procedure** regulating the effective deletion of personal data at the end of their retention period, 26 institutions replied that they have one. Two more noted that the creation of such a standard procedure was a "future" or "ongoing" project. One institution indicated that such a standard procedure exists "for some processing operations only".

ECHA: "ECHA has adopted a Procedure for the Control of Documents and Records... It sets the high-level principles regarding the retention of documents. The detailed retention times of all records identified in the Agency are documented in another formal document, the ECHA Records Retention Schedule. The annex to the Procedure for the Control of Documents and Records gives detailed and practical instructions on how paper and electronic documents shall be destroyed after the expiry of their retention time."

Only 11 institutions claim to have **automated processes supporting the deletion procedure** across all systems in place (11 institutions do not have any respective systems and thus replied "NA"). An additional five institutions noted that the creation of such automated processes was a "future" or "ongoing" project. Examples given often relate to CCTV footage (five institutions).

On the **erasure of information in back-ups**, 42 institutions mentioned that they ensure the erasure of back-ups, but most provide little to no description as to *how* they actually ensure this.

2.5. Your Data Protection Officer and you

Sounds familiar? In the **2013 Survey**, we had asked for information on how DPOs are involved during the design of new processing operations involving personal data, then referring to governance documents (especially in IT) where available, or simply descriptions of established best practices, be they formalised or not.

As this **question had been intentionally phrased in a very open way**, the form of replies had varied widely, but showed ample evidence that many EU institutions are aware of the necessity of thinking about data protection from the beginning and involving their DPOs. We then concluded that the ways to ensure this differ between EU institutions.

So what's new? For the present **2015** edition of the Survey, building on these previous results, the EDPS asked **more targeted questions**. In a separate section, for which the EDPS explicitly asked that replying to it *not* be delegated to the DPO, the EDPS requested information on whether

The importance of the Data Protection Officer (DPO) as a partner both for controllers in the EU institutions as well as for the EDPS cannot be overstated. ***DPOs play a key role in ensuring compliance with the Regulation****. They are the first point of contact for staff in the EU institutions of the EU when it comes advising them on their rights and obligations and fostering a data protection culture. Additionally, they are also the main liaison point for the EDPS. Internally, DPOs can disseminate good practices within their EU institutions, act as a hub of knowledge, and give advice to controllers and flag problems. Involving DPOs early in the process of designing new processing operations is a good way of ensuring privacy by design.*

the DPO's tasks are part of his/her job description, if the performance of the DPO's tasks forms part of his/her performance evaluation and how the DPO is involved in the design of new processing operations.

As highlighted in the **EDPS Strategy**[34], we rely on close cooperation with DPOs to support EU institutions in moving beyond a purely compliance-based approach to one that is also based on accountability.

The DPO's involvement: Whilst for the 2013 Survey, several replies had mentioned that DPOs are not involved (early) enough or that consultations were framed too generally. In their replies for the 2015 edition, ***all*** **institutions claim DPO involvement in designing new processing operations,** although most institutions did not actually describe *how* their DPO is involved, but simply replied in the affirmative[35]. Two institutions specifically noted an increased involvement of their DPOs. Several institutions, however, noted **gradual reservations** ranging from "may be consulted" to "from time to time", "where appropriate", "whenever necessary" or on a "needs"/"ad hoc"/"case-by-case" basis.

Council: "With respect to processing operations that do not entail the development of new IT systems, the DPO is usually consulted at an early stage to ensure that the envisaged processing operations comply with data protection requirements. The questions that more frequently arise are: quality of data, recipients, security measures, data retention periods and information to data subjects.
In the development of new IT systems, the DPO works closely with DGA CIS (IT Department) to improve and document the involvement of the DPO at the earliest stages of the planning of a new IT tool. The aim is to facilitate the identification of privacy risks and the introduction of privacy enhancing technologies to mitigate those risks. The need for or the appropriateness of such technologies is identified through the use of a model Privacy Impact Assessment (PIA) which allows the project manager and the DPO to have an overview of the personal data involved and of the main risks that the processing operation presents.
In addition, the DPO attends the HR/IT Committee, which is the Committee in charge of planning, approving and managing all IT systems and applications for HR and Administration of the GSC."

EIOPA:
"- Bi-weekly meeting with the Data Controller (i.e. the Executive Director);
- Monthly meetings with middle management of the Corporate Support Unit (i.e. Head of Unit, the IT Team Leader and the Procurement Team Leader);
- Monthly meeting with middle management of the HR Team (i.e. their team leader);
- Involvement in business plan requests;
Adoption/revision of standard operating procedures (such as Policy and Procedure) includes a legal check from the DPO;
- Establishment of Data Protection Coordinators located in every EIOPA's Team and regular meetings with them;
- Regular general DP trainings open to all staff which is always a good forum to share information.
The fact that the DPO is not a full time DPO and is located within the Legal Team is seen as an advantage since it allows the DPO to be kept up-to date of new processing operations about to be launched."

EP: "... DPO is by design and set-up regularly involved in the drafting and verification of all new internal decisions involving personal data...The DPO is also regularly involved in new IT projects...Furthermore, regular meetings with the hierarchy and the DPCs allow the DPO to be aware of new processing operations. Finally, trainings and information sessions are organised twice or three times per year with the staff most involved in data protection issues in the different DGs".

[34] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-07-30_Strategy_2015_2019_Update_EN.pdf, p. 20.
[35] E.g. EUSC noting that "All new processing operations must be reviewed by the DPO for compliance".

To gain an **additional stakeholder perspective** on the matter, the **EDPS anonymously consulted the DPOs**, of whom (at a participation rate of roughly 50%) only a bit more than half indicated that they considered that they were adequately consulted (17 "yes" vs 15 "no"). Overall, they rated their satisfaction about being consulted at 6,4 (on a scale from 0 -basically never consulted- to 10 -always consulted-). Comments ranged from encouraging ones ("Regularly involved in business decisions of all kind"; "Good cooperation between DPO and business areas, high awareness of data protection"; "Significant improvement over past 1,5 years") to not so positive ones ("Consultation is consistent and regular, but too late in the process, rather fire-fighting than privacy by design") and suggestions that, in some instances, the DPO was intentionally excluded or at least purposefully kept in the dark until certain decisions had become irreversible, thus excluding a true privacy by design approach. A majority of comments made related to being consulted on (or actually *discovering*) processing operations too late in the process.

Where the **kind of involvement** of the DPO was specified by the institutions, three main characteristics emerge: the involvement through a defined and structured procedure (six institutions), by participation of the DPO in working groups, steering committees or management meetings (13 cases, in particular IT steering committees = five) and by including the consultation of the DPO as mandatory step in project management templates or routing slip checkbox(es) (four institutions).

This confirms earlier findings of the 2013 Survey, in which the EDPS had found regular meetings with relevant departments (HR, IT...) and the inclusion of a "data protection check" in project management templates to be especially valuable tools to ensure the DPO's proper involvement. The replies also confirmed that the larger the institution, the more likely formalised procedures are. Again, some institutions mentioned part-time DPOs' other tasks that made sure they were kept up-to-date (e.g. roles in IT or as legal advisor to the Director). This was especially the case in smaller agencies.

The EDPS would like to reiterate that, while this may work for small agencies or agencies that have just been set up, **a more formalised consultation process seems to be necessary for larger organisations**.

EMA: "...a formal procedural step is foreseen aimed at informing the data protection officer whenever a new policy is proposed by the competent services...Moreover, quarterly bi-lateral meetings are scheduled between the DPO with the Executive Director for the discussion of both issues related to current application of policies and design of future policies/activities".

ERCEA: "The ERCEA's DPO is a member of the IT Steering Committee. The ERCEA Instructions on preparation and validation of internal procedures (ICS8) expressly foresee the early consultation of the DPO by the business process owners before launching the validation of an internal procedure. In addition, the DPO must be consulted on all draft procedures or amendments thereof which involve processing of personal data (VISA required in the ARES routing slip)...".

OHIM: "...close relationship stems from our internal rules, implementing Regulation (EC) No 45/2001, which constitute for the responsible data controllers the commitment to give prior notice to the DPO of any personal data processing operation and of any substantial change affecting any of the already existing. In particular, in every internal note sent to the President of the Office, there a field to be completed by the relevant department, indicating the "DPO consultation". This promotes DPO consultation for all projects and activities of the office, but also allows the management of the office to have assurance that data protection issues were duly covered when concluding the proposal to the Presidency. Moreover, the DPO is member of the Information Security Forum. The Forum is in charge of assuring the security of processing of data, personal or not, within the OHIM, in compliance with ISO 27001. ...".

Council: "The need for or the appropriateness of such technologies is identified through the use of a model Privacy Impact Assessment (PIA) which allows the project manager and the DPO to have an overview of the personal data involved and of the main risks that the processing operation presents."

"Data protection by design" is a good practice. It helps to spot problems early in the design process – thus avoiding e.g. costly software re-designs at later stages[36] – and to integrate a data protection culture into the development cycle. **Involving DPOs early in the process of designing new processing operations is a good way of ensuring privacy by design**.

***

For the majority of DPOs, their tasks are part of their **job description**. Only for six institutions (EDA, EMSA, ERCEA, Eurofound, INEA, OSHA), this is not the case. Two institutions (ERCEA, INEA) mentioned that the existing system of *job descriptions* is too generic to cater for DPO specificities, but these specificities (including part-time occupation as DPO) have been acknowledged in the context of the DPO's *objectives*.

The vast majority of institutions confirm that the performance of the DPO's tasks forms part of his/her **performance evaluation**; only for four institutions (CJEU, EDA, EMSA, Ombudsman), this is not the case. One institution notes concerns as to the independence of the DPO should his/her performance be evaluated. In this context, the EDPS in the 2005 **Position Paper on the role of DPOs**[37] has clarified that, whilst the DPO may not receive any instructions, this does not exclude performance evaluation. However, because of the independence of the DPO, "...the **DPO should only report to his/her appointing authority and not to a direct superior** "[38].

The 2010 **Professional Standards for Data Protection Officers**[39] published by the Network of Data Protection Officers of the EU institutions and bodies provides further guidance on the Issue, in particular for **part-time DPOs**:

- On p. 6, this document explains that "A DPO who reports to, and is reviewed by, a direct superior in the hierarchy (director or head of unit) may feel pressure to cooperate and get along smoothly with management and other colleagues, as vigorous performance of DPO duties may have a negative impact on career. The proper performance of DPO tasks often requires that the DPO take a firm and insisting attitude also with controllers who have a high position in the organisation, which may be perceived, at best, as bureaucratic or, at worst, unpleasant "trouble-making". Thus, the DPO must be able to withstand the pressures and difficulties, which accompany this important position. To alleviate this pressure, the DPO should report to, and be

[36] One institution specifically mentioned this problem, noting that it was less the case for HR-related systems now that the DPO regularly participates in the HR/IT steering committee.
[37] Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, see https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf.
[38] Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, p. 8.
[39] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 published by the Network of Data Protection Officers of the EU institutions and bodies, see http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf .

reviewed by, the administrative head of the institution or body. This is particularly important for part-time DPOs, who should report directly to, and be reviewed by, the appointing authority for their DPO duties, and to/by the normal superior in the hierarchy for other duties".

- On p. 7, the document states inter alia that "... When reviewing the DPO's performance, the evaluator should be careful neither to reprimand the DPO for taking unpopular positions nor to consider data protection requirements as an administrative burden. For a part-time DPO, performance on the DPO duties should be given equal weighting to performance on the non-DPO duties. If provided in the implementing rules of the institution/body, the EDPS should be given the opportunity to provide input on the DPO's performance".

The examples cited by institutions in their replies to the 2015 Survey illustrate that such recommendations have been smoothly integrated into the evaluation process for many DPOs:

CdT: "The performance evaluation of the DPO is carried out by means of two evaluation processes, one being carried out by the Director (concerning only the DPO tasks) and the other one being carried out by the hierarchical superior."

Cedefop (part-time DPO): "...two separate and distinct performance evaluations carried out by different reporting officers, one for the DPO function and one for the other job function."

EBA: "The appraisal is carried out by the DPO's middle manager, with input from the Executive Director in relation to the individual's duties as DPO."

ECDC: "Performance on the DPO duties is given equal weighting to performance on the non-DPO duties. As the DPO reports directly to the Director, the evaluation of the performance on the DPO duties is carried out by the Director. These rules have been formalized internally."

EMA: "...the reporting line manager...consults with the Executive Director about the evaluation of the performance of the DPO and receives his/her input / comments before finalising the report".

Given that all institutions note that their DPO is involved in designing new processing operations, the **EDPS invites all institutions to ensure that the DPO's activities are valued in the context of the DPO's performance evaluation**.

In turn, the EDPS encourages DPOs to develop their own common principles of good supervision (requirements, annual work programme, annual report...) which can serve to measure the performance of their work[40].

2.6. Bodies that have not replied to the survey

By the time of adoption of this text, only one body, the SESAR JU, had not replied to the survey on substance.

The SESAR JU noted a "lack of capacity" due to the unforeseen need to appoint an acting DPO.

[40] See also Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, p. 8.

The fact remains that the Regulation needs to be complied with. As mentioned in the introduction, the results of this Survey will feed into the planning of enforcement actions for 2016. When EU institutions do not reply at all or on time, this can be a cause for concern.

3. Follow up of the previous survey: compliance visits

3.1. General remarks

As a consequence of the previous Survey –apart from general follow up and some specific cases – the EDPS has visited five institutions that were flagged during the 2013 exercise.

At the time, an inspection as such was not envisaged for these institutions because the level of compliance with Regulation (EC) 45/2001 was generally low. It would have been difficult to "check the reality" of processing operations not yet notified or of non-existent compliance tools (inventory, register), as there would have been no baseline of expectations against which to check.

These compliance visits serve to secure commitment from top and middle management. This "top down" approach is meant to ensure buy-in from management; experience has shown that effective data protection is not only a matter of resources, but also of organisational will. In a nutshell, these visits are **"visits with courtesy, but not courtesy visits**". The instrument of such compliance visits has since been codified in Article 36 of the Rules of Procedure of the EDPS[41].

***Compliance visits**: A visit is a compliance tool, the aim of which is to engage the commitment of the senior management of an institution or agency to comply with the Regulation. The decision to visit is usually taken when there has been a lack of compliance with the data protection rules, a lack of communication or simply to raise awareness. This is based on the information we have gathered when monitoring compliance, for example, in a general survey. The visit comprises an on-site visit by the EDPS or Assistant EDPS and is followed-up with correspondence relating to a specific road map agreed between us and the body visited.*

To boost compliance, the EDPS used the visits to set up precise roadmaps, in agreement with the hierarchy of the institution concerned. The roadmaps included specific objectives and deadlines on matters such as the establishment of an inventory, progress in the level of Articles 25 and 27 notifications, the notification of targeted procedures for which the EDPS has issued Guidelines[42], and other matters specific to the institution visited (e.g. ensuring a long term DPO function, providing training to staff on data protection, etc.).

As for the previous exercise, a comparison of the notification levels between the Survey 2013 and the present results has been conducted to evaluate the effects of such visits.

Name	**Results in 2015 Survey**		**Results in 2013 Survey**		**Change in rates**	
	Article 25	**Article 27**	**Article 25**	**Article 27**	**Article 25**	**Article 27**
EIGE	50%	86%	**63%**	**86%**	**-13**	**+/- 0**
EIF	34%	47%	**Not comparable**		-	-

[41] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013D0504(03)&from=EN.
[42] https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.

GSA (GNSS)	52%	54%	**Not comparable**			
EUSC	52%	100%	**No reply**			
EUISS	25%	17%	**0%**	**0%**	**+25**	**+17**

Figure 4: Evolution of notification rates for visited agencies

The table above shows the percentages for Article 25 and Article 27 notifications both in 2013 and 2015 for each of the institutions visited, as well as the change in percentage points. It confirms that visits have a clearly positive compliance effect. The following sections provide additional information about each of the visits and the improvements seen afterwards.

3.2. EIGE

The European Institute for Gender Equality (EIGE) in Vilnius officially became operational in summer 2010. The EIGE replied late to our 2011 Survey and, by early 2013, had not submitted a single prior check notification. For this reason, the Assistant Supervisor visited EIGE in May 2013. The half-day visit consisted of meetings with management, the staff in charge of processing operations, as well as the DPO and Deputy DPO. Following the visit, the EIGE and the EDPS agreed on a roadmap towards compliance. EIGE has shown good performance for an agency of its age in the 2013 Survey and also provided follow-up on the other items in the roadmap. However, notification rates for Article 25 notifications have gone down since the 2013 Survey, indicating that the initial effort may not have been sustained.

3.3. EIF

The European Investment Fund (EIF) is a public-private partnership with the EIB, the European Commission and several financial institutions as shareholders based in Luxembourg. Its core business is to provide risk finance to SMEs. The decision to visit the EIF was based on a reconsideration of the relevant roles in relation to data processing between EIF and EIB, which lacked clarity and the consequent identification of low notification scores in the 2013 Survey for EIF's processing operations it manages on its own (independently from the EIB). . During the visit, we identified various areas of non-compliance, e.g. regarding the clarity of the inventory and the lack of notifications under both Articles 25 and 27 of the Regulation. The EIF committed to take measures in order to achieve compliance in the context of a mutually agreed roadmap. It has in the meantime completed the inventory, updated the Article 25 register and filed a series of Article 27 notifications with the EDPS. The numbers in section 2.1 reflect the situation as of the EIF's reply to the survey - since then, the EIF has cleaned its backlog and is on a good track towards finishing the roadmap.

3.4. EUSC (EU SatCen) and GSA (European GNSS Agency)

The EU Satellite Centre (EU SatCen) and the European GNSS Agency (GSA) were also selected for a visit based on our Survey 2013, where we had found communication to be a problem. Given that neither agency had provided sufficient evidence of satisfactory compliance by the deadline we set them, we decided to conduct these visits at working-level on issues ranging from human resources management to IT security and the tasks of different actors within the organisation in relation to data protection. This involved trainings and Q&A sessions conducted by EDPS case officers, with the aim of providing hands-on help to the agency and educating staff and management on how best to integrate data protection

principles into their working environment. Both agencies fully engaged with us and have expressed their commitment to improve compliance with data protection principles - both with a view to achieving full compliance for this 2015 Survey. While cooperation with GSA has improved, notification levels remained below average for an agency of its age at the cut-off date of this survey. However, several new Article 27 notifications have been submitted by the date of publication of this report. Regarding EU SatCen, a secondment of an EDPS staff member took place in November 2014, followed by a meeting at Directors' level in December 2014. Since then, all Article 27 notifications have been submitted and almost all cases are closed. Regarding IT specific notifications, a close cooperation with the EDPS will be ensured where necessary.

3.5. EUISS

The European Union Institute for Security Studies (EUISS) was chosen as a target for a visit because of its performance in the Survey 2013. A former second pillar agency, EUISS updated its legal basis in early 2014. For practical reasons, the visit was split into a meeting between the EUISS' Director and the Assistant Supervisor in June 2014, and a visit to the EUISS in Paris at staff level in October 2014. In the meeting between the Director and the Assistant Supervisor, EUISS stated its commitment to improve compliance. During the visit in Paris, EDPS staff met EUISS' newly appointed Head of Administration, the DPO and relevant staff for discussions and a training session on data protection principles. The test for improved compliance is the present Survey 2015. While EUISS has started to work on its compliance, notification levels remain low, even for an agency with a recently established data protection function (EUISS' first DPO was only appointed following the 2013 Survey). Further efforts are necessary, notably by the business units to fulfil their notification obligations to the DPO.

3.6. Evaluation of the visits programme

As was the case for the previous Survey, the results show that visits have proven to be a useful tool in improving compliance by providing information, sensitising top management and agreeing on concrete targets and deadlines for most of the visited entities. The programme will thus be continued in the following years. The results of the present Survey will also be an important factor in deciding on the EU institutions to be visited in the future.

Most visits have led to increased compliance; however, in case a visit does not lead to positive changes, further follow-up action needs to be considered. In such cases, the EDPS may decide to carry out an inspection or make use of enforcement powers granted under Article 47(1) of the Regulation[43].

[43] See the EDPS Policy Paper on "Inspections conducted by the EDPS" (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_Policy_EN.pdf), p. 5.

4. Conclusion & Planned Follow-up

In general, the results of this year's survey again confirm steady progress towards full implementation of the Regulation in the EU institutions.

For the well-established and mature institutions, not much has changed in terms of the replies - notification rates are high and the DPO function is consolidated. The task at hand for these EU institutions continues to be the proper maintenance of the inventory and the register. In some cases notification rates fell slightly, due to new processing operations being set up. This is as such no cause for alarm, but shows that keeping inventories and registers in shape requires constant attention and is not a one-off exercise. The task for these EU institutions now is to mainstream data protection and to have it become a reflex.

The results in Group B are similar. On Article 27 notifications, they have closed the gap to those in Group A; on Article 25, a slight gap remains. Agencies that were lagging behind have also made up ground, such as EASA. Several agencies reported perfect scores and several more just missed that target by a few notifications.

Group C now show average notification rates better than Group B in the 2013 survey and has almost caught up with that group in this survey. INEA is a success story here, as well as Frontex, which moved from being a cause for concern to a solid middle-field performer.

It is understandable that Group D shows lower rates. However, after the striking improvements between the 2011 and 2013 surveys, progress seems to have slowed down somewhat, notably on Article 27 notifications. The EDPS will provide support and coaching where necessary to ensure proper implementation of the Regulation.

This survey is not only meant to provide a state of play on the implementation of the Regulation. It also feeds into the choices the EDPS makes as regards supervision and enforcement activities.

Based on the results of the survey, it seems that a number of bodies still have problems in complying with the Regulation.

Additionally to visits, the EDPS may consider other enforcement measures, using his powers under the Regulation.

IV. Annex (1) Methodology

As was the case for previous exercises, the survey was carried out as a desk exercise, requesting information in writing from EU institutions. The list of questions was sent to the EU institutions in April 2015; reminders were sent in June 2015 at working level. Replies arrived throughout June and July 2015. In December 2015, EU institutions were consulted on the draft report.

EU institutions were asked to supply information on the following aspects:

1. **Inventory and Register**[44]: the number of processing operations (1) identified in inventory, (2) those notified to the DPO and included in the register, (3) those identified as subject to Article 27 and (4) those actually already notified to the EDPS under Article 27[45];

2. **Transfers of personal data under Article 9** in the years 2013 and/or 2014:
   - transfers under Articles 9(2), 9(6) or 9(7) and those transfers under Article 9 to recipients which are established in EEA countries, but conduct types of activities that are excluded from the application of Directive 95/46/EC;
   - specifications on the processing activity (as mentioned in notification Article 25), the recipient, the basis, the field (e.g. law enforcement), the "how" of the transfer, the categories of personal data as well as the frequency of such transfers;
   - any particular difficulties encountered in the above activities;
   - existence of an internal monitoring and registration system of Article 9 transfers;

3. **Information security**: (1) existence of a process specifically dedicated to information security, (2) performance of risk assessments, (3) existence of a general security policy[46], (4) existence of a formal process for the handling of security incidents and (5) whether the DPO is notified in case the information security incident involves personal data.

4. **Ensuring effective deletion of personal data**: (1) existence of a written policy and a standard procedure regulating the effective deletion of personal data at the end of their retention period, (2) existence of automated processes supporting the deletion procedure across all systems, (3) measures to ensure the erasure of information in back-ups, if any.

5. **Your Data Protection Officer and you**: In a separate section, for which the EDPS explicitly asked that replying to it *not* be delegated to the DPO, the EDPS requested information on whether the DPO's tasks are part of his/her job description, if the performance of the DPO's tasks forms part of his/her performance evaluation and how the DPO is involved in the design of new processing operations.

An overview of the answers given to question 1 is displayed in a comparative table (see section 2.1 above). Questions 2 to 5, which do not lend themselves easily to quantitative analysis, are analysed qualitatively in the body of this report.´

[44] Unlike previous exercises, the EDPS did not request to receive copies of the actual inventory or register.
[45] Where such information is also available on a more granular basis, such as per Directorate-General of the institution or body, EU institutions were invited to provide such information as well.
[46] This question did not regard the application-specific security policies.

V. Annex (2) Some limitations of the methodology

I. An institutions which does not properly identify all the procedures involving processing of personal may appear to have a better compliance record than is actually the case.

II. Inventories may already contain procedures involving processing operations identified by the institution but not yet fully developed. Obviously the procedure cannot be notified before it is defined more fully. In the calculation however it will appear as a non-notified processing operation and thus show a lower level of notifications.

III. An institution may identify in its inventory a future risky processing operation, but as the procedure linked to this processing operation is not sufficiently developed, it cannot yet be notified under Article 27. In the calculation, this will appear as a non-notified processing operation and show a lower notification rate.

IV. Inversely, institutions that identify many additional processing operations may see their notification rates decline, even though they spend considerable effort in doing the notifications. This "uphill race" effect is mentioned where it is observed.

V. Similarly, updating notifications may lead to temporary drops in the notification rates. For Article 25 notifications, where such drops were observed, the EDPS requested clarification; in many cases the changes are minor (e.g. a new head of unit as contact point), so they were counted as done, to avoid penalising institutions that made an effort to keep their registers up to date. For Article 27 notifications where updates would require updates or entirely new notifications to be sent to the EDPS, these were counted as not done. Where this occurred, it is mentioned in the report.

VI. The EDPS may suspend the analysis of a notification if EDPS Guidelines on the same procedure are under way. In the calculation however it may appear as a non-notified processing operation and thus show a lower level of compliance. If the EDPS receives notifications on such processing operations before the Guidelines are published, they will be counted as notified; only their analysis will be suspended.

VI. Annex (3) Groups of EU institutions

Group A (12): Institutions that were founded before 2004 and had appointed a DPO before the establishment of the EDPS:
European Commission, Committee of the Regions, Council, European Court of Auditors, European Central Bank, European Court of Justice, European Economic and Social Committee, European Investment Bank, European Parliament, OLAF, European Ombudsman, Translation Centre for the bodies of the European Union.

Group B (17): Bodies that were established (or started their activities) before or in 2004, but appointed a DPO at a later stage:
CEDEFOP, CPVO, EASME, EASA, EDPS, EEA, EFSA, EIF, EMCDDA, EMA, EMSA, ENISA, ETF, EUROFOUND, FRA, OHIM, EU-OSHA.

Group C (18): Bodies that were established (or started their activities) after 2004, but before 2011:
EFCA, EACEA, Chafea, ECDC, ECSEL (as successor to ARTEMIS and ENIAC), ERA, FRONTEX, GSA, INEA, Clean Sky JU, ECHA, ERCEA, F4E, FCH JU, IMI JU, REA, SESAR.

Group D (15): Bodies that were established (or started their activities) in 2011 or later, as well as former second and third pillar bodies:
ACER, BEREC, EASO, EBA, EIOPA, EIGE, EIT, ESMA, ESRB, EEAS, eu-LISA, CEPOL, EDA, EUISS, EUSC.

VII. Annex (4) List of institutional acronyms

ACER	Agency for the Cooperation of Energy Regulators
BEREC	Body of European Regulators for Electronic Communications
CdT	Translation Centre for the bodies of the European Union
Cedefop	European Centre for the Development of Vocational Training
CEPOL	European Police College
Chafea	Consumers, Health and Food Executive Agency
CJEU	Court of Justice of the European Union
Clean Sky JU	Clean Sky Joint Undertaking
CoR	Committee of the Regions
Council	Council of the European Union
EC	European Commission
CPVO	Community Plant Variety Office
EACEA	Education, Audiovisual and Culture Executive Agency
EASA	European Aviation Safety Agency
EASME	Executive Agency for Small and Medium-sized Enterprises
EASO	European Asylum Support Office
EBA	European Banking Authority
ECA	European Court of Auditors
ECB	European Central Bank
ECDC	European Centre for Disease Prevention and Control
ECHA	European Chemicals Agency
ECSEL JU	Electronic Components and Systems for European Leadership Joint Undertaking
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EEA	European Environment Agency
EEAS	European External Action Service
EESC	European Economic and Social Committee
EFCA	European Fisheries Control Agency
EFSA	European Food Safety Authority
EIB	European Investment Bank
EIF	European Investment Fund
EIGE	European Institute for Gender Equality
EIOPA	European Insurance and Occupational Pensions Authority
EIT	European Institute of Innovation and Technology
EMA	European Medicines Agency
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
EP	European Parliament
ERA	European Railway Agency
ERCEA	European Research Council Executive Agency
ESRB	European Systemic Risk Board
ESMA	European Securities and Markets Authority
ETF	European Training Foundation
EUISS	European Union Institute for Security Studies
eu-LISA	European Agency for the operational management of large-scale IT system in the area of freedom, security and justice
EUROFOUND	European Foundation for the Improvement of Living and Working Conditions
EUSC	European Union Satellite Centre
F4E	Fusion for Energy
FRA	European Union Agency for Fundamental Rights
Frontex	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
FCH-JU	Fuel Cells and Hydrogen Joint Undertaking
GSA (GNSS)	European Global Navigation Satellite Systems (GNSS) Agency
IMI JU	Innovative Medicines Initiative Joint Undertaking
INEA	Innovation and Networks Executive Agency
OHIM	Office of Harmonization for the Internal Market (Trade Marks and Designs)
OLAF	European Anti-fraud Office
Ombudsman	European Ombudsman
EU-OSHA	European Agency for Safety and Health at Work
REA	Research Executive Agency
SESAR JU	Single European Sky ATM Research Joint Undertaking