EUROPEAN DATA PROTECTION SUPERVISOR

REPORT
Survey 2017

Measuring compliance with data protection rules in EU institutions

27 November 2017

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 ("EUI")** 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 EUI in moving beyond a purely compliance based approach to one that is also based on accountability in close cooperation with the Data Protection Officer (DPO) appointed in each EU institution. EUI 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 EUI 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 EUI. This report is the result of the sixth consecutive exercise; it is based on the responses received from 64 **EUI** by mid-July 2017.

In line with the EDPS enforcement policy[3], this report is published with the intention to encourage greater accountability for compliance with data protection by EUI. The report is part of our efforts to train and guide EUI 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**.

The responses received and previous compliance and accountability 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 EUI. Rather, it looks at the overall performance of each EUI 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 EUI.

The EDPS will take the results of this Survey into account in planning further supervision and enforcement activities. However, in our supervision of EUI, we will act through education, persuasion and example, preserving our powers of enforcement as a last resort. Our activities will combine **guidance** to EUI, **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 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 EUI 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 2018, which, with the entry into force of the GDPR as well as a new Regulation amending Regulation (EC) 45/2001 will mark a new era in data protection.

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

The well-established and mature EUI now need to focus on maintaining their achievements in terms of maintaining proper inventories. Those EUIs who have complete and up-to-date registers under Regulation (EC) 45/2001 will have an easier time adapting to the new rules. It follows that EUIs should not slow down their efforts to complete their registers now. Less mature institutions have made up ground again. Where progress has slowed down, we will provide the necessary support to ensure that data protection becomes a reflex.

As was the cases for previous editions, the Survey covers questions on international transfers, a hot topic in the light of recent and upcoming jurisprudence and resulting political developments. With almost half of the EUI conducting some form of international transfer under Article 9 of the Regulation, these transfers are no longer a rarity. As the Survey shows, EUI are pro-actively considering how to best react to the resulting challenges. Other topics covered in this Survey include the collection of identification documents by EUI and specific training needs identified by EUI in this busy and exciting transition period.

TABLE OF CONTENTS

1. Inventory and Register of Processing Operations, state of play Article 27

1.1 Notification rates

Like in the 2015 Survey, we 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 institutions also had such information also available on a more granular basis, such as per Directorate-General, we invited them to provide this as well.

A **large majority** of EUI keep –as recommended by the EDPS– **both an inventory and a register**. Those EUI 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.

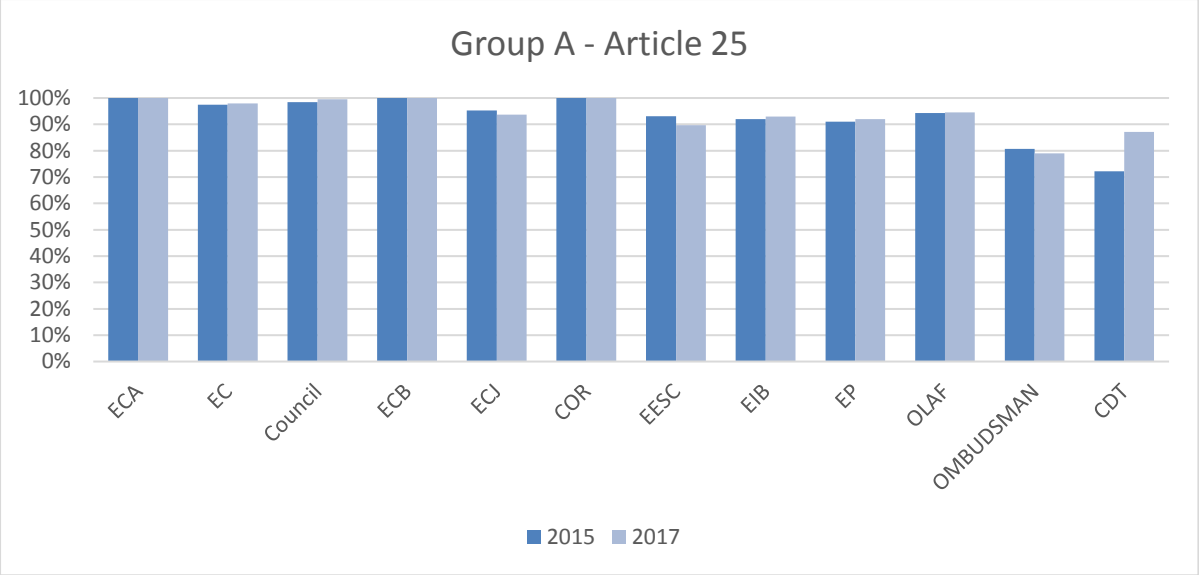
*Article 25 of the Regulation provides that the DPO shall receive a notification of all processing operations involving personal data. According to Article 26 of the Regulation, these are to be kept in a **Register**, whose minimum content is defined in that Article. Processing operations considered 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 2015, **notification rates have risen in general**. The tables below provide an overview of the rates in the current Survey and changes compared to the 2015 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.

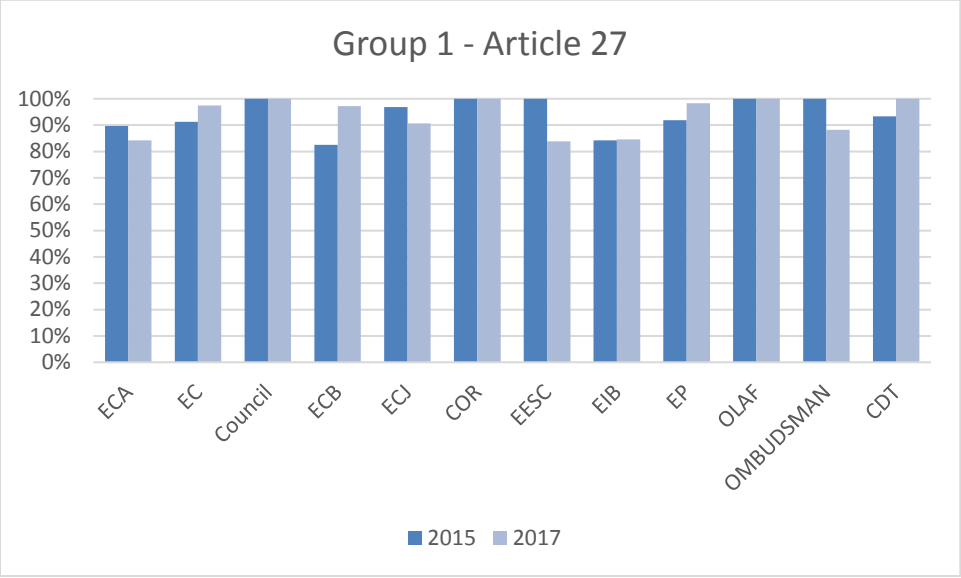
In some cases, rates have declined. This usually concerns EUI with a high compliance rate in cases where updates of the inventory have led to DPOs becoming aware of additional processing operations. This can lead to fluctuations in the 90% to 100% range and is not as such a cause for concern. Given that 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[4].

The purpose of these benchmarks is to compare EUI 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 setting up. For this reasons, we compare institutions to others of similar maturity in terms of their data protection functions, resulting in four groups (A to D)[5].

[4] The average number of processing operations falling under Article 27 is 20 per EU institution, if excluding the Commission, which has more than 200.
[5] See annex 3 for an explanation on how we created the groups.

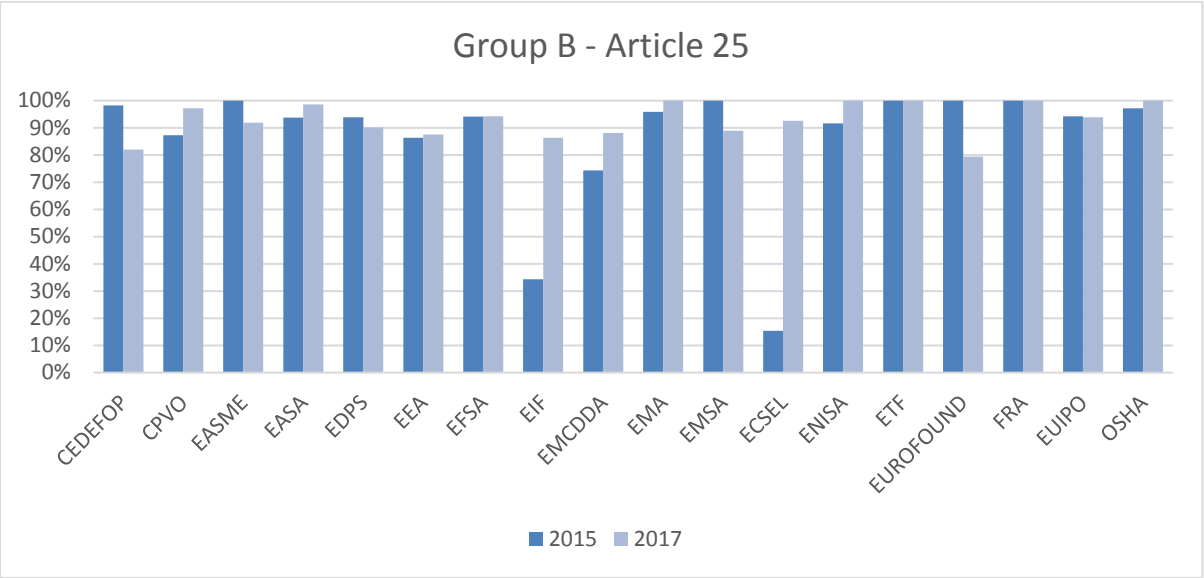


For Article 25 notifications, institutions in group A show on average quite high notification rates, mostly in the 90% range. As mentioned earlier, starting from such a high level limits the room for improvement and some institutions have reported lower levels compared to the 2015 Survey. If such fluctuations 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.



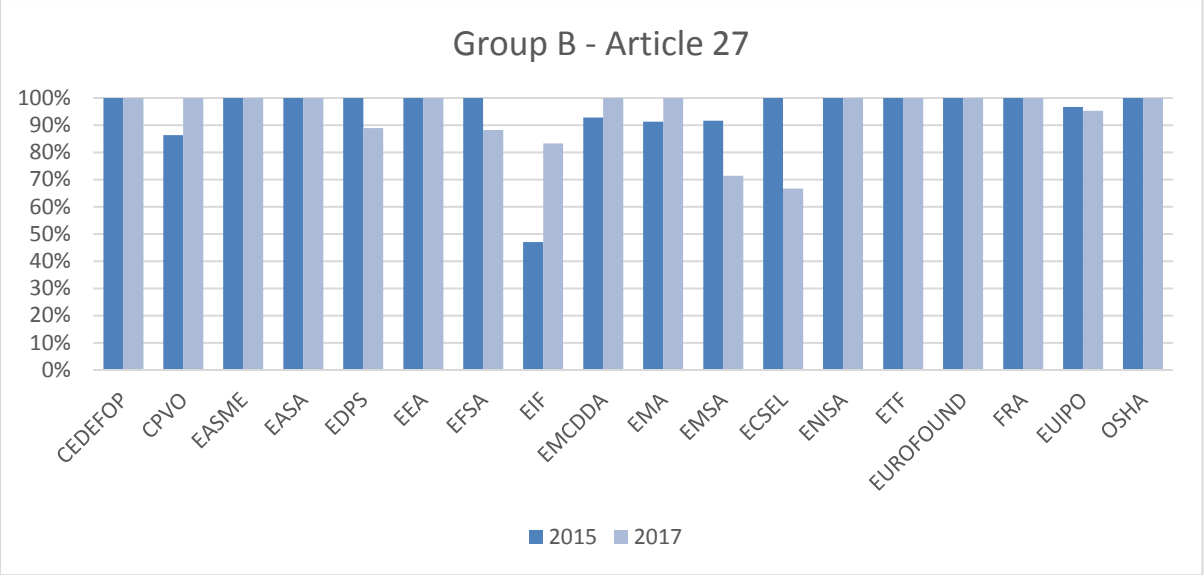
The picture on Article 27 notifications is a bit more mixed. The explanation for ECA's decrease are a number of new/updated processing operations identified for Article 27 notification - in the time between the deadline for replying and publication of the Survey report, the ECA has started notifying these operations. The EESC's drop has the same explanation - in 2015, the EESC had a perfect score on Article 27 with 29 out of 29 operations notified; following the identification/creation of a number of new processing operations subject to prior checking, it is now at 31 out of 37 notifications. Similarly, the Ombudsman's decrease follows the same pattern: 15 out of 17 notifications done now, compared to 14 out of 14 in 2015.

On the other hand, EC, ECB, EP and the CDT increased their notification rate; the EIB remained at a constant percentage, which masks the rising numbers.



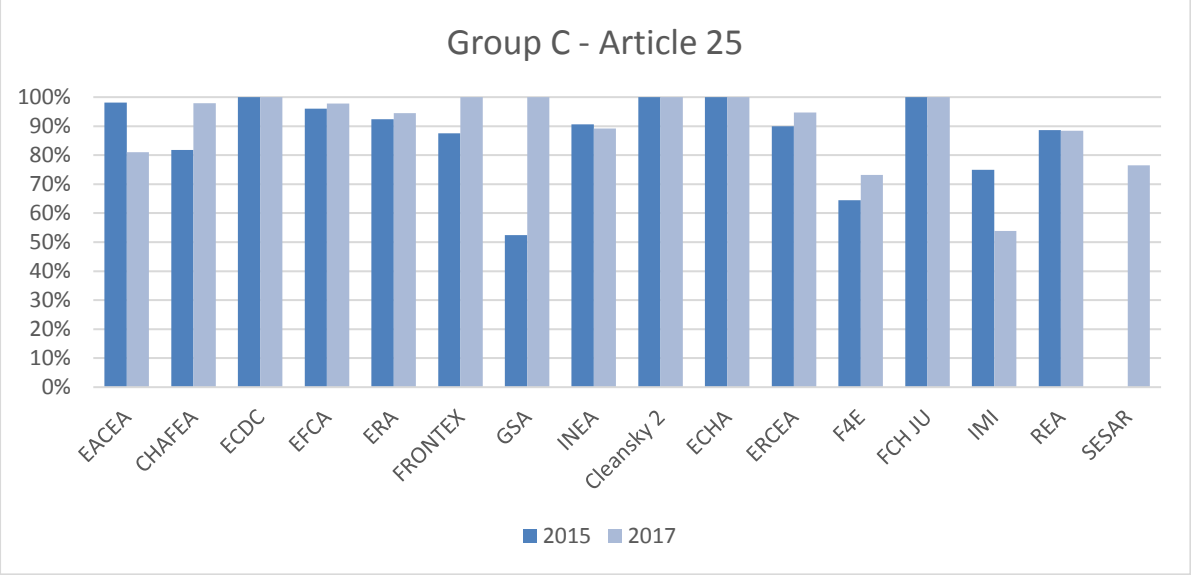
As a whole, group B has closed the gap to group A. The EIF and ECSEL made the biggest progress. In both cases, there is a story behind it. ECSEL replaced and merged two older joint undertakings (ARTEMIS and ENIAC). In 2015, ECSEL was still setting up its register, explaining the very low notification rates. For this year's edition of the Survey, ECSEL has closed this gap and is a midfield performer in group B. The EIF cooperates closely with the EIB for many administrative matters. In the past, it also relied on the EIB's register for documenting processing operations that happened identically or in a very similar way in both bodies. Over the last years, the EIF disentangled its register from the EIB, reflecting the fact that it is a separate EU body. The EDPS accompanied this process with a compliance visit in 2016. While those two bodies showed the biggest improvements, EMCDDA closed the gap it used to have compared to its peers.

In the cases of CEDEFOP, EMSA and Eurofound, new processing operations explain the drop in the rates – CEDEFOP was at 57 out of 58 notifications done in 2015 and now is at 64 out of 78. For EMSA, the numbers are 113/113 and 112/126 respectively. Eurofound had a perfect score with 60/60 in 2015 and is now at 58/73.



Concerning Article 27 notifications, the EIF showed the biggest increase, mirroring its improvements under Article 25.

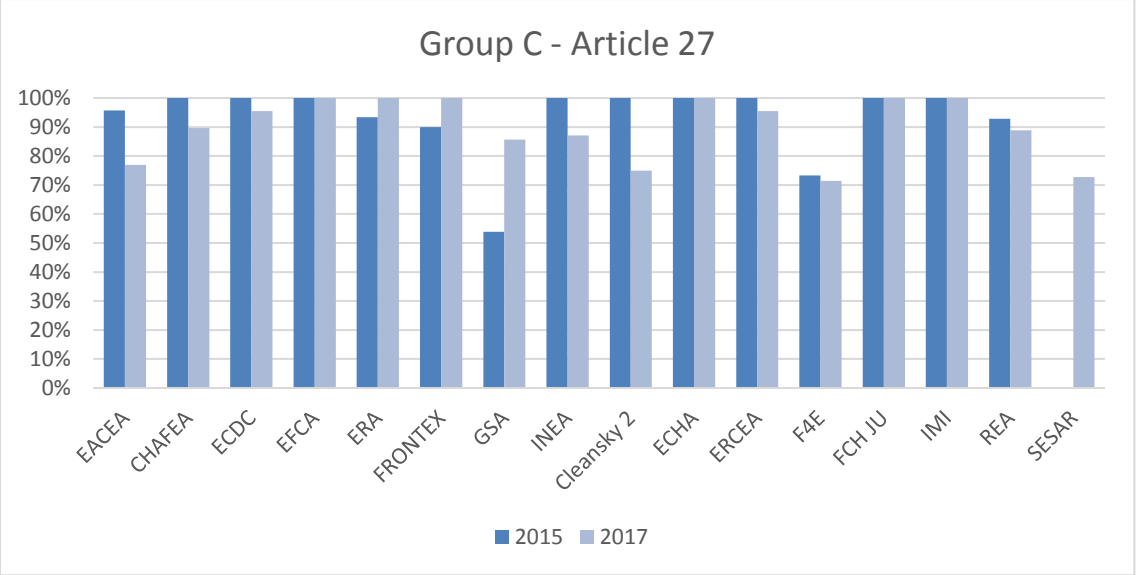
The case of ECSEL illustrated how Article 27 notification rates can be more volatile, especially for bodies that do not have many Article 27 cases. What looks like a massive drop is in fact due to just two newly identified processing operations under Article 27. EMSA's situation is similar, with 10/14 instead of 11/12.



GSA showed the biggest improvements in this group, completing its register.

IMI's reduction in the notification rate masks an increase in the actual numbers: IMI's register grew, but simply not in pace with its inventory list. This situation should be temporary.

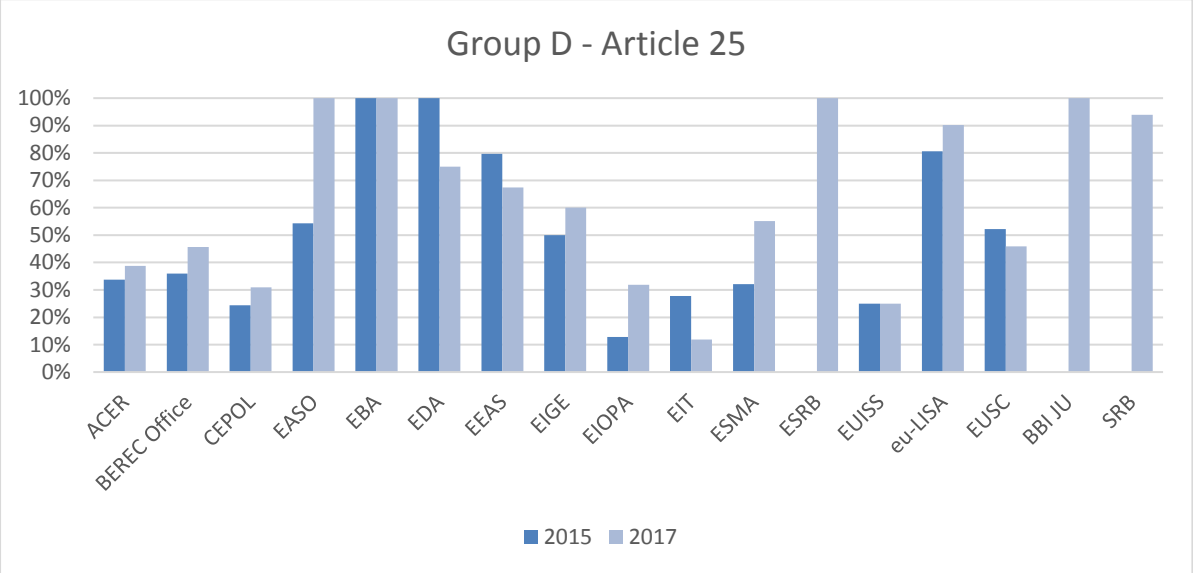
The SESAR Joint Undertaking did not reply to the 2015 Survey, so no direct comparison is possible. In 2013, it reported an Article 25 notification rate of 76%, close to the current rate of 78%.



GSA's progress on Article 27 mirrors its progress on Article 25.

The reduced rates for EACEA, INEA and Cleansky2 are due to newly identified or changed processing operations requiring either new or updated notifications.

The SESAR Joint Undertaking did not reply to the 2015 Survey, so no direct comparison is possible. In 2013, it reported an Article 27 notification rate of 67%, so the current rate of 73% is only a slight improvement.



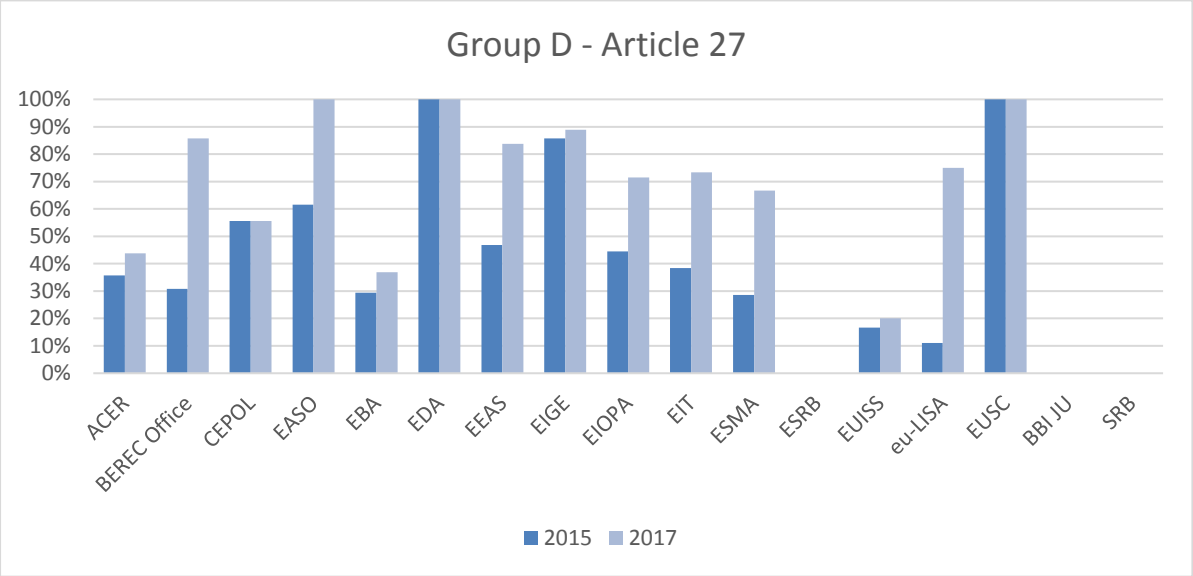
EASO completed its register.

The ESRB depends (according to Regulation 1096/2010) on the ECB for many administrative processing operations; the ESRB thus only sees itself as controller for those processing operations which it manages independently of the ECB. This Survey is the first time it is counted separately from the ECB.

EDA's reduced rate is simply due to the fact that its inventory grew faster than the number of notifications done (42 out of 56 done, instead of 37/37 in 2015). EIOPA has consolidated its inventory, improving the situation since the moment it submitted the reply to the survey report.

While the EIT showed progress on Article 27 (see below), its Article 25 notification has dropped even further. EIT focussed on Article 27 first, but should not neglect Article 25 either.

In this year's edition of the Survey, there are two new entries: SRB and BBI JU. Both have first focussed on their internal Article 25 notification, which are almost done in the case of SRB and completely done for the BBI JU.



As EUI in group D are relatively new, it is to be expected that their notification rates will still be lower than those of more mature organisations. On the other hand, they should show a steady upwards trend.

BEREC Office, EASO, EEAS, and eu-LISA show such clear improvements. EIOPA[6], EIT, and ESMA are also improving, but to a lesser extent.

On the other hand, ACER, CEPOL, EBA[7] and EUISS show very small to no improvements. These agencies should make a renewed effort to get their processing in order before the new rules will become applicable.

As mentioned, BBI JU and SRB first focussed on Article 25 notifications. The next step for them will then be to clear their Article 27 notifications to the EDPS, as they had not notified any.

The ESRB depends (according to Regulation 1096/2010) on the ECB for many administrative processing operations; the ESRB thus only sees itself as controller for those processing operations which it manages independently of the ECB. It has only identified a single processing operation subject to prior checking, which is still outstanding.

[6] Since the cut-off date for replying to the survey, EIOPA has consolidated its inventory, improving the situation.
[7] Since the cut-off date for replying to the survey, EBA has submitted several notifications, narrowing the gap.

1.2 Anticipating the phase-out of notifications under Article 27

To help the EDPS anticipate the phase-out of notifications under Article 27 of the Regulation (and the phase-in of the new Regulation, including e.g. DPIAs), we asked for guestimates on which of two scenario sounds more likely:

- a rush to notify processing operations under Article 27 of the Regulation before the revised Regulation enters into force *or*
- a reluctance to notify before the new Regulation leading to a backlog upon its entry.

Where EUI indicated that these scenarios apply, the replies indicated a certain balance between rush and reluctance: 12 EUI indicated that a "rush" might occur, whereas 14 institutions indicated that there might be a reluctance to notify. 29 EUI replied "neither/nor", either because they estimated that all processing operations had already been notified (or only very few were likely to occur) or because they do not foresee any bottlenecks, but rather "business as usual" or, in one case, because staff is unaware of upcoming changes (!). The rest of the EUI were unable to position themselves on the question.

Chafea: "*Business as usual. We do not expect bottlenecks as to the notifications done*."

EMA: "*...At this stage, there is not a foreseeable need to notify additional processing operations under Article 27..., however it cannot be excluded that this need might materialize in the upcoming year and due to unforeseeable circumstances. ...the approach of EMA would be to seek in a timely manner, in this transitional period ending with the entry into force of the new Regulation, the assistance of the EDPS to clarify whether such new processing operations are subject to a prior check procedure in accordance with... Regulation (EC) 45/2001*."

1.3 Phase-out of notifications under Article 27 / transition rules

EUI will not have to create records and other documentation from scratch. Under Article 25 of the Regulation, controllers already had to submit notifications containing essentially the same information as records under Article 31 of the Proposal to their DPOs. If an EUI chooses to have the DPO manage the central repository of records, then the register kept by her/him can be the starting point for the EUI's records. These notifications can serve as a starting point for records under the new rules. In turn, this means that those EUIs who have complete and up-to-date registers under Regulation (EC) 45/2001 will have an easier time adapting to the new rules. It follows that EUIs should not slow down their efforts to complete their registers now.

Should the processing operations change, the documentation will have to be updated to have proper records under Article 31 of the Proposal. In any case, EUIs need to make sure that eventually, they update all their old Article 25 notifications to records. EUIs should finish this process at the latest by 25 May 2020.

EUI also already carry out processing operations that will trigger the criteria for conducting DPIAs. Many of these have been prior-checked under Article 27 of the Regulation in the past. While the criteria for prior checking under the Regulation and the proposal are not identical, there is a certain overlap – most processing operations requiring a DPIA under the proposal already required prior checking under the Regulation. There are also processing operations that required prior checking under the Regulation, but which will not require a DPIA.

- ***Closed prior checking cases***

Processing operations that will require a DPIA and that have been prior-checked with a positive result (with a closed follow-up procedure, where applicable) under the Regulation can benefit from a 'grace period' of two years, so no DPIA will be necessary immediately.

However, if/when procedures and/or risks change, a DPIA will be necessary in order to verify compliance with the new rules. Additionally, this only offers a 'grace period': EUI will have to bring such legacy processing operations into line with the adopted proposal by two years after its applicability, i.e. 25 May 2020.

- ***Prior checking Opinions still in follow up phase***

If follow-up for processing operations that required prior checking under Article 27 of the Regulation and a DPIA under the new Regulation is still ongoing, EUI should try to have it closed before the new rules become applicable. That way, they will have a clean slate. If follow-up is still ongoing by the time the new Regulation will become applicable, EUI should check if a DPIA is needed by conducting a threshold assessment and if this confirms the need for a DPIA, start carrying it out immediately.

2. Identifying the correct data subject correctly

In order to verify the identity of data subjects exercising their data subject rights (e.g. in the context of access requests), data subjects are invited by a number of EUI to provide a **copy of an identification document** for confirmation of their identity.

This issue will become particularly relevant in the implementation of Article 12(6) GDPR ("*Where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject*") and its Recitals 57 and 64 GDPR.
It seems likely that the **revised Regulation will contain similar provisions**[8].

Recital 57 GDPR reads: *"If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.""*).

Recital 64 GDPR reads: *"The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests."*

2.1. Collecting a copy of an identification document

Against the above background, we asked for information on whether EUI collect a copy of an identification document for confirmation of the identity of data subjects exercising their data subject rights.

According to the replies, two EUI always collect a copy of an identification document for confirmation of the identity of data subjects and one will do so in the future. 16 EUI only sometimes do so, out of which three clarified that they only request identification from data subjects that are not staff members of the respective EUI.

The **vast majority of EUI will need to revise their procedures** upon entry of the revised Regulation (foreseen for May 2018, i.e. coinciding with the GDPR), as a total of 45 EUI indicated that they never collect a copy of an identification document for confirmation of the identity of data subjects exercising their data subject rights[9].

[8] See Article 14 (1) and (6) of the Commission Proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017)8 final, of 10 January 2017.
[9] The EDPS previously dealt with **access control cases** raising similar issues (not published); for a resulting limited set of data collected by the EP for the purpose of visitor access control, see http://www.europarl.europa.eu/pdf/data/data_EN.pdf, point a).

ECB: "*For external requesters, we request an identification document. If the request is submitted by a known ECB staff member, we refrain from requesting identification*."

EEA: "*...so far the EEA has not deemed it necessary to request such an identification document, as there were only few cases were data subjects had requested to exercise their rights of access as to their personal data and all those cases related to members of staff. The EEA however does not discard the possibility to request in the future the submission of an identification document...*".

ESMA: "*...ESMA never received so far such a request and therefore never processed personal data in this particular context*."

SESAR: "*...the SESAR JU has not received any request from a data subject that is not an employee of the SJU. In the future, should the SESAR JU receive any request of the type, the SJU would request an identification document only in the case that this document would constitute the only valid evidence to identify the data subject correctly. In line with the provisions of the GDPR, would not retain the data for any other purpose than identification.*"

2.2. Retention period

Out of those 18 EUI that (always or sometimes) collect a copy of an identification document, five retain the copy only as long as necessary to establish the identity of the data subject exercising his/her data subject rights and delete them immediately after. Four EUI keep the copy until they have replied to the data subject exercising his/her data subject rights. Six EUI indicated a standard retention period ranging from several months (two to six months), two to five years and, for one EUI, up to ten years in recruitment cases.

EEA: "*...the document will be stored for a maximum of three months from the date of receipt of the request from the data subject, which corresponds to the period in which the request shall be dealt with*."

EEAS: "*...Copy of ID documents within the dossier of payment related financial documents linked to reimbursement of travel expenses are kept for up to five years from the date on which the European Parliament grants discharge for the budgetary year to which the data relates*."

EMA: *In relation to a request for access to pseudonymised medical records stored in the EudraVigilance database, a copy of the identification document will not be retained beyond the period needed to verify identification. As regards a request submitted by a former member of staff for access to a file held by the Agency, a copy of the identification document will only be retained until identification has been confirmed*."

CJEU: "*Identity control occurs for staff members in order to grant them physical access to their personnel file. No copy of the ID is retained after verification of the identity of the data subject*."

The principle of **purpose limitation** suggests that the personal data obtained for confirmation of the identity of data subjects exercising their data subject rights can only be used to verify the requestor's identity; they cannot become part of the data inventory of the EUI. The EDPS therefore suggests a retention period for the copy of an identification document that is **limited to the period required to establish the identity of the requestor**, including for cases of doubt.

2.3. Full copy or selected data set?

Out of those 18 EUI that collect a copy of an identification document, 12 collect a full copy of the document (two EUI indicated that this practice is under revision). Ten EUI indicated that they only collect a limited data set (or plan to do so in the future).

FRA: "*The intention is to collect as little as possible provided that the data subject is identified.*"

EMA: "*...the Agency does not request the submission of the entire document, but merely a proof of identification. It is therefore for the applicant making the request to decide whether to send the full copy of the ID document or only part of the document which would enable identification*."

ECB: "*So far (we collect) the copy of the identification document, but we are in the process of re-evaluating this in light of the new requirements*."

Where EUI only collect a limited data set, we asked them to indicate what that limited data set consists of ("If you collect only a limited number of personal data, which ones are these?") in line with the box below.

a) identity document number;
b) country of issue
c) first and last name;
d) address;
e) date and place of birth;
f) document expiration date;
g) photo;
h) personal characteristics (height, eye colour etc.);
i) other; please specify:_____

Six EUI indicated that they collect "all" (i.e. a - h of the items listed above, one collects all items listed below except item h) (personal characteristics), two additionally exclude the collection of the photo (item g)) and one additionally does not request to know the document expiration date (item f)) and one does ask for the document expiration date (item f)), but not for the data subject's address.

The EDPS considers that for the purpose of confirming a requestor's identity, normally only a **limited number of personal data** (identity document number, country of issue, first and last name, address, date and place of birth and document expiration date) needs to be visible on the copy of the identification document. In line with the data minimisation principle and with the requirements stipulated in Recitals 57 and 64 GDPR, all **other personal data** on the copy of the identification document (e.g. the photo, any personal characteristics) **can be blacked out** on the copy (but do not have to be blacked out[10]).

2.4. Inform the data subjects about this possibility

For EUI that collect only a limited number of personal data (e.g. by allowing data subjects to blacken out certain elements), we inquired whether the data subjects are informed about this possibility and, if so, how. The EEA provided a **request form for the exercise of data subject rights**, which contains respective clauses (see **Annex 5** and box below). Six EUI currently inform data subjects that they can blacken out certain parts of the copy of their identification document when they provide this for confirmation of their identity in exercising their data subject rights; two institutions have plans to do so in the future. One institution clarified that this information was sent to data subjects by email.

FRA: "*The data subject is requested to provide an identification document in order to confirm that they do not use "fake names" and they are who they say they are. This is because the agency was faced with such cases in the past, especially in relation with access to documents requests. The possibility to limit the amount of submitted personal data could be explicitly mentioned when sending the request to the data subject*."

[10] See Recital 57 GDPR: *"... the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights..."*.

EMA: "*With regard to the specific issue of blackening/redacting certain parts of the identification documents, this was specifically addressed during the EDPS inspection of EudraVigilance...*". Recommendations by the EDPS included "*Formally establish that users may black out irrelevant parts of the documentation submitted in order to gain access to the system (e.g. in the user guide)*".

At any rate, in order for data subjects to have the possibility of blackening out personal data not required to confirm their identity, they should be informed about this possibility *before* sending in their copy of the identification document.

2.5. Conclusions

It should be noted that the identification of a data subject is obviously not an issue requiring the collection of any additional data, where the data subject is actually already known to the EUI, e.g. as current or past staff member.

Where there are, however, doubts regarding the identity of the data subject wanting to exercise his/her data subject rights, in the light of future provisions of the new Regulation, all EUI that never collect a copy of an identification document will need to revise their procedures upon entry of the revised Regulation (foreseen for May 2018, i.e. coinciding with the GDPR).

- The principle of purpose limitation suggests that the personal data obtained for confirmation of the identity can only be used to verify the requestor's identity; the retention period should therefore be limited to the period required to establish the identity of the requestor.

- For the purpose of confirming a requestor's identity, normally only a **limited set of personal data** (identity document number, country of issue, first and last name, address, date and place of birth and document expiration date) needs to be visible on the copy of the identification document. All other personal data on the copy of the identification document (e.g. the photo, any personal characteristics) can be blacked out on the copy. The data subjects should be informed about this possibility before sending in their copy of an identification document.

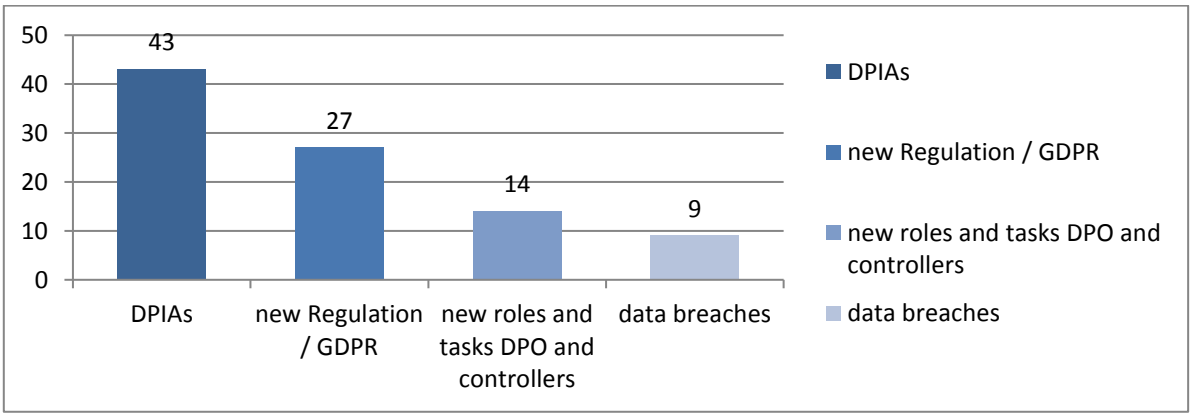
3. Future training needs

With only several months left until the new data protection framework becomes fully applicable, EUI will need to have the knowledge and resources to lead by example in their application of data protection law. The EDPS will continue to work closely with our DPO partners and provide them with more guidance on transparency, rights and obligations, to make sure that they are ready when the new rules come into force[11]. One way to do this is by supporting and providing training for EUI.

3.1 Which target audience for future EDPS training?

We asked which target audience the EDPS should focus on for our training activities: staff, DPO, both, any other or none (in case no training needs exist). All EUI identified training needs, with 46 EUI suggesting to target both DPOs and staff. 14 EUI indicated a preference for training primarily targeting DPOs; only two EUI suggested that their staff rather than their DPO should be primarily targeted by training measures. Among other potential target groups, middle, upper and top management were mentioned by five EUI, specific staff (such as IT, Human Resources team, Legal team, LISO[12], LSO[13], DPO office/assistants and Data Protection Coordinators) were also mentioned. One EUI explicitly noted that the DPO's training had been outsourced to a private company.

3.2 Topics for future training



We further asked for the top three topics institutions consider the most relevant for such training and an indication of the respective target audience. Many EUI mentioned more than three topics, with one clear frontrunner: training on **DPIAs** (nominated by no less than 43 institutions). Training on the **new Regulation and / or the GDPR** came second (27), with training on **new roles and tasks of DPOs and / or controllers** coming third (14, with eight requests for DPOs and six for controllers). Other items on the wish list also relate to topics related to the new Regulation, such as data breaches (nine) and accountability (five). Furthermore, EUI requested training on more "traditional" topics, such as IT specific training (eight), training on international transfers (six) or special categories of data (five) and "general awareness raising" (five).

[11] For existing guidance documents, please turn to the EDPS website under https://edps.europa.eu/data-protection/eu-institutions-dpo/case-law-guidance_en.
[12] Local Information Security Officer
[13] Local Security Officer

The **EP** reply split this into replies by different Directorates General, noting a wide variety of training needs as a result:
"DG PERS: ...If the notifications are abolished, we would need to have specific training to learn how to deal with the new system. A training should in this case be organized for staff, but also for HoU's and DPC's. ...
SJ: Training for data controllers, especially on accountability and the implications of it for their activities. ...
DG INLO: Training on the subject of the upcoming changes to the legislation on data protection would be very useful. It should preferably be offered to middle and senior management and be compulsory for current data controllers. ...
DG COMM: Training along with guidelines (and examples) on how to fill in the DPIA. ..."

A practical suggestion was the request to conduct training activities in Luxembourg in addition to Brussels. This ties in with previous suggestions for **delivering training in a more decentralised manner**; this includes the idea for an "Iberian" cluster (sessions targeted at all the agencies on the Iberian Peninsula) and previous grouped training sessions held in Frankfurt, possibly also grouping along thematic lines (e.g. EUI with financial sector core business).

4. International data transfers

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 EUI, and also not for transfers to most recipients in the EU.

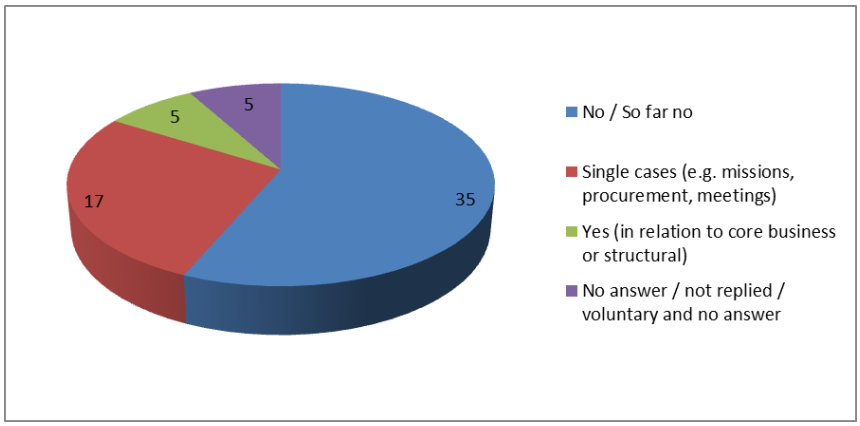
For transfers to other third parties, this can become a problem, as their data protection standards are often weaker than the EU standard. For this reason, Article 9, which regulates such transfers, is more restrictive than the rules for intra-EU transfers. This reflects the **increased risk associated with such transfers**.

The rapid development of technology, including cloud computing and mobile applications, creates new challenges, which have to be addressed to ensure that the fundamental rights of individuals are fully respected. In the course of their tasks, EUI increasingly need to transfer personal data to third countries[14] or international organisations, for reasons such as cross-border cooperation[15] and the use of transnational services.

The **2014 EDPS Position Paper** on the transfer of personal data to third countries and international organisations by EUI and bodies[16] aimed to provide technical and practical guidance to the EUI on how to interpret and apply transfer rules.

During the previous exercise (**Survey 2015**), the EDPS requested information on transfers of personal data under Article 9 of the Regulation in the years 2013 and 2014, inviting clarifications in particular on the types of transfers under Article 9 of the Regulation (for a diagram of **types of Article 9 transfers**, please consult the Survey 2015[17]), specifications on the processing activity, 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 as well as the existence of an internal monitoring and registration system of Article 9 transfers.

4.1. Transfers over the years



[14] Countries that are not members of the European Economic Area (EEA).
[15] See **EDPS Prior checking Opinions** on Fraud investigations at the EIB (2009-0459), Transmission of BFT inspection reports (2011-0615), Commission Asset freezing (2010-0426), OLAF internal and external investigations (2005-0418, 2007-0047 to 0050, 2007-72) and FRONTEX Joint Return Operations (2009-0281), available at: https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/priorchecking/OpinionsPC
[16] See https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf
[17] https://edps.europa.eu/sites/edp/files/publication/16-01-21_report_Survey_2015_en.pdf

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

For the **2015** exercise, the EDPS enquired about transfers of personal data under Article 9 in the years 2013 and/or 2014 (without differentiation as to whether these occur in relation to core business / structurally or rather in individual cases). Only **18 out of 61** EUI replied in the affirmative, leading the EDPS to conclude that "*Article 9 transfers as part of the core business activities of EUI are thus still rare*".

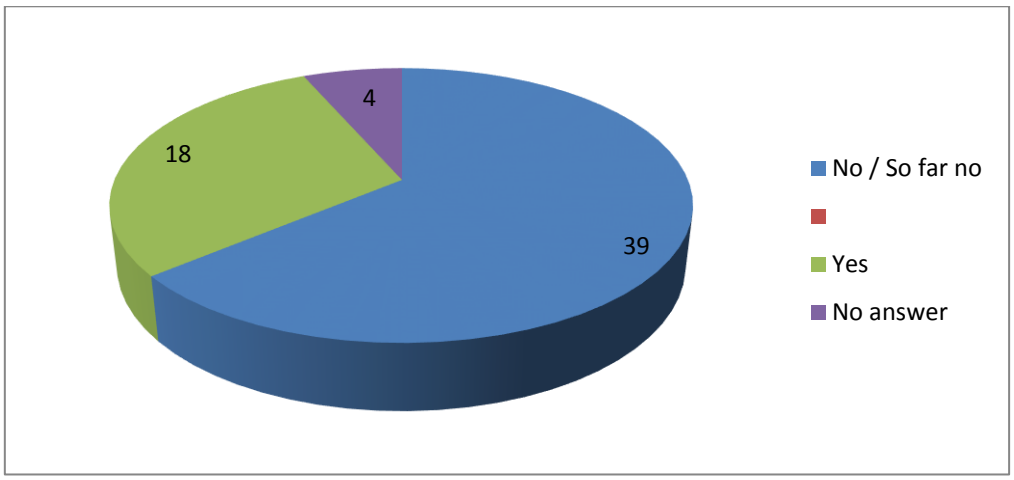


Figure 2: Overview of Article 9 transfers (2015 exercise)

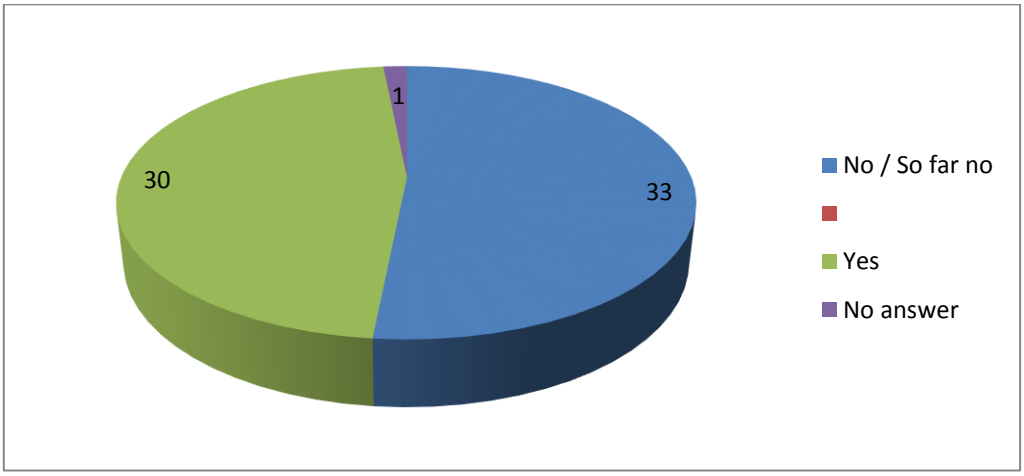


Figure 3: Overview of Article 9 transfers (2017 exercise)

During this **2017** exercise, **30 out of 64** EUI confirmed that they had carried out transfers in the period 2015 to 2016. This in turn means that a small majority still did not, but clearly indicates that **Article 9 transfers by EUI are no longer a rarity**, although not necessarily part of the respective EUI's core business.

ECDC: "*ECDC also transfers data as part of its Epidemic Intelligence Information System (EPIS). This is a web-based communication platform that allows nominated public health experts to exchange technical information to assess public health threats and their potential impact on the EU. The legal basis for these transfers is Article 9 (6) (d) on public interest grounds. ECDC has, in addition, concluded data protection agreements with those international recipients of the data who do not fall within the scope of EU data protection law. These agreements are based on the EU Commission's Standard Contractual Clauses*."

SESAR: "*It should be noted... that within the frame of projects funded by SESAR JU grant agreements there is a low number of transfers. Standard contractual clauses are applied in these cases*."

EMSA: "*The only data that EMSA would transfer, to actors outside of the EU, is related to implementation of contracts following procurement procedures when the contractor exceptionally is a non-EU based company or for travel agency service contracts. In those case would be limited data used for booking travel services for missions of the EMSA staff: transport and hotels*."

EO: "*The Ombudsman carries out international data transfers in a rather limited manner. In particular, in the context of complaint-handling, we transfer the names, email addresses and professional telephone numbers of the case handlers to complainants residing outside the EU. These transfers are necessary for the performance of the Ombudsman's tasks carried out in the public interest (Article 9, para 6 (d) of the Regulation). Communication of the data in question allows the Ombudsman to comply with the European Code of Good Administrative Behaviour and to handle complaints in a transparent and citizen-friendly manner, whether the complainant resides within or outside the EU territory*."

4.2. Existence of appropriate safeguards

Out of the 30 EUI confirming that they had carried out transfers, 23 confirmed that they have entered into appropriate safeguards (one institutions stated that such safeguards only exist partially in the form of a data protection clause in some grant agreements). As safeguards, one EUI mentioned the Privacy Shield for Twitter, others referred to a licence agreement, sealed envelopes, consent and information as well as standard contractual clauses. One EUI noted that no appropriate safeguards had been entered into "*despite having warned business owners*".

ESMA: "*With respect to international transfers of personal data, for the period covered by this Survey, ESMA performed the following transfers... With respect to transfer No 1, the country ... is subject to an adequacy decision of the EC. In case No 2 the transfer took place before Case C-362/14 (Schrems) of the Court of Justice of the European Union. Finally, with respect to case No 3, the transfer was an exceptional case implying a very small flow of personal data... which was therefore performed under the public interest derogation."*

ECHA: "*The Agency is not in a position to negotiate specific contractual clauses when purchasing a limited amount of e.g. Windows licenses or Google Android phones, nor can it realistically look for alternatives. ... There were no direct international transfers, but as explained above, ECHA is not in a position to negotiate additional safeguards with big providers over just a few licenses*."

In an Opinion published in April 2017[18] on a 360° feedback tool used by the Office for Infrastructure and Logistics in Brussels (OIB), involving a subcontractor's data center located in the **United Kingdom**, the EDPS issued a **forward-looking** recommendation, highlighting that **future transfers might come under Article 9 of the Regulation** requiring an adequate level of protection within the recipient's legal framework for transfers to third countries.

4.3. Transfers to recipients under the Privacy Shield

The Privacy Shield: State of Play and Challenges

On 12 July 2016, the European Commission adopted the Privacy Shield as a replacement scheme for the invalidated Safe Harbor decision[19]. It had stronger data protection obligations on U.S. companies

[18] See https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/360%C2%B0-tool-feedback-and-leadership_en.

[19] See http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm; see EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision (available under https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf) .

receiving EU personal data, contained U.S. commitments providing safeguards on access to data by U.S. authorities and more procedures for redress for individuals and foresees an Annual Joint Review (first: September 2017).

However there are concerns that the level of protection provided by the Privacy Shield is still inadequate. On 6 April 2017, the EP Plenary adopted a Resolution that acknowledges progress made, but warns that data subjects do not have access to legal remedies as would be required under the *Schrems* ruling[20]. Indeed, two legal challenges are currently pending with the CJEU[21]: Cases T-670/16, *DRI II*, and T-738/16, *La Quadrature du Net*.

Furthermore, there are gaps in the authorities entrusted with guaranteeing the Privacy Shield: the provisions regarding the Ombudsperson seem inadequate to guarantee her independence - and no Ombudsperson has been appointed so far; there are only two FTC Commissioners and only one member of the Privacy and Civil Liberties Oversight Board (PCLOB)[22] remains, which means that the PCLOB no longer has a quorum to adopt decisions. In addition, there are concerns what happens if foreign surveillance measures under section 702 of the Foreign Intelligence Surveillance Act are renewed.

16 EUI confirmed that they currently carry out transfers to recipients under the Privacy Shield (one indicated an intended move to standard contractual clauses), 46 explicitly denied this. Google Analytics, Survey Monkey, MailChimp, Twitter and Eventbrite were explicitly mentioned; two EUI noted the use for recruitment activities.

EIB: *"The EIB's Personnel Department had outsourced some parts of the recruitment tests like e.g. psychometric tests used to screen candidates...the company...is Privacy Shield certified. There is also an Intragroup Agreement in place between all... (of the company's) entities, which includes the EU Model contractual clauses. According to the notification, and while the data will be stored in their UK data centre (and thus be processed mainly by an EU sub-processor), access cannot be limited to only EU personnel, as some personnel from the US and India need to have access to the data in order to provide some of the maintenance services. Data are encrypted readable for those with authorized access, including the staff from the US and India."*

EO: **"***The Ombudsman also has a Twitter account, a Google+ account, a LinkedIn account, a YouTube account, and an Instagram account to communicate information about her activities. Entries containing personal data, such as, for example, names and pictures of high rank officials of EUI and bodies who meet the Ombudsman in their official capacities thus occasionally appear. The Ombudsman also re-tweets entries, both from her staff and other Twitter users, relating to public events in which she personally, or members of her staff, participate. Such entries may contain personal data. To the extent that the providers of these services are established outside the EU or may have backup service outside the EU, the uploading of information on their servers could be considered*

[20] Judgment of the Court (Grand Chamber) of 6 October 2015 (Case C-362/14)
[21] Additionally, the High Court of Ireland decided on 3 October 2017 in *Data Protection Commissioner vs Facebook and Schrems* to refer the question of the validity of the EU Standard Contractual Clauses to the CJEU.
[22] See https://pclob.gov/.

as an international data transfer. Twitter, Google and Facebook, by which Instagram was acquired in 2012, are considered to comply with the Privacy Shield principles."

COM: "*DG TRADE...: subscription to and management of newsletters for external and internal communication by DG TRADE using Mailchimp, a U.S. based newsletter emailing service, where user databases are processed on U.S. servers*."

ACER: "*For its web-services the Agency has in the reporting period used services of US based companies (Google Analytics and MailChimp). Due to privacy concerns, Agency is currently exploring different solutions, which would notably include engagement of EU based companies for the purpose of delivering these services*."

EEA: "*...the EEA website currently uses Google Analytics for the purpose of evaluating EEA website visitors' use of the website. In consultation with the DPO, the EEA is currently assessing the possibility to use an alternative solution for web-monitoring services*."

4.4. Transfers of personal data to international organisations

21 EUI carry out transfers to international organisations; 39 EUI explicitly denied this.

The organisation of meetings and conferences, training activities and Erasmus+ as well as transfers to recipients such as the UN, the African Union and the WHO were mentioned.

EACEA: "*EACEA students' mobility tool, transfer to African Union Commission (AUC) on the basis of Art. 9(6)(d) / Commission Implementing Decision of 13.11.2015 C(2015) 7705 final, Annex I according to which the AUC participates in the management and monitoring of mobility; the transfer regards names and information relating to the mobility (type and duration) of Kenyan students in the context of a monitoring visit in which the AUC participated*."

EFSA: "*EFSA maintains numerous bilateral and multilateral relations in its food safety business remit which sporadically entail the processing of personal data, mainly in the form of contact details of representatives, scientific experts and staff. In the context of these international relations, no personal data transfers happen in any structured manner*."

COM: "*EWS (Early Warning System...: Personal data may be transferred... to the WHO and 3rd country parties to the International Health Regulations*."

Annex 1: Methodology

As was the case for previous exercises, the Survey was carried out as a desk exercise, requesting information in writing from EUI. The list of questions was sent to the EUI in March 2017; reminders were first sent 18 May 2017 at working level. Replies arrived from March to mid-July 2017. In October 2017, EUI were consulted on the draft report.

EUI were asked to supply information on the following four aspects:

1. **Inventory and Register**[23]: 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[24];

2. **Collection of identification documents from data subjects exercising their data subject rights:** (1) Whether such collection takes place; (2) which retention period applies; (3) whether a full copy or only a limited data set is collected; (4) whether data subjects receive information on the possibility to only provide a limited set of data;

3. **Future training needs of EUI**: (1) Which is the preferred target audience for future training by the EDPS and (2) which are the topics the EDPS should provide training on;

4. **International data transfers:** (1) International transfers in the period 2015-2016; (2) existence of appropriate safeguards; (3) transfers to recipients under the Privacy Shield; (4) Transfers to international organizations.

For question 1, see the tables in section 1.1 and their explanations. Questions 2 to 4, which do not lend themselves easily to quantitative analysis, are analysed qualitatively in the body of this report.

[23] Unlike in exercises up to 2013, the EDPS did not request to receive copies of the actual inventory or register.
[24] Where such information is also available on a more granular basis, such as per Directorate-General of the institution or body, EUI were invited to provide such information as well.

Annex 2: Some limitations of the methodology

I. An institution 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. The numbers reported in the survey are a snapshot taken at the moment when the institution replied to the survey questionnaire. The report does not include possible improvements between the time an institution replied and the publication of the survey.

III. 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.

IV. 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.

V. 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.

VI. 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.

VII. 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.

Annex 3: Groups of EUI

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[25]:
ACER, BEREC, EASO, EBA, EIOPA, EIGE, EIT, ESMA, ESRB, EEAS, eu-LISA, CEPOL, EDA, EUISS, EUSC, BBI JU, SRB.

[25] At the time of the launch of the 2017 Survey (22 March 2017), Europol was not yet under the supervision of the EDPS (as of 1 May 2017). Europol is therefore not included in this exercise.

Annex 4: List of institutional acronyms

ACER	Agency for the Cooperation of Energy Regulators
BBI JU	Bio-based Industries Joint Undertaking
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
ESMA	European Securities and Markets Authority
ESRB	European Systemic Risk Board
ETF	European Training Foundation
EUIPO	European Union Intellectual Property Office
EUISS	European Union Institute for Security Studies
eu-LISA	European Agency for the operational management of large-scale IT systems 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
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
SRB	Single Resolution Board

Annex 5: EEA request form for the exercise of data subject rights

How to exercise your data protection rights

- If the EEA is processing your personal data and you would like to exercise your data protection rights, please send us a written request.
- You can send your request to the EEA by post in a sealed envelope or use our application form.
- Your request should contain a detailed description of the data you wish to have access to.
- You must provide a copy of an identification document to confirm your identity, for example a passport, an ID card or a driving licence. The document shall contain an identification number, country of issue, period of validity and your full name.
- Any other data contained in the copy of the identification document (e.g. photo, personal characteristics, date and place of birth, address) will not be processed and may thus be blacked out.
- Our use of the information contained in the copy of your identification document is strictly limited: the data will only be used to verify your identity.
- The document will be stored for a maximum period of three months from the date of receipt of your request.

European Environment Agency

EXERCISE OF RIGHTS OF A DATA SUBJECT UNDER REGULATION (EC) No 45/2001 APPLICATION FORM

Fields marked with an asterisk (*) are mandatory

1. Originator of the request	
Frist name (*):	
Last name (*):	

2. Rights exercised		
I would like to request:		
☐	Access to my Personal Data held by the EEA	
☐	Rectification of my Personal Data[1]	
☐	Blocking of my Personal Data[2]	
☐	Erasure of my Personal Data[3]	
☐	Object to the processing of my Personal Data[4]	

[1] Please specify the Personal data you would like the EEA to rectify.
[2] Please specify the Personal data you would like the EEA to block and on what ground.
[3] Please specify the Personal data you would like the EEA to erase and on what ground.
[4] Please specify the processing of which Personal data you are objecting to and on what ground.

3. Preferred means of access[5]			
Please send the reply and any accompanying document			
☐	By post at the following address:	Street + No	
		ZIP code + Town	
		Country	
☐	By fax at the following No:		
☐	By email at the following address:		

☐	I would like to have access to the Personal Data/information on the spot

Please send the completed form to the Data Controller identified in the Register of data processing operations or to the Data Protection Officer at Data.ProtectionOfficer@eea.europa.eu.

Alternatively, you may send your request by fax to +45 33 36 71 99 or by mail to

European Environment Agency

Data Protection Officer

Kongens Nytorv 6

1050 Copenhagen K

Denmark

Data Protection

All personal data contained in this application form shall be processed in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of their personal data by the Community Institutions and bodies and on the free movement of such data[6]. Such data will be processed solely in connection with the implementation and follow-up of the present application by the responsible services of the EEA. On written request, you may be sent your personal data and correct any information that is inaccurate or incomplete. For any question regarding the processing of your personal data, you may contact the EEA's Data Protection Officer by e-mail at Data.ProtectionOfficer@eea.europa.eu. You are entitled to have recourse at any time to the European Data Protection Supervisor (https://edps.europa.eu; EDPS@edps.europa.eu) if you consider that your rights under Regulation (EC) No 45/2001 have been infringed as a result of the processing of your personal data by the EEA.

[5] Please complete at least one of these three fields in order to enable the information requested to be sent.
[6] OJUE L 8/1 of 12.1.2001.