EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

28 April 2021

Report on the remote audit of information provided to data subjects when they sign up to newsletters and other subscriptions (case 2020-0611)

edps.europa.eu

Executive Summary

In the absence of face-to-face possibilities for outreach activities in the current COVID-19 context, European institutions, bodies and agencies (EUIs) need to connect increasingly with their stakeholders through online information activities such as newsletters. In doing so, EUIs should lead by example in providing transparent information to EU citizens.

This is why the EDPS decided to examine remotely the information provided to stakeholders when they sign up to **Newsletters and other subscriptions listed on the eu.domain** mailing list portal[1]. In conducting this remote audit, the EDPS looked at:

- Compliance with the **information** requirements under Article 15 of the Regulation[2] of the data protection statements and other information made available in the subscription process;
- Compliance with the **transparency** requirements under Articles 14, 4(1)(a) of the Regulation of the data protection statements made available in the subscription process;
- Compliance with Article 7 of the Regulation regarding the **consent** of data subjects obtained in the subscription process.

In assessing compliance, the EDPS took into account in particular the following guidance:

- EDPS Guidance Paper Articles 14-16 of the new Regulation 45/2001: Transparency rights and obligations ('Transparency GL');
- EDPB Guidelines 05/2020 on consent under Regulation 2016/679 ('Consent GL').

Section 1 of this document gives an **overview** of the elements examined, refers to specificities identified for different EUIs as **preliminary findings** and identifies some **best practices**.

In September / October 2020, the EDPS launched the audit in signing up to newsletters and other subscriptions listed on the eu. domain mailing list portal[3]. The **subscription process** was evaluated using a checklist containing all pieces of information required under Article 15 (see Annex 2). **Interim findings** were then shared (November and December 2020) with the EUIs concerned to avoid any misunderstandings or technical hick-ups. As a next step, the EDPS unsubscribed from newsletters and other subscriptions (December 2020 + January 2021), thus testing whether **withdrawing consent** is indeed as easy as giving it.

Section 2 of this document provides an **update** on the current situation, which has developed very positively in the meantime, as **the majority of EUIs proactively took interim measures** to further align.

As explicitly noted in the announcement letter, Section 1 outlining the findings of this remote audit takes into account the state of play on the date of remote evidence collection.

[1] See https://europa.eu/newsroom/subscription-services_en, see Annex 1.

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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, OJ L 295/39 of 21.11.2018.

[3] See https://europa.eu/newsroom/subscription-services_en, see Annex 1. For one EUI, no subscription took place, as a subscription would have required two-factor authentication (app to be installed on mobile phone).

However, Section 2 reports on these **proactive measures improving compliance**, which will of course also be taken into account in the context of the individual follow-up to this audit.

Contents

Section 1: Overview of elements examined

In signing up for newsletters and other subscriptions, data subjects provide their own personal data (name, email address etc.) and consent to their use.

- **Article 15** contains a list of pieces of information that must be provided where personal data are collected from the data subject;
- **Articles 14 and 4(1)(a)** define transparency requirements for the data protection statements made available in the subscription process (see Annex 2);
- **Articles 7 and 8** define what the controller needs to do to obtain valid consent in this context (see Annex 3).

This section follows the structure of these Articles and outlines the main findings.

1. "At the time when personal data are obtained", Article 15(1)

Under this heading, the EDPS looked into whether a data protection statement is made available upon clicking on the subscription link contained in Annex 1 as well as the ease of identifying and accessing it.

No, generic or outdated data protection notice

Under Article 15(1), the controller shall provide the data subject with all of the information listed at the time when personal data are obtained.

- Regrettably, four EUI had no data protection statement in place at the respective date of remote evidence collection.
- Several other EUIs had a generic data protection notice in place, but not one specifically informing about the processing at hand.
- One EUI's data protection notice referred to the **"old" Regulation (EC) 45/2001**, i.e. a data protection framework applicable to EUIs only until December 2018: "The processing of data related to your newsletter subscription is held in accordance with the provisions of Regulation (EC) No 45/2001…".

Somebody else's data protection statement

Two EUIs refer data subjects to the data protection statement of their contractor, rather than their own (e.g. "e-Subscription via the website: For the registration and management of subscriptions to its newsletter, (EUI) relies on (a US-based service provider). More information is available in the relevant section of the (EUI) website", which includes a **link to a 20 page Privacy Statement of a US contractor**).

Data protection notice and record merged in the same document

One EUI argued that the record and the data protection statement can be merged in the same document serving "a double function of an easy to understand information notice (as per Article 15 EDPR) and a comprehensive record (as per Article 31 EDPR)". The EUI argued that "the requirements of both legal articles are quasi identical", which enables one document to serve both purposes."

However, whilst the part of the record that needs to be made publicly available under Article 31(5) of the Regulation might indeed be very similar in content to the data protection statement of the processing operation at stake, it **does not necessarily encompass all**

pieces of information required for a record. E.g. parts of the compliance check and risk screening[4] will remain internal, i.e. they will be part of the record, but not be made public and not be part of the data protection statement.

In addition, the record and the data protection statement serve **different purposes**:

- Records (whether based on reused texts or not) will go to a central register under Article 31(5) of the Regulation, serving the purpose of transparency vis-à-vis the general public (see also Article 15(1) TFEU), helping to strengthen public trust and making knowledge sharing between EUIs easier[5];

- Data protection statements aim at informing individual data subjects concerned by a specific processing operation. This implies e.g. that they must be transparent, clear and concise, i.e. targeted vis-à-vis the data subjects concerned. This can be quite different from the (usually more elaborate) information that needs to be contained in a record, e.g. when a particular processing operation aims at children.

The record and the data protection statement should therefore not be merged in the same document.

"Hidden" data protection statements

As stated in Recital 20 and noted in the Transparency GL, the principle of transparency requires that any communication relating to the processing of personal data be easily accessible. The respective rule of thumb is **"The less clicks needed to get there, the better!"**

For two EUIs, the number of clicks required exceeds three. Two EUIs use a link located **at the very bottom of the screen** leading to a data protection statement.

Several EUIs (e.g. ECHA) refer data subjects to a **generic webpage on data protection** instead of a specific data protection statement ("For (EUI's) personal data protection policy and more information on personal data protection, the User shall refer to (EUI's) webpage on personal data protection: (link)").

2. Identity and contact details of the controller, Article 15(1)(a)

The majority of EUIs correctly stated that the respective EUI is the controller and which specific unit is responsible for the processing (along the lines of "The EUI is data controller and the processing is managed by Unit XYZ").

Two EUIs (JRC, EUIPO) seemingly **struggled to identify who is responsible** for the processing. One noted that "The Head of Unit, acting as Controller, manages the processing itself, under the responsibility of his/her Director who acts as Processor". Another one stated that "The processing of personal data is carried out under the responsibility of X. However, X acts as processor when the use of Tool Y is requested by other Departments/Services of

[4] See EDPS Accountability Guidance Part I, pp 16-18 for further details.
[5] EDPS Accountability Guidance Part I, p. 8.

the EUI. In this situation, the requesting department/service will act as controller." It seems unlikely that the latter information helps the data subject to identify the entity responsible for dealing with e.g. data subject requests.

Several EUIs gave **no contact details**, one referred data subjects to their DPO ("...you can contact the ERCEA Data Protection Officer for any questions or complaints. Please choose "data protection" as the category for which you would like to ask a question in the contact form").

3. Contact details of the data protection officer, Article 15(1)(b)

All but one EUIs provided contact details of their DPO (e.g. "You may contact the Data Protection Officer (DPO) of EUI (DataProtectionOfficer@eui.europa.eu) with regard to issues related to the processing of your personal data under Regulation 2018/1725."). One EUI noted the possibility to "contact the EUISS Data Protection Officer via the online contact form if there are any difficulties or questions regarding the processing", but provided no link or email address to do so.

4. Purposes of the processing for which the personal data are intended, Article 15(1)(c)

Most EUIs had no problems in clearly describing why they collect personal data of subscribers to their newsletters, e.g.:

- "Purpose of processing: The data is held for the purpose of sending the monthly (EUI) newsletter, and occasionally, a survey to obtain feedback on the (EUI)'s performance in relation to the Annual Management Plan and the Multi-annual Strategic Programme."
- "The purpose of processing these data is to have the necessary information to deliver the (EUI) Electronic Newsletter and to identify very generic information of the readers to better focus on the content of our newsletter."

Some EUIs, however, **struggled to specify what the purpose of processing is**. Unsurprisingly, this often coincides with the **absence of a specific data protection statement** (see above section 1). In not providing any or staying very generic in their purpose description, these EUIs fail to explain adequately to data subjects why their personal data is being processed.

> Example: "An e-service on the (EUI) website aims to improve the communication between the website user and (EUI). For each e-service, a controller determines the purposes and means of the personal data handling, if any, and ensures the conformity with Regulation (EU) 2018/1725. For the specific information on how your data is handled by (EUI) in relation to a particular e-service, please refer to the relevant section of our website. In relation to each e-service, the following information will be provided: ... What information is collected, for what purpose and through which technical means: (EUI) collects personal information only to the extent necessary to fulfil a specific purpose. The information will not be re-used for a different purpose".

5. Legal basis for the processing, Article 15(1)(c)

No legal basis mentioned

Three EUIs did not mention any legal basis for the processing operation.

Not a "task carried out in the public interest", Article 5(1)(a), ...

A number of EUIs note **Article 5(1)(a)** as legal basis for processing newsletter subscriptions instead of consent. One EUI refers to its Founding Regulation, which stipulates that "The (EUI) shall communicate on its own initiative in the fields within its mission...".

Four more EUIs opted for a hybrid model of relying on **both, Article 5(1) (a) *and* (d)** (e.g. "Personal data shall only be processed for the performance of tasks carried out in the public interest on the basis of EU law or in the legitimate exercise of official authority vested in the Agency. Alternatively, processing is lawful if it forms part of a legal or contractual obligation or when the individual concerned has given their unambiguous consent."). One EUI additionally refers to Recital 22 of the Regulation stipulating that "Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies".

However, Article 5(1)(a) provides for processing of personal data ***necessary*** for the fulfilment of an EUI's tasks. Although reaching out to stakeholders by means of a newsletter is a very useful communication activity and as such **part of many EUIs' business, but not all** actually publish newsletters (whilst still fulfilling all of their tasks). Also, in the light of **existing alternatives** for outreach activities, publishing a newsletter can thus not be considered *necessary* for the fulfilment of EUIs' tasks in the sense of Article 5(1)(a).

...but consent, Article 5(1)(d)!

All other EUIs correctly referred to consent in the sense of Article 5(1)(d) as legal basis (e.g. "Data subjects unambiguously give their consent to the processing of the personal data when filling the online subscription form.").

6. Recipients or categories of recipients of the personal data, Article 15(1)(d)

Internal recipients

Most EUIs only refer to **internal recipients**, roughly along the following lines:

- "Members of the (EUI) Information and Communication sector have access to these email addresses on a need-to-know basis."
- "Do we share your data with other organisations? Personal data is processed by the Agency only. In case that we need to share your data with third parties, you will be notified to whom your personal data has been shared with."

External recipients: The good, the bad and the ugly...

A number of EUIs somewhat cryptically refer to "an external entity assisting the (EUI)", an "external provider" or "the employees of the contractor" or note that "Following the creation of a user account, email address and email notification content will be shared with email dispatch providers for email notifications" without further clarifications.
Three EUIs explicitly refer to US-based external providers:

- "(the US-based provider) may transfer and process Customer Data to and in the United States and anywhere else in the world where (the US-based provider), its Affiliates or its Sub-processors maintain data processing operations."
- "Following consent by the user, appropriate data will be shared with Google Analytics services."

Obviously, **external providers and contractors** could be regarded as a category of recipients, but in such it could be considered more reassuring for data subjects to phrase the explanation regarding recipients as follows:

- "Who can see your data? During this process, your personal data can be accessed by:
  1. The selected (EUI) staff of the relevant units;
  2. The authorised staff of the (EUI) web **contractors based in EU countries** that are compliant with the EU Data Protection Regulation."
- "The (EUI) uses (an external provider). All personal data of this processing is stored on the **servers located on the territory of the EU**."

7. Intention to transfer personal data to a third country, Article 15(1)(e)

Where applicable, data subjects need to be told about the controller's intention to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 48, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Many EUIs **clearly state that no such intention exists**:

- "The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.").
- "7. Do we share your data with other organisations?
  Personal data is processed by the Agency only. In case that we need to share your data with third parties, you will be notified to whom your personal data has been shared with.
  8. Do we intend to transfer your personal data to Third Countries/International Organizations?
  No."

A number of EUIs transfer personal data to third countries and clearly communicate this.

- "(The US-based provider) may transfer and process Customer Data to and in the United States and anywhere else in the world where (the US-based provider), its Affiliates or its Sub-processors maintain data processing operations".

Regrettably, only some refer to the existence (albeit not to the nature) of safeguards applicable to such transfers:

- "In the framework of the external relations cooperation and tasks, provision of contacts to third parties, including third countries or international organisations, could be foreseen. Appropriate safeguards are to be ensured in case of the transfer. The given information will not be communicated to third parties, except where necessary for the purposes outlined above."

One EUI leaves the information and explanation to their US-based contractor's data protection statement (available after several clicks on the EUI's website):

- "Email campaigns sent from our platform may include a web beacon that allows us to determine, on behalf of our customers, if you open an email, as well as the email delivery status and your geographic location. Email campaigns may also contain other tracking technology that allows us to determine what you click on in an email and if you unsubscribe or change your subscription preferences. This web beacon and other tracking technologies also allow us to collect log data, including your IP address, browser type and version. We share information about email delivery, email opens, email clicks, and subscription preferences, as well as aggregated information about browser types, with our customers so they can optimize their campaigns, customize offerings to you, understand your level of engagement with them and any other uses the customer describes in its online privacy policy."
  "We offer our customers certain features that allow them to better target who they contact through our products and services. In order to do this, we partner with third parties who can provide our customers with information about you."
  "We may share your information with third parties who develop certain features and functionality that integrate with our products, provided that such sharing is authorized by our customers. This allows us to make certain features of our services available to Constant Contact customers. We impose obligations on our third party service providers to ensure they use data in a manner consistent with our use and consistent with applicable privacy laws.
  We are located in, and store and process your information in, the United States, although we may use third party service providers anywhere in the world. When we transfer your information to third party service providers, we do so in compliance with applicable privacy laws.
  We may update the information on this page at any time, so please review it frequently..."

8. Retention period, Article 15(2)

The data subjects must receive information about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

Several EUIs do not stop there, but have incorporated an **update mechanism ensuring continuous data quality**:

- "Furthermore, in order to keep data accurate regarding e-mail addresses and mobile numbers of subscribers, the GSC regularly seeks to update these contact details. If you do not react to an invitation to update or rectify your contact details, your subscription will be cancelled."
- "Contact information is kept until the user decides to unsubscribe from the CRM system. However, user accounts are deleted after a defined period of 6 months inactivity (e.g. no subscriptions, no opening of e-mails)"; "...in April each year an email is sent to all database users allowing them to amend and review their information preferences. It also provides users with the possibility to unsubscribe from CRM-related services such as newsletters, thus to delete their accounts."

- "An automated process ensures that 12 months after the registration, the user has to confirm the subscription or they will be removed from the system."

One EUI does not conduct regular updates, but **reacts to invalid email addresses:** "The email addresses on the list will be kept as long as the newsletter is issued. Specific emails will be removed upon receiving an automated message stating that the email address is not functioning any longer, or if the person asks to have his or her data removed from or changed in the database."

A number of EUIs, however, have **no clearly defined retention period** in place. Instead, they refer to

- A **potentially unlimited period of time:**
  - "Your personal data is kept as long as (EUI) continues to work in support of (core business of EUI)";
  - "The (EUI) only keeps the data for the time necessary to fulfil the purpose of collection or further processing."
  - "The EUI only keeps the data for the time necessary to fulfil the purpose of collection or further processing. Some statistical data may be kept, with the appropriate safeguards in place, for a longer period in order to analyse the use of the website."

- Only the **possibility to unsubscribe**:
  - "Data is kept until the person either requests deletion from the database by contacting the (EUI) team at the aforementioned e-mail address or unsubscribes from all (EUI) mailings by clicking on the "Unsubscribe" link in one of the mailings."
  - "The data will be kept as long as the subscription to the newsletter remains active."
  - "Once included in a newsletter distribution list, you remain on this list until you ask to be removed from it. Removal from any newsletter distribution list or from an (EUI) database can always be requested at any time by email."

9. The existence of data subject rights, Article 15(2)

Data subjects need to be informed about the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability.

The majority of EUIs manage to inform appropriately, for example:

- "You have the right to access your personal data and to rectify any inaccurate or incomplete data. In order to exercise your rights, please direct your query to the (EUI) team's e-mail: team-EUI@EUI.europa.eu. The query will be dealt with within fifteen (15) working days."

- "You have the right of access to your personal data and to relevant information concerning how we use it. You have the right to rectify your personal data. Under

certain conditions, you have the right to ask that we delete your personal data or restrict its use. You have the right to object to our processing of your personal data, on grounds relating to your particular situation, at any time. We will consider your request, take a decision and communicate it to you. You can send your request to the EDPS by post in a sealed envelope or use our contact form on the EDPS website (see section on contact details below)."

However, two EUIs rely on the **20 page data protection statement of their US-based contractor** to inform data subjects of their rights, which **contains no respective information** and reads as follows: "Certain data protection laws (like those in Europe) make the distinction between those who act as 'controllers' and those who act as 'processors' of personal information. Put simply, a controller is the organization who determines how and why your personal information are to be used for certain purposes. A processor is an organization who acts as a service provider and only processes personal information on behalf of the controller under their instruction. The reason we point this out is because for many of our services, our Members are the controller and we are simply acting as their processor. For instance, if you signed up to receive a newsletter from one of our Members, that Member may ask us to help them send out their newsletters by using our services. In that case, the Member is the controller of your personal information and (US-based contractor) is merely a processor."

10. The right to withdraw consent, Article 15(2)

Where the processing is based on consent, data subjects needs to be told about the right to withdraw this consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

For two EUIs there is **no reference to this right at all**. Although the right to withdraw consent exists *at any time*, one EUI in the wording used made it look as if such right was time limited and conditional upon receipt of a newsletter: "Each time you receive a newsletter..., you have the right to unsubscribe from the newsletter".

Most EUIs correctly inform data subjects in this respect, e.g.:

- "You have consented to provide your personal data to (EUI unit) for the present processing operation. You can withdraw your consent at any time by notifying the Data Controller. The withdrawal will not affect the lawfulness of the processing carried out before you withdrew consent."

- Doc 3, point 7: "You can also edit/request deletion of your data from our database at any time by sending an e-mail to the aforementioned e-mail address. You can further unsubscribe from receiving specific or all content from the (EUI) at any time by clicking on the "Unsubscribe" link, which appears at the bottom of each mailing. If you opt out of all (EUI) content, your data will be deleted."

11. The right to lodge a complaint with the EDPS, Article 15(2)

All EUIs mentioned the right to lodge a complaint with the EDPS, some in combination with the possibility to address issues to the EUI's DPO (e.g. "For questions or complaints

concerning the processing of your personal data, you can turn to the Agency's Data Protection Officer. Alternatively you can also have recourse to the European Data Protection Supervisor."). Ideally, this information should be combined with e.g. a functional email address to facilitate making contact.

12. Whether the provision of personal data is mandatory, Article 15(2)

The legal basis for the processing operation at hand is consent (see above section 5), which means that the provision of personal data will not be a statutory or contractual requirement and no data subject is obliged to provide the personal data. However, one EUI remains somewhat unclear regarding a possible obligation of the data subject: "Personal data shall only be processed for the performance of tasks carried out in the public interest on the basis of EU law or in the legitimate exercise of official authority vested in the Agency. Alternatively, processing is lawful if it forms part of a legal or contractual obligation or when the individual concerned has given their unambiguous consent."

13. Existence of automated decision-making, Article 15(2)

Data subjects should be informed of the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. One EUI explicitly clarified that this is not the case: "Your personal data will *not* be used for automated decision-making including profiling."

14. Further processing, Article 15(3)

Under Article 15(3), where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller must provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

- Those EUIs which failed to mention or clearly define the initially pursued purpose (see above section 4) obviously also fail to distinguish properly between the initial and any possible further purpose. This will leave data subjects guessing what their personal data are used for.

- One EUI, which had been transparent on its intention to transfer personal data to a third country, remained unclear in what the purpose of further processing might be: "(US-based provider) may transfer and **process Customer Data to and in the United States and anywhere else in the world** where (US-based provider), its Affiliates or its Sub-processors maintain data processing operations."

- For one EUI, the confirmation email data subjects receive after following the subscription process cryptically referred to '**marketing permissions**'.

15. Ability to demonstrate consent, Article 7(1)

The controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

The EDPS invited EUIs to provide proof of the consent given by the audit team leader when subscribing[6]. This was only conducted for EUIs

- for which the subscription process had been successfully concluded (and once a news item had actually been received);
- which rely on consent as legal basis (see above section 5).

Several EUIs store proof of consent in the form of **timestamps** (e.g. "Subscription consent is stored as part of the database including a timestamp of when (date/time) the subscription took place").

16. Written declaration which also concerns other matters, Article 7(2)

If the data subject's consent is given in the context of a written declaration, which also concerns other matters, the request for consent shall be presented in a manner, which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Two EUIs refer data subjects to the data protection statement of their contractor, rather than their own, which consists of **a 20 page Privacy Statement of a US contractor**. In those two cases, the actual scope of the consent given by the data subject remains vague.

17. Withdrawal of consent, Article 7(3)

Prior to giving consent, the data subject shall be informed of the possibility to withdraw consent (see above section 10) and it must be as easy to withdraw as to give consent.

For the vast majority of EUIs, unsubscribing was indeed as easy as subscribing, if not easier. Most EUIs provide a possibility to unsubscribe either by clicking on a link in each publication or through the portal initially used to subscribe. Some EUIs require some additional identification to ensure that only the data subject who has initially subscribed resigns. One EUI requires the sending of a separate email. Some EUIs give individuals unsubscribing the **possibility to give feedback and/or send a 'remorse' email** "We have removed your email address from our list. We're sorry to see you go. Was this a mistake? Did you forward one of our emails to a friend, and they clicked the unsubscribe link not realizing they were in fact unsubscribing you from this list? If this was a mistake, you can re-subscribe at: (link)").

For one EUI, though, no possibility to unsubscribe or otherwise withdraw the consent exists, as all **personal data submitted when subscribing is kept for 12 months** (period after which the personal data is automatically deleted, see above section 8).

In one instance, unsubscribing failed ("Error - Key/User not found, please contact the Administrator of this website").

[6] This was only conducted for EUIs for which the subscription process had been successfully concluded (i.e. a news item had actually been received).

18. Consent by children, Article 8(2)

The controller must make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

None of the EUIs covered by this inspection **specifically targets children** with their newsletters and other subscriptions and for most, the steps involved in subscribing would seem complex enough to exclude children subscribing without adult supervision. Four EUIs have particularly involved subscription processes, involving e.g. a verification of whether a human is subscribing, the request to send confirmatory emails or two-factor authentication.

Section 2: Current state of play

As explicitly noted in the announcement letter, the findings of this remote audit (outlined in Section 1) take into account the state of play on the date of remote evidence collection. However, this Section reports on some of these **proactive measures improving compliance**, which are most welcome and have, of course, been taken into account in the context of the individual follow-up to this audit.

The majority of EUIs (15 out of 27) proactively took interim measures to achieve better compliance - **even before receiving any audit recommendations**.

- Not less than **ten data protection notices were created or (partially) revised** to take into account initial findings.
    - "Since your inquiry, the (EUI) has updated the data protection notice, the record of processing activity and uploaded both on the website. The Newsletter sign-up page has been updated and now includes a link to the data privacy statement."
    - "The (EUI) communication team in cooperation with (the DPO) have rectified this issue, and a Specific Privacy Notice regarding the rights of data subjects has been published in the disclaimer section."
    - "In addition a direct link to the DPN is being created under the Legal Notice page. Please find herewith attached the draft text of the DPN for your information."
    - "References to old Regulation 45/2001 … have been replaced with references to new Regulation 2018/1725".

- **Accessibility** has been improved in several cases (e.g. "In addition the IT colleagues are working to bring the notice and link closer to the tick box so that it is much more visible when someone is about to tick the box.").

The **best performing EUIs** had no reason to amend anything, as there have been no or only minor audit findings which by their nature would not have required any audit recommendations.

ANNEX 1

See https://europa.eu/newsroom/subscription-services_en[7]:

1) Council of the EU and European Council: E-mail and SMS distribution list
2) European Commission
    a) Press corner (email notifications)
    b) Brexit updates
3) Joint Research Centre: JRC Newsletter
4) European External Action Service – Newsletters and alerts
5) European Committee of the Regions – eNewsletter
6) European Economic and Social Committee - Press Mailing List
7) European Data Protection Supervisor - EDPS Newsletter
8) Publications Office of the European Union - Newsletter
9) European Agency for Safety and Health at Work (OSHA) - newsletter
10) European Aviation Safety Agency (EASA) - newsletter
11) European Banking Authority (EBA) - Email alerts
12) European Centre for the Development of Vocational Training (Cedefop) - newsletter
13) European Chemicals Agency (ECHA) - newsletter
14) European Food Safety Authority (EFSA) - newsletters
15) European Foundation for the Improvement of Living and Working Conditions (EUROFOUND) - news
16) European Institute of Innovation and Technology (EIT) - newsletter
17) European Joint Undertaking for ITER and the Development of Fusion Energy (Fusion for Energy) - F4E News
18) European Maritime Safety Agency (EMSA) - newsletter
19) European Medicines Agency (EMA) - human medicines highlights
20) European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) - Drugnet Europe
21) European Police Office (EUROPOL) - press release subscription
22) European Research Council Executive Agency (ERC Executive Agency) - newsletter
23) European Union Agency for Railways (ERA) - newsletter
24) European Union Institute for Security Studies (EUISS) - newsletter
25) Fundamental Rights Agency (FRA) - newsletter
26) European Union Intellectual Property Office (EUIPO) - newsletter
27) The European Union's Judicial Cooperation Unit (EUROJUST) - newsletter

[7] To avoid an imbalanced focus on the activities of the European Commission, all DG-specific publications for the European Commission were excluded.

ANNEX 2

Checklist Article 15

EUI, date

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

Article 15(1)	Finding(s)	OK?
at the time when personal data are obtained		
(a) the identity and the contact details of the controller;		
(b) the contact details of the data protection officer;		
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;		
(d) the recipients or categories of recipients of the personal data, if any;		
(e) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 48, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.		

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing[8]:

[8] Transparency GL, para 41: "Items listed in Article 15(1) of the Proposal are mandatory, except where the data subject already has them. The items under Article 15(2) of the Proposal should be included where they are necessary for the fairness and transparency of the processing."

Article 15(2)	Finding(s)	OK?
at the time when personal data are obtained		
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;		
(b)the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;		
(c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;		
(d) the right to lodge a complaint with the European Data Protection Supervisor;		
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;		
(f) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.		

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

ANNEX 3

Checklist consent

EUI, date

Article 7(1)	**Findings** (Section 2)b) DIP)	**OK?**
the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.		

Article 7(2)	**Findings**	**OK?**
If the data subject's consent is given in the context of a written declaration which also concerns other matters,	**Y / N**	
the request for consent shall be presented in a manner which is clearly distinguishable from the other matters,		
in an intelligible and easily accessible form,		
using clear and plain language.		

Article 7(3)	**Findings**	**OK?**
Prior to giving consent, the data subject shall be informed thereof.	See Annex 2	
It shall be as easy to withdraw as to give consent.		

Article 8(2)	**Findings**	**OK?**
The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.		