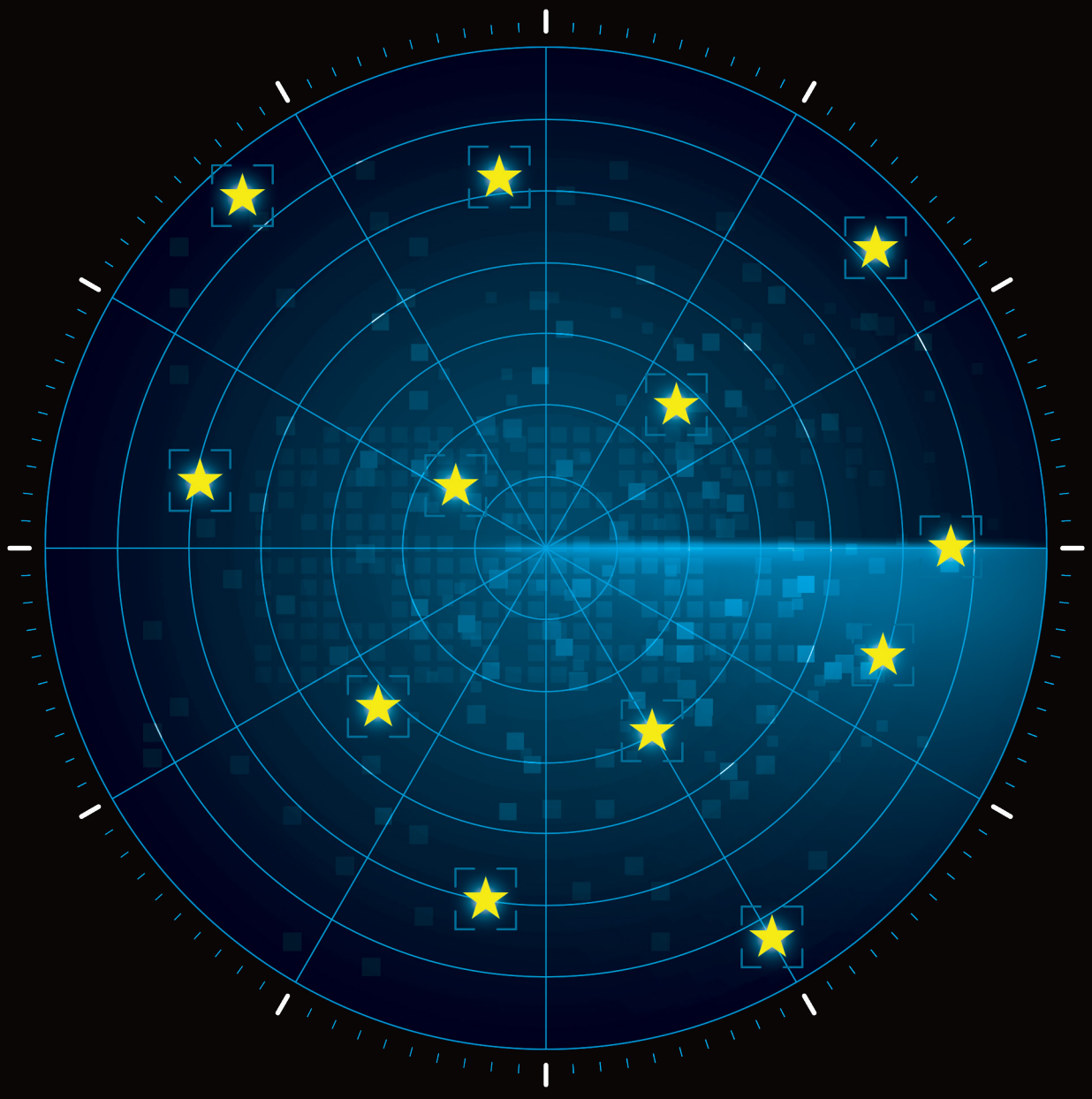
Deloitte.



Processing of personal data by European Institutions

Introducing more accountability with Regulation (EU) 2018/1725

February 2019

Introduction

Regulation (EU) 2018/1725[1] (the Regulation) is the new Data Protection Regulation applicable to the EU Institutions (EUIs). It was published in the Official Journal of the EU on 21 November 2018. The Regulation came into force on 11 December 2018 and replaced the Regulation (EC) 45/2001.

By adopting this regulation, the ambition of the EU legislator is to bring the data handling rules and practices of the EUIs in line with the General Data Protection Regulation (GDPR), which is applicable to data controllers and processors other than EUIs. According to the European Data Protection Supervisor (EDPS), one of the emphases of the Regulation 2018/1725 is on the **accountability principle**, requiring EUIs to demonstrate their compliance with the data protection rules[2].

Some of the **novelties** brought by regulation 2018/1725 are:

- New **obligations** and **responsibilities** for the controllers (EUIs)
- New principle of **accountability** for the controllers
- New obligation to **notify personal data breaches** to the EDPS
- New **investigative** and **corrective** powers of the EDPS

1. 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 (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1725&from=EN.
2. EDPS (2018), "EDPS welcomes agreement on new data protection rules for the EU institutions and bodies", Press Release. 23 May 2018. Available at: https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-welcomes-agreement-new-data-protection-rules_en.

What is new?

Modified definition of the controller

The Regulation defines "controller" as the union institution, body, the Directorate-General (DG) or any other EU organizational entity, which alone or jointly determines the purposes and means of the processing of personal data[3]. Additionally, the Regulation refers to "*controllers other than union institutions and bodies*" within the meaning of "controller" under the GDPR[4].

Furthermore, in case of "joint controllers" there could be one or multiple controllers of the EUIs together with one or multiple controllers other than EUIs (e.g. a private company). However, such wording may increase the complexity in respect to how responsibilities are shared between the EUIs where they act as controllers and other legal persons, which are processing jointly personal data.

In most cases, examples of controllers, joint-controllers, processors and data subjects can include:

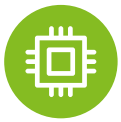
Figure 1 - Who can be a controller, processor or data subject

(Joint-)Controllers

- EU institutions, bodies, offices and agencies
- DGs, Directorates, Units, etc.
- Other EU organizations

Controllers other than EUIs

- External service providers
- International organizations
- National public authorities



Processors

- External service providers
- Suppliers
- Cloud providers
- National public authorities

Data Subjects
(Staff and external)

- Members of EC, EP, etc.
- Experts
- Trainees
- Employees
- Visitors
- Etc.

3. Article 3 (8) of the Regulation (EU) 2018/1725.
4. Article 4 (7) of the GDPR and Art. 3 (9) of the Regulation (EU) 2018/1725.

Enhanced principle of accountability

The Regulation sets out the accountability principle under which the controller must be responsible for the processing operations and must **be able to demonstrate compliance** with the data protection rules and principles[5]. It is not sufficient to describe only the privacy rules in a policy, procedure, guideline, etc.

The EUIs as data controllers are the entities responsible for ensuring compliance with the accountability principle. However, in practice the **top management is accountable** for ensuring compliance with the data protection rules while the responsibility is usually assigned to a different level such as Heads of Unit or Heads of Department, which could be the "person responsible acting on behalf of the controller"[11].

Figure 2 - Actions to be taken to ensure the adherence to the accountability principle include:

01 **Generate records** for all the processing operations and have them regularly reviewed[6]

02 **Implement** in the new and existing processing operations the **data protection by design** and **by default** principles[7]

03 Implement appropriate **technical** and **organizational measures** to ensure that the processing operation is done in accordance with the principles of the Regulation[8]

04 Demonstrate compliance with the general principles

05 Perform a **compliance check** in respect to Art. 4 and 5[9]

06 Carry out a **Data Protection Impact Assessment** where the processing operation is likely to result in a high risk to the rights and freedoms of natural persons[10]

Records of data processing activities

Under Art. 25 of The regulation 45/2001, the person responsible for the processing operation on behalf of the controller had to submit a prior notification to the Data Protection Officer (DPO) for any processing operation. Similarly, according to The regulation 2018/1725, the same responsible person will have to document all the ongoing and upcoming personal data processing activities by generating records in line with Art. 31 by including the following elements:

Furthermore, the records of processing activities will have to be maintained by each EUI internally and should be organized in a **central registry**[12].

Figure 3 - Key elements of the central registry

01 Who is in charge of the processing operation (i.e. who is the **controller**)

02 The **purpose** of the processing

03 The **categories of persons** whose data are processed

04 The **types of personal data** processed

05 Who are the **recipients** of the data

06 Whether there are any **transfers** of personal data to third countries or international organizations;

07 The **retention period** for the personal data processed

08 The **technical and organizational security measures** are in place

5. Article 4 (2) of the Regulation (EU) 2018/1725.
6. Article 31 of the Regulation (EU) 2018/1725.
7. Article 27 of the Regulation (EU) 2018/1725.
8. Article 26 (1) of the Regulation (EU) 2018/1725.
9. EDPS (2018), "Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies Summary", July 2018. Available at https://edps.europa.eu/sites/edp/files/publication/18-07-05-intro_summary_brochure-v.1.1_en_0.pdf.
10. Article 39 of the Regulation (EU) 2018/1725.
11. EDPS (2018), "Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments", Toolkit. February 2018. Available at: https://edps.europa.eu/sites/edp/files/publication/18-07-05-accountability_on_the_ground_part_i_records_and_threshold_assessment-v.1.1_en_0.pdf
12. Article 31 of the Regulation (EU) 2018/1725.

Compliance and risk check

According to the EDPS, when **documenting** the processing operations by **generating** the above-mentioned records, the EUIs should also check whether the processing operations **comply** with the data protection rules. By doing so, the EUIs will be expected to be able to **demonstrate** the "substantive compliance" with the rules and principles set up in the Regulation[13].

The EUIs should check **two** main aspects (in sequence):

- Whether the processing operation is done **lawfully** in line with Art. 5
- Whether the EUIs **comply** with the **data protection principles**

Data Protection Impact Assessment (DPIA)

The Regulation introduces a new obligation for the EUIs, to perform DPIAs. A DPIA is an analysis of the risks that the processing operations may introduce to the data subjects[14]. Accordingly, the EUIs shall not conduct the DPIA for all processing operations, but only for those that:

- Are on the **list of risky processing activities** to be issued by the EDPS under Art. 39 (4)
- Are likely to pose a high risk to the rights and freedoms of the data subjects according to the **threshold assessment** done by the EUIs[15]

If the processing operation that is planned by a EUI is not on the list mentioned above, and the person responsible on behalf of the controller considers that there could be a **high risk**, the EUIs should conduct and document a **threshold assessment**.

The Regulation sets out a non-exhaustive list of **cases** when planned processing may result in a high risk[16]. Notably, a systematic and extensive evaluation of personal aspects such as automated processing of personal data, including profiling (e.g. evaluating personal aspects related to the data subject's economic situation, personal preferences, health, behavior, location, etc.) will require performing a DPIA. On the other hand, simple processing operations, such as the maintenance of a list of subscriptions to a newsletter, should not be subject to the obligation to conduct a DPIA. The high level steps of a DPIA can be summarized as visible on the next page.

13. EDPS (2018), "Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments", Toolkit. February 2018. Available at: https://edps.europa.eu/sites/edp/files/publication/18-07-05-accountability_on_the_ground_part_i_records_and_threshold_assessment-v.1.1_en_0.pdf.
14. Article 39 of the Regulation (EU) 2018/1725.
15. EDPS (2018), "Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments", Toolkit. February 2018. Available at: https://edps.europa.eu/sites/edp/files/publication/18-07-05-accountability_on_the_ground_part_i_records_and_threshold_assessment-v.1.1_en_0.pdf.
16. Article 39 of the Regulation (EU) 2018/1725.
17. Article 45 of the Regulation (EU) 2018/1725.

"DPIA helps Institutions to comply with the requirements of data protection by design."

EDPS

Figure 4 - High level steps to perform a Data Protection Impact Assessment (DPIA)

Step 01 — Understand if DPIA is needed

- Check if high risk processing activities are listed
- **Threshold** assessment methodology

Step 02 — Perform DPIA

- Describe context of processing activity
- Assessment of **fundamental principles** (necessity, proportionality)
- **Risk analysis** (including risk treatment)
- **Evaluation** and **Validation** of the DPIA (sign-off)

Step 03 — Consult EDPS if necessary

- Assess whether a **prior consultation** is required
- Request for prior consultation

"EUIs need to notify the EDPS in case a personal data breach is likely to result in a risk to the data subject."

Function of the Data Protection Officer

According to Art. 45 of the Regulation, the Data Protection Officer (DPO) plays an important role in **assisting the controller** to reach compliance with data protection rules. Thus, the DPO has **to inform** and **advise** the controller or the person responsible on behalf of the controller, of their obligations and **monitor compliance** with applicable data protection. The DPO must also **provide recommendations** with regards to data breach notifications, the outcome of DPIAs and the relevant consultations of the EDPS[17].

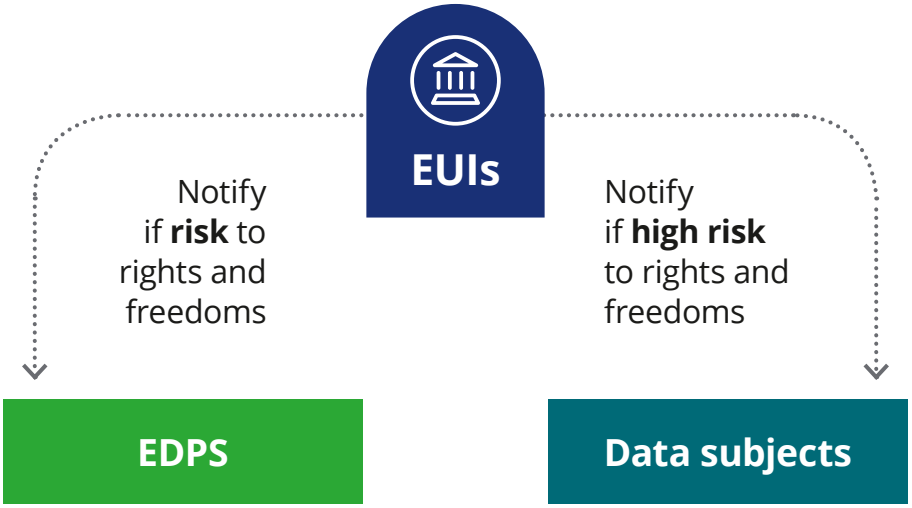
New powers of the EDPS

The European Data Protection Supervisor (EDPS) is the data protection authority for the EUIs. One of its core tasks is to supervise the EUIs to help them to process personal data. By monitoring the processing operations of the EUIs, the EDPS ensures that the rules for processing personal data are respected and applied[18].

Furthermore, Art. 58 of the Regulation grants the EDPS powers similar to those of national supervisory authorities under Art. 57 of the GDPR in terms of monitoring and enforcement of the application of the Regulation. There are four types of powers: **investigative**, **corrective**, **authorization** and **advisory**[19]. Moreover, the EDPS can receive at **any time** complaints from the data subjects whose rights have been infringed by any EUI when processing personal information.

Data Breach Notifications

Under regulation 45/2001 there was no specific obligation for the EUIs to notify any 3rd party in case of a data breach. However, the Regulation 2018/1725 introduces an obligation for EUIs to **notify the EDPS** in case a personal data breach is likely to result in **a risk** to the data subject[20]. Furthermore, the EUIs have the same obligation to **notify the data subjects**, where the data breach is likely to result in a high risk to the data subject[21].



18. EDPS, Press Release "EDPS welcomes agreement on new data protection rules for the EU institutions and bodies" (23 May 2018), accessible at https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2018-05-revised_reg_45_en.pdf.
19. Article 58 of the Regulation (EU) 2018/1725.
20. Article 34 of the Regulation (EU) 2018/1725.
21. Article 35 of the Regulation (EU) 2018/1725.

How and to whom will administrative fines be imposed?

In accordance with the Art. 66 of the Regulation, the EDPS is empowered to impose administrative fines on the EUIs as a sanction of a last resort , and only when the EUIs fail to comply with the Regulation (e.g. non-compliance with the order of the EDPS to communicate data breach to the data subject). Fines under Art. 66 are lower than those provided under Art. 83(4) to (6) of the GDPR. This can be explained by the fact that unlike the GDPR, the Regulation does not target operators pursuing lucrative activities.

There are two levels of administrative fines set by the Regulation. The lower level of fines, which are up to 25 000 EUR per infringement and up to a total of 250 000 EUR per year, and a second level which can go up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year that will be **imposed for the infringement of the obligations within the Regulation**.

"Unlike the GDPR, the Regulation (EU) 2018/1725 does not target operators pursuing lucrative activities."

How to get ready?

Next steps for the person responsible on behalf of the controller

- Implement in the new and existing processing operations the principle of **privacy by design** and **by default**
- Use the privacy notifications based on Art. 25 under the Regulation 45/2001 as a basis for **generating new records** for all processing operations that involve personal data
- **Upload information items in the new records** such as names and contact details of the controller, the purpose of the processing, a description of the categories of data subjects and which type of personal data will be processed, the categories of persons who will have access to the information, if applicable transfers to 3rd parties, 3rd countries or international organizations, the retention period and a description of the security measures adopted
- Check if the processing operation complies with the data protection rules by doing a compliance check when generating the new records (i.e. two main questions should be asked at this step: if the processing operation is done lawfully and if the processing operation complies with the data protection rules)
- Check together with the IT team or the DPO if the EUI concerned has a proper **information security risk management process** in place and which are the controls to mitigate any risk that might appear during and after the processing operation
- Check if the processing operations are likely to result into a "high risk to the rights and freedom of data subjects"; if the answer is "YES", the person responsible should prepare the DPIA assisted and guided by the DPO of that EUI
- Check if the **privacy statements** are up to date and are written in a clear and plain language.

Next steps for the DPO:

- **Monitor compliance** with applicable regulation (EU) 2018/1725 and any other applicable EU Law in respect to data protection
- **Provide feedback** on the draft records and any other draft documentation
- Keep the **central register** of the new records similar to the "inventory" of all processing operations that was kept according to the Art. 25 under the Regulation (EC) 45/2001
- Ensure that **some parts of the records are publicly accessible**
- Guide and assist the person responsiblele on behalf of the controller in preparing the DPIA

“Accountability means that the controller is in charge of ensuring compliance and being able to demonstrate that compliance.“

EDPS

Contacts

Roland Bastin
Partner - Risk Advisory
+352 451 452 213
rbastin@deloitte.lu

Charles Delancray
Director - Technology & Enterprise Application
+352 451 452 618
cdelancray@deloitte.lu

Georges Wantz
Director - Technology & Enterprise Application
+352 451 454 363
gwantz@deloitte.lu

Alexander Cespedes
Senior Manager - Cyber Risk for EU Institutions
+352 451 454 234
alcespedesarkush@deloitte.lu

Nastassia Salash
Analyst - Cyber Risk for EU Institutions
+352 451 453 395
nsalash@deloitte.lu

Deloitte.

Designed and produced by MarCom at Deloitte Luxembourg.

Deloitte Luxembourg
Grand Duchy of
Luxembourg

Tel.: +352 451 451
www.deloitte.lu