Deloitte.

Deloitte's view on the implementation of Regulation (EU) 2018/1725

the 'GDPR for European Union Institutions'

Introduction

On 23 May 2018, only two days before the entry into force of all General Data Protection Regulation[1] (GDPR) provisions, representatives from the European Parliament and the Council also agreed on a Regulation on the processing of personal data by EU Institutions, agencies and bodies (EUIs)[2]. On 11 December 2018, Regulation (EU) 2018/1725[3] also referred to as the 'GDPR for EUIs', came into force and therefore applies to all EU institutions and bodies in their processing of personal data and is practically replacing Regulation (EC) 45/2001[4].

The Regulation is to be considered the 'public sector counterpart'[5] of the GDPR, with the latter applying to all companies and organisations that process personal data within the EU and that operate in the private sector. Key roles like data controller and processor are also defined in the Regulation, similar with the GDPR case.

The objective of the new rules is to offer EU citizens the same rights as they enjoy under the GDPR when interacting with EUIs.

Novelties introduced by Regulation (EU) 2018/1725

The reinforced principle of accountability and demonstrating compliance

Just as the GDPR for the private sector, Regulation (EU) 2018/1725 leaves little room for interpretation: its content and applicability come down to creating a culture of accountability[6], as the controller shall be able to demonstrate compliance with the Regulation and shall be responsible for it. To this end, the controller shall implement appropriate technical and organisational measures.

Records of processing activities

As for the GDPR, the European Data Protection Supervisor[7] (EDPS) states that, in light of the principle of accountability, the focus should be put not only on complying with the new rules, but also on being able to demonstrate compliance'[8].

EUIs must ensure an adequate documentation of their personal data processing activities. Furthermore, the records of processing activities should be kept in a central register, which should be made publicly accessible. This obligation, laid down in article 31 of the Regulation, is the successor of the prior notification mechanism to the Data Protection Officer (DPO) ex article 25 of Regulation (EC) 45/2001. EUIs may of course re-use all the relevant information from this prior notification mechanism[9].

The risk mindset

Regulation (EU) 2018/1725 emphasises the risk mindset[10], a key change compared to Regulation (EC) 45/2001. Indeed, it affirms the necessity to always keep in mind what processing does to data subjects, i.e. how that particular processing affects them. The controller shall take into account the nature, scope, context and purpose of the processing, as well as the risks the processing activities create to the rights and freedoms of natural persons.

Data breaches and the obligation to notify the EDPS

Regulation (EU) 2018/1725 brings the new obligation to notify personal data breaches to the EDPS. Article 34 of the Regulation defines that a EUI shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the EDPS, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons[11].

A personal data breach should be interpreted broadly as 'every breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'[12].

Key suggestions for EU Institutions

Records of processing activities: the first indispensable step

The starting point and the key success factor for compliance is the creation and maintenance of adequate records of processing activities[13]. These are the foundations of data protection documentation and one of the first elements the EDPS will assess in order to evaluate EUIs' compliance[14]. The EDPS strongly recommends that EUIs keep a central register of records that is to be kept by the DPO[15] who is the most appropriate person to consult when drawing up the registers.

The EDPS also provides a helping hand by issuing guidance on documenting processing operations for EUIs[16].

Performance of compliance and risk checks

While drawing up the records of processing activities, the EUIs also have the opportunity to perform a substantive compliance and risk check. This comes down to (1) assessing the legality of the processing and (2) assessing compliance with the data protection principles. The most time- and cost-efficient way to perform these checks is by including them in the record-generation phase, as this implies cash on the barrel and reducing the chance of surprises afterwards. All the more so since this could trigger a first indication for the need to perform a Data Protection Impact Assessment (DPIA). The compliance check and the risk screening should enable EUIs to gain insights on the legal basis and the necessity of the processing, on the principles of purpose limitation, data minimization, accuracy, storage limitation, transparency and on the data subject rights[17]. As this list already indicates, it is by not cutting corners that EUIs will be able to reap the benefits from those efforts at every later stage in the compliance story.

Embrace privacy by design and by default

Once the processing activities are mapped and the EUIs have a clear view on those activities, another step is to assess the extent to which privacy by design and by default principles have already been taken into account in the (lifecycle of the) processing activities. To fresh up memories and in another attempt to demystify the concepts, the EDPS clearly defines privacy by design as 'the principle that controllers have to consider data protection both during the development and deployment' and privacy by default as 'the principle that the default settings of products and services should be privacy-protective'[18].

Update privacy statements

As the private sector has extensively done (in the GDPR context), creating and updating privacy statements should be a mandatory action for all EUIs. From a positive perspective, updating privacy statements is an excellent way to (re)assess significant aspects of personal data processing, as the Regulation prescribes the controller to provide transparent information, communication and modalities for the exercise of the rights of data subjects[19]. Adhering to those provisions, EUIs take an important step towards compliance, and importantly, towards demonstrating that compliance.

When a privacy statement is not present or not up to date, this creates reputation and non-compliance risks and is easy to spot by both data subjects and by the EDPS. In this matter, privacy statements really function as a first line of defence and their absence can effortlessly reveal a (non-compliant privacy) fortress that is easy to take in. It is important to stress that a privacy statement should be available for all natural persons whose personal data is processed by EUIs, both EUI staff and external data subjects. In practice, think not only about the members of the European Commission, the European Parliament, Agencies, etc., but also about trainees, visitors, employees, experts and contractors.

When updating or drafting privacy statements, a lot of information from the records of processing activities may be used as a basis. At this stage, the importance of properly-generated records of processing activities will be clearer than ever.

Conduct DPIAs

Processing operations that are likely to pose a high risk to the rights and freedoms of data subjects are subject to performing a DPIA[20]. In practice, this means EUIs will have to perform a DPIA when (1) the processing is listed on an EDPS established public list of processing operations[21] or (2) the processing is likely to result in high risks according to EUIs' threshold assessment. For more information on the necessity and methodology to conduct a DPIA, EUIs can consult the EDPS *Accountability on the ground* toolkit (Part I and Part II)[22].

Who is responsible for ensuring compliance with these new rules?

The EDPS warns that, although in practice top management is accountable for compliance with Regulation (EU) 2018/1725, responsibility is usually assumed at the level of the 'controller in practice', being the business owner[23]. This reasoning is justified by the EDPS, as the business owner usually is the 'main driver', assisted by the DPO and Data Protection Coordinators (DPCs), where appointed[24]. For example, while top management is accountable for generating records of processing activities and performing DPIAs, it is the responsibility of the business owner to generate the records and to verify if a DPIA needs to be conducted. The DPO can clearly assist, but it is the job of every business owner to get the work done.

The key to success here is proactivity, alignment and collaboration. For a better understanding of roles and responsibilities, the EDPS has published a RACI matrix, serving as an example of the different roles involved when generating records of processing activities[25].

	Responsible	Accountable	Consulted	Informed
Top management		X		
Business Owner	X			
DPO			X	
IT Department			X	
Processors, where relevant			X	

RACI matrix records/documentation process. Source: EDPS Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, p.4, https://edps.europa.eu/sites/edp/files/publication/18-12-13_accountability_on_the_ground_part_i-_records_and_threshold_assessment_v.1.2_en.pdf.

Act as a team

While the controller/business owner is responsible for drafting the records, answering compliance check questions and verifying whether a DPIA needs to be performed, it is the task of the DPO to keep those records, to provide feedback on them and on other documentation, to reply to questions from controllers/business owners and to provide liaison between EUIs and the EDPS. Other functions, such as the IT or legal unit/department may support controllers/business owners as needed[26].

Conclusion

Thanks to the Regulation (EU) 2018/1725, the EUIs set a very high standard with regard to data protection. This enables EUIs to lead by example and take proactive steps and actions in order to adopt the necessary measures aimed to ensure a secure overall environment for the processing of personal data.

Endnotes

1 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). See Link

2 The Regulation defines the controller as follows: 'The Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law'.

3 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. See Link

4 REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December2000 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. See Link

5 Or, as stated by the EDPS, 'the EU institutions' equivalent to the GDPR'. See: European Data Protection Supervisor Annual Report 2018. See Link

6 Article 4.2. of Regulation (EU) 2018/1725 states that the controller shall be responsible for, and be able to demonstrate compliance with the principles relating to processing of personal data, such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality.

7 The European Data Protection Supervisor or EDPS is the Data Protection Authority for the EUIs. See Link

8 European Data Protection Supervisor Annual Report 2018, p. 12 See Link

9 To provide a helping hand, the EDPS has published a table with similarities and differences between the old and the new Regulation. For more information, see: European Data Protection Supervisor, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, p. 23. In what follows, we refer to the document as 'EDPS, Accountability on the ground Part I'. See Link

10 The risk mindset means taking into account the risks caused by the processing operations and this principle is established in article 26 and recital 38 of Regulation (EU) 2018/1725.

11 For more information and guidance on personal data breach notification to the EDPS, please consult the EDPS guidelines of 7 December 2018 on personal data breach notification for the European Union Institutions and Bodies. See Link

12 Article 3(16) of Regulation (EU) 2018/1725.

13 Article 31 of Regulation (EU) 2018/1725 establishes the requirement to maintain records of processing activities, containing a set of mandatory information to provide. All processing activities must be included, going from a EUI's newsletter, to staff selection, to the core business tasks, to administrative obligations that come with them as well as disciplinary measures involving processing of personal data.

14 The EDPS mentions this in a straightforward way: 'Failure to keep records may result in an administrative fine against your EUI. When the EDPS checks how your EUI complies with its data protection obligations, you can be sure that we will have a look at your records.' See EDPS, Accountability on the ground Part I, p. 12.

15 EDPS, Accountability on the ground Part I, p. 7.

16 Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies. The first version of the toolkit was published in February 2018 and an updated version was provided in December 2018. See Link

17 For more information, see: EDPS, Accountability on the ground Part I, p.16-18.

18 See: EDPS, Accountability on the ground Part I, p. 29. The principles are set out in article 27 of Regulation (EU) 2018/1725. For more information on privacy by design, see: EDPS Opinion 5/2018 Preliminary Opinion on privacy by design, 31 May 2018. See Link

19 See: article 14 to article 16 of Regulation (EU) 2018/1725.

20 Article 39 of Regulation (EU) 2018/1725.

21 At the time of writing, the list is not established yet. However, the EDPS already provides a non-exhaustive list with examples that can guide EUIs during an interim period. See: EDPS, Accountability on the ground Part I, p. 23-24.

22 To be consulted via the following link: See Link
While Part I provides guidelines on how to generate records and registers and when to perform DPIAs, Part II focuses on actually conducting DPIAs and on how to proceed to prior consultation to the EDPS.

23 EDPS, Accountability on the ground Part I, p. 4.

24 Ibid.

25 Ibid.

26 EDPS, Accountability on the ground Part I, Annex 1: 'Who does what?', p. 13

Contacts

Dan Cimpean
Partner – Cyber Risk Services
for European Institutions
+32 2 800 24 37
dcimpean@deloitte.com

Erik Luysterborg
Partner – EMEA Privacy and Data
Protection Leader
+32 2 800 23 36
eluysterborg@deloitte.com

Georgia Skouma
Director – Information Protection
and Privacy
+32 2 800 24 93
gskouma@deloitte.com

Karim Moueddene
Global Lead Client Service Partner
for European Institutions
+ 32 2 600 61 91
kmoueddene@deloitte.com

Deloitte.

56718