Getting the picture right: 12 common misconceptions about GDPR[i]

CHIOMENTI CUATRECASAS GIDE Gleiss Lutz Stibbe

Table of Contents

1. Does the GDPR apply to any organization controlling or processing data of an EU resident?

Although the territorial scope of application of the GDPR is defined rather broadly, it does not apply to any organization controlling or processing data of an EU resident. In fact, Article 3 of the GDPR lays down several criteria or connecting factors for its application.

Firstly, if a controller or a processor has an establishment in the EU whose activities include the processing of personal data, then the GDPR applies to that controller or processor. This is irrespective of whether the actual data processing takes place in the EU or not.

Secondly, if the controller or processor is not established in the EU but processes personal data of data subjects who are in the EU (i.e., also data subjects who are non-EU residents but find themselves in the EU), then the GDPR applies to that controller or processor if it offers goods or services to those data subjects in the EU, whether in return for payment or not, or if it monitors data subjects' behaviour taking place within the EU.

Thirdly, the GDPR also applies to personal data processing by a controller who is not established in the EU but in a place where Member State law applies by virtue of public international law, such as in a Member State's diplomatic mission or consular post outside the EU.

2. Will all companies be required to appoint a data protection officer?

It is a common misunderstanding that all companies will be required by the GDPR to appoint a Data Protection Officer ("DPO").

The designation of a DPO is only mandatory and thus only truly required for entities that act as a data controller or data processor in the three specific cases which have been described: (i) if the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (ii) if the core activities (i.e., the primary activities or key operations that are necessary for achieving the goals of the controller or processor) consist of processing operations that require regular and systematic large-

scale monitoring of data subjects, e.g., businesses that engage in profiling or tracking of online behaviour; or (iii) if the core activities consist of processing on a large scale the so-called "sensitive" categories of personal data, such as health data, biometric data, data revealing ethnic origin or religious beliefs, and information relating to criminal convictions. Additionally, Member State law may require the mandatory appointment of a DPO in other situations as well, as is already the case for Germany for example.

In other cases than those referred to above, the voluntary appointment of a DPO is merely recommended, thus not mandatory. Moreover, if an organization designates a DPO voluntarily, the requirements under the GDPR will fully apply to his or her designation, position, and tasks as if the designation were mandatory. This needs to be considered when deciding to appoint a DPO voluntarily.

3. Will organizations be required to undertake Privacy Impact Assessments when conducting any kind of personal data processing?

Privacy Impact Assessments or Data Protection Impact Assessments ("DPIA") are only required in the exceptional situation in which the processing is likely to result in a high risk to the rights and freedoms of natural persons. Whether the processing entails such a high risk will depend on the presence of one or more of the following factors: automated decision-making, evaluation or scoring, systematic monitoring, sensitive data, scale of processing, vulnerable data subjects, data transfers outside the EU, etc. In particular, a DPIA will be required if the processing entails: (i) any systematic and extensive evaluation of personal aspects of natural persons based on automated processing or profiling upon which decisions are based; (ii) processing of so-called "sensitive" categories of personal data on a large scale; or (iii) a systematic monitoring of a publicly accessible area on a large scale. National supervisory authorities are moreover required to establish a list of the types of processing operations that require a DPIA, which is what Belgium has already done, for example.

Conversely, a DPIA is not required if the processing is not likely to result in a high risk. Moreover, other scenarios in which a DPIA is not required are (i) if a DPIA has already been carried out for very similar processing activities or (ii) if the processing has a legal basis under EU law or Member State law and a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis. National supervisory authorities may also draw up a list of the kinds of processing operations for which no DPIA is required.

Furthermore, the Article 29 Working Party has clarified in the meantime that DPIAs are only required for processing operations that have been initiated after the GPDR applies effectively on 25 May 2018 or that change significantly after that date. In addition, it is recommended, thus not mandatory, to also carry out DPIAs for processing operations already underway prior to May 2018 if there is a change to the risk represented by the processing operation or if the organizational or societal context of the processing activity has changed.

4. Will entities be required to report any serious contraventions of the GDPR to the regulators and to data subjects affected?

According to Article 33.1 of the GDPR reporting those contraventions will not be required in all cases, but only if the breach in question implies a risk to the rights and freedoms of the individuals whose data have been affected by the contravention.

The Article 29 Working Party has clarified that there is a "risk to the rights and freedoms" if the breach can lead to physical, material, or non-material damage to the individuals whose data have been breached. Any such risk should appear to be related to a third party's non-authorized access to the individual's information, leading to the violation of that individual's rights to privacy or any other relevant right (e.g., economic loss derived from the use of a credit card number of an individual whose data have been unduly accessed). When evaluating this risk, one should do so on the basis of an objective assessment while taking into account criteria such as the type of breach, the nature, sensitivity, and volume of personal data concerned, the ease of identification, the severity of consequences for individuals, etc.

Hence, according to this approach, incidents that have no consequences on the rights and freedoms of individuals (e.g., loss of information, without any third party having accessed to such data) should not be reported under the GDPR.

5. How freely given, specific, informed and unambiguous must the consent be under the GDPR?

The GDPR qualifies the data subject's consent as consent that is freely given, specific, informed, and unambiguous. These requirements are substantial elements of a valid consent under the GDPR, which is necessary for the related personal data processing to

be lawful. An effective and actual consent to personal data processing by the data subject is, in fact, a core principle of the GDPR.

In light of the above, it is worth clarifying that consent is considered:

a) freely given if the data subject is *(i)* actually aware of the elements based on which they give their consent to the data processing; *(ii)* not conditioned by external circumstantial influences; and *(iii)* aware of his or her right to withdraw the consent at any time;
b) specific if the data subject explicitly gives his or her consent to each separate data processing activity envisaged by the data controller;
c) informed if the data subject – before giving his or her consent – is informed through an intelligible and easily accessible form about the data processing activities envisaged by the data controller; and
d) unambiguous if there is an objective certainty both regarding the actual existence of the data subject's consent and the contents of that consent, meaning that the consent must be given through a clear, affirmative act of the data subject (*i.e.,* an *ex silentio* consent is not a clear, affirmative act, hence not acceptable).

6. How should valid consent be proven?

Article 7 of the GDPR reads: "*the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data*". However, the GDPR does not contain specific, compulsory provisions in relation to the conditions for proving how the consent was given or obtained.

In that respect, the GDPR is inconsistent with the provisions of certain previous national legislations implementing Directive 95/46/EC (such as, *e.g.*, the Italian Legislative Decree no. 196 of June 30, 2003, whereby the data subject's consent could be deemed to be effective only if it is "*documented in writing*").

As a consequence, data controllers have the right to demonstrate how the valid consent was obtained by using any means allowed under their legal systems. In that respect, the use of any means for keeping a record of the data subjects' consent – such as, for example, written statements, also statements stored by electronic means, or tick boxes to be set on internet websites specifically addressing the consent to be sought for the envisaged data processing activities – could be recommended.

7. Will data controllers be required to maintain records of processing activities in all cases?

The GDPR requires each controller to keep a record of processing activities under its responsibility, and each processor to keep a record of the processing activities that it has carried out on behalf of a controller. However, these obligations do not apply if the controller or the processor is an enterprise or an organization employing fewer than 250 persons, unless the processing it carries out:

- is likely to result in a risk to the rights and freedoms of data subjects and is not occasional, or

- includes sensitive data, i.e., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9 of the GDPR), or data relating to criminal convictions and offences (Article 10 of the GDPR).

The rationale for these exceptions is that small and medium-sized enterprises and organizations that do not carry out risky processing should be exempt from the requirement to keep a record of its processing activities.

8. How are controllers and processors required to demonstrate its compliance with the GDPR and to whom?

Data controllers are required to demonstrate to the supervisory independent public authorities of the EU Member States that they comply with the GDPR. These authorities have investigative powers to verify the lawfulness of the data processing activities performed.

Such verifications are relevant because data controllers and processors are responsible ("*principle of accountability*") for implementing – both at the time the means used for processing are determined and at the time of the processing itself – appropriate technical and organizational measures to ensure an effective level of protection of the processed personal data (known as "*data protection by design and by default*").

The GDPR indicates various modalities that data controllers or processors can put in place for the purpose of demonstrating that their data processing is lawfully carried out. These include:

a) implementation of internal data protection policies;
b) adoption of codes of conduct approved by associations and other bodies representing categories of controllers or processors;
c) obtainment of data-protection certifications by certification bodies accredited by the supervisory independent public authorities of EU Member States;
d) compliance with guidelines issued by the European Data Protection Board; and/or
e) compliance with specific indications given by a data protection officer.

9. Will periodic data protection audits be mandatory under the GDPR?

Under Article 32.1.d of the GDPR, data controllers and data processors must implement appropriate technical and organizational measures to ensure a level of security that is appropriate for the risk and, among those measures, they must regularly test and evaluate the effectiveness of the measures adopted for ensuring security of files.

Having said this, the GDPR does not lay down specific procedures or a specific format for those review and evaluation tasks. Consequently, unless binding national regulations set forth otherwise, data controllers and data processors are not required to conduct a specific type of mandatory audit – as defined in national regulations adopted under Directive 95/46. On the contrary, the general rule would be that the data controller or processor has the discretion to define the procedures for review and evaluation, provided that those procedures ensure complete verification and assessment of risks connected with the security of files.

This approach will differ if the data controller or processor has voluntarily adhered to a given code of conduct (which could define detailed procedures for testing and reviewing purposes) or if they are bound by national regulations that, being aligned with the GDPR anyway, impose specifically defined (and mandatory) audit procedures.

10. Will processors have to fulfil the same compliance obligations, meet the same legal requirements, and have the same sanctions for not complying with the GDPR as controllers do?

Under the GDPR, processors must adhere to more compliance obligations and legal requirements compared to the current regulatory framework, but not to the same extent as that which are required of the controllers.

For example, processors will have to implement appropriate technical and organizational measures to ensure a level of security that is appropriate to the risk, designate a data protection officer, satisfy the conditions of transfers of personal data to a recipient in a third country or an international organization under very similar conditions to the ones that apply to controllers.

Processors will have to keep records of their processing activities, but the information to be included in such records differs from the records to be kept by the controller.

Privacy impact assessments or notification of personal data breaches will remain the main responsibility of the controller, even though the processor will have to assist in complying with obligations pertaining to such assessments and data breaches.

Sanctions for violations of the GDPR are the same for both controllers and processors, but the application thereof will of course depend on the circumstances of each individual case, including the degree of responsibility of the controller or processor for the violation at stake.

11. Will administrative fines for violation of the GDPR increase compared to the fines imposed by current national regimes?

The maximum level of administrative fines will effectively increase compared to the fines imposed by current national regimes. The GDPR sets two categories of administrative fines.

Some violations, including violations concerning aspects such as privacy by design and privacy by default, records processing activities, security, personal data breach notifications, data protection impact assessments, the designation of a data protection officer etc., are subject to administrative fines up to EUR 10 million or up to 2% of the total worldwide annual turnover of the preceding financial year of the undertaking, whichever is higher.

Other violations, including violations concerning the basic principles for lawful processing, the conditions for valid consent, data subjects' rights, transfers of data outside the EU, etc., are subject to administrative fines up to EUR 20 million or up to 4% of the total worldwide annual turnover of the preceding financial year of the undertaking.

Nevertheless, the GDPR puts forward as a key principle that each supervisory authority must ensure that the administrative fines in each case must be effective, proportionate, and dissuasive with respect to the violation. When deciding whether to impose an administrative fine and on the amount thereof, regard should be given to the specific circumstances of the violation, including the nature, gravity, and duration of the infringement, the intentional or negligent character, the degree of responsibility, any previous infringements, the financial benefits gained, etc.

12. Will GDPR guidelines from national authorities be binding?

Doubts exist as to the binding effects of guidelines issued by the different national authorities that further elaborate the different aspects of the GDPR. This could lead to potentially contradictory instructions for multinational corporate groups that have subsidiaries in different Member States where the corresponding data protection authorities could have issued differing guidelines on the application of a same provision of the GDPR.

In that respect, the interpretation adopted by a national authority on specific provisions of the GDPR will only be binding for those companies (or groups of companies) whose

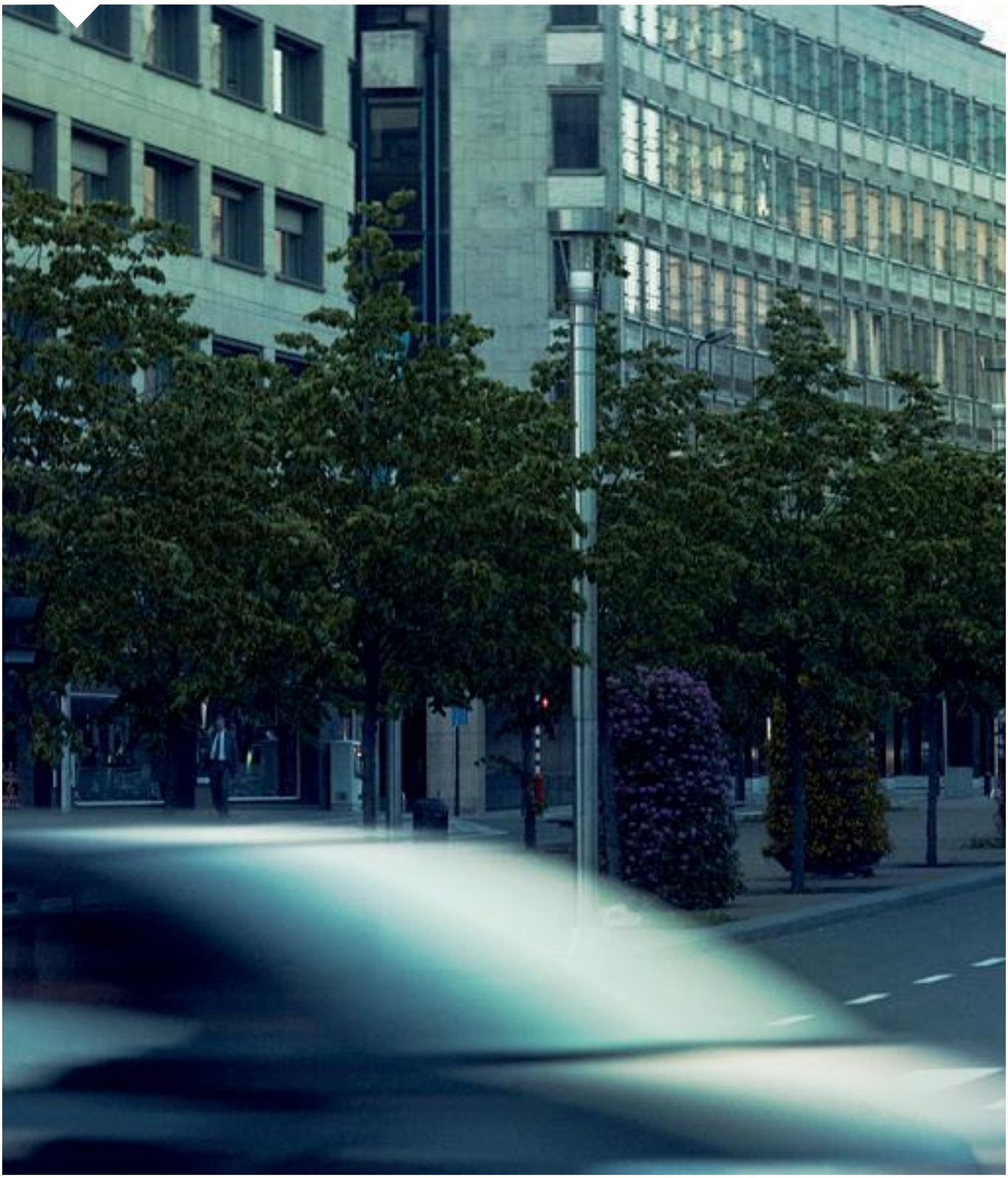
"main establishment" (i.e., the place where decisions on data processing are taken in the European Union) is located in the territory of the country in question.

In any event, and as a general rule under the GDPR, the European Data Protection Committee holds an ultimate power to interpret any provision on a number of subject matters listed in Article 70 (including, for example, those related to profiling, notification of security breaches, international data transfers, or sanctions).

Contact

Erik Valgaeren
Partner
T +32 2 533 53 43
M +32 477 50 62 92
erik.valgaeren@stibbe.com

CHIOMENTI CUATRECASAS GIDE Gleiss Lutz Stibbe



CHIOMENTI CUATRECASAS GIDE LOYRETTE NOUEL Gleiss Lutz Stibbe

[i] This contribution is produced thanks to the cooperation between Chiomenti, Cuatrecasas, GIDE, Gleiss Lutz, and Stibbe. This contribution is no legal advice and should not be relied upon as such. Existing guidance from regulatory authorities at the time of writing this contribution has been taken into account, but such guidance might continue to evolve.