Strategic Perspectives

Wolters Kluwer

May 17, 2018

FAQ: "The Best Of" GDPR Questions

By Cynthia J. Cole and Neil Coulson, Baker Botts L.L.P.*

In preparation for the upcoming deadline of the EU's General Data Protection Regulation (GDPR), Baker Botts' special counsel Cynthia J. Cole and partner Neil Coulson, in collaboration with Wolters Kluwer, presented a webinar on GDPR for US companies on April 10, 2018, entitled "A Global Paradigm Shift? General Data Protection Regulation."

"While we packed as much information as we could into the one-hour webinar, we were unable to meet the amount of questions at that time," said Ms. Cole. "The quantity of responses received after the webinar was a telling reaction to the impending GDPR deadline."

Preparation for GDPR does not end on May 25, 2018, and the legal and contractual landscape will continue to evolve well past May. Ms. Cole and Mr. Coulson have therefore selected various follow-up questions and provided responses.

"GDPR compliance and implementation will shift based on individual fact patterns and events," said Mr. Coulson. "We hope that this FAQ provides you a little more insight."

Recap:

- WHAT IS GDPR?

GDPR is the European Union's new General Data Protection Regulation. It comes into force on May 25, 2018. It introduces a stricter compliance regime for personal data privacy across the European Union and aims to harmonize data privacy laws across each country of the European Union. It applies directly in the United Kingdom until the United Kingdom leaves the European Union, following which we expect the United Kingdom to adopt GDPR into its national law.

- WHAT INFORMATION DOES IT COVER?

GDPR defines personal data broadly. It covers any information that can identify a living individual. This includes obvious identifiers such as a name, address, or email address. But it also extends to, for example, an IP address. Sensitive personal data is a further protected subcategory. It covers data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation. There are stricter processing rules for sensitive person data and you must obtain explicit consent from the data subject.

---

* Cynthia J. Cole is Special Counsel in the Palo Alto office of Baker Botts L.L.P. Neil Coulson is a partner in the London office of Baker Botts L.L.P.

- WHY IS IT RELEVANT IN THE UNITED STATES?

GDPR applies to all businesses with an establishment in the European Union that process (widely defined to cover any act, including **deletion**) personal data. It impacts United States' businesses who have subsidiaries or parents that are established in the European Union and who transfer personal data to, and store personal data in, the United States. GDPR has extra-territorial effect. It covers all businesses located outside the European Union that sell, offer goods, services or market to or **monitor** residents in the European Union, whether or not that business has an establishment in the European Union.

Questions from Webinar Attendees:

1. *Does GDPR have retroactive effect?*

GDPR comes into force on May 25, 2018 and its provisions apply as of that date. While it is not expressly retroactive, compliance is required as of May 25.

2. *Are, for example, email addresses and cell phone numbers considered personal information under GDPR?*

Yes, email addresses and cell phone numbers are considered personal information under the GDPR. *Personal Data* is defined in Article 4(1) as: *any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

3. *Does GDPR apply to data from EU citizens that are located within a country (like the USA) collected from them while they are in the USA, for example a British national resident in the USA and employed by a company in the USA?*

No, it does not. The test for the application of GDPR is residence not citizenship. This means that an EU citizen resident in the United States in not covered by GDPR, but an American citizen resident in the EU is covered.

4. *Is there a private right of action?*

There are wide private rights of action. The relevant provisions of GDPR are Articles 77 to 82. In particular, an individual data subject has the right to lodge a complaint with the supervisory authority in their country of residence (Article 77(1), to appeal a decision of a supervisory authority to the courts of the applicable Member State (Article 78(1) to 78(3)), or a direct right to bring a private right of action in the courts of the Member State in which the data controller is established, without prior reference to a supervisory authority (Article 79(1)). The data subject specifically has the right to be compensated for *material or non-material damage* (i.e. not just financial loss, it includes such things as hurt feelings). Finally, there is the right for a data subject to mandate a not-for-profit body, organisation or association (such as an organised consumer protection body) to lodge a complaint or bring an action on his or her behalf (Article 80(1)).

5. *If a company receives personal data of EU residents and then anonymises it, can it use the anonymised data to perform analytics without further consent?*

GDPR does not apply to anonymised data, i.e. data from which no natural person can be identified or is identifiable (see the commentary in Recital 26). If the analytics are to be performed by a third party, the anonymised data set can be provided to that third party without consent. If the analytics are to be performed in-house, you must examine whether that the data is **truly anonymous** and not **pseudonymous** (see the distinction in Recital 26). If it is truly anonymous no further consent is required. However, it is likely to be best practice to inform the data subject (for example, through a privacy policy) that you intend to anonymise their data and use it for analytical purposes and get consent at the point of collection.

6. *How do you anonymise data?*

Recital 26 makes it clear that anonymised data is outside the scope of GDPR. It states: *The principles of data protection should [therefore] not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.*

There is no specific guidance either in the Recitals or in the main body of GDPR as to what steps need to be taken to define data as anonymous beyond the generality: that it is in a form that does not permit the data subject to be identified, i.e. it is stripped of all personal identifiers. Recital 26 states that, in assessing whether a natural person is identifiable, *account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.* What is reasonably likely takes into account all objective factors, namely the cost and amount of time required for identification, considering the available technology at the time of processing and technological developments. Thus, what technical steps can be taken will depend on how much is needed to render the personal data to a form that does not permit the data subject to be identified.

7. *How does pseudonymous differ from anonymous?*

Recital 26 sets out the basic differences between data that is considered pseudonymous under GDPR and data that is considered anonymous. Personal data that has undergone pseudonymisation has been rendered anonymous but the controller retains additional information on the data subject separately to the anonymised data which could be used to identify the natural person. Anonymous data is information which does not relate to a natural person or data that has been rendered anonymous in such a way that the data subject is no longer identified or identifiable.

Pseudonymous data is further addressed in Recitals 28 and 29. In Recital 28, there is what amounts to a policy statement that *the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations.* Recital 29 confirms that the further information held by the controller to identify the natural person must be kept separately.

8. What is automated processing and what are examples of it?

Recital 15 of GDPR specifically extends the scope of the regulation to automated processing. It states that: *in order to prevent a creating a serious risk of circumvention, the protection of natural persons should apply to the processing of personal data by automated means as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system.*

This requires a look at two terms, *processing* and *automated. Processing* is defined in GDPR as *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* (Article 4(2)). The UK Information Commissioner's Office defines *automated* as *making a decision solely by automated means without any human involvement.*

An example, therefore, would be where personal data is processed, for example organised into a structured database, solely by the operation of a software program and without human analysis of where in that database the personal data should rest. There are specific rules around automated processing and its effect on a data subject. These are set out in Article 22. In short, a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her (Article 22(1)). Recital 71 gives two examples of automated processing: automatic refusal of an online credit application or e-recruiting practices without any human intervention. There are exceptions to the general rule in Article 22(1). These are if the automated decision is necessary to enter into or perform a contract between the data subject and a data controller (Article 22(2)(a)), if it is authorised by EU or Member State law to which the controller is subject (and there are suitable measures to safeguard the data subject's rights, freedoms and legitimate interests) (Article 22(2)(b), or the controller has the data subject's specific consent (Article 22(2)(c)). In each of these exceptions, the controller is obliged to implement suitable measures to safeguard a data subject's right, freedoms and legitimate interests (the UK Information Commissioner's Office describes this as providing information about the processing) and permit the data subject the right to human intervention to review the decision.

9. What constitutes lawful processing? If you can establish a basis under contract or legitimate interest, do you still need consent, particularly with reference to a B2B situation?

There are a number of bases on which personal data can be processed lawfully. The controller needs to identify at least one of those bases in order to assure itself that its processing is lawful. There are six: consent, contract, legal obligation, vital interests, public task, and legitimate interests. These are set out in Article 6 of GDPR.

Consent is only one of the lawful bases for processing. Consent is not necessary if the controller can show that one or more of the other five bases applies. In particular, we shall look at contract and legitimate interest. The grounds for lawful processing are discussed in Recitals 39 to 50 of GDPR.

Looking at contract, this is addressed in general terms in Recital 44: *Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.* There is further

guidance in Article 6(1)(b) which states: *processing is necessary for the performance of a contract to which the data is party or in order to take steps at the request of the data subject prior to entering into a contract.* This ground, therefore, requires that the contract, or intention to enter into a contract, be with the data subject and it does not apply to a B2B situation. If you are receiving personal data as part of a B2B contract, then it is best practice to verify with the provider of the personal data that it has the ability to pass that data across and to seek contractual assurances and remedies to that effect. Equally, if you are the provider of the information you should check before provision that you have the ability to pass that personal data across.

Legitimate interest is discussed in Recital 47. Here, a legitimate interest is stated to be: *The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.* The example given is situations where the data subject is a client or in the service of the controller. The operative part of Recital 47 is then re-stated in Article 6(1)(f). The UK Information Commissioner's Office provides some further commentary. Legitimate interest is likely to apply where the controller uses people's data in a way in which they would reasonably expect. The UK ICO identifies a three-part analysis. First, identify a legitimate interest (of the controller, a third party or the data subject). Second, show that the processing is necessary to achieve that interest. Third, balance that decision against the data subject's rights and freedoms. For the third limb, the UK ICO gives the example that if the data subject would not reasonably expect the processing, or it would cause unjustified harm, then the data subject's interests are likely to override.

This is unlikely to apply to a B2B contract, as the exchange of data is between two businesses rather than a data subject and a business. However, it could be relied upon, for example, where employee data is provided to a third party payroll vendor as this should satisfy all three limbs of the UK ICO's test (although it is likely that the main ground would be employee consent, based on the employment contract or a policy).

In general terms in a B2B context, it is best practice to use that contract to obtain assurances that the data provider has the right to provide that data and remedies if that proves not to be the case.

10. What does it mean to process more than 5,000 data subjects in a 12-month period?

The relevance of the number and frequency of data subjects processed is to whether an organisation is required to have a data protection officer (Article 37) and the importance of data protection impact assessments (Article 35).

A data protection officer is required if the core activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. 5,000, therefore, should be looked at in the context of whether it constitutes a core activity and the scope in the context of other aspects of the business (Article 37(1)(b)). If the conclusion is that the processing step is *monitoring of data subjects* and that this constitutes a *core activity* then a data protection officer is required.

Regardless, if 5,000 data subjects are being processed annually, given the number it is best practice to carry out a data protection impact assessment (Article 35(1)), looking at the risks to the rights and freedoms of natural persons as a result of the processing steps. This shows internal compliance with the underlying concept of the GDPR which is to build privacy concepts and privacy assessments into business operations.

11. Does GDPR address the individual liability of a Data Protection Officer?

A data protection officer is not personally liable for a failure to comply with GDPR.

The role and requirements for a Data Protection Officer are set out in Recital 97 and in Articles 35 to 39 and 83 of the GDPR.

12. Can you have multiple Data Protection Officers?

Under the GDPR there must be a single DPO for each undertaking, although a group of undertakings can appoint a single DPO to cover them all (Article 37(2)). It is possible (if appropriate) to sub-contract the role of DPO out to a third-party organisation. The DPO needs to be someone senior within, or someone who is accountable to, your business.

13. What is your risk if a breach is due to a subcontractor and you cannot notify it within 72 hours of it occurring?

Recital 85 of GDPR sets out that a controller should notify a personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. For the controller, therefore, the clock starts ticking when the controller becomes aware of it. There is further guidance. The obligation to report applies unless the controller can demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. So the first determination to make is whether the breach does in fact create a risk. If it does not, the controller needs to log the breach and set out the reasons why there is, in its opinion, no risk. Investigation is permitted and Recital 85 sets out that if notification cannot be achieved within 72 hours, two things are required. First, when notifying, the reasons for delay should be specified. Second, there is no requirement to provide all details within 72 hours. Information can be provided in stages, provided it is done without undue delay.

Notification of a personal data breach is set out in Article 33.

Article 33(1) sets out the requirement to notify unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s).

Under Article 33(2), there is an obligation on the processor to notify the controller without undue delay. This means that if there is a delay on the part of the processor in notifying the controller, the controller (besides any contractual obligation that the processor may have breached) may have a right it can assert against the processor for breach of this Article.

Article 33(3)(a) to (d) sets out the contents of the notification. It must: describe the breach, the categories and number of data subjects and the number of personal records (Article 33(3)(a)), provide contact details for the data protection officer or other contact points (Article 33(3)(b)), describe the likely consequences (Article 33(3)(c)), and describe the measures taken, or proposed to be taken, to address the breach (Article 33(3)(d)).

Article 33(4) provides that information may be provided in phases, and Article 33(5) obliges the controller to document all breaches.

Further obligations are set out in Article 34, under which there is an obligation on a controller to notify the data subject without undue delay where there is a high risk to the rights and freedoms of the data subject. The UK Information Commissioner's Office provides the example of when this would be necessary as when a hospital loses medical records.

A personal data breach is a security incident. The UK Information Commissioner's Office lists the following as non-exhaustive examples of a data breach: unauthorised access by a third party, deliberate action or inaction by a controller, sending personal data to an incorrect recipient, computing devices containing personal data being lost or stolen, i.e. a mobile phone, alteration of personal data without permission, and loss of availability of personal data.

14. What court(s) will have jurisdiction over challenges to US-based entities?

This will be based on the normal rules of jurisdiction. If the US-based entity has an establishment in the EU, we would expect the case to be brought in the courts of the Member State in which it is established in the EU in accordance with Article 78(1) (or Article 79(1) if it relates to a challenge to the handling of a complaint by a supervisory authority). If the complaint is to a supervisory authority, the complaint will be to the home supervisory authority of the data subject, which will then likely take it forward against any establishment that the US-based entity has in the EU. If the US-based entity has no establishment or presence in the EU, then I expect the complaint to be made to the local supervisory authority which will make a ruling, potentially then validated by a court in the EU which considers itself to have jurisdiction. In a private action, if there is no establishment in the EU, a plaintiff would need to persuade a court that it had jurisdiction and then obtain the leave of the court to serve the proceedings out of the jurisdiction. Whether a court considered it had jurisdiction would be a question of fact in each individual case. Following that, the US entity would decide whether to defend and submit to the jurisdiction. The data subject would try to enforce any favourable judgment in the United States under the rules of international recognition and enforcement of judgments. Again, whether this was successful would be fact specific.