Keane Vgenopoulou & Associates LLC

Q&A

Q&A: GDPR in a glance

Authors: Thomas Keane, Christina Vgenopoulou & Loukiana Protopapa

Introduction

Almost three years have past since the General Data Protection Regulation (EU) 2016/679 (the "GDPR") has entered into force. The GDPR is a European Union law that was implemented in May 2018, replacing the 1995 Data Protection Directive. It is essentially the bedrock of data protection and personal privacy rights and its main goal is the facilitation of a standardized legal framework that regulates and harmonizes the way personal data is safeguarded and upheld by organizations across the European Union (the "EU").

This Q&A aims to answer some of the burning questions surrounding the GDPR.

1. Who must comply with the GDPR?

All organizations processing the personal data of people in the EU must comply with the GDPR. Article 3.1 states that the GDPR applies to organizations that are based in the EU even if the data are being stored or used outside of the EU. Article 3.2 goes even further and applies the law to organizations that are not in the EU if two conditions are met: the organization offers goods or services to people in the EU, or the organization monitors their online behaviour.

It should be noted that "Processing" is defined broadly under GDPR and it encompasses any operation which is performed on personal data, 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. On the other hand, "Personal data" means any information that relates to a person, such as names, email addresses, IP addresses, eye color, political affiliation, and so on.

2. What are the main improvements brought by the GDPR?

The GDPR introduces a single regulatory framework for business to adhere to ensuring harmonization across the EU. Moreover, the scope of the regulation is wide enough to cover not only EU established organizations but also those who operate in the EU without being established there, creating a level playing field in the market. Consequently, businesses benefit from an equal opportunity market that does not discriminate based on where a business is established and where the processing takes place.

On the other hand, the GDPR enhances transparency and increases customer awareness. It offers citizens enforceable rights, such as the right of access, rectification, erasure, the right to object and the right to data portability. As a result, individuals are now empowered to be actively involved in the protection of their data. Furthermore, the GDPR plays a crucial role in

the facilitation of a trust-worthy environment for innovation to flourish and in the creation of a market that is built on principles such as data protection by design and by default.

3. What does the principle of "accountability" mean in practical terms?

The principle of "accountability" is a key principle for data protection as it aims to ensure that organizations are responsible for complying with the GDPR and can demonstrate their compliance.

There is no standard checklist or approach to achieve accountability. Organizations need to be proactive and organised about their approach to data protection and able to evidence the steps they take to comply. Compliance with the "accountability" principle could include inter alia:

- ✓ implementing internal and external policies and compliance procedures;
- ✓ keeping detailed and up-to-date documentation on the processing of personal data;
- ✓ carrying out data protection impact assessments for high-risk processing operations;
- ✓ applying data protection by design and by default;
- ✓ ensuring security and confidentiality by all internal and external parties involved in data processing operations;
- ✓ carrying out audits and certification;
- ✓ establishing appropriate reporting structures;
- ✓ ensuring a good level of understanding and awareness of data protection amongst staff; and
- ✓ appointing a Data Protection Officer.

4. What are the GDPR rules on security processing?

The GDPR requires organizations to ensure that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". Effectively, this is GDPR's security principle.

The regulation furthers this security principle through Article 32, which lists a set of rules on achieving security of processing and provides a short list of options for doing so, including:

- The pseudonymisation and encryption of personal data;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational security measures.

In many cases, encryption is the most feasible method of securing personal data. For instance, if you regularly send emails within your organization that contain personal information, it may be more efficient to use an encrypted email service than to anonymize the information each time.

In any case, the GDPR does not impose which specific measures a business should implement. Instead, it prescribes that the measures used must be "appropriate" to the risks presented by processing. Therefore, data controllers and processors need to take account of the risks involved in processing by performing risk assessments or data protection impact assessments when choosing the most appropriate security measures to implement.

5. So do we have to use pseudonymisation and encryption?

Pseudonymisation and encryption are two examples of measures that may be appropriate for an organization to implement. There is no obligation to use these measures. The measures and practices that will be implemented depend on the nature, scope, context and purposes of processing, and the risks posed to individuals.

6. When is processing considered lawful?

Processing under the GDPR is lawful only if, and to the extent that, one of the following applies:

1. The data subject has given their unambiguous consent to the processing of their personal data for one or more specific purposes.
2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject before entering into a contract.
3. Processing is necessary for compliance with a legal obligation to which the controller is subject.
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child. (This basis does not apply to processing carried out by public authorities in the performance of their tasks.)

The most common legal basis used by business is perhaps, the reliance on 'legitimate interests'. This basis offers greater flexibility as it could theoretically apply to any type of processing carried out for any reasonable purpose. Nevertheless, the onus remains on the organization to balance the legitimate interests against the interests, rights and freedoms of the individual.

7. How has the legal basis of "consent" changed under the GDPR?

While consent remains a lawful basis under the GDPR, the definition of consent is significantly restricted in comparison to the previous legal framework. Consent under Directive 95/46/EC could be inferred from an action or inaction, however, the GDPR eliminates the possibility of implicit or 'opt-out' consent as it requires the data subject to demonstrate consent through a statement or a "clear affirmative action" (i.e. express consent).

In addition, consent must be "freely given, specific, informed and unambiguous. To be "freely given", the individual must be making a genuine choice over how the organization uses their data. If the individual has no real choice, consent is not freely given and it will be invalid. Individuals must be able to refuse consent without detriment and must be able to withdraw consent easily at any time. It also means consent should be unbundled from other terms and conditions (including giving separate granular consent options for different types of processing) wherever possible. Moreover, GDPR introduce a presumption that consent is not freely given if there is an imbalance of power between the data subject and the controller, this could include for example cases where the controller is a public authority or cases involving minors.

Furthermore, Article 7 also sets out further 'conditions' for consent, with specific provisions on:

- ✓ keeping records to demonstrate consent;
- ✓ prominence and clarity of consent requests;
- ✓ the right to withdraw consent easily and at any time; and
- ✓ freely given consent if a contract is conditional on consent.

8. Can the purpose of collecting personal data change?

The GDPR places some restrictions on changing the specified purpose for the collection of personal data. Organizations can change their purposes only if:

- the new purpose is compatible with the original purpose;
- they get the individual's specific consent for the new purpose; or
- they can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

If the new purpose is compatible, the organization does not need a new lawful basis for the further processing. However, if the original legal basis for collecting the data was "consent", the organization would usually need to get fresh consent to ensure the new processing is fair and lawful.

9. Which are the main rights offered to individuals under the GDPR?

The main rights afforded to data subjects under the GDPR are the following:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

10. When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which was originally collected or processed for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

11. Can an organization refuse to comply with a request for erasure?

The GDPR provides several exemptions to the right of erasure, also known as the "right to be forgotten". If one of the exceptions applies, the organization can refuse to comply with a request for erasure (wholly or partly).

Beyond the exceptions, an organization can refuse to comply with a request if it is:

- manifestly unfounded; or
- excessive.

Nevertheless, organizations must be able to demonstrate to the individual why they consider the request is manifestly unfounded or excessive.

12. Can we still profile data subjects?

Profiling is defined as “any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person” including analysing or predicting aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. While profiling is a practice that can arguably lead to more efficient, consistent and faster decisions, it can also result in great risks for data subjects.

The GDPR endeavours to mitigate these risks by empowering data subjects to object to the use of profiling (depending on the legal basis of the processing and possible overriding interest of the controller). Organizations are restricted from making solely automated decisions (such as those based on profiling), that have a legal or similarly significant effect on data subjects. The GDPR also prohibits profiling decisions based on sensitive personal data, and systemic use of profiling will require a prior data protection impact assessment.

Essentially, GDPR provides that an organization can only carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- ✓ necessary for entering into or performance of a contract between an organisation and the individual;
- ✓ authorised by law; or
- ✓ based on the individual’s explicit consent.

If an organization is using special category personal data, it can only carry out solely automated decision-making with legal or similarly significant effects if:

- ✓ it has the individual’s explicit consent; or
- ✓ the processing is necessary for reasons of substantial public interest.

13. What is a Data Protection Officer and a Data Controller?

A data controller is defined under GDPR as the “natural or legal person, public authority, agency or any other body that, alone or jointly with others, determines the purposes and means of the processing of personal data”. They are essentially the main decision-makers and those who exercise control over the personal data.

The GDPR requires most organizations that handle people’s private information to appoint an employee charged with overseeing the organization’s GDPR compliance. The Data Protection Officer, or DPO, is an organization’s GDPR focal point and will have to possess expert knowledge of data protection law and practices. The DPO is also the main point of contact for the data protection authority.

14. What does a DPO do?

The DPO has wide-ranging responsibilities and is involved in all issues which relate to the protection of personal data. The GDPR shields the position of a DPO from potential interference from the organization, requiring a DPO to only report directly to the highest level

of management at the organization and bounds the DPO by confidentiality in the performance of their tasks.

The GDPR assigns six major tasks to the DPO:

- To receive comments and questions from data subjects related to the processing of their personal data and the GDPR.
- To inform an organization and its employees of their obligations under the GDPR and any other applicable EU member state data protection provisions.
- To monitor an organization's compliance with the GDPR and any other applicable EU member state data protection provisions, train staff on compliance, and perform audits.
- To perform data protection impact assessments.
- To cooperate with the data protection supervisory authority.
- To act as the focal point for the data protection supervisory authority on matters relating to the processing of personal data and other matters, where appropriate.

The DPO position requires a high level of technical expertise and a legal understanding of GDPR and privacy laws in all jurisdictions in which their organization operates. In addition, given the degree of independence and minimal oversight available to DPOs, meanes that in practice, the role of a DPO cannot be performed by a junior employee.

15. Are all organizations required to have a DPO?

Under the GDPR, you must appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

Your core activities are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity.

When determining if processing is on a large scale, you should take the following factors into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

There are no restrictions under the GDPR for a DPO to be hired or shared among several smaller organizations, provided the DPO can effectively carry out their duties for each organization.

An organization could also decide to designate a DPO even when not required to under the GDPR. Arguably, all organizations, regardless of the type or size, that handle EU residents' personal information could benefit from having someone in the organization who is tasked with monitoring GDPR compliance.

16. What information should data controllers provide to individuals?

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓
The contact details of your data protection officer	✓	✓

When the organization collects the data from the individual it relates to, it must provide them with privacy information at the time it obtains their data.

When the organization obtains personal data from a source other than the individual it relates to, it needs to provide the individual with privacy information:

- within a reasonable period of obtaining the personal data and no later than one month;
- if it uses the data to communicate with the individual, at the latest, when the first communication takes place; or
- if it envisages disclosure to someone else, at the latest, when it discloses the data.

Organizations must actively provide privacy information to individuals, however, the GDPR provides for certain exceptions in providing individuals with privacy information. For example, organizations do not need to provide individuals with any information that they already have.

17. How are data protection breaches reported?

Data processors are required to notify the data controller and the data controller must notify the supervisory authority without undue delay after becoming aware of a personal data breach. Where feasible, this must be done within 72 hours, however, where that is not possible and there is sufficient justification for the delay, the GDPR allows the provision of the information in phases.

Data controllers are also obliged to notify data subjects without undue delay if there is a high risk to their rights and freedoms. However, the GDPR provided that if the breached data is anonymised or encrypted and present no risk to the rights and freedoms of the subject, then no notification is required.

When reporting a breach, data controllers must provide the following information to the supervisory authority:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned;
- The name and contact details of your DPO or other contact point from whom more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures you have taken, or propose to take, to deal with the breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

18. What are the GDPR fines?

The GDPR introduces two tiers of fines depending on the severity of the violation.

The less severe violations could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

Examples of less severe violations include:

- Breach of Article 8 of GDPR regarding the conditions for children's consent;
- Breach of Article 11 of GDPR regarding processing that does not require identification;
- Breach of Articles 25-39 of GDPR regarding the general obligations of processors and controllers;
- Breach of Articles 42 and 43 of GDPR regarding certification and Certification bodies; and
- Breach of Article 41 of GDPR regarding Monitoring bodies.

The more serious infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

These include any violations of the GDPR governing:

- Article 5 regarding the basic principles for processing;
- Article 6 regarding the lawfulness of processing;
- Article 7 regarding the conditions for consent;
- Articles 12 to 22 regarding the data subjects' rights; and
- Articles 44 to 49 regarding the transfer of data to an international organization or a recipient in a third country

They also include:

- Any violation of member state laws adopted under Chapter IX and
- Non-compliance with an order by a supervisory authority.

Beyond the administrative fines stated above, Article 82 of the GDPR gives data subjects the right to seek compensation from organizations that cause them material or non-material damage as a result of a GDPR infringement.

19. Does outsourcing lift the organization's responsibility under GDPR?

No. Many organizations outsource data handling to third parties. This practice does not absolve the hiring organization (i.e. the controller) from ensuring that personal data is processed in accordance with the GDPR, unless the controller can clearly demonstrate that it was "not in any way responsible for the event giving rise to the damage".

20. What are the European Commission's goals for the future?

According to the Q&A published by the European Commission in June 2020, the key objective is to support a consistent implementation and enforcement of the GDPR across the EU. This necessitates active engagement from all parties:

- making sure that national legislation, including sectoral ones, are fully in line with the GDPR;
- Member States providing data protection authorities with the necessary human, financial and technical resources to properly enforce the data protection rules but also reaching out to stakeholders, both citizens and – very importantly – SMEs;
- data protection authorities developing efficient working arrangements regarding the functioning of the cooperation and consistency mechanisms, including on procedural aspects;
- making full use of the toolbox under the GDPR to facilitate the application of the rules, for instance through codes of conduct;
- closely monitoring the application of the GDPR to new technologies such as AI, Internet of Things, blockchain.

Additionally, the European Commission will continue to promote harmonization by furthering convergence of data protection rules as a way to ensure safe international data flows.

The foregoing should not be read or construed or relied upon as legal advice in any specific or individual circumstance.

In the event of any query or need for clarification please contact the undersigned.

Keane Vgenopoulou & Associates LLC

For further information, please contact:

Thomas Keane	**Christina Vgenopoulou**	**Loukiana Protopapa**
Partner	Partner	Associate
Tel: +357 25 25 7900	Tel: +357 25 25 7900	Tel: +357 25 25 7900
Email: tkeane@kvlaw.eu	Email: cvgenopoulou@kvlaw.eu	Email: lprotopapa@kvlaw.eu