McAfee
Together is power.

General Data Protection Regulation

Frequently Asked Questions

Overview

Q1: When did the General Data Protection Regulation (GDPR) become enforceable?

A: The GDPR replaced the 1995 Data Protection Directive (Directive 95/46/EC). It was adopted on 27 April 2016 and became enforceable on 25 May 2018, following a two-year transition period.

Q2: What is the potential maximum fine for organisations not complying with the GDPR?

A: An organisation can be fined up to 4% of annual global turnover, or €20 million, whichever is greater. This is the maximum fine that can be imposed for the most serious infringements. A lower category of fines (up to 2% of annual global turnover, or €10 million, whichever is greater) may be imposed for lesser infringements.

Q3: Does the GDPR only apply to European organisations?

A: No. It will apply to all organisations, regardless of geographic location that:

- Collects, targets, or processes personal data concerning any European Union (EU) resident
- Processes data anywhere in the EU

Q4: What are some examples of "personal data" per the GDPR?

A: Standard personal data (examples: name, email address, IP address), special categories of data (example: healthcare), children's data, and data regarding criminal offences. Personal data encompasses information collected and processed on all EU residents, no matter who they are or how the information is collected. This can apply to customers, internal employees, and contractors. The McAfee® Privacy Notice has been updated to include "personal data" per the GDPR: https://www.mcafee.com/us/about/legal/privacy.aspx.

Q5: What's the difference between PII and personal data?

A: Personally Identifiable Information (PII) is a term used mainly within the US. Personal data is considered to be the European equivalent of PII. However, it doesn't completely correspond to the PII definition popular in the US. Personal data as defined by the GDPR is broader—for example: any physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, even online identifiers, such as IP address and cookies, that enable to identification directly or indirectly of a natural person.

Connect With Us

Q6: What is a trusted source for me to find out more about the GDPR?

A: Visit: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en. The GDPR has two sections. The first part consists of Recitals numbered 1 through 173, and the second part consists of Articles numbered 1 thru 99. The Articles are the specific acting terms of the Regulation, whereas the Recitals give indications on how the Articles are to be interpreted.

Q7: Does the GDPR replace Safe Harbor or Privacy Shield?

A: One of the requirements of GDPR (which existed under the Data Protection Directive, the predecessor to The GDPR) is a lawful means of transferring data out of the EU. Safe Harbour was, for many years, a valid way to transfer data exclusively from the EU to the US. However, Safe Harbour was invalidated and replaced by Privacy Shield, a more rigorous means to self-certify. Privacy Shield also only covers the transfer of data from the EU to the US.

In addition to the fact that personal data may be transferred to countries offering adequate protection (mainly the European Economic Area (EEA) and a handful of other countries), there are currently two other lawful means to transfer data out of the EEA: Model Clauses/Standard Contractual Clauses and Binding Corporate Rules. McAfee relies on Standard Contractual Clauses, which need to be in every agreement where there is a transfer of data outside the EU. The advantage of Model Clauses is that they are not specific to the US. Binding Corporate Rules are an internal framework that enables the transfer solely within a given organisation. They enforce a policy around data protection throughout a given group of companies.

Q8: Can the EU-imposed rules and fines, such as the GDPR, carry weight in the US?

A: The short answer is yes. If the data relates to an EU resident, the US company processing the data must respect the personal rights of the EU resident. GDPR applies to data collected on EU residents, regardless of where the company/processor/owner is located. As many companies operate globally, failure to comply could have a negative impact on their ability to do business in the EU, not to mention the potential fines that may be applied.

Q9: Are any vertical industries or sectors exempt from the GDPR?

A: No. Any organisations that store or process personal data of EU residents are subject to the regulation—whether they are a commercial organisation, a local government agency, or a charity.

Data Residency

Q1: How are data residency requirements addressed in the GDPR?

A: Under the GDPR, where the data is held is not relevant. What is relevant is to whom the data belongs. For example, if an EU resident lives in China and the data is hosted in India, then it is subject to the GDPR because the EU resident owns the data and the processor is targeting EU residents. The GDPR does not specify data residency requirements. The GDPR requires organisations (even the organisations that are hosting data in the EU) to make sure that they protect EU resident personal data, implement Privacy Impact Assessments, and have appropriate security and breach response plans in place.

Q2: Will storing data in global cloud services (Microsoft Azure/Amazon Web Services) or services provided on those platforms, be allowed under GDPR?

A: Yes. Many cloud services allow customers to "pin" data in the EU. If a cloud service does not include this feature, it will need to comply with GDPR data transfer requirements (discussed above). Encryption can be used before data is transferred to reduce the risk. But, overall, the data controller needs to get confirmation from any data processor that they understand their responsibilities.

Q3: If I have servers in the EU but only have personal data on US customers, does GDPR apply?

A: The GDPR applies even where there is no EU presence of the controller or the processor, and it is still applicable whenever (1) an EU resident's personal data is processed in connection with the offering of goods/services or (2) the behaviour of individuals (irrespective of their citizenship) within the EU is "monitored."

Technology and Implementation

Q1: The GDPR places a requirement on companies to "implement appropriate technical and organisational" measures about how they handle and process personal data. What does it mean?

A: It means an organisation needs to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. The pseudonymization and encryption of personal data
2. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
4. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Q2: What does "privacy by design" mean?

A: It means companies must consider and incorporate personal data protection features at the very beginning of developing and designing a product by implementing their security project(s), which may result in major internal process changes for some organisations as they bring new products, services, or processes to market and in their continual evaluation of existing products and services.

Q3: The GDPR mentions the use of encryption, but it does not specify to what level. Is there any guidance available on the minimum level of encryption? (Examples: databases, inflight, and other types)

A: The regulation does not specify the details of encryption levels. It is the responsibility of the data controller and the data processor that the encryption should be "appropriate to the risk."

Q4: A company laptop is lost with personal data on it but is protected with full disk encryption. Does the company still have to declare the loss to the authorities?

A: In the case of a personal data breach, the controller 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 applicable supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The GDPR sets out exceptions to the notification, amongst which is where measures have been taken to render personal data unintelligible, for instance, by use of encryption.

Q5: What about Shadow IT brought in by the users?

A: It is the data controller's responsibility to know where the data is stored and processed, and this includes Shadow IT. Not knowing or claiming not to know is not an excuse. You should have processes, procedures, and the technology to investigate and secure Shadow IT services if they contain personal data subject to the GDPR.

Q6: Is browser history subject to the GDPR?

A: The GDPR is about protecting the rights of the data subject, but those rights are balanced against other considerations. The goal is not to stop commerce or the free flow of information. When McAfee® products are watching web browsing activity, we need to make sure we are transparent and clear in disclosing what our products do. A major part of the GDPR programme at McAfee has been to review and document data collection and use in our products.

Q7: Where can I find information on how McAfee products support GDPR-compliancy for my customers?

A: Refer to our GDPR Central section, "Personal data collection and compliance" at https://www.mcafee.com/enterprise/en-us/about/gdpr.html.

Disclaimer: The information provided on this General Data Protection Regulation (GDPR) paper is our informed interpretation of the GDPR and is for information purposes only. It does not constitute legal advice, contractual commitment or advice on how to meet the requirements of any applicable law. This paper is subject to change without notice and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance. If you require legal advice on the requirements of the GDPR, or any other law, or advice on the extent to which McAfee technologies can assist you to achieve compliance with the GDPR or any other law, you are advised to consult a suitably qualified legal professional. If you require advice on the nature of the technical and organizational measures that are required to deliver operational privacy and security in your organization, you should consult a suitably qualified privacy professional. No liability is accepted to any party for any harms or losses suffered in reliance on the contents of this publication.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847 8766
www.mcafee.com