What You Need to Know about the EU's 2018 General Data Protection Regulation

Author, Summer Phillips

A Data Science Foundation White Paper

May 2018

---

www.datascience.foundation

Data Science Foundation
Data Science Foundation, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ
Tel: 0161 926 3641 Email: contact@datascience.foundation Web: www.datascience.foundation
Registered in England and Wales 4th June 2015, Registered Number 9624670

What You Need to Know about the EU's 2018 General Data Protection Regulation

We live firmly in the midst of the Information Age. Data is everything. In fact, thieves are now targeting consumer and business information rather than financial assets, simply because there is so much more value in data. The explosion of data being used on a daily basis, the increasing threat to that data from thieves and hackers, and the growing number of businesses utilizing that data all add complexity to how that information is processed and stored.

In Europe, the ways businesses, organizations, and even government agencies process data are changing. The General Data Protection Regulation (GDPR) goes into full force on May 25, 2018, replacing the long-outdated Data Protection Act of 1998. However, it was actually applied on May 24, 2016 (the 2018 date is the deadline for compliance on the part of organizations, businesses and others). What should businesses, organization heads, and even consumers, know about the GDPR?

Within this guide, we will explore the most important aspects.

What Is the GDPR?

GDPR stands for General Data Protection Regulation. It is an EU-wide law that governs how all bodies (organizations, state governments, businesses, etc.) interact with and process data. What data? The GDPR primarily deals with consumer personal information, which includes health data, financial data, and other "personally identifiable information". The language of the GDPR specifies:

- Online identifiers, such as IP addresses
- Economic data
- Cultural data
- Physical health data
- Mental health data
- Pseudonymized personal data (associated with a pseudonym)
- Biometric information
- Genetic data
- Sexual orientation
- Location/geographic data
- Analytics data
- Name and address
- Email address
- Photos
- Religion
- Trade union membership

In addition to governing how this data can be processed, handled, stored, and accessed, the regulation

also mandates that organizations, agencies, businesses, charities, and others must provide consumers with access to the information held that pertains to them.

Why Was the GDPR Necessary?

All members of the EU, including the UK, previously had laws governing data processing. However, they were extremely outmoded, being adopted in 1995-1998. Moreover, each member in the EU also applied its own national laws to data processing, which could differ substantially from one member state to another. Really, the GDPR is an attempt to:

- Create a cohesive body of law governing the processing of data
- Give all EU citizens equal rights under an EU-wide law
- Ensure that businesses, organizations, etc. are able to apply the same data processing rules regardless of the EU member state in question

Ultimately, the new regulation should level the playing field, ensuring that not only do businesses and organizations have a simpler time ensuring that data processing rules are being followed in all EU member states, but that consumers have better protection, better access to the information pertaining to them being stored by companies, and that inpiduals have stronger protections with defined rights pertaining to their personal data.

Key Considerations with the GDPR

The GDPR is a massive body of law, with three separate, yet related, drafts. It is also considered a living document, and will be revised, updated, and changed when and as needed. Making sense of the regulation and how it applies to your personal data, or to your company's use of consumer personal data, can be quite daunting. In this section, we've broken down some of the most important considerations so we can address them separately.

Article 5, Section 1 A – F, provides perhaps the best illumination of the key areas of focus and consideration within the GDPR:

"1. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to inpiduals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of inpiduals; and

f) 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."

Article 5, Section 2 further states:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

What's New?

Quite a few of the rules contained within the regulation are unchanged from the previous Data Protection Act. However, there are some new additions, as well as changes to older rules.

- **Increased Scope:** The single largest change with the adoption of the GDPR is the increase in terms of geographic scope. The GDPR applies to all member states of the EU, as well as to all businesses processing data belonging to EU citizens.

As such, UK businesses will still need to follow GDPR specifications even after Brexit, when the UK is no longer a member of the EU. Companies in the US must follow GDPR mandates when dealing with any information pertaining to EU citizens, and so on, so long as the activity relates to "offering goods or services to EU citizens, irrespective of whether payment is required, and the monitoring of behavior that takes place within the EU."

- **Stronger Penalties:** In order to make the GDPR effective, legislators needed to give it teeth. They did this in the form of stronger penalties than previously enforced. Under the new law, any organization in breach of the GDPR can be fined the greater of: 4% of its annual global turnover, or €20 million.

Note that this is the maximum fine possible. A tiered approach is taken with penalties. It's also important to realize that the GDPR applies to both those who control the data, and those who process it, meaning there are no exemptions for cloud providers.

- **Informed Consent:** The GDPR mandates that any organization, company or other body seeking to process consumer personal information obtain informed consent. In addition, the regulation mandates that consent be obtained in an intelligible and easily accessible form.

This means that terms and conditions documents that bury important information in legalese are no longer acceptable. In addition, opt-outs and pre-ticked boxes will no longer be allowed. All consent must be given in an active, affirmative way. All processors/controllers are required by law to maintain a history of when how consent was given, and to provide all consumers with the means to withdraw their consent at any time.

- **Breach Notification:** Given the dramatic increase in data breaches over the past few years, the focus on breach notification within the GDPR should come as no surprise. Consumers must be notified of any breach that may "result in a risk for the rights and freedoms of inpiduals" within 72 hours of the organization learning of the breach. Processors must also notify controllers as soon as possible regarding any breach.
- **Right to Access:** One of the most interesting of the key changes under the GDPR is the inpidual's right to access. Essentially, this forces all organizations and businesses to first notify an inpidual of exactly what data is being processed or accessed, and, if the consumer so wishes, to provide them with a copy of all personal data in electronic form at no cost. This provides immense transparency, and once more puts consumers in control of their own data, rather than allowing organizations complete control.
- **Right to Be Forgotten:** Another powerful change that has grown directly out of the struggles inpiduals have had with search giant, Google, the right to be forgotten is granted in the GDPR. Also called data erasure, the right to be forgotten ensures that consumers are in control of their personal information and have the right to force all processors to stop using, sharing or storing it. This can be due to any reason, including lack of relevance, but also if the consumer simply chooses to revoke his or her consent for the information to be processed or shared.
- **Data Portability:** This is a new focus for the EU, and it allows consumers to receive their personal data previously provided to an organization or business, and to transmit that information to another processor. An excellent example of this would be health records, or mental health records.
- **Privacy by Design:** The GDPR mandates that data protection be handled from the outset, rather than being dealt with as an afterthought. Data protection steps, technology and procedures must be in place from the beginning, rather than being added later. This includes holding and processing only the information necessary to completing the processor's duties, and minimizing the holding of any other data. It also touches on limiting who can access information to those who have an actual need in order to complete the processing.
- **Data Protection Officers**: Many organizations are now required to appoint a data protection officer, or DPO (but not all organizations – this applies to heavy data processors, primarily). The DPO will take the place of local DPAs, reducing the workload and onerous burden of dealing with different notification requirements in different EU member states.

The Six Bases

In order for an organization or business to process consumer personal information, they must have a lawful basis for doing so. There are six acceptable bases, including consent, contract, legal obligation, vital interests, public tasks, and legitimate interests. After the deadline, companies will need to prove they have a transparent, specific and lawful purpose for processing consumer personal information. Failure to prove such puts the company in danger of being fined.

- **Consent:** In this situation, the company would have the consumer's express, affirmative consent to process their personal data. However, the consumer can withdraw that consent at any point. In order for a company to continue processing that consumer's data, another lawful basis would need to be found.
- **Contract:** A company may be legally able to process a consumer's personal data if there is a contract in place requiring it.
- **Legal Obligation:** A company may process consumer personal data if there is a legal obligation to do so.
- **Vital Interests:** A company may process consumer data if it is in the consumer's best interests, with a particular emphasis on being essential to that consumer's life.
- **Public Tasks:** If processing the information is deemed in the public's best interests, or deals with publicly available records, the company may process it.
- **Legitimate Interests:** Legitimate interests is a wide-ranging category that includes things like preventing information theft and stopping fraud. For example, a company attempting to stop fraudulent activity on a consumer's credit card would have a legitimate (and legal) basis for processing information.

At least one lawful basis must be present in order for a company to process any consumer personal data. In addition, the data must then be deleted as soon as it is no longer being processed.

Inpidual Rights

One of the most important parts of the GDPR is the number of new inpidual rights that have been spelled out. These are all tied to the information collected about consumers, and how consumers can interact with that information, even if it is being processed or stored by a business. These rights are as follows:

- **The Right to Be Informed:** The right to be informed simply means that consumers have the right to know what information a company holds about them, and how that information is being used.
- **The Right of Access:** The right of access simply means that consumers must be able to obtain a copy of all the information a company or organization holds that pertains to them, at no cost, and in electronic format. This right also includes access to supplementary information, such as would be provided in a privacy notice.

- **The Right to Rectification:** The right to rectification is nothing more than the right of a consumer to have erroneous, outdated or otherwise inaccurate information pertaining to themselves rectified.
- **The Right to Erasure:** This right was touched on previously as the right to be forgotten, and is the right of the consumer to have information removed at their request, when it is no longer accurate, and in other situations, including at the withdrawal of the inpidual's consent for the information to be processed or disseminated.
- **The Right to Restrict Processing:** The right to restrict processing means that consumers can dictate the ways in which businesses and organizations can use their data in some instances. This includes in cases where information accuracy is in question, data was unlawfully processed, the data is no longer necessary but is still being used, or the consumer has objected to the data being processed.
- **The Right to Data Portability:** The right to data portability is simply the right of the consumer to take their personal data from one business and provide it to another. This can include financial data, health and mental health data, and more. It also means that consumers can request data processors to transmit the data in question to another organization.
- **The Right to Object:** Consumers have the right to object to their data being processed. If a consumer objects, the organization or business in question must cease processing the information immediately. However, this right only applies in some instances. If the information is being used for a public interest-related task, in a legal capacity, or in a legitimate interest, the right to object is not absolute. However, it is absolute in regards to marketing activities.
- **Rights in Automated Decision Making:** In settings where decisions are made by automated systems rather than by human beings, companies and organizations are prohibited from making solely automated decisions (including those involving profiling) that have a legal or otherwise significant effect on the consumer.

All consumer rights are spelled out in the 99 articles that make up the bulk of the GDPR. Note that some rights are attested to, mentioned, or born on by more than one article.

What's Needed for GDPR Compliance?

Complying with the GDPR is not optional for businesses and organizations that fall under its purview. However, it can be difficult to determine exactly what steps must be taken to ensure compliance. The Information Commissioner's Office (ICO) has issued a streamlined compliance guide that walks business owners, and organization decision makers through a simple 12-step process, which is as follows. Note that the guide is free to download and includes more in-depth information concerning each of the 12 steps.

1. **Awareness:** Key stakeholders within the organization must know about the GDPR deadline and what it means for your organization.
1. **Information You Hold:** Document the personal information your organization holds, where it originated, and how it is used.

1. **Communicating Privacy Information:** Review your organization's current privacy policy, and create a plan for making GDPR-related changes.
1. **Inpidual Rights:** Verify that your procedures do not infringe on any inpidual rights.
1. **Subject Access Requests:** Update all organization procedures and create a strategy to handle consumer requests moving forward.
1. **Lawful Basis for Processing Personal Data:** Know the lawful basis for your organization's use of consumer personal information. Explain this in your privacy policy.
1. **Consent:** All consent-gaining methods must now adhere to GDPR standards. Any existing consents that do not meet current standards must be refreshed.
1. **Children:** Have systems in place to verify ages and obtain parent/guardian consent for underage consumers (if applicable).
1. **Data Breaches:** Create procedures to adhere to GDPR requirements for detecting, reporting and investigating personal data breaches.
1. **Data Protection by Design and Data Protection Impact Assessments:** Follow the ICO's code of practice on Privacy Impact Assessments and requirements in Article 29.
1. **Data Protection Officers:** If applicable, designate a data protection officer for your organization.
1. **International:** Using Article 29 Working Party guidelines, determine your lead data protection supervisory authority of you conduct business in more than one EU member state.

In Conclusion

GDPR will soon be the law of the land for all EU-member states. However, it will have a profound impact on any organization that processes personal data for EU citizens – this legislation will have a truly global impact, even though non-EU citizens will not benefit from the increased control over personal data provided under the law.

Businesses and organizations that must comply with GDPR have had two full years to determine what elements of the sweeping legislation apply to them, and to implement systems, procedures, solutions and policies to uphold their responsibilities. For all of that, the EU will not be looking for scapegoats. Chances are good that there will be some lenience in terms of full adoption by organizations, particularly those that either lack financial resources to enable swift implementation, and those with a significant number of employees.

With that being said, some companies are attempting to minimize the impact of GDPR on their operations. For instance, Wired magazine pointed out in an article published in late May 2018, that Facebook had moved 70% of its Irish user locations from Ireland to the US in an attempt to prevent GDPR from applying to them, although the company claims it will uphold treatment of user data no matter where those users are located.

Moreover, according to a survey by Imperva, only 43% of European IT staff are taking steps to ensure their firms are GDPR compliant, and a full one-third of IT security professionals say they are not changing anything in the way their firms handle personal data.

Ultimately, the GDPR is a necessary step that puts consumers back in control of their personal information, and puts the onus of safeguarding that data firmly on the shoulders of data processors. We'll simply have to wait and see how it plays out, though.

Source:

Client provided +

https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

http://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know

https://www.nbcnews.com/tech/internet/what-gdpr-look-european-data-privacy-rules-could-change-tech-n868646

About the Data Science Foundation

The Data Science Foundation is a professional body representing the interests of the Data Science Industry. Its membership consists of suppliers who offer a range of big data analytical and technical services and companies and individuals with an interest in the commercial advantages that can be gained from big data. The organisation aims to raise the profile of this developing industry, to educate people about the benefits of knowledge based decision making and to encourage firms to start using big data techniques.

Contact Data Science Foundation

Email:contact@datascience.foundation
Telephone: 0161 926 3641
Atlantic Business Centre
Atlantic Street
Altrincham
WA14 5NQ
web: www.datascience.foundation