Jargon-buster guide to GDPR

Your expert guide to successfully navigating the EU data protection regulation

In this e-guide

In this e-guide:

The European Union's General Data Protection Regulation (GDPR) comes into effect on 25 May 2018. GDPR will introduce new accountability obligations and stronger rights and restrictions on international data flows.

GDPR introduces new obligations for any organisation that handles data about EU citizens - whether that organisation is located in the EU or not. It introduces data breach notification into European law for the first time. And it places stricter responsibilities on organisations to prove they are adequately managing and protecting personal data.

In this guide, we provide the 10 most important things you need to know about GDPR, and a jargon-buster explanation for some of the key terminology.

Bryan Glick, editor-in-chief

In this e-guide

10 key facts businesses need to note about the GDPR

Warwick Ashford, security editor

The European Union's new data protection regulation is complicated, but there are 10 key facts businesses need to know, says privacy lawyer and KuppingerCole analyst Karsten Kinast.

"The General Data Protection Regulation (GDPR) comes into force in less than two years' time, but it is not too late for organisations to start responding to these key facts," he told the European Identity & Cloud Conference 2016 in Munich.

1. GDPR applies to all

The GDPR applies to all companies worldwide that process personal data of European Union (EU) citizens.

"For the first time, the European Commission [EC] is exporting European data protection principles to the rest of the world," said Kinast.

This means that any company that works with information relating to EU citizens will have to comply with the requirements of the GDPR, making it the first global data protection law.

Kinast believes this aspect alone will contribute significantly to all companies around the world – including those in Europe – taking data privacy more seriously.

2. The GDPR widens the definition of personal data

While the definition of personal data has always been fairly wide, Kinast said the GDPR broadens it even further, bringing new kinds of personal data under regulation.

“This means parts of IT that have been unaffected by data protection laws in the past will need attention from businesses to ensure they comply with the new regulation,” said Kinast.

The GDPR considers any data that can be used to identify an individual as personal data. It includes, for the first time, things such as genetic, mental, cultural, economic or social information.

“From now, hardly any personal data will not fall under the GDPR, making it difficult for organisations to avoid having to comply with its requirements,” said Kinast.

In this e-guide

3. The GDPR tightens the rules for obtaining valid consent to using personal information

Having the ability to prove valid consent for using personal information is likely to be one of the biggest challenges presented by the GDPR, according to Kinast.

“Organisations need to ensure they use simple language when asking for consent to collect personal data, they need to be clear about how they will use the information, and they need to understand that silence or inactivity no longer constitutes consent,” he said.

The GDPR requires all organisations collecting personal data to be able to prove clear and affirmative consent to process that data. However, Kinast said most of the consent mechanisms he is seeing in the market are not valid under the GDPR.

“In the future, it will be more important than ever for organisations to explain exactly what personal data they are collecting and how it will be processed and used. Without valid consent, any personal data processing activities will be shut down by the authorities,” he said.

4. The GDPR makes the appointment of a DPO mandatory for certain organisations

The GDPR requires public authorities processing personal information to appoint a data protection officer (DPO), as well as other entities, when "core activities" require "regular and systematic monitoring of data subjects on a large scale" or consist of "processing on a large scale of special categories of data".

According to a study by the International Association of Privacy Professionals (IAPP), this requirement means that, in Europe alone, 28,000 DPOs will have to be appointed in the next two years.

"This will affect even Germany companies, where there has been a requirement to appoint a DPO for organisations with more than 10 employees," said Kinast.

"This is because, with today's technology, there are many organisations with fewer than 10 employees that process the personal data of thousands of people and have a much higher risk than many larger organisations.

"The GDPR does away with the criterion of number of employees and focuses instead on what organisations do with personal information.

"Therefore, any business that depends on processing personal information will have to appoint a DPO, who will be an extension of the data protection

authority to ensure personal data processes, activities and systems conform to the law by design," he said.

5. The GDPR introduces mandatory PIAs

According to the Kinast, the inclusion of mandatory privacy impact assessments (PIAs) in the GDPR is mainly due to the influence of the UK's Information Commissioner's Office, which has worked a lot with PIAs in the past.

The GDPR requires data controllers to conduct PIAs where privacy breach risks are high to minimise risks to data subjects.

"This means before organisations can even begin projects involving personal information, they will have to conduct a privacy risk assessment and work with the DPO to ensure they are in compliance as projects progress," he said.

6. The GDPR introduces a common data breach notification requirement

The GDPR harmonises the various data breach notification laws in Europe and is aimed at ensuring organisations constantly monitor for breaches of personal data.

"The regulation requires organisations to notify the local data protection authority of a data breach within 72 hours of discovering it. This means

organisations need to ensure they have the technologies and processes in place that will enable them to detect and respond to a data breach," said Kinast.

"For many organisations, this may require quite a bit of training. It may also require making changes to internal data security policies and how this is promoted in the organisation to ensure data breaches are properly understood and will be recognised easily," he said.

7. The GDPR introduces the right to be forgotten

The GDPR introduces very restrictive, enforceable data handling principles, said Kinast.

One of these is the data minimisation principle that requires organisations not to hold data for any longer than absolutely necessary, and not to change the use of the data from the purpose for which it was originally collected, while – at the same time – they must delete any data at the request of the data subject.

"This means organisations will have to get fresh consent before they can alter the way they are using the data they have collected," he said.

It also means organisations have ensure they have the processes and technologies in place to delete data in response to requests from data subjects.

8. The GDPR expands liability beyond data controllers

In the past, only data controllers were considered responsible for data processing activities, but the GDPR extends liability to all organisations that touch personal data.

“The GDPR also covers any organisation that provides data processing services to the data controller, which means that even organisations that are purely service providers that work with personal data will need to comply with rules such as data minimisation,” said Kinast.

9. The GDPR requires privacy by design

The GDPR requires that privacy is included in systems and processes by design.

“This means that software, systems and processes must consider compliance with the principles of data protection,” said Kinast.

“However, the proper erasure of information, for example, is not something often seen in software. But in the future, all software will be required to be capable of completely erasing data, which will be a challenge for a lot of software engineers,” he said.

10. The GDPR introduces the concept of a one-stop shop

In the past, Ireland has been popular with large US corporations, such as Google, because of the country's relatively permissive data protection authority, said Kinast.

"However, that all disappears with the GDPR, which allows any European data protection authority to take action against organisations, regardless of where in the world the company is based," he said.

Kinast noted this enforcement is also backed by significant fines of up to €20m or 4% of group annual global turnover.

The benefit for business, he said, is that they will have to deal with only one supervisory authority rather than a different one for each EU state.

"This will make it simpler and cheaper for organisations, but at the same time, EU citizens sill have the right to approach any data protection authority of their choice to lodge complaints," said Kinast.

Next definition

In this e-guide

Information Commissioner's Office (ICO)

Margaret Rouse, WhatIs.com

The Information Commissioner's Office (ICO) is an independent authority in the UK that promotes openness of official information and protection of private information. According to its Web site, the ICO does this "by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken."

The ICO oversees:

- The Data Protection Act
- The Freedom of Information Act.
- The Environmental Information Regulations.
- The Privacy and Electronic Communications Regulations.

Next definition

In this e-guide

EU Data Protection Directive (Directive 95/46/EC)

Margaret Rouse, WhatIs.com

EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Directive 95/46/EC encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive is based on the 1980 OECD "Recommendations of the Council Concerning guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data."

These recommendations are founded on seven principles, since enshrined in EU Directive 94/46/EC:

- Notice: subjects whose data is being collected should be given notice of such collection.
- Purpose: data collected should be used only for stated purpose(s) and for no other purposes.

- Consent: personal data should not be disclosed or shared with third parties without consent from its subject(s).
- Security: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- Disclosure: subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
- Access: subjects should granted access to their personal data and allowed to correct any inaccuracies.
- Accountability: subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

In the context of the Directive, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Article 2a). Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link. Examples of such data include address, bank statements, credit card numbers, and so forth. Processing is also broadly defined and involves any manual or automatic operation on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction (paraphrased from Article 2b).

In this e-guide

These data protection rules apply not only when responsible parties (called the controller in this EU directive) is established or operates within the EU, but whenever the controller uses equipment located inside the EU to process personal data. Thus, controllers from outside the EU who process personal data inside the EU must nevertheless comply with this directive. EU member states set up supervisory authorities whose job is to monitor data protection levels in that state, and to advise the government about related rules and regulations, and to initiate legal proceedings when data protection regulations are broken. All controllers must notify their governing authority before commencing any processing of personal information, and such notification prescribes in detail what kinds of notice is expected, including name and address of the controller or representative, purpose(s) of the processing, descriptions of the categories of data subjects and the data or categories of data to be collected, recipients to whom such data might be disclosed, any proposed transfers of data to third countries, and general description of protective measures taken to ensure safety and security of processing and related data.

Next definition

EU-US Privacy Shield

Margaret Rouse, WhatIs.com

EU-US Privacy Shield is a framework for adherence to E.U. data protection laws for companies that deal with the private data of European Union citizens that is transferred to the United States. Privacy Shield replaces Safe Harbor within the U.S.

The legal privacy framework provides assistance with privacy policies for companies in either country handling private data of E.U. citizens. It also offers legal remedies for E.U. citizens' privacy complaints.

US companies dealing with data from E.U. individuals must apply to the U.S. Department of Commerce for self-certification. Members of the EU-US privacy shield framework are required to state their adherence to the Privacy Shield Principles, making the commitment enforceable under law.

The members submitting to the framework must provide an independent system for complaint and dispute resolution and present links to Data Protection Authorities (DPA) and the U.S. Department of Commerce and include these complaint processes in their online privacy statements. The Privacy Shield framework includes mandated time frames for responses to individual and E.U. Data Protection Authority complaints.

The agreement represents cooperation between EU DPA, the Department of Commerce and the FTC. As stated by the Director of U.S. National Intelligence, the new framework bulk gathered info from E.U. citizens is only used in specific circumstances. Previously, international Safe Harbor privacy practices covered the trans-Atlantic transfer of private data.

Next definition

In this e-guide

Privacy and Electronic Communications Regulations (PECR)

Margaret Rouse, WhatIs.com

Privacy and Electronic Communications Regulations (PECR) is an implementation of the European Union (EU) e-Privacy Directive in the United Kingtom.

PECR regulations restrict the processing and sharing of personal traffic data and location data and provide for access to users' personal data in the interest of national security. The information commissioner has the power to audit the measures taken by a provider of public electronic communications services to comply with personal data breach notification and recording requirements.

The main changes for the 2012 revision relate to new rules for websites using cookies, or similar technologies, as well as new powers that allow the information commissioner to fine organizations up to Â£500,000 for serious breaches of the regulations. The PECR cookie rules now demand website owners get consent from visitors before using cookies. This is in addition to the existing requirement for websites to provide information about their cookie usage. The cookie rules apply to any means of storing information or

gaining access to information stored on a user's device, except for where the storage or access is vital for a service requested by the user. The latest PECR rules also require communications providers to set up procedures for responding to requests for access to users' personal data for national security and law enforcement purposes.

Next definition

In this e-guide

Privacy impact assessment (PIA)

Margaret Rouse, WhatIs.com

A privacy impact assessment (PIA) is a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system.

A privacy impact assessment states what personally identifiable information (PII) is collected and explains how that information is maintained, how it will be protected and how it will be shared.

A PIA should identify:

- Whether the information being collected complies with privacy-related legal and regulatory compliance requirements.
- The risks and effects of collecting, maintaining and disseminating PII.
- Protections and processes for handling information to alleviate any potential privacy risks.
- Options and methods for individuals to provide consent for the collection of their PII.

Under the E-Government Act of 2002, federal agencies are required to conduct privacy impact assessments for government programs and systems that collect personal information online. Federal agency CIOs, or an equivalent official as determined by the head of the agency, are responsible

for ensuring that the privacy impact assessments are conducted and reviewed for applicable IT systems. The Act also mandates a privacy impact assessment be conducted when an IT system is substantially revised. Federal agencies such as the U.S. Department of Homeland Security and the Department of Health and Human Services offer guidance for writing PIAs, such as providing blank privacy impact assessment templates to assist and facilitate their development.

Next definition

In this e-guide

Data breach

Margaret Rouse, WhatIs.com

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

The most common concept of a data breach is an attacker hacking into a corporate network to steal sensitive data. However, not all data breaches are so dramatic. If an unauthorized hospital employee views a patient's health information on a computer screen over the shoulder of an authorized employee, that also constitutes a data breach.

A number of industry guidelines and government compliance regulations mandate strict governance of sensitive or personal data to avoid data breaches. Within a corporate environment, for example, the Payment Card Industry Data Security Standard (PCI DSS) dictates who may handle and use sensitive PII such as credit card numbers, PINs and bank account numbers in conjunction with names and addresses. Within a healthcare environment, the Health Insurance Portability and Accountability Act

(HIPAA) regulates who may see and use PHI such as name, date of birth, Social Security number and health history information.

If anyone who is not specifically authorized to do so views such information, the corporation or healthcare organization charged with protecting that information is said to have suffered a data breach. If a data breach results in identity theft and/or a violation of government or industry compliance mandates, the offending organization may face fines or other civil or criminal prosecution.

Next definition

In this e-guide

Personally identifiable information (PII)

Margaret Rouse, WhatIs.com

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

PII can be sensitive or non-sensitive. Non-sensitive PII is information that can be transmitted in an unencrypted form without resulting in harm to the individual. Non-sensitive PII can be easily gathered from public records, phone books, corporate directories and websites.

Sensitive PII is information which, when disclosed, could result in harm to the individual whose privacy has been breached. Sensitive PII should therefore be encrypted in transit and when data is at rest. Such information includes biometric information, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers.

Next definition

In this e-guide

Express consent

Margaret Rouse, WhatIs.com

Express consent is permission for something that is given specifically, either verbally or in writing.

Express consent contrasts with implied consent, which is an assumption of permission that is inferred from actions on the part of the individual. The terms are often heard in relation to email marketing campaigns and anti-spam legislation. Express consent is generally valued more highly than implied consent, and marketers are often less restricted when email recipients have opted-in to receive their mailings.

Best practices for email marketing include asking recipients specifically to consent to mailings and requiring double opt-in procedures (such as replying to an email or signing up online and also clicking a follow-up link to confirm). Marketers should provide the name of the party requesting permission and the company's name, address website, phone number and physical / postal addresses. It's also crucial to included a functional unsubscribe link.

See also: permission marketing, unsolicited bulk email (UBE)

Implied consent

Margaret Rouse, WhatIs.com

Implied consent is an assumption of permission to do something that is inferred from an individual's actions rather than explicitly provided.

In the context of commercial email and text messages, for example, implied consent may be assumed by the senders because the recipient purchased a product from the sender's website or volunteered with the sender's charitable organization recently.

Implied consent is a fairly broadly-applied legal concept. Here are a few examples in other contexts:

- Drivers are assumed to consent to blood alcohol testing. The inference is that the driver understands that driving under the influence is illegal and that they may be subject to testing.
- If an individual rolls up their sleeve for an injection or to have their blood pressure tested, they are assumed to have given consent and have no legal grounds to claim it was done against their will.
- In court, if an individual fails to object to a line of questioning within a reasonable time span, implied consent is assumed and they will not be able to object to it in the future.

Implied consent contrasts with express consent, which is explicit verbal or written permission. Anti-spam regulations, such as CAN-SPAM and CASL, differentiate between implied consent and express consent. As a rule, email senders have much greater latitude if recipients have explicitly consented to receive their mailings.

See also: permission marketing, opt-in email, unsolicited bulk email (UBE)

Next definition

In this e-guide

Privacy policy

Margaret Rouse, WhatIs.com

A privacy policy is a document that explains how an organization handles any customer, client or employee information gathered in its operations.

Most websites make their privacy policies available to site visitors. A privacy page should specify any personally identifiable information that is gathered, such as name, address and credit card number, as well as other things like order history, browsing habits, uploads and downloads. The policy should also explain if data may be left on a user's computer, such as cookies. According to best practices, the policy should disclose if data may be shared with or sold to third parties and if so, what the purpose is.

There is no concensus as to whether or not privacy policies are legally binding and no consistency in enforcement. In the United States, the Federal Trade Commission (FTC) promotes enforcement of existing laws and industry self-regulation. Generally for the FTC, data breaches are not sufficient for legal action if there is no loss of money associated with the breach.

In this e-guide

The European Union's Data Protection Directive has confronted companies such as Google about privacy changes that went contrary to E.U. law, threatening sanctions on the massive company.

Often, the first statement found in an online privacy policy is one to the effect that, by visiting the web page (which you are doing if you're reading the policy), you agree to the details of the site's privacy policy.

In this e-guide

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 120+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively – and faster – than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; Fotalia