The General Data Protection Regulation (GDPR): A Practical Overview

1.1 Title Screen

<music only>

(onscreen text that isn't in the narration appears in italicised blue)
How are you protecting personal data?
When can you process personal data?
What are data subject rights?
Across the EU, the GDPR protects personal data.
What does that mean for your organsation?
Let us show you.

Privacy Core® e-learning
POWERED BY ONETRUST, DEVELOPED BY THE IAPP

The GDPR: A Practical Overview

1.2 Why Data Protection Laws?

Personal data has become a valuable commodity, due to recent advances in technology and processing. To prevent personal data from being misused, many countries around the world have passed data protection laws.

To create common ground for the various European data protection laws and policies, and address the growing concerns of individuals, the EU passed the Data Protection Directive in 1995. However, each member state implemented the Directive in its own manner, and the differences continued to affect trade.

In an effort to minimise the different implementations and provide a more uniform law, the EU voted in 2016 to replace the Directive with the General Data Protection Regulation (GDPR).

The GDPR applies directly in each member state, which should result in fewer opportunities for different implementations and a more uniform data protection law.

(*EU Reveal*) *European Union, also known as the EU, is an economic and political partnership. The EU emerged after World War II as a way to promote economic co-operation with the idea that countries that trade with each other are less likely to engage in conflict.*

1.3 What is the GDPR?

The GDPR is a framework for fair and responsible handling of personal data.

The GDPR applies to any organisation that:

- Is established in the EU
- Offers goods or services to individuals in the EU; or
- Monitors the behaviour of individuals in the EU

It holds every organisation to the same basic data protection standards no matter where the organisation is based. This means that even an organisation operating out of Australia or the United States targeting the EU market must comply with the GDPR for its personal data processing, relating to its EU operations or business.

1.4 Objectives

To ensure compliance with the GDPR, your organisation has policies in place to guide the processing of personal data. To better understand those policies and the GDPR, you will need to know the answers to the following questions:

- What are the key terms used in the GDPR?
- What are the central principles of the GDPR?
- What do you need to know about processing personal data under the GDPR?

1.5 Introduction to Personal Data

The GDPR is concerned with the processing of personal data. So, what is personal data?

Under the GDPR, personal data is any information relating to an identified or identifiable natural person. This means the GDPR only applies to data about individual human beings, not data about companies, governments or other organisations. Trade secrets or confidential government information may need to be protected but they are not personal data and are not covered under the GDPR.

1.6 Introduction to Personal Data, Part II

Personal data is information about people, such as: names; location information like a home address or current GPS position; a mobile phone number; email address; mobile device ID and IP address. While not identifying an individual, some data, such as browsing history or geolocation, *relate* to a specific individual which makes it personal data. Even a job title can be personal data.

Personal data can relate to an individual directly or indirectly. For example, if you are describing someone to a co-worker and you say, “Mateo Picard in accounting”, you have directly identified him. If, however, you say, “The tall young man with short hair in accounting”, you have indirectly identified him. Information that allows you to single someone out, such as an online profile that doesn’t include either an image or name but includes interests and habits, (*onscreen: list of boxes, some ticked off, showing various interests – art, photography, music, travel, science, technology, sports, video games,*

cooking, outdoors, health, cars; then onscreen ID of jallman88, Valencia, Following: 1,293, Followed: 592, See friends list) is also a type of indirect identification and is considered personal data under the GDPR.

1.7 Combining Personal Data

One piece of data by itself may not be enough to relate to an identified individual *(Onscreen: Anna)*; there may be several people in a database with the same name, multiple individuals living at one address, several people sharing an IP address, and so on.

To identify an individual correctly, organisations combine data that comes from many different sources, including online browsing, social media sites, shopping preferences and surveys. Much of this data may seem non-specific when taken alone, but as that data is combined, the identity of the individual may become clear.

1.8 Special Categories and Sensitive Data

Some types of personal data are considered more sensitive than others and are classified as special categories of data under the GDPR. These special categories include data about an individual's race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life or sexual orientation; genetic data; and biometric data.

When processing any personal data, organisations must be prepared to provide proof of why they need it and how it is protected. However, because improper use or disclosure of sensitive personal data can have a more significant and negative impact on individuals, organisations may need to comply with stricter requirements when processing it.

1.9 Processing

What does 'processing personal data' mean? 'Data processing' refers to any action an organisation takes with respect to personal data.

Can you identify which of the following situations can be categorised as processing data?

(Interaction) Click Yes or No depending on what you think is processing.

Mateo filling out a paper application then not sending it in (yes/no)
No – if the data is not transferred to the controller, then it is not being processed
Mateo's data being shared from one organisation to another (yes/no)
*Yes – Sharing data with a data processor means that **both** companies are now processing that data*
Mateo filling out an application then submitting it to the organisation (yes/no)
Yes – as soon as a controller receives personal data, it is being processed
Mateo's data in a digital file marked 'Storage' or 'Inactive' (yes/no)
Even data that is being stored and not actively used is being processed
Mateo's details being destroyed from a computer (yes/no)

While data is being destroyed, it is still being processed

(Feedback) An organisation is processing personal data from the moment the data is collected until it is destroyed. This includes collecting, using, adapting, sharing, storing, restricting the use of and destroying personal data. Under the GDPR, even if personal data is just stored in a file unused, that data is being processed.

1.10 Data Subject, Controller or Processor

The GDPR has specific terms to describe the different parties involved in data processing. Data subjects are the individuals whose information is collected and used by an organisation. Data controllers are those who collect the data and decide how it will be used. Data processors are those hired by data controllers to perform specific tasks.

Can you identify the data subject, data controller and data processor in the following scenarios?

(Drag and drop Interaction)
Jean applies for a credit card through ZYX Bank, which uses Statement Co. to handle sending monthly bills to credit card customers. The bank approves the card and issues one to Jean.
(selections: Jean, ZYX Bank, Statement Co. – drag each to appropriate title: data subject, data controller, data processor)

When WVZTek's business doubled, the CEO hired an outside company to help prepare and deliver each incoming customer's order.
(selections: Outside company, WVZTek, Each customer)

Hanna works or Call Center Inc., which handles customer service calls for Trekkit Chair. She receives a call from Raj Patel and accesses his file.
(selections: Call Center, Inc., Trekkit Chair, Raj Patel)

(Feedback) Data controllers and data processors both use personal data and are subject to the GDPR. However, data controllers are ultimately responsible for the data processors they hire, so your organisation may require additional approval procedures before allowing you to work with a vendor. Your organisation may need to verify whether the vendor will have access to personal data and, if so, take specific steps before working with it. Be certain you know and follow all your organisation's procedures when working with a vendor to avoid creating potential risks.

1.11 Consent

There are many reasons organisations process personal data: to provide services or goods to individuals; for market research or analytics; for public safety; as part of a business relationship; for employment purposes and so on. However, under the GDPR, an organisation must be able to point to a legitimate legal justification to process personal data, such as contract requirements, legal obligations or a data subject's consent.

1.12 Consent Part II

The GDPR is very specific about what qualifies as consent.

- Consent must be expressed clearly.
- Consent is freely given, not compulsory. Organisations can only require individuals to provide personal data or consent to processing that is necessary to deliver the product or service being offered.
- Consent must be in clear, precise language and easily accessible.
- It must be distinguishable from other consent items or check-boxes.
- Silence is not consent.

Be certain that you are familiar with your organisation's consent procedures.

1.13 Data Minimisation and Purpose Limitation

Data controllers have specific obligations under the GDPR when processing personal data. They must be conscious of what personal data they collect and why they are collecting it. Data minimisation means that organisations may collect only the data they actually need for specific business purposes and must destroy or anonymise data once it is no longer necessary for those purposes. Purpose limitation restricts how that data is used to only those purposes for which the data was collected and typically agreed upon by the individual.

1.14 Data Minimisation and Purpose Limitation Interaction

Karl needs to change KCF Interactive's website. Currently, customers who wish to receive monthly email newsletters are asked to provide the following information:
Name, email, street address, city, country, age, gender, mobile number and payment information.
KCF newsletters address customers by name and are often tailored by region, as some products may not be available or may be delayed in some countries. Can you help Karl decide which items are necessary to obtain from customers who want to receive the email newsletter?

(Interaction) Click submit once you've selected the necessary fields.

Newsletter sign up. To be completed in order to receive our monthly newsletter.
(fields to choose from) Name, email, street address, city, country, age, gender, mobile number, payment information

If your organisation collects personal data for its own use, then it is a data controller and must minimise data collection and limit use in much the same way.

1.15 Data Subject Rights

The GDPR sets forth specific data subject rights. Data controllers are obligated to respect those rights, and ensure data subjects can exercise them. Controllers must notify their data processors of any subjects' requests with respect to the data the processors hold, so they can fulfil their obligations as well.

You, as an employee, need to recognise when such a request is made and know your organisation's compliance procedures. Be aware that the GDPR specifically requires authenticating the identity of the data subject properly before complying with his or her request. Never change or release data without following all your organisation's authentication procedures. You don't want to release personal data to the wrong person.

1.16 Data Subject Rights Interaction

Do you think you know what rights data subjects have? Let's test your knowledge. Mark each of the following requests YES if you must comply, NO if you do not have to comply or IT DEPENDS if more details are needed.

(Interaction)

Caller asks how your organisation plans to use his personal data. (yes/no/it depends)

Data subject have the right to know how their data is being used. Most organisations use a privacvy notice to comply with the GDPR's requirement that data controllers give clear and transparent details as to how personal data is being processed.

Caller asks to have a printout of her file. (yes/no/it depends)

Data subject have the right to see and have a copy of the personal data the controller has about them.

Caller informs you that her house number is incorrect and asks that it be changed.

If any of the data is incorrect or incomplete, the data subject has the right to request that it be corrected or completed. Data controllers must reasonably ensure that the data they process is accurate.

Caller cancels account and requests that his data be deleted.

This is also referred to as the 'right to be forgotten'. Data subjects have the right to have their data deleted in certain circumstances, including when the controller has relied on the subject's consent to process data and the subject withdraws that consent. However, there are circumstances where controllers may not be required to comply with this request, so data deletion should only be done by authorised employees. Make sure you know your organisation's data deletion and retention policies before complying with a request.

Caller says the data you hold about her, obtained from a third party, is incorrect, so she does not want you to process it. The individual and the third party provide conflicting details.

You should restrict the processing of her personal data while you verify the accuracy of the contested data.

Caller asks to be taken off mailing lists and for his data to be removed from shared marketing lists.

Data subjects have the right to object to personal data being processed for direct marketing. Controllers must respect this right and stop the marketing.

Caller informs you she is transferring her account to a competitor and wants her records transferred to them.

In certain circumstances, data subject have a right to obtain a copy of the data and to have it transferred to a competitor in a standard, machine-readable format.

(Feedback) The GDPR places time limits on when organisations must meet their obligations with respect to data subject rights, so be certain to address these requests promptly in accordance with your organisation's policies and procedures. If you are unfamiliar with your policies, or have questions, contact the appropriate person in your organisation.

1.17 Data Security

Data controllers must keep data safe and confidential the entire time it is being processed. Organisations should protect personal data by restricting access and can reduce risk by making data less identifiable.
Data can be encrypted; that is, changed from a readable format into a random string of symbols that cannot be read without a decryption key. This protects data from being accessed or used for unauthorised purposes.

Data may also be pseudonymised. This method requires the removal of direct identifiers—and sometimes also indirect identifiers—from a database. For this method to be effective, an unauthorised person should not be able to connect the data that remains to a specific individual. The removed data must be kept separate from the pseudonymised data to prevent unauthorised use.

1.18 Security Breach Notification

A data breach under the GDPR is where personal data is accidentally or unlawfully destroyed, lost or altered; or where there is unauthorised disclosure or access to it. In some situations, data controllers must ensure that they notify the appropriate supervisory authority within 72 hours. In addition, notice may need to be given to data subjects affected by the breach.

If you think there may be a data security issue, such as an encryption key given to an unauthorised person, a lost computer or file, a stranger on the premises or data being

transmitted to the wrong party, report the situation right away. Time matters when preventing or addressing a potential breach.

1.19 Privacy by Design

The GDPR requires organisations to consider privacy throughout all processing of personal data. This is often referred to as privacy by design. Privacy by design is the process of considering privacy from the moment a product, service or business effort is being designed or planned, throughout its development and after it is put into place.

Organisations are required to demonstrate and prove they implement privacy by design. To fulfil this obligation, you may be required to document privacy considerations, risks and mitigating solutions as part of the project development process.

1.20 Accountability

An organisation may not only have to provide proof that it implements privacy by design but may also need to provide proof of compliance with other aspects of the GDPR. To meet this accountability requirement, you may need to document what data you have, how it is being used, with whom it is being shared, where it is stored and for how long, and when and how data was destroyed. Keeping accurate records helps your organisation respond promptly.

1.21 Summary

Information about people is valuable to your organisation and needs to be managed as carefully as you would any other asset. You need to handle the personal data of others in the same way you expect organisations to handle yours. The GDPR provides organisations with the minimum requirements to meet those expectations.

By understanding data subjects' rights and organisations' obligations, and following your organisation's policies and procedures, you help your organisation comply with the GDPR, avoid regulatory sanctions and maintain consumer trust.

1.22 Assessment

1. *A large retail chain recently opened a new store. At the grand opening, town residents were invited to enter a drawing for a €500 store credit. To enter, residents had to provide their names, addresses, and contact phone numbers. This data would be entered into the retail chain's database for future use. Peter decided he preferred his old store, so did not give the new store his information. Leonard liked the new store and entered the drawing.* ***Who is the data subject?***

Retail chain
Peter
Leonard

There is no data subject in this example

2. ***What term would you apply to the retail chain?***
   Data processor
   data controller
   data subject
   none of the above

3. *Data processors determine how personal data may be used. T/F*

4. *Which of the following are reasons an organisation should provide a privacy notice to customers and clients? (Select all that apply)*
   To inform individuals how their personal data will be used
   To comply with the law
   To provide transparency about sharing of personal data
   To prevent third parties from using your customers' personal data

5. *When a customer contacts you to request a change of address, what is the first thing you should do?*
   Change address
   Authenticate customer identity
   State the customer's current address for confirmation
   Deny request

6. *Data subjects have the right to request that you remove them from mailing lists. T/F*

7. *With which of the following requests from data subjects does an organisation need to comply? Select all that apply, then click submit.*
   Request to correct the spelling of data subject's name
   Request to forward details to the data subject
   Request to meet customer in-person to review collected data
   Requests made by individuals who cannot be verified

8. *Data controllers must destroy or anonymise data once it is no longer needed for its specified purpose or for legal compliance. T/F*

9. *Privacy by design means taking privacy concerns into consideration: (Select all that apply then click Submit)*
   While a project is being developed
   Once a project is complete
   During the planning phase of a project
   When a project is being updated

1.23 Results

1.24 Congratulations

Congratulations! You have completed the unit.