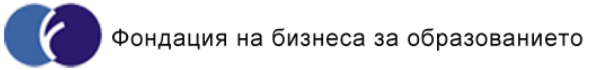
DiGiPort

Protecting personal data and privacy - GDPR

antic PAYS BASQUE

Co-funded by the Erasmus+ Programme of the European Union



Partnership

Co-funded by the
Erasmus+ Programme
of the European Union

Table of Contents

DiGiPort

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

When you are an artist in any profession, at some point you find yourself collecting personal data from clients, future clients, future collaborators, admirers etc.

This personal data may be recorded in a notebook such as on a computer or may be collected automatically by online forms for example. These personal data can be written in a notebook as well as on a computer or can be collected automatically by online forms for example.
This learning module provides a better understanding of how to protect personal data and privacy in digital environments ? How to use and share personally identifiable information while being able to protect oneself and others from damages ? Use "Privacy policy" in digital services to inform how personal data is used ? And thus be in compliance with the GDPR regulation.

Co-funded by the Erasmus+ Programme of the European Union

Learning outcomes

UNDERSTAND The GDPR and its key concepts
Evolution of data protection
Definition of the processing of personal data
Who does the GDPR apply to?

KNOW Data protection principles
The eight golden rules for the processing, the data, the security and transparency : Purpose of the processing - legal compliance of the processing - Minimisation of data - Particular protection of certain data - Limited data retention - Security obligation - Transparency with respect to stakeholders - Individuals' rights to their data

Co-funded by the Erasmus+ Programme of the European Union

Learning outcomes

03

DEFINE Actors' responsibilities
New accountability logic - sharing of responsibilities - Specific responsibilities of sub-contractors - Sanctions and appeals -

04

SET UP The DPO and compliance tools
The DPO and the data register - Data breach notification - The data protection impact assessment - Code of conduct and certification

Co-funded by the Erasmus+ Programme of the European Union

Theory

DiGiPort

01

Evolution of data protection – a little history to better understand

1978

The beginnings: **in France, with the** Law "Informatique et Libertés"

24 October 1995

European directive 95/46/EC adopted with the following objectives
- the protection of individuals and the free circulation of data
- to provide a common framework for all EU countries in terms of personal data protection - mandatory to adopt legislation by country + an independent supervisory body

25 May 2018

New European regulation which comes into force in each country - the **RGPD**

Co-funded by the Erasmus+ Programme of the European Union

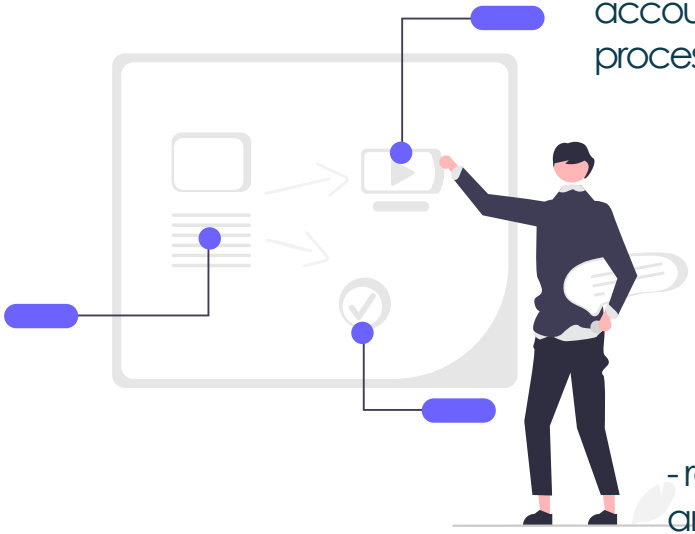
DiGiPort

01

> 3 main principles of the GDPR

- a new logic of accountability of all data processing actors

- the quantitative and qualitative reinforcement of individuals

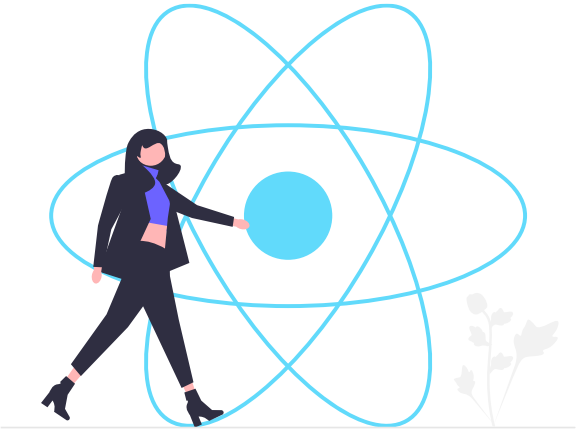


- reinforcement of control and sanction of dedicated structures at national level

Co-funded by the Erasmus+ Programme of the European Union

With the development of dematerialisation, connected objects, algorithms, GDPR guarantees an adequate level of security for the information processed and gives people the possibility to better understand and control the use of their data.

01



Did you know that?

- Personal data is the basis for the development of the digital economy.
- The risks linked to the use of personal data : "95% of smartphone owners can be re-identified by cross-referencing at least 4 of their geographical locations (e.g. photo metadata)" Source: Arvind Narayanan citing a study by YA de Montjoye - Unique in the Crowd: the privacy bounds of human mobility

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

01

Definition of the processing of personal data

The terms data protection and data privacy are often used interchangeably, but there is an important difference between the two.

Data privacy defines who has access to data, while data protection provides tools and policies to actually restrict access to the data. Compliance regulations help ensure that user's privacy requests are carried out by companies, and companies are responsible to take measures to protect private user data.

Personal data :

- indirectly identifying data: customer number associated with a name

- directly identifying data: surname, first name, photo, email name

- any combination of information that can identify the person: various information on a social network account such as what you like where you live or work etc.

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

01

''processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, 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, deletion or destruction.

Co-funded by the
Erasmus+ Programme
of the European Union

Who does the GDPR apply to?

The GDPR applies to all public or private organisations established in the European Union whose activities are targeted at European residents. This is true whether they process personal data on their own behalf or as a processor.

Conclusion: if you are a freelancer, if you process personal data of European citizens and if your company is based in the EU, you must comply with the RGPD rules!

You are concerned if you collect data from your prospects and clients for yourself. This is also the case if you are involved as a service provider in projects involving the processing of personal data (website development for example).

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

01

Data controller and processor

It is important to understand that The GDPR does not apply to the course of strictly personal activities such as the directory of a phone, the cloud with family photos (domestic exception).

However, the data controller is subject to the GDPR, the cloud, the telephone operator, the manufacturer of the connected speaker etc.

Co-funded by the
Erasmus+ Programme
of the European Union

Data protection principles

8 golden rules summarised in 4 good reflexes to adopt:

1- only collect data that is really necessary

2- be transparent

3- think about people's rights

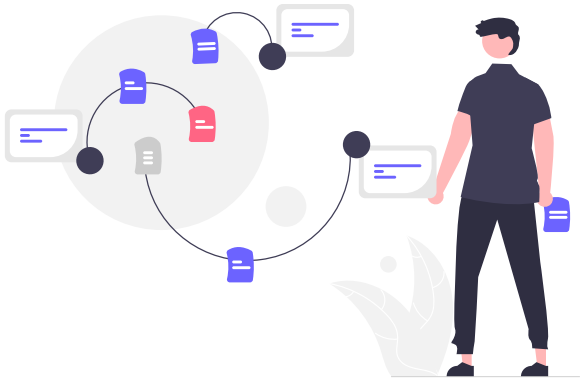
4- secure the data

The legal basis of the processing: A processing operation can only be carried out if it is based on one of the 6 conditions of compliance with the law

Co-funded by the
Erasmus+ Programme
of the European Union

Data protection principles: (see details in Annex 1)

1- Purpose of processing : Personal data collected may only be processed for a precisely defined and legitimate purpose - The purpose defines the link between the data, the processing operations and the bodies that implement them. The purpose defines the link between the data, the processing operations and the organisations that carry them out. It defines the scope of their use.



2- Minimisation of data: Only data that is strictly necessary to achieve the purpose may be collected and processed - Data is relevant if it has a direct link with the purpose of the processing.

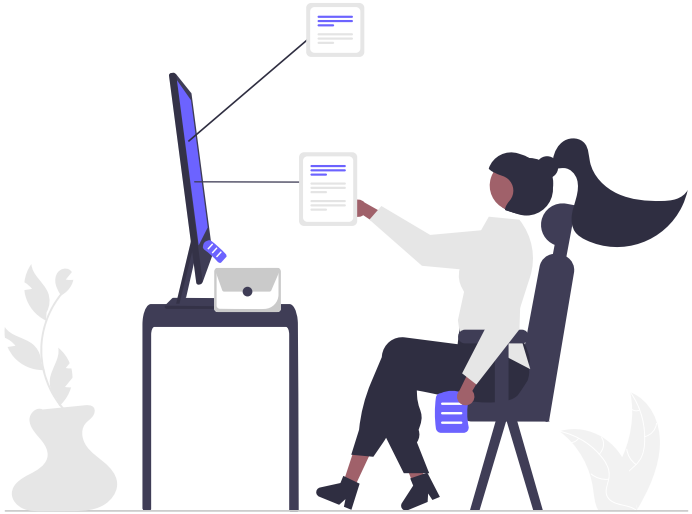
3- Special protection of sensitive data: Sensitive data may only be collected and processed under certain conditions

Co-funded by the Erasmus+ Programme of the European Union

4- Limited data retention: Data must be archived, deleted or anonymised as soon as the purpose for which it was collected has been achieved: - Security obligation (In view of the risks, measures must be implemented to ensure the security of the processed data)

5- Transparency: Individuals must be informed about the use of their data and how to exercise their rights

6- Individuals' rights: Individuals have a number of rights that allow them to retain control over their data.



Co-funded by the
Erasmus+ Programme
of the European Union

Actors' responsibilities

> New accountability logic : In concrete terms, all actors involved in a processing operation will have to implement and update both technical and organisational measures to ensure compliance with the main principles of the Regulation at all times.

- minimisation

- limited storage time

- security

- etc.

Co-funded by the
Erasmus+ Programme
of the European Union

Depending on the context, they must appoint a data protection officer, keep a register of processing activities, apply a confidentiality policy, carry out a privacy impact assessment, etc.

The mandatory tools
- the register of processing activities
- the data protection officer
- in some cases impact assessment for certain processing operations
- data breach notification under certain conditions.

Co-funded by the
Erasmus+ Programme
of the European Union

> sharing of responsibilities :

1/2
Where two or more controllers jointly define the purposes and means of the processing, they are joint controllers of the processing operation, they are joint controllers. In this case, the joint controllers must define their respective obligations by contract.

- Specific responsibilities of sub-contractors : Organisations that process personal data on behalf of their clients have responsibilities defined by the GDPR.

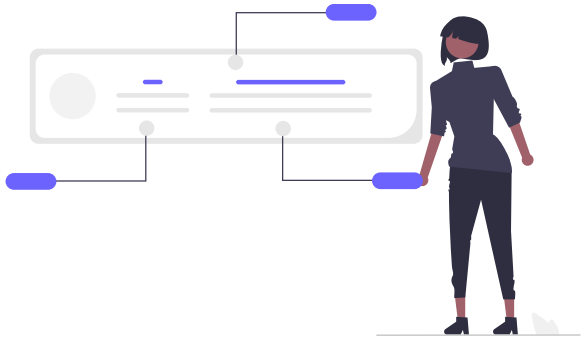
-> IT service providers (hosting, maintenance ..)
-> Digital service companies or formerly IT service and engineering companies (SSII) which carry out data processing
...

Co-funded by the
Erasmus+ Programme
of the European Union

2/2

-> Companies offering remote monitoring services
-> Marketing or communication agencies that process personal data on behalf of their clients
-> Payroll service providers

Data controllers, for their part, must pay attention to the conditions under which they call on a service provider: the protection of data subjects must be ensured throughout the outsourcing chain.



Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

03

> Sanctions and appeals

REMEDIES: Complaints to a supervisory authority.

Any person who considers that the processing of personal data concerning him or her constitutes a breach of the GDPR may lodge a complaint with a supervisory authority.

This can be the authority in the Member State .
- where the individual's habitual residence is located
- where his place of work is located
- where the breach occurred.

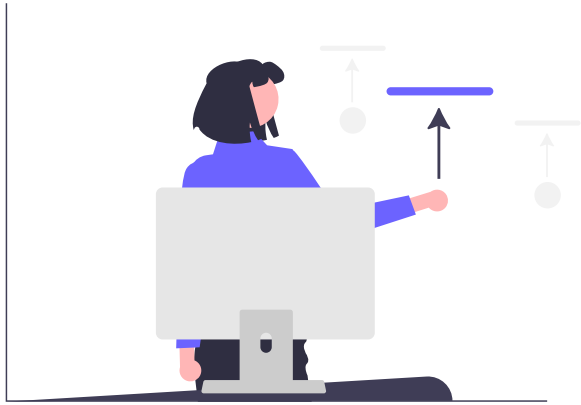
Co-funded by the
Erasmus+ Programme
of the European Union

Graduation of administrative fines
The maximum amount of administrative fines differs according to the seriousness of the breach.

The GDPR provides in Article 83 that the country's independent body may decide to impose a fine of up to .

- either 10 million euros or 2% of the worldwide turnover

- 20 million or 4% of worldwide turnover



Co-funded by the
Erasmus+ Programme
of the European Union

The DPO and compliance tools

> The DPO – internal or external full or part-time - it can be shared. Must be trained but no certification required.

His/her tasks .

1-Inform and advise the organisation
2-Check the compliance
3- Act as an interface between his/her organisation, the national body dedicated to the GDPR and the persons concerned.

The DPO is mandatory if it is a public service, or a private company that processes a lot of personal data, or an organisation that processes sensitive personal data. The DPO is not liable for any breach.

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

04

> The data register

A register of processing activities must be set up by every controller or processor.
It is an essential tool in compliance operations, it allows to identify It is an essential tool in compliance operations, making it possible to identify processing activities, and at the same time, to have an overview of what is done with personal data in organisations.

The GDPR requires the register to be in written form. Its format is free and can be in paper or electronic form.

Co-funded by the
Erasmus+ Programme
of the European Union

The register is an inventory and analysis document, which must reflect the reality of the processing operations and make it possible to identify precisely

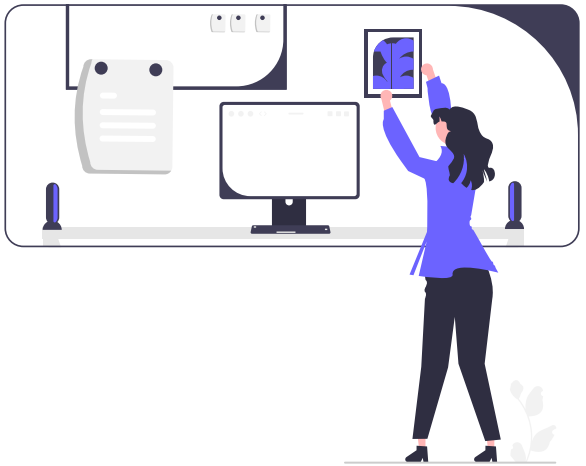
- the stakeholders (representative, subcontractors, joint controllers, etc.) involved in the data processing

- the categories of data processed what the data are used for

- who accesses the data and to whom it is communicated

- how long the data is kept

- how it is secured



Co-funded by the
Erasmus+ Programme
of the European Union

Companies with less than 250 employees benefit from a derogation. They are allowed to enter only the following processing operations in the register

- recurrent processing operations (e.g. payroll management, management of customers, prospects and suppliers, etc.)

- processing operations likely to involve a risk to the rights and freedoms of individuals (e.g. geolocation systems, video surveillance, etc.)

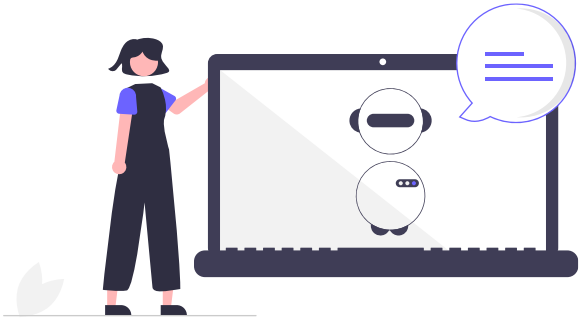
- processing operations involving sensitive data (e.g. health data, offences, etc.).

Co-funded by the
Erasmus+ Programme
of the European Union

Examples of data breaches :

- A hacker accesses the source code of a website and overwrites the display of the payment form in order to retrieve the bank details entered while allowing the payment to go through so that neither the user nor the website publisher is aware of the theft.

- An organisation specialising in the treatment of patients with serious illnesses fails to back-up more than a thousand people when sending out a survey.



Co-funded by the
Erasmus+ Programme
of the European Union

Notification deadlines

If the incident constitutes a risk to the privacy of the individuals concerned,
the organisation must notify the relevant body in your country where your organisation is registered

> Code of conduct and certification

Codes of conduct and certifications are vehicles for compliance. The GDPR calls for the development of codes of conduct and/or certification schemes to to facilitate the application of the provisions of the Regulation by controllers and processors. and processors.
They are aimed at all professional audiences, for both small and large companies.

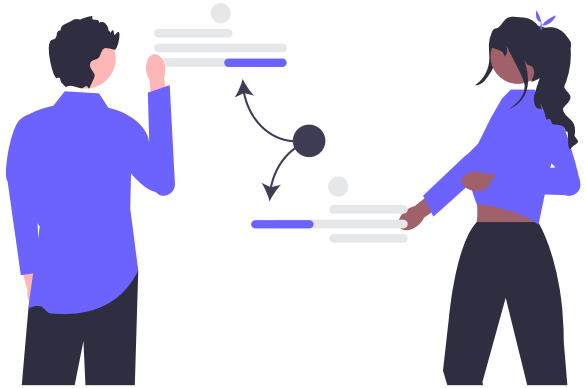
Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

04

Codes of conduct are useful aids to compliance for organisations as they are tailored to their sector of activity.

The certification of products, processes, services and delegate competences is a significant asset for an organisation in its relations with with its partners or with the persons concerned by the data processing data processing in question.



Co-funded by the
Erasmus+ Programme
of the European Union

Examples/Good Practices

DiGiPort

https://www.blogdumoderateur.com/conformite-rgpd-bonnes-pratiques/
Extract from an article (FR) by an RGPD specialist

Jérôme de Mercey, co-founder of Dastra and former CNIL agent, shares his advice for companies.

(…) **Which departments are most affected within organisations?**
The sales/marketing department will be in the front line due to the commercial prospecting activity, which can generate numerous complaints from prospects who are increasingly alert to the use of data. The HR department is historically very affected because the data processed is very sensitive and often requested in the context of disputes with employees.

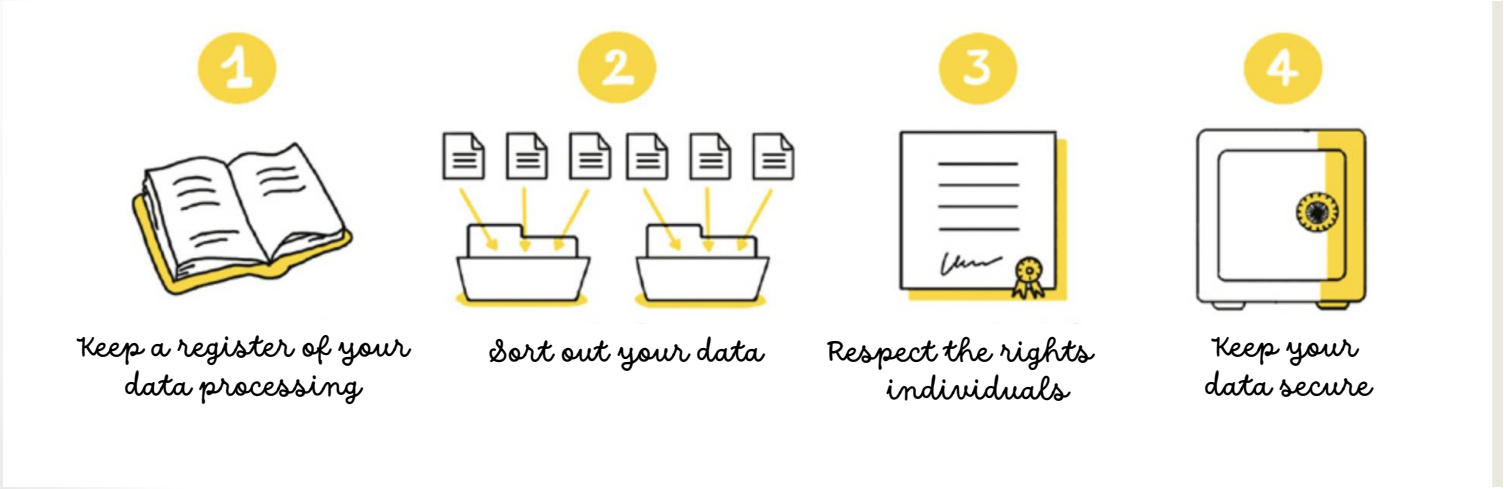
Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

Examples/Good Practices

GDPR - Take Action in Four Steps (Source : https://www.cnil.fr/fr/rgpd-par-ou-commencer)



Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

Examples/Good Practices

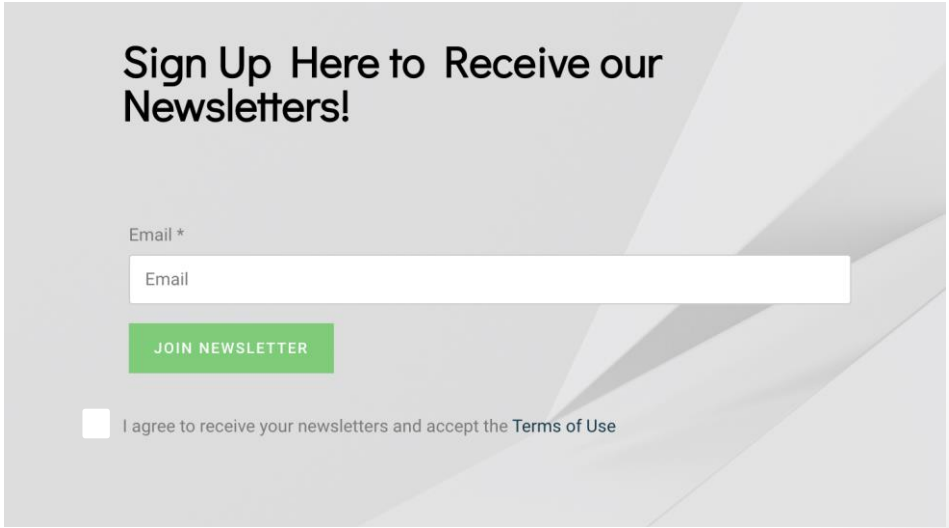
Article with best practices

Data Protection Policy: 9 vital things and 3 Best Practices
https://cloudian.com/guides/data-protection/data-protection-policy-9-things-to-include-and-3-best-practices/

An exemple – Website of DIGIPORT project

Insert a checkbox for consent in your contact forms or newsletter subscriptions

–>>>>>



Examples/Good Practices

DiGiPort

https://www.blogdumoderateur.com/conformite-rgpd-bonnes-pratiques/
Extract from another article (FR) by an RGPD specialist

Jérôme de Mercey, co-founder of Dastra and former CNIL agent, shares his advice for companies.

(…) **How to set up a good cookie management on a website? What are your recommendations in this area?** Cookies are a complex subject because it doesn't stop at just cookies. You also need to see everything that passes through the network and be able to understand the purpose and recipients of each request. So you need to ask the 'knowers': the website development teams and challenge them on what is being deposited, read and requested when browsing the website. You must then translate these behaviours and qualify them with regard to the regulations, set up a cookie banner and ask for the consent of Internet users if this is justified. The easiest way to do this is to use a specialised tool or to get advice on how to implement this banner. You can also read the CNIL guidelines on the subject which are very explicit. (…)

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

Examples/Good Practices

12 good Practices

https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

1.Formalising management commitment

The first and essential step is to formalise the commitment of management. Indeed, it is the CEO who is responsible for the processing. He therefore represents the company in the event of legal action, whether it is an SME or a large company.

2.Communicating the content of the RGPD

It is then necessary to disseminate the information on the regulation within the company, in a clear and comprehensible manner, in order to raise awareness among employees.

Co-funded by the Erasmus+ Programme of the European Union

Examples/Good Practices

DiGiPort

12 Good Practices
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

3.Train employees
Once the communication stage has been completed, the company can then undertake the training of its employees and ensure that the various documents referring to data processing (contracts, HR documents) are updated.

4.Keep a register of processing operations
The company must also maintain a register of processing activities, which is an obligation for the controller. In case of processing operations requiring regular monitoring or big data processing, it must appoint a Data Protection Officer ("DPO"), with the possibility of using an external DPO if necessary.

Examples/Good Practices

12 Good Practices
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

5.Conduct privacy impact assessments
The company must study the impact on privacy of the various processes carried out on the personal data of its customers and employees.

6.Establish a processing audit plan
The company must also implement a processing audit plan to ensure that processing remains within the framework authorised by the regulations. Particular vigilance is required for data transfers outside the European Union.

Co-funded by the
Erasmus+ Programme
of the European Union

Examples/Good Practices

DiGiPort

12 Good Practices
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

7.Enabling the reporting of breaches
The company must put in place a procedure to allow anyone to report personal data breaches.

8.Be vigilant in ensuring the exercise of rights
Companies should be particularly careful to respect the rights of any individual about whom they hold data, whether customers or employees, such as the right to be forgotten.

9.Monitoring compliance over time
Companies should monitor their overall data protection policy over time.

Co-funded by the
Erasmus+ Programme
of the European Union

Examples/Good Practices

DiGiPort

12 Good Practices
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

10.Checking provider compliance
It is important to assess the compliance of strategic service providers and subcontractors, particularly those who have access to company data. Contracts should be reviewed to include a certain number of mandatory mentions, delimiting the authorised uses.

11.Integrating "Privacy by design" into practices
On a technical level, care must be taken to comply with the RGPD as soon as new application services are designed, by integrating the principle of "Privacy by design" into development practices. This principle also applies if the company has applications developed by a service provider or buys third-party software: it must determine as soon as possible the data collected, the processing, the types of recipients and the retention period.

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

Examples/Good Practices

12 Good Practices
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

12.Provide for a data backup plan
The implementation of a data backup plan is also essential, with appropriate protection measures for personal data. The company is in fact required to ensure reinforced IT security, with an obligation, in the event of a security breach, to notify the CNIL within 72 hours and, in certain cases, the persons concerned. For the time being, only 51% of companies have reported incidents in the last twelve months, which suggests that there is a shortfall in this area.

Co-funded by the
Erasmus+ Programme
of the European Union

Examples/Good Practices

GDPR – Email Marketing -(Source : https://www.cnil.fr/fr/rgpd-par-ou-commencer)

When it comes to email marketing, the following best practices should be in place:
- Do not use a pre-ticked box or other default option.
- Separate the consent statement from the other conditions.
- Word it differently: yes I want to be informed.
- Give the choice to consent to independent processing operations.
- Demonstrate that unsubscribing and exercising various rights is easy.
- Ensure that children's consent is legally obtained.
- Document the obtaining of consent as well as possible (e.g. double opt-in).

Co-funded by the Erasmus+ Programme of the European Union

Quizzes

A FEW QUESTIONS TO SEE WHAT YOU HAVE LEARNED :

1- Is consulting the data in a customer file considered as processing personal data?
Yes-No

2- Does the notion of processing also apply to paper documents?
Yes-No

3- A cultural association usually has its members complete an information members to complete an information sheet. Each form is filed in alphabetical order in a dedicated folder. Does the RGPD apply?
Yes-No

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

Quizzes

A FEW QUESTIONS TO SEE WHAT YOU HAVE LEARNED :

4-"We are happy to count you among our new users! In accordance with the RGPD, if you do not want your email address to be used for commercial prospecting, please send us an email at gdpr@myservice.fr" Is this method of collecting consent valid?
Yes-No?

5- Is the collection of a person's date of birth relevant for any type of processing?
Yes-No?

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

Quizzes

A FEW QUESTIONS TO SEE WHAT YOU HAVE LEARNED :

6- Should the collection of the age range be required or optional?
Optional-Required

7- Does video surveillance have to apply the RGPD?
Yes-No

8- Consent? Must be :
explicit - univocal - revocable - informed?

9- For how many months can the bank card details be archived following an online purchase?
24 months – 15 months - 6 months - 13 months

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

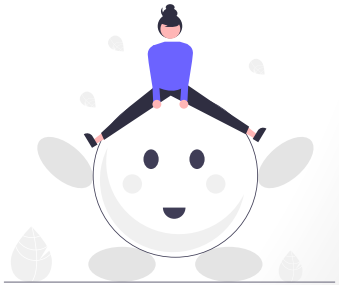
Quizzes

A FEW QUESTIONS TO SEE WHAT YOU HAVE LEARNED :

10-When we talk about data encryption, what are we talking about?
encoding-saving-crypting-dupplicable?

11-Is it possible that the independent RGPD body of each country can issue a tariff fine?
Yes – No?

12- Where does the RGPD apply?
In the EU? - Outside the EU? Everywhere?



Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

References

https://www.cnil.fr/fr/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie

https://www.cnil.fr/en/home

https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

https://globalprivacyassembly.org/

https://www.oecd.org/

https://www.coe.int/en/web/portal/home

Co-funded by the
Erasmus+ Programme
of the European Union

ANNEXES

ANNEX 1 : The legal basis of the processing operation: A processing operation may only be carried out if it is based on one of the 6 conditions of lawfulness (see details in Annex 1)

- Purpose of processing : Personal data collected may only be processed for a precisely defined and legitimate purpose - The purpose defines the link between the data, the processing operations and the bodies that implement them. The purpose defines the link between the data, the processing operations and the organisations that carry them out. It defines the scope of their use.
- Minimisation of data: Only data that is strictly necessary to achieve the purpose may be collected and processed - Data is relevant if it has a direct link with the purpose of the processing.
- Special protection of sensitive data: Sensitive data may only be collected and processed under certain conditions

Co-funded by the
Erasmus+ Programme
of the European Union

ANNEXES

ANNEX 1 : The legal basis of the processing operation: A processing operation may only be carried out if it is based on one of the 6 conditions of lawfulness

- Limited data retention: Data must be archived, deleted or anonymised as soon as the purpose for which it was collected has been achieved: - Security obligation (In view of the risks, measures must be implemented to ensure the security of the processed data)
- Transparency: Individuals must be informed about the use of their data and how to exercise their rights
- Individuals' rights: Individuals have a number of rights that allow them to retain control over their data.

Theory

DiGiPort

ANNEX 1

Data minimisation (Only data that is strictly necessary to achieve the purpose can be collected and processed - Data is relevant if it is directly related to the purpose of the processing - To check whether you are complying with the minimisation principle. To check whether you are complying with the minimisation principle, ask yourself the right questions What is my purpose? What data is essential to achieve this purpose? to achieve this purpose? Do I have the right to collect this data? Have I made a clear distinction between mandatory and optional data?

Special protection of sensitive data (Sensitive data can only be collected and processed under certain conditions - Sensitive data are those which reveal or concern: - racial or ethnic origin - political opinions - philosophical or religious beliefs - trade union membership - health (physical or mental) - sex life or sexual orientation - genetic data - biometric data for the purpose of uniquely identifying a natural person).

Co-funded by the
Erasmus+ Programme
of the European Union

Theory

DiGiPort

ANNEX 1

Limited retention of data (Data must be archived, deleted or anonymised as soon as the purpose for which it was collected is achieved - Organisations must be able to justify the life cycle of the data they hold: needs corresponding to the different phases, data and retention period retained for each).

Security obligation (In view of the risks, measures must be implemented to ensure the security of the data processed - A CONCRETE PASSWORD I A good password must contain 12 characters, of at least 4 different types: lower case, upper case, numbers and special characters. It can be shorter if your account is equipped with additional security features!) - Transparency (Individuals must be informed about the use of their data and how to exercise their rights) - Individuals' rights (Individuals have a number of rights that allow them to keep control of their data).

Co-funded by the
Erasmus+ Programme
of the European Union

Theory

DiGiPort

ANNEX 1

Transparency (Individuals must be informed about the use of their data and how to exercise their rights) - Individuals' rights (Individuals have a number of rights that allow them to retain control over their data - Limitation of processing can only be requested in one of the following 4 situations.

-when the person has exercised his or her right of rectification.
The right to restriction applies while the controller verifies the accuracy of the personal data concerned. the personal data concerned (he has 1 month)

- When the person has exercised his/her right to object.
The right to restriction applies for the time needed to determine whether the legitimate interests of the controller override those of the data subject

Co-funded by the
Erasmus+ Programme
of the European Union

Theory

DiGiPort

ANNEX 1

- when data are about to be deleted while they are still necessary
to the data subject for the establishment, exercise or defence of legal claims

- where the processing is unlawful but the data subject prefers restriction, rather than erasure of the data. The GDPR thus allows data controllers to not to comply with a request)

The GDPR puts in place mechanisms to compensate for the lack of data protection in some third countries. The aim is to ensure that the "protection bubble" follows the data at all times.

Co-funded by the
Erasmus+ Programme
of the European Union