EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova MD 13ENPI JH0317 (MD/29)

The GDPR

one set of rules designed to give *greater control to users over their personal data*

EU Twinning Project Expert: Ian Deguara

Project Activity: 3.5

Date: 22nd May 2018

This project is funded by the European Union

Convention 108

- international treaty to address the rights of individuals to the protection of their personal data.

- on 18th May 2018, the Council of Europe adopted an Amending Protocol to modernise Convention 108 and bring it in line with the GDPR.

Charter of Fundamental Rights of the EU

"*Everyone has the right to the protection of personal data concerning him or her.*"

Regulation (EU) 2016/679

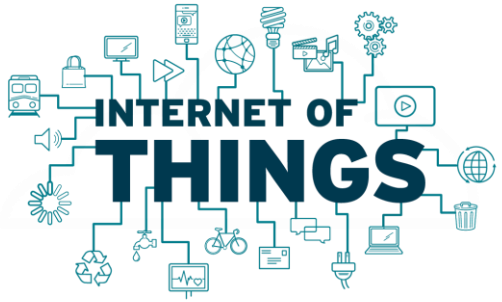
…on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

Timeline


EC presented a proposal for a GDPR
25 January 2012
15 June 2015
Council agrees on a general approach
Council confirms agreement with EP
18 December 2015
8 April 2016
Council adopts position at first reading
GDPR published in the OJ of the EU
4 May 2016
24 May 2016
GDPR enters into force - *transition period of 2 years*
GDPR starts to apply
25 May 2018

Technology and global players radically changed the way personal data is processed

Google™



Microsoft Cloud

skype™

Need for change

Information is becoming increasingly exposed and vulnerable leading to security breaches, hacking or other unlawful action especially in the globalised online environment.

Data protection and privacy challenges are on the increase.

Modernising the existing set of data protection rules was part of the EC's Digital Single Market strategy.

More accountability, consistency and harmonisation across the EU.

Rebalancing of rights in a digital world.

Provide legal certainty for economic operators.

Territorial Scope

Controllers and Processors with an establishment in the EU

Effective and real exercise of activity through stable arrangements (Recital 22)

Controllers and Processors **with an establishment outside the EU**

Offering of goods and services to individuals in the Union – *currency and language used in the MS or mentioning the customers or users who are in the Union (Recital 23)*

Monitoring of data subjects' behaviour which takes place within the Union - *profiling*

Designate a **representative** in the Union UNLESS (1) processing is occasional (2) does not include special categories of data or data relating to criminal convictions and offences (3) public body

Legal basis for processing

1. CONSENT

freely-given, specific, informed and unambiguous indication of the data subject's wishes given by a statement or by a clear affirmative action

Data controller shall be able to demonstrate that the data subject has consented to the processing of data.

Consent shall be presented in a manner which is clearly distinguishable from other matters.

Use of clear and plain language in the information clauses.

Silence, pre-ticked boxes or inactivity should not therefore constitute consent (Recital 32).

The right to withdraw consent (easy to withdraw as to give consent).

Legal basis for processing

In principle, consent is not a valid legal ground in the employment context.

Not freely-given due to imbalance of powers (recital 43):

- dependency resulting from employer/employee relationship where the employee may experience fear or risk of detrimental effects as a result of a refusal.

Exceptions may exist (e.g. filming activity at the workplace).

Conditionality (A.7(4)):

- not desirable (lack of choice) to tie the provision of a contract to a request for consent to process data that are not necessary for the performance of such contract.

Legal basis for processing

Explicit consent is required:

- in certain situations of serious data protection risks
- where a high level of individual control is deemed appropriate.

Explicit consent applies in the following cases:

- processing of special categories of data (A.9)
- data transfers to third countries in the absence of adequate safeguards (A.49)
- automated individual decision making (profiling) (A.22).

Shall be obtained in a clearly separate fashion.

Ideally, in a written statement to remove doubt and potential lack of evidence.

Legal Basis for Processing

2. PERFORMANCE OF A CONTRACT

- Contract of employment
- Rendering professional services to a client (e.g. legal services)
- Mobile telephony services

3. COMPLIANCE WITH A LEGAL OBLIGATION

- Requirement to process data deriving from law e.g. tax legislation, health and safety, national official statistics, law enforcement etc..

4. VITAL INTERESTS OF DATA SUBJECT

5. PERFORMANCE OF A TASK IN THE PUBLIC INTEREST OR OFFICIAL AUTHORITY

Legal Basis for Processing

6. LEGITIMATE INTEREST

- Relying on this legal ground requires a **balancing test** to assesses **the legitimate interest of the controller** or third party **and the impact on the data protection rights of data subjects.**

- Factors to be taken into account include: nature of data, the way data is being processed, the reasonable expectations of the data subject, safeguards applied by the controller.

Examples when to invoke this legal ground to legitimise a processing activity:

- Use of CCTV cameras for security reasons
- Monitoring of employees' mailboxes and internet usage
- Installation of biometric devices for high risk areas
- Sending of marketing material by conventional means (post or telephone)
- In-vehicle tracking devices

Principles

- **Lawfulness, Fairness and Transparency**
- **Purpose Limitation**
- **Data Minimisation**
- **Accuracy**
- **Storage Limitation**
- **Integrity and Confidentiality**

Information to data subjects

Transparency principle (A. 5(1)(a))

Provided at the time the personal data are collected from the data subject (A.13)

Information to include:

- purposes of processing
- the intention to transfer personal data to a third country
- retention period or criteria used to determine that period
- the existence of data protection rights
- the right to withdraw consent
- the right to lodge a complaint with the DPA
- the existence of automated decision making.

Information to data subjects

Using clear and plain language

Easily accessible

Use of layered notices to avoid information fatigue:

- information is not provided in a single notice
- allowing users to navigate through the section they wish to read
- first layer should provide a clear overview of the information *(information which has the most impact on the data subject*)
- clear indication where to find additional information

Incorporating in the architecture a privacy dashboard – a single point where to view privacy information and manage preferences.

Right of access

Data controller shall provide , **within one month**, **a copy** of the personal data undergoing processing together with access to other information:

- purpose of processing
- categories of personal data concerned
- recipients to whom the personal data have been disclosed
- where possible, the envisaged retention period
- the existence of the rights to rectify, erase or restrict processing
- the right to lodge a complaint with the DPA
- the existence of automated decision-making, including profiling, and other meaningful information about the logic involved and envisaged consequences.

Right to data portability

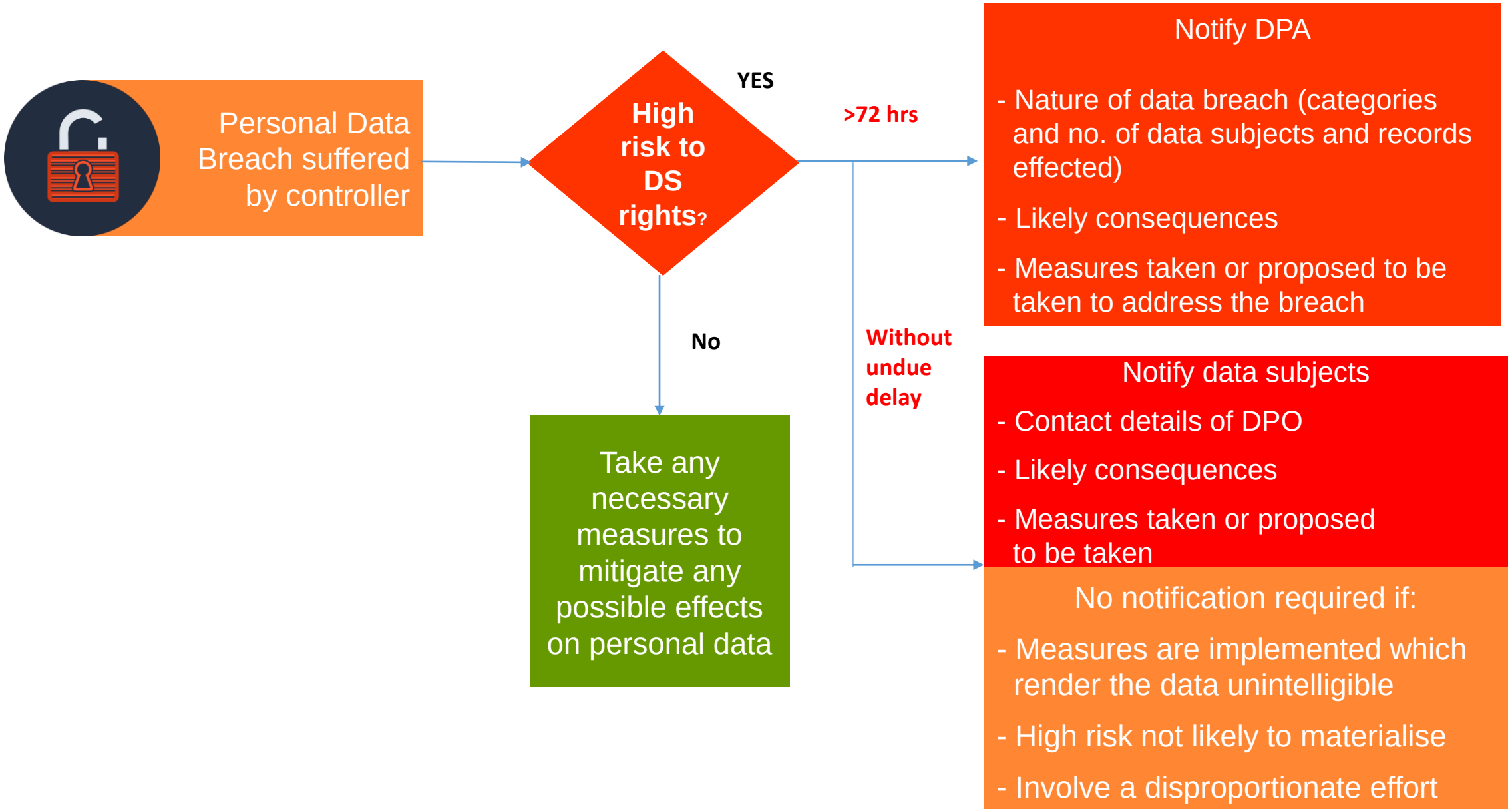
The right to receive personal data which the data subject has provided to the controller:

- **in a structured, commonly used and machine-readable format**.

Applies where processing is based on consent or a contract and by automated means.

Transmitted to the data subject or directly to another data controller without hindrance from the original controller and where technically feasible.

Notification of personal data breach



Security of processing

Data controller shall implement adequate organisational and technical measures to ensure a level of security appropriate to the risk including:

- pseudonymisation, encryption of data, firewalls
- ability to ensure ongoing integrity and resilience of processing systems
- ability to restore the availability of processing systems in a timely manner in the event of an incident
- the regular testing, assessing and evaluating the effectiveness of security measures.

Controllers must assess the risk inherent with the processing activities and take mitigating measures to reduce (if not eliminate) such risks

Have in place the necessary information security policies, including, an incident response plan in case of a data breach.

Cybercrime is one of the fastest growing forms of transnational crime, in particular, ransomware, phishing, malware and brute-force attacks;

Data Protection Impact Assessment

Required to be carried out by the controller in the following cases:

- processing operation is likely to result in high risk;

- systematic and extensive evaluation of data subjects based on automated processing (including profiling);

- processing of special categories of personal data on a large scale.

Prior consultation with DPA required if the Data Protection Impact Assessment indicates that processing involves a high risk to data subjects.

Templates for conducting a DPIA is available on various EU DPA portals.

Data Protection by design and default

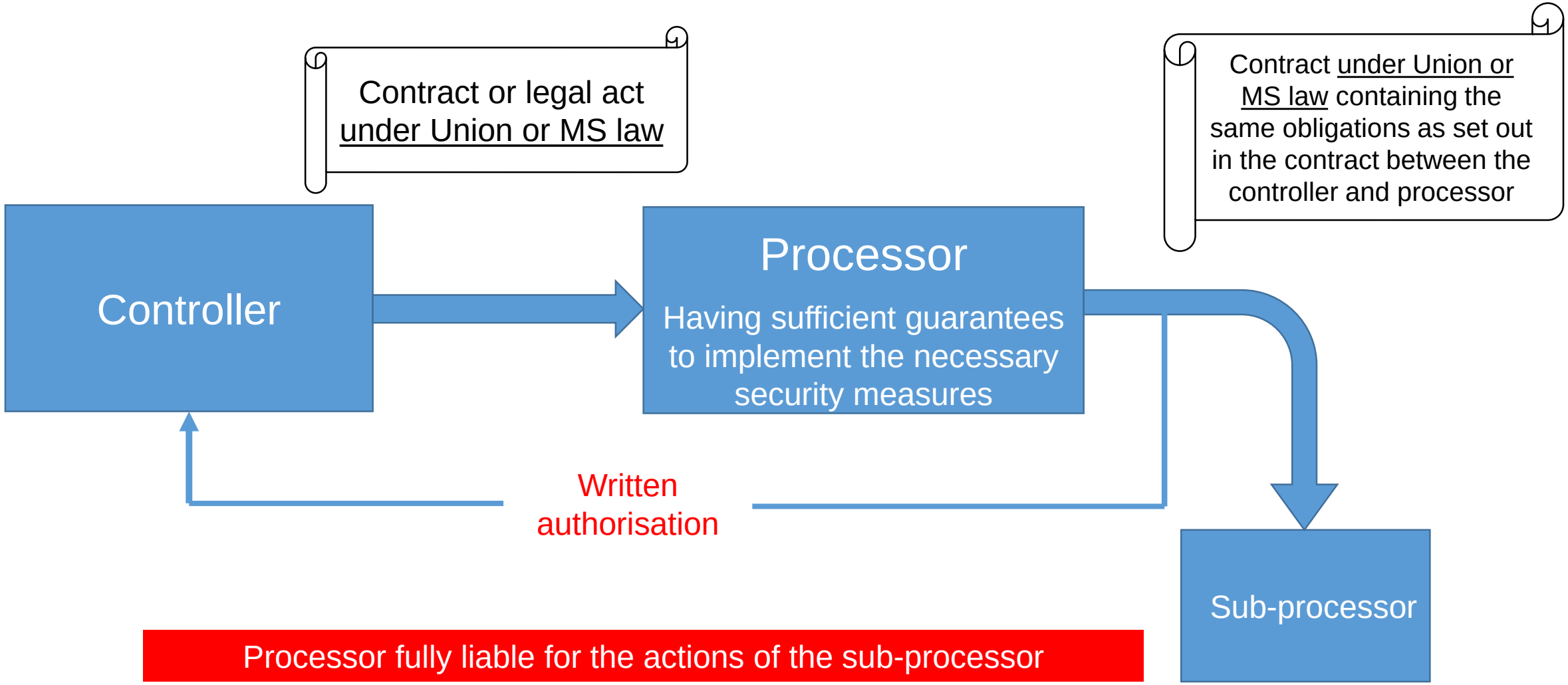
Considerations should be made at an early stage and throughout the lifecycle (e.g. developing IT systems, introducing legislation or measures affecting privacy).

Data protection embedded in the design.

Proactive and preventive privacy-friendly measures (e.g. pseudonymisation, data minimisation).

Default measures tailored to automatically protect individual’s privacy (e.g. preset storage periods, limited data collection and accessibility, user-friendly options).

Controller – Processor relationship



Obligations of a processor

Article 27
Where the processor is not established in the EU and Article 3(2) applies, appoint a representative in the Union unless one of the exceptions under 27(2) is engaged.

Article 31
Cooperate with the supervisory authority.

Article 32
Ensure the security of processing.

Article 33(2)
Notify the controller without undue delay after becoming aware of a data breach.

Article 37
Designate a DPO where applicable.

Chapter 5
Transfer of personal data to third countries or international organisations.

Transfer of personal data to third countries

Legitimised on the following legal grounds without the authorisation of the supervisory authority:

1. Adequacy Decision issued by the European Commission.
2. A legally binding and enforceable instrument between public authorities.
3. BCRs.
4. Standard data protection clauses adopted by the Commission (EU Controller to Non-EU/EEA Controller and EU Controller to Non-EU/EEA Processor).
5. Approved code of conduct or certification mechanism.

With the approval of the SA:

1. Contractual clauses other than those adopted by the Commission.
2. Provisions to be inserted in administrative arrangements between public bodies.

Direct Marketing

OPT-OUT

Promotional messages sent by conventional means (post or telephone) – *Recital 47 GDPR Processing of personal data for marketing purposes may be regarded as carried out for the legitimate interest.*

OPT-IN

Direct marketing messages sent by electronic means (email, SMS, fax, automated calling machine)

Exception - Soft opt-in (opt-out) when data is collected in the context of a sale of a product or service and is used to direct market the organisation's similar products or services. Recipient shall be given the opportunity to object on each message - *Article 13 of the ePrivacy Directive*

Key Messages

Ensure to legitimise the processing on the strength of the proper legal basis.

Consider the capabilities of your systems to ensure, *inter alia*, their ability to:

- handle requests for access, portability, rectification, restriction and erasure
- safeguard the personal data
- detect data breaches
- facilitate the execution of certain requirements e.g. automated deletion.

Key Messages

Develop policies to govern the processing of personal data, *inter alia*, concerning:

- Employee monitoring (email and internet access, vehicle tracking)
- CCTV cameras
- Recruitment process
- Other HR practices - access to employees' email following termination of employment

Place data protection and cyber security at the top of your business priorities.

Key Messages

Employers can rely on legitimate interest when conducting monitoring at the workplace. Lack of information, excessive and/or disproportionate processing constitutes an unjustifiable and intrusive activity.

Conduct an internal audit to identify any gaps in the processes and address them accordingly.

Properly assess your nature of your activities, determine whether you are a controller or a processor and establish whether you need to appoint a representative in the Union.


THANK YOU