

LAURIUS

ANTWERP – BRUSSELS

Preparing for the General Data Protection Regulation

GDPR: COUNTDOWN!

Directive 95/46 EC: objectives & principles remain sound

- ⇒ Substantial increase in cross-border flows of personal data
- ⇒ Rapid technological developments and globalization
- ⇒ Scale of collection and sharing personal data increased

GDPR: consistent and high level of protection of natural persons

- ⇒ Enhancement rights of the data subject
- ⇒ Accountability of controllers / processors
- ⇒ Role of the supervisory authority – huge fines possible, up to 20,000,000 EUR or 4% of global turnover!

TOPICS

- Key terms
- Basic principles
- Data Governance Obligations
- GDPR Compliance: to do!

KEY TERMS

Personal data: “Any information relating to identified or identifiable natural person”

Information

- ⇒ broad concept
- ⇒ objective information, such as the presence of a certain substance in one's blood.
- ⇒ Subjective information, opinions or assessments (e.g. John is a reliable employee)

Relating to

Example:

The service register of a car held by a mechanic or garage contains the information about the car, mileage, dates of service checks, technical problems, and material condition. This information is associated in the record with a plate number and an engine number, which in turn can be linked to the owner. Where the garage establishes a connection between the vehicle and the owner, for the purpose of billing, information will "relate" to the owner or to the driver. If the connection is made with the mechanic that worked on the car with the purpose of ascertaining his productivity, this information will also "relate" to the mechanic.

KEY TERMS

Identified or identifiable person

- Identification through the name: common occurrence in practice,
- Other "identifiers" are used to single someone out (e.g. web surveillance, asylum seekers)

Natural person

- Legal persons
- Alive
- Children



Special categories of personal data: prohibited!
(exceptions)

KEY TERMS

Controller

Entity which alone, or jointly with others, determines the purposes and means of the processing of personal data

Processor

Entity which processes personal data on behalf of the controller

Liability

CONTROLLER / PROCESSOR: EXAMPLE

Example: Controller or processor?

Q. Organisation A provides payroll processing services to corporate customers. Organisation A provides those services to its customers in accordance with each customer's instructions. Organisation A also uses those data to perform benchmarking analysis, so that it can sell further services allowing customers to compare their payroll data to industry averages. Does Organisation A fall within the definition of a "controller" or a "processor"?

A. Depending on the facts, the same entity can be a controller in respect of some processing activities and a processor in respect of other processing activities. In this example, Organisation A is a **processor** in respect of the payroll processing services it provides directly to its customers, **and** a **controller** in respect of the benchmarking services, as it is processing personal data to create benchmarks for its own purposes.

BASIC PRINCIPLES

- Lawfulness
- Purpose Limitation
- Accountability
- Transparency
- Data Transfer
- Rights of data subject

LAWFUL GROUNDS TO PROCESS

- **Consent** data subject:
 - Freely given, specific, informed and unambiguous indication of agreement
 - Clear affirmative act
 - May be withdrawn at any time



Silence, pre-ticked boxes or inactivity do not constitute consent

Other legitimate basis include:

- Agreement with the data subject
- Legal obligation of the controller
- Legitimate interest of a controller

LAWFULNESS OF PROCESSING: EXAMPLE

Acquisition of a car

Legal Basis	Personal Data Processed
Agreement	Personal data required to buy the car
Legal obligation	Personal data necessary to obtain official documents related to the car
Legitimate interest	Client management (for example to allow car repairs in various workshops)
Consent	To allow transfer of the personal data to third parties for marketing purposes

LAWFULNESS OF PROCESSING: CONSENT

Keep in mind:

Unbundled: Consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

Active opt-in: Pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods.

Granular: Give granular options to consent separately for different types of processing wherever appropriate.

Named: Name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.

Easy to withdraw: Tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place.

CONSENT

Form of consent	Unambiguous?	Explicit?
A customer contract includes a written declaration of the customer's consent to specified types of processing (the request being clearly distinguishable from other matters in the contract)	Yes	Yes
An online retailer offers customers the opportunity to opt-in to specified processing through a tick-box during the order process	Yes	Yes
At an event sign-in, participants are informed that the organisers would like to use their registration details for specified types of profiling and are asked (verbally) whether they consent to such processing	Yes, consent may be given verbally. However, the organisers may wish to consider how the consent can be documented with greater certainty, particularly in light of the GDPR's accountability requirements	
Employees are informed that photographs will be being taken in a section of the building during a particular time and that such photos will be included on the company's intranet. Employees, having been so informed, decide to go to the area in which photographs are being taken	Yes, consent may be inferred from employees' actions in going to the areas of the building in which photographs are being taken during the relevant times	No, whilst consent may be inferred from the employees' actions, it cannot be said to be explicit
A social media website requires users to provide certain personal data in order to participate on the site. The site contains a notice, accessible in the privacy section, indicating that, by using the site, users are consenting to their data being processed by third parties to deliver them marketing information	No, the GDPR is clear that inactivity cannot constitute consent. This is consistent with the "no doubt" analysis: ongoing use of the site may indicate consent to the processing, but may also mean users have not read the notice. As there is doubt as to users' intentions, ongoing use of the site cannot constitute unambiguous or explicit consent	

PURPOSE LIMITATION

Specified, explicit and legitimate purposes:

- Not further processed in a manner incompatible with those purposes
- Data minimization:
 - adequate relevant and limited to what is necessary in relation to the purposes
- Storage limitation:
 - Stored no longer than is necessary for the purposes for which the data are processed
- Accuracy:
 - Accurate / kept up to date

PURPOSE LIMITATION: EXAMPLE

Q. Organisation A is a reinsurer. It provides services to insurance companies. Over the years it has collected large amounts of personal data relating to insured data subjects. It would now like to combine data from its various customers into a single database, to enable it to price its products more accurately. Can it do this?

A. Personal data collected for one purpose (e.g., performance of an insurance contract) cannot be used for a new, incompatible purpose (e.g., creating a database of information about insured data subjects to set prices more accurately). Organisation A might be able to achieve its aims by taking additional steps (e.g., obtaining the consent of the data subjects) or by anonymising the data before creating the database (subject to the need to ensure that such anonymisation is, itself, lawful processing of personal data).

DATA TRANSFER

- Adequacy decision
- Appropriate safeguards
 - Contractual basis: standard data protection clauses
 - Binding corporate rules
- Explicit consent by data subject

TRANSPARENCY: WHAT?

- Identity and contact details of the controller (or its representative, for a non-EU established controller);
- Contact details of the Data Protection Officer.
- Purposes of processing and legal basis for processing – including the “legitimate interest” pursued by the controller (or third party) if this is the legal basis.
- Recipients, or categories of recipients.
- Details of data transfers outside the EU, including how the data will be protected (e.g. the recipient is in an adequate country; Binding Corporate
- Rules are in place etc. and how the individual can obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.
- The retention period for the data – if not possible, then the criteria used to set this.
- That the individual has a right to access and port data, to rectify, erase and restrict his or her personal data, to object to processing and, if processing is based on consent, to withdraw consent.
- •hat the individual can complain to a supervisory authority.
- Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data.
- If there will be any automated decision taking – together with information about the logic involved and the significance and consequences of the processing for the individual.
- The controller must also tell individuals the categories of information and the source(s) of the information, including if it came from publicly accessible sources.

TRANSPARENCY: HOW?

- Information must be concise, easily accessible and easy to understand, clear and plain language, visualization if appropriate
- In writing – by other means (electronic means)

TRANSPARENCY: WHEN?


Data collected from the data subject

- At the time of collection
- Tell data subjects what information is mandatory and the consequences of not providing information

Data collected from another source:

- Within a reasonable period of having obtained the data (max one month); or
- If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

DATA SUBJECT RIGHTS

- Subject access
 - Rectification
 - Erasure “right to be forgotten”
 - Right to object (direct marketing)
 - Right to obtain human intervention in certain automated decision making
 - Restriction of processing
 - Data portability
- 
- New rights

DATA SUBJECT RIGHTS

Exercise of data subject rights:

- Modalities to be provided
- Action to be taken in one month (extension by two months – complexity – number of requests)
- Free of charge (unless manifestly unfounded or excessive)

DATA SUBJECT RIGHTS: EXAMPLE

A data broker undertakes profiling of personal data. The data broker should inform the individual about the processing, including whether it intends to share the profile with any other organisations. The data broker should also present separately details of the right to object.

The data broker shares the profile with another company. This company uses the profile to send the individual direct marketing.

The company should inform the individual about the purposes for using this profile, and from what source they obtained the information. The company must also advise the data subject about their right to object to processing, including profiling, for direct marketing purposes.

The data broker and the company should allow the data subject the right to access the information used to correct any erroneous information, and in certain circumstances erase the profile or personal data used to create it. The data subject should also be given information about their profile, for example in which ‘segments’ or ‘categories’ they are placed.

If the company uses the profile as part of a solely automated decision-making process with legal or similarly significant effects on the data subject, the company is the controller subject to the article 22 provisions.

ACCOUNTABILITY

Controller:

- Demonstrate consent
- Demonstrate compliance with the data protection principles
- Implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with GDPR
- Implement appropriate data protection policies

DATA GOVERNANCE OBLIGATIONS

- Privacy by design & default
- Processor
- Record of processing activities
- Data Processing Impact Analysis (DPIA)
- Data Protection Officer
- Data Breaches

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

Organisations adopt internal policies and implement technical and organisational measures:

- relating to pseudonymisation, data subject transparency and access
- which provide that only personal data which is necessary for each specific purpose of the processing is processed
- limited accessibility

This principle means that compliance with EU data protection law should be treated as a key issue in the planning and implementation of any new product or service that affects personal data!

PROCESSOR

- Sufficient guarantees
- Contract
 - Range of information such as data processed, duration
 - Obligations: assistance in case of breach, technical and organizational matters etc.

RECORD OF DATA PROCESSING ACTIVITIES

- Controller/processor

- Not applicable:
 - Controller employs fewer than 250 employees unless:
 - Processing is not likely to result in a risk for the rights and freedoms of data subjects;
 - Processing is not occasional;
 - Processing of a special category of data,

RECORD OF DATA PROCESSING ACTIVITIES

Content (controller):

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if applicable, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

Content (processor): article 30.2 GDPR

DATA PROTECTION IMPACT ASSESSMENT

- Controllers in case a type of processing is likely to result in a high risk for the rights and freedoms of individuals

- Non-exhaustive list:
 - Systematic monitoring of a publicly accessible area
 - Large-scale processing operations
 - In the context of profiling on which decisions are based that produce legal effects
 - “profiling”: “*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*”
(e.g. tracking customers' browsing habits to offer discounts)

- To evaluate origin / nature / particularity and severity of risk:
=> high risk ⇔ mitigation by appropriate measures: supervisory authority

PROFILING

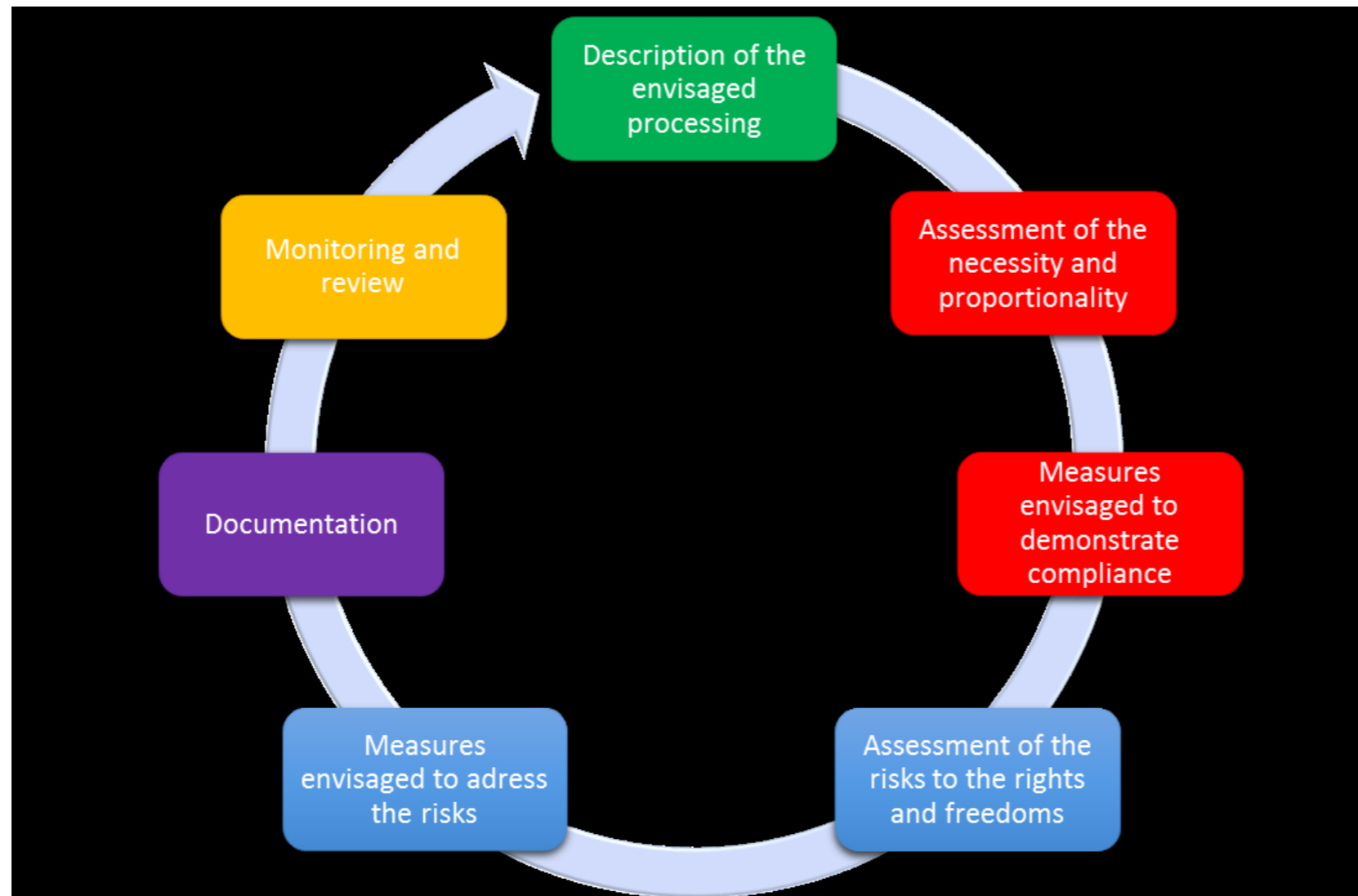
Example:

A data broker collects data from different public and private sources, either on behalf of its clients or for its own purposes. The data broker compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. The data broker carries out profiling by placing a person into a certain category according to their interests.

DPIA REQUIRED?

Examples of processing	Possible Relevant criteria	DPIA required?
A hospital processing its patients' genetic and health data (hospital information system).	<ul style="list-style-type: none"> - Sensitive data - Data concerning vulnerable data subjects 	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	<ul style="list-style-type: none"> - Systematic monitoring - Innovative use or applying technological or organisational solutions 	
A company monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	<ul style="list-style-type: none"> - Systematic monitoring - Data concerning vulnerable data subjects 	
The gathering of public social media profiles data to be used by private companies generating profiles for contact directories.	<ul style="list-style-type: none"> - Evaluation or scoring - Data processed on a large scale 	
An online magazine using a mailing list to send a generic daily digest to its subscribers.	<ul style="list-style-type: none"> - (none) 	Not necessarily
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on past purchases behaviour on certain parts of its website.	<ul style="list-style-type: none"> - Evaluation or scoring, but not systematic or extensive 	

DPIA: METHODOLOGY



Source: WP29 Guidelines on Data Protection Impact Assessments (DPIA)

DATA BREACH

Notification by processor to controller

- without undue delay after becoming aware of it

Notification to supervisory authority:

- 72 hours
- Exemptions

Notification to data subject

- Without undue delay
- Exemptions

Documentation requirements

DATA PROTECTION OFFICER

Who?

- Controller and processor
- Conflict of interest!

When?

Organisations whose core activities require:

- Regular and systematic monitoring of data subjects on a large scale or
 - Examples: profiling and online tracking, including for the purpose of behavioural advertising and email retargeting, data driven marketing activities
- Large scale processing of sensitive data

Voluntary appointment – alternative?

DATA PROTECTION OFFICER

Role:

- Informing organisation and employees who or processing personal data of their obligations under the GDPR
- Monitor compliance with GDPR
- Providing advice regarding DPIA
- Cooperating with supervisory authority
- Point of contact for supervisory authority

GDPR Compliance Ladder

Deadline - 25th May 2018

learn - apply - comply
www.dpnetwork.org.uk



Source: <https://www.dpnetwork.org.uk/>

GDPR COMPLIANT?

1. Awareness
2. Documentation: GDPR compliant?
 - a. Privacy policy
 - b. Consent
 - c. Cookie policy
 - d. Contracts
3. Safety
4. Data governance obligations
 - a. Record
 - b. DPO
5. Internal procedures
 - a. Data subject rights
 - b. Data breaches

AWARENESS

Management:

- Resource allocation

Employees:

- Sales, marketing, HR, IT, Purchasing
- Provide appropriate training

DOCUMENTATION

Privacy policy:

- Review current privacy policy
- Ensure information is given at appropriate time

Rely on consent?

- Review how consent is sought, recorded and managed
- Ensure quality of consent meets all requirements:
 - Consent must be active, no pre-ticked boxes!
 - Consent must be distinguishable, clear and not bundled with other agreements/declarations
 - Data subjects must be informed of the right to withdraw consent at any time, without impact on the processing based on consent before withdrawal
 - Separate consents for distinct processing operations
 - Consent may not be relied upon if clear imbalance between data subject / controller
 - Consider whether rules on children affect you and if so, act accordingly!
 - Consider whether rules on sensitive data affect you and if so, act accordingly!

DOCUMENTATION

Cookie policy

HR Policy Review

Contracts:

- Processors
- Suppliers

SECURITY

- Controllers are responsible for ensuring that personal data are kept secure, both against external threats (e.g. malicious hackers) and internal threats (e.g. poorly trained employees).
 - Do you have adequate protection levels for your data?
 - Are systems secured using encryption techniques and secure storage?
 - How are your backups handled?
 - Who has access to your IT system?
 - How are leavers / joiners handled within your organisation?
 - Are all of your mobile devices protected and encrypted?
 - Are there central policies for loss of mobiles / laptops etc
 - Where is your data held? Do you know where it is?
 - Check security of all software that customers may access

- Map international data flows (if any)

DATA GOVERNANCE OBLIGATIONS

DPO:

- appointment?
- Budget – responsibility

Record of data processing activities:

- Determine what personal data is held, where it came from and who you share it with

Need for DPIA?

Review technical and organisation measures

INTERNAL PROCEDURES

Internal procedures:

- Are processes and procedures in place sufficient under GDPR (access, portability, right to object etc);
- Ensure that personal data can be provided in a structure commonly uses and machine readable form
- Develop template response letters
- Review marketing suppression lists and processes
- Check if significant automated decision-taking is used and on what basis
- Data breaches:
 - Procedures in place to detect, report and investigate data breaches?
 - Update internal breach notification procedures
- Insurance policy?

ADMINISTRATIVE FINES

Infringement of the following GDPR provisions are subject to administrative fines up to **€20,000,000 or in the case of undertakings, up to 4% of global turnover**, whichever is higher:

- the basic principles for processing, including conditions for consent;
- data subjects' rights;
- international transfers;
- obligations under Member State laws; and
- non-compliance with an order imposed by supervisory authorities or a failure to comply with a supervisory authority's investigation.

ADMINISTRATIVE FINES

Other infringements are subject to administrative fines up to **€10,000,000 or, in the case of undertakings, up to 2% of global turnover, whichever is higher**. Contraventions subject to these maximum fines include infringement of the following obligations:

- to obtain consent to the processing of data relating to children;
- to implement technical and organisational measures to ensure data protection by design and default;
- on joint controllers to agree to their respective compliance obligations;
- on controllers and processors not established in the EU to designate representatives;
- on controllers in relation to the engagement of processors ;
- on processors to subcontract only with the prior consent of the controller and to process data only on the controller's instruction;
- to maintain written records;
- on controllers and processors to co-operate with supervisory authorities;
- to implement technical and organisational measures (Article 32);
- to report breaches when required by the GDPR to do so
- in relation to the conduct of privacy impact assessment ;
- in relation to the appointment of Data Protection Officers;

LAURIUS

ANTWERP - BRUSSELS

NEED ASSISTANCE?
PLEASE CONTACT KAREN
VERMAERE

Werf & Vlasnatie, Oudeleeuwenrui 19, B-2000 Antwerp T +32 3 260 88 00 - F +32 3 260 88 10
Kunstlaan / Avenue des Arts 56, B-1000 Brussels T +32 2 313 87 87 - F +32 2 313 87 88