Part 1 – Data Protection Introduction

FOCUS ON THE GDPR

Agenda

1. RETHINKING DATA PRIVACY FOR AI
2. SCOPE OF THE GDPR
3. DATA PROTECTION PRINCIPLES AND AI
4. CONSEQUENCE OF A VIOLATION

1 RETHINKING DATA PRIVACY FOR AI

Concerns over consumer privacy

- **Concerns over consumer privacy** have peaked in recent years—roughly in step with the rise of advanced technologies like artificial intelligence.

- About **9 in 10** American internet users say they are **concerned about the privacy and security** of their personal information online.

- **67%** are now **advocating for strict national privacy laws**, according to a study by Intouch International.

A moving target

- The notion of privacy **has changed over time.** In post-modern, information-based societies, the issue of data protection and informational privacy has become central, but other aspects [such as old-school, bodily privacy] still remain relevant. (ECJ / ECHR)

- Over time, the concept of privacy has become **increasingly complex**.

- That complexity has reached a tipping point of sorts with **the rise of AI**.

AI and data privacy

- **Several tendencies** re AI and processing of personal data
  - The collection of “all data” or “as much data as possible” to be able to further learn and analyze;
  - Re-purposing or multi-purposing of data

- **Devices** are becoming slightly but steadily precious supporters (especially in smart environments).

AI and data privacy

- AI **may affect privacy** in various aspects (profiling, influence a person's sense of self, no control over data)

- Without doubt, AI systems are subject **to data protection laws and their respective requirements.** The law governs AI in a **twofold** aspect:
  1. while ***designing*** and ***creating*** best practices for key aspects of a - legally and socially acceptable – development AI systems
  2. and while ***applying*** such systems, regardless of data processing being /is the goal or the result of the use of AI.

Tackling The Problem With The Law

- The **GDPR** fired a first volley at the problem. **California's forthcoming privacy la**w gave the U.S. a major toehold on the issue, as it will apply to nearly 40 million Americans.

- While privacy is a hard concept to define and safeguard, especially today, there are some **basic principles** that can help with protecting privacy. GDPR has in fact included many of them.

- GDPR does not specifically address AI.

2 SCOPE OF THE GDPR

Definitions (Art. 4 GDPR)

Central concepts remain, as before:

- **Personal Data** = Information about personal/factual circumstances relating to an identified or identifiable individual („Data Subject“)
- **Processing** = Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means.
- **Special types of personal data** = Information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, health or sex life; in addition now genetic and biometric data, to uniquely identify a person and sexual preferences (Art. 9 (1) GDPR)
- **Controller** = Body, which alone or jointly with others determines the purposes and means of the processing of personal data
- **Processor** = Body, which processes personal data on behalf of the controller

In addition, a number of new definitions (e.g. genetic data, biometric data, health data, profiling…)

Examples of “Personal Data”

- Internal identification number of employees of a company
- Client numbers
- Serial number of an equipment (e.g. car engine)
- IP address or online search preferences of a user of the controller's website.
- Customer information collected by sales representatives (e.g. tenant file in a real estate agency)

Examples of “Sensitive Personal Data”

- E-mail from an employer who complains about an engineer because of his or her racial background or religious beliefs.
- Recording information on the skin colour and racial origins of a new customer when training an algorithm.
- HR file recording the political opinions of certain employees or their union membership.
- Biometric fingerprints collected for security purposes (to control access to restricted areas or unlock phones).

Examples of “Processing”

Collect

- Obtaining
- Registration
- Access to the site
- Conservation
- Detention
- Reception
- Recuperation
- Follow-up

Use

- Use of the system
- Modification
- Organization
- Sharing
- Transfer
- Analysis
- Deduction
- Backup

Delete

- Erase
- Destruction
- Anonymization (alternative to destruction)
- Shredding

Examples of “Data Subjects”

Employees of the controller and other staff members, trainees, etc.

Visitors or **customers** browsing the website of the controller's website.

The **staff** of the controller's customers, end **customers** and **suppliers.**

The **general public** in certain circumstances, e. g. in the context of video surveillance.

Any other person whose personal data are consulted, collected or otherwise used by the controller.

Material Scope (Art. 2 GDPR)

- Processing of personal data at least partly by automated means or other than by automated means as part of a filing system
- Special exceptions, e.g. for personal activities of individuals or in the context of law enforcement
- Purposes: Protection of the personal rights of the data subjects, but also ensuring the free availability of data
- Anonymous vs. pseudonymous data

Territorial Scope (Art. 3 GDPR)

- **Establishment in the EU** or **processor in the EU** (regardless of whether the processing itself takes place in the EU or not);

- Controllers or processors outside of the EU, where the processing activities are related to
  - The offering of goods or services
  - The monitoring of the **behaviour of the data subjects, as far as their** behavior takes place within the EU (analysis of preferences or behavior via the internet)

- Obligation for controllers located outside the EU to designate in writing a representative in the EU (Art. 27 GDPR)

Obligated Bodies

1. Data Controller
2. NEW: Also the data processor in a further extent than previously, e.g.:
    - Documentation obligations (Art. 30 GDPR)
    - Designation of a data protection officer (Art. 37 et seq. GDPR)
    - Responsibility for violations of the GDPR (right to compensation (Art. 82 GDPR)), administrative fines (Art. 83 GDPR) …

Responsibility for Data Processors (1)

The data controller is also responsible for engaged data processors („DP“), in particular the data controller has to

1. **Carefully select the DP in terms of its qualification and the availability of adequate TOMs**
2. **Conclude a written contract with the processor, which inter alia stipulates:**

- The purpose and the scope of the processing
- The concerned personal data and the categories of data subjects
- The obligation to process personal data only on the instruction of the data controller
- The obligation to commit persons employed to confidentiality
- The TOMs
- The conditions for the use of subcontractors
- The obligation to support the data controller with all necessary information to enable it to fulfill its own obligations (e.g. data breach notification)
- The control rights of the data controller

Responsibility for Data Processors (2)

- Subcontractors may be used only with **prior special or general consent**;
- Sub-processing contract is subject to the **same requirements** as processing contract;
- A data processor which establishes own purposes and means of the processing is seen as a **data controller.**

3 DATA PROTECTION PRINCIPLES AND AI

Central Principles of Data Protection Law

Overview – **Art. 5 GDPR**:

- Lawfully, fairly and transparent processing
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality of the processing

Lawful Data Processing

What is not allowed, is prohibited!

Collection, processing and use of personal data is only permissible to the extent permitted/arranged by law or to the extent the data subject has consented (Art. 6 GDPR)

➢Check statutory permissions, Art. 6 para. 1 GDPR, inter alia:

- Necessary for the performance of a contract (Art. 6 para. 1 lit. b GDPR)
- Necessary for compliance with a legal obligation (Art. 6 para. 1 lit. c GDPR)
- Legitimate interests of the controller & balancing of interests (Art. 6 para. 1 lit. f GDPR)

Consent

- **Definition of consent** in Art. 4 (11) GDPR: any **freely** given, **specific**, **informed** and **unambiguous** indication of the data subject's wishes by which he or she, either by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her:
  - Data controller must be able to prove that the data subject has given his or her consent
  - Not sufficient: „Silenty“ pre-checked boxes or inaction of the data subject
  - No free choice is assumed in the case of a clear imbalance between the data subject and the data controller
  - Different data processing purposes require separate consents

- **Critics** re consent.

- Challenge re **withdrawal of consent**.

Specific Categories of Personal Data

- **Principle here as well**: Processing is prohibited, unless authorized by consent or specific justifications (Art. 9 GDPR) ;

- In an employment relationship processing is allowed if necessary in order to meet legal rights and obligations ;

- Member States can exclude possibility to consent and in terms of genetic, biometric and health data set additional conditions and restrictions ;

- Criminal records are no specific category of personal data, but are likewise permitted only under restrictive conditions (Art. 10 GDPR).

The Principle of Purpose Limitation

- Personal data **shall be collected for specified, explicit and legitimate purposes** and shall not be processed in a way incompatible with those purposes (Art. 5 (1) lit. b GDPR)

- **Exception**: Processing for certain archiving purposes in the public interest or specific scientific, historical or statistical purposes pursuant to Art. 89 GDPR

- Determining the compatibility of the purposes using a check list (Art. 6 (4) GDPR):
  - Any link between the purposes
  - The context in which the personal data have been collected, in particular regarding the relationship between the data subject and the controller
  - The nature of the personal data
  - Possible consequences for the data subject
  - The existence of appropriate safeguards (e.g. pseudonymisation)

- In the case of incompatible purposes: Consent of the data subject or on the basis of specific national legislation (e.g. to protect national security)

Data Minimisation

- The collection, processing and use of personal data and the design and setting of data processing systems **has to align with the aim to collect, process or use none or as little personal data as possible,** and in particular to make use of anonymisation and pseudonymisation when possible and proportionate.

- This principle is not "just" a simple declaration, but may influence the admissibility of proposed measures:
  - Is an interest to be qualified as a legitimate interest?
  - How are the legitimate interests of the data subjects to be weighted?

- Data minimisation vs Big Data analytics and machine learning systems ?

Accuracy

- Personal data have to be **accurate** and, where necessary, **kept up to date**.

- **Issue re AI** : EVEN IF data is accurate, it does not ensure the accuracy of analysis due to possible biases in datasets.

- **Consequence**: The accuracy principle requires that data controllers that perform machine learning processes need to ensure that the training data is **representative** of the environment in which the trained algorithm will be deployed

Transparency

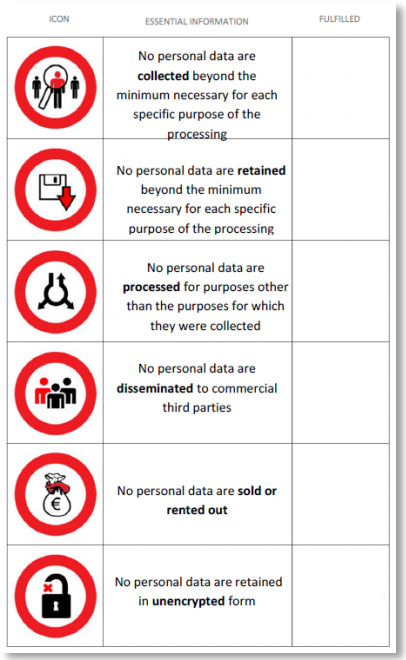
- Individuals are often not aware of the use of personal data for processing.

- **Major challenge with AI:** How to ensure transparency – how to trace outcomes ? → Transparency is articulated as a need to face the “opacity of the algorithm”.

Information Obligations (Art. 13, 14 GDPR) (1)

Data subjects shall be **informed** about:

- Identity and contact details of the controller and, if any, of the controller‘s representative and of the data protection officer, if any
- Purposes and legal basis of the processing
- Categories of processed data
- Where processing is based on the balancing of interests, the overweighing legitimate interest
- The recipients or categories of recipients of the personal data
- Transfer to a third country and legal basis of the transfer
- Period for which the data will be stored



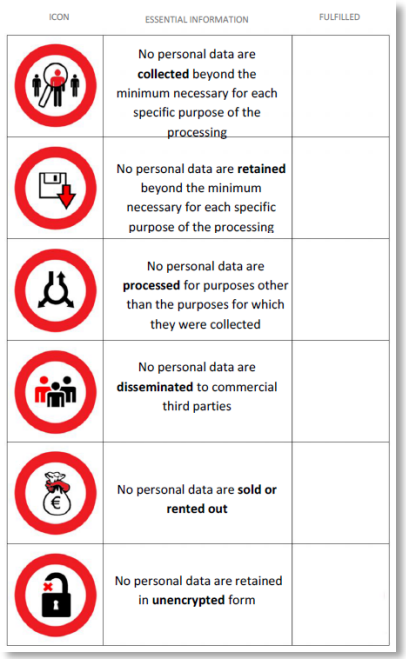
ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to commercial third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

Significant extension of information/transparency obligations

Information Obligations (Art. 13, 14 GDPR) (2)

Data subjects shall be informed about:

- The data subject‘s rights
- The right to withdraw consent at any time
- The right to lodge a complaint with a supervisory authority
- Whether the provision of personal data is a statutory or contractual requirement, or necessary to enter into a contract
- The existence of automated decision making, including profiling
- Sources, from which the personal data originate



ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to commercial third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

Significant extension of information/transparency obligations

Accountability principle

- **Shift** from **notification system** and nominal responsibility to **accountability** for controllers. How ? For instance:
  - “Appropriate technical and organisational measures” to be able to ‘demonstrate’ compliance
  - DPIA
  - Privacy by design and by default…

- **Data processors** are also bound by the accountability principle.

- **Challenging when it comes to AI…**

Rights of the Data Subject (Art. 12 et seq. GDPR) – Overview

- Information, access, erasure etc. (see the following slides)
- Information and communication must be easily accessible and be done in a precise, transparent and understandable form
- Information must generally be given in writing or in electronic form
- Rights of the data subject must be fulfilled without undue delay, at least within one month (extension up to max. two additional months in exceptional cases)
- Exercise of the rights is generally free for the data subject
- Data controller may examine the identity of the claimant
- Restrictions based on national law possible, inter alia, to protect national security or public safety (Art. 23 GDPR)

Right of Access by the Data Subject (Art. 15 GDPR)

The data subject has the right to **obtain confirmation** as to whether or not and where personal data concerning him is being processed and has the right to obtain information about

- The purposes of the processing
- The categories of personal data
- The recipients (in particular in third countries or international organisations)
- The period for which the personal data will be stored
- The legal rights of the data subject (inter alia the right to lodge a complaint with a supervisory authority)
- The source of the data
- The circumstances in connection with automated decisions
- In the case of international data transfers, the appropriate safeguards

Data subject can generally request a **free copy** of the data processed.

Rectification, Erasure, Restriction of Processing

1. Inaccurate personal data shall be rectified (Art. 16 GDPR).
2. Personal data shall be erased without undue delay („**right to be forgotten**“ – Art. 17 GDPR), inter alia, if
   - The knowledge of the data is no longer necessary for the controller for the purposes for which the data were stored
   - The data subject has withdrawn his or her consent and there is no other legal ground for the processing
   - The processing is unlawful
   - There is a legal obligation to erase the data
3. An absolute claim to erase the data does not exist!
4. No erasure obligation, inter alia, in the case of retention obligations under national law
5. Personal data are subject to a restriction of processing (Art. 18 GDPR), inter alia, if their accuracy is contested by the data subject, as long as the accuracy cannot be determined
6. Restriction of processing means that data may, with the exception of storage, only be processed with the data subject‘s consent
7. Notification obligation (Art. 19 GDPR)

Other Rights

- **Right to data portability** (Art. 20 GDPR): Shall facilitate the „relocation“ of data to another provider

- **Right to object** (Art. 21 GDPR):
  - Data subject may object to the processing in the public interest or on the basis of a balancing of interests; controller can continue processing, when the controller presents overriding legitimate interests
  - Right to object to processing in the context of direct marketing
  - In the context of information services, objection can be made by automated means
  - Information of the right to object

- **Automated decisions, including profiling** (Art. 22 GDPR) → VERY IMPORTANT RE AI.

Ensuring an adequate level of data protection in the case of international transfers of data

- Personal data **must not** be transferred to or accessed from non-EEA countries unless **appropriate measures** are in place to protect the data.
- **Appropriate measures** must ensure that the data to be transferred will enjoy the same level of protection outside the EEA as in the EEA.
- If the data are transferred outside the EEA, this transfer must be subject to appropriate safeguards (e.g. EU standard clauses, EU-US Privacy Shield, approved codes of conduct).
- It is important to ensure that you have control over the international transfer of subcontractor data.

Data Breach Notification (Art. 33 et seq.)

- The controller has to inform the competent supervisory authority, where feasible, within 72 hours after having become aware of the personal data breach, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals
- "Risk for the rights and freedoms of individuals" is not defined more specifically in the GDPR
- Controllers must document all data breaches internally
- After having become aware of a data breach, the processor has to notify the controller without undue delay
- If the data breach is likely to result in a high risk for the rights and freedoms of individuals, the controller has to communicate the data breach to the data subject without undue delay (there are possible exceptions to this rule)

4 CONSEQUENCES OF A VIOLATION OF DATA PROTECTION LAW

Overview

1. Claims for damages
   - Claim for damages pursuant to Art. 82 GDPR
   - Possibly, claims based on contract, and, as the case may be, law of torts

2. Rights of the data subjects to seek legal protection before authorities and courts (Art. 77 et seq. GDPR)

3. Administrative fines (see next slide)

4. Further sanctions pursuant to Member State law (Art. 84 GDPR)

5. Powers of the supervisory authorities (see the following slides)

Administrative Fines

"Minor" infringements:

- EUR 10 million or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher

"Serious" infringements:

- EUR 20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher

Other Powers of the Supervisory Authorities (Art. 58 GDPR)

Investigative powers of the supervisory authorities

- Controller, processor and/or, if any, the representative may be ordered to provide any information required for the performance of the supervisory authority's tasks.
- Investigations in the form of data protection audits
- Access to all personal data and to all information necessary for the performance of the supervisory authority's tasks
- Access to any premises, including to any data processing equipment and means

Corrective powers of the supervisory authorities, e.g.

- Warnings that intended processing operations may infringe provisions of the GDPR
- Orders to comply with data subjects' rights (e.g. information request, right to data portability, erasure)
- Orders to suspend data processing or data transfers

Powers can be compared to those of a criminal prosecutor

Part 2 – Data Governance

Key elements of an efficient data governance

I. Organizational measures
II. Awareness
III. Training
IV. The implementation of measurement indicators
V. Incident management
VI. Transparency

I. Organisational measures

FOSTERING A CULTURE OF COMPLIANCE MUST START AT THE TOP !

Involve top management!

- Data protection in the company **requires an impetus** that must be given by **decision-making bodies,** and whose sustainability must be ensured by the **allocation of appropriate budgets and the allocation of time dedicated to data protection** (*e. g*., for a functional position, predict how much of the time will be dedicated to data protection functions).

- **The board of directors** must approve, establish and maintain data governance in the company, with the assistance of the DPO.

- Governance should introduce the chain of officials and **identify key contacts** at each key stage of data protection, **defining their roles and responsibilities in this area**.

With the help of a DPO

Data Protection Officer (1)

Data Controller and data processors have to appoint a data protection officer, if

- The core activities require a regular and systematic monitoring of data subjects on a large scale
- The core activities affect special categories of personal data or data relating to criminal convictions
- Required by EU or Member State law

- A group of undertakings may appoint a single data protection officer provided that he or she is easily accessible from each establishment
- Data protection officer must have the required expertise to perform its tasks
- Data protection officer may perform other tasks, insofar as no conflict of interests exists
- Internal – external data protection officer: advantages and disadvantages

Data Protection Officer (2)

Tasks of the DPO under the GDPR:

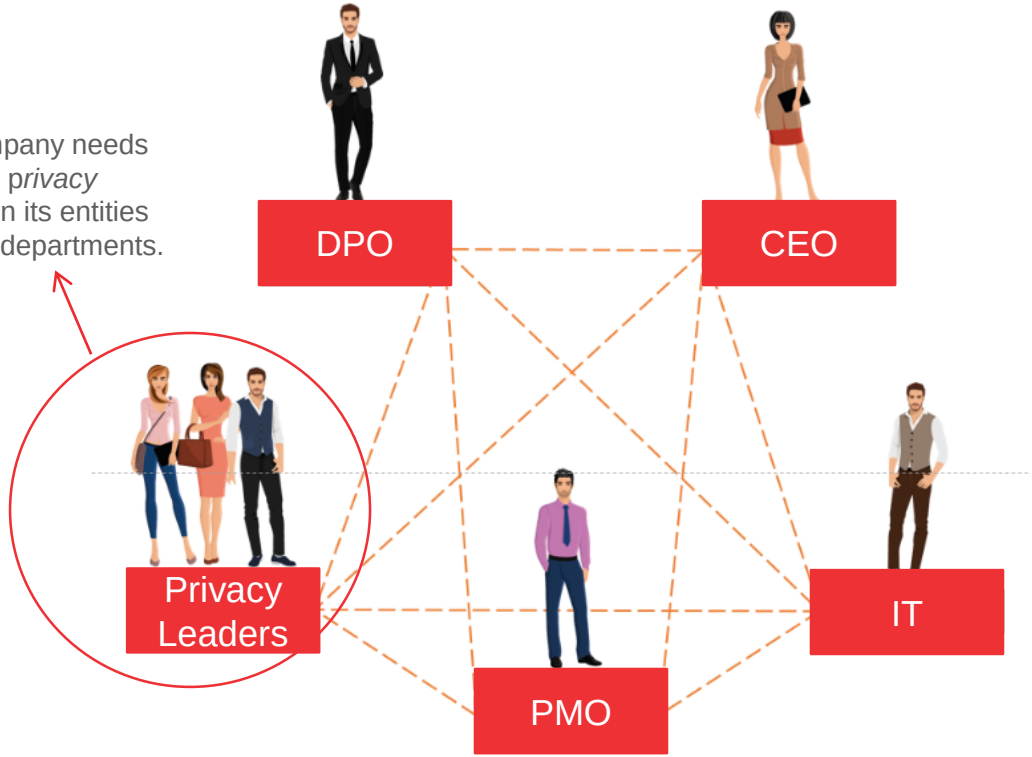
1. **Informing and advising the data controller or the processor** and the employees about their duties under the GDPR as well as other data protection provisions of the EU or the Member States
2. **Monitoring compliance** with the GDPR and with other data protection provisions of the EU or the Member States
3. **Training** of staff involved in processing operations
4. **Providing advice** regarding the *Data Protection Impact Assessment* and monitoring its performance
5. **Contact point** for the supervisory authority(ies)

Data Protection Officer (3)

- ✓ The data protection officer must be provided with the necessary resources
- ✓ No instructions regarding the exercise of the tasks
- ✓ Partial protection against dismissal
- ✓ The data protection officer‘s contact details shall be published and communicated to the supervisory authority
- ✓ Member States may establish stricter/further national rules in the area of „Data Protection Officer“

A DPO cannot operate alone !

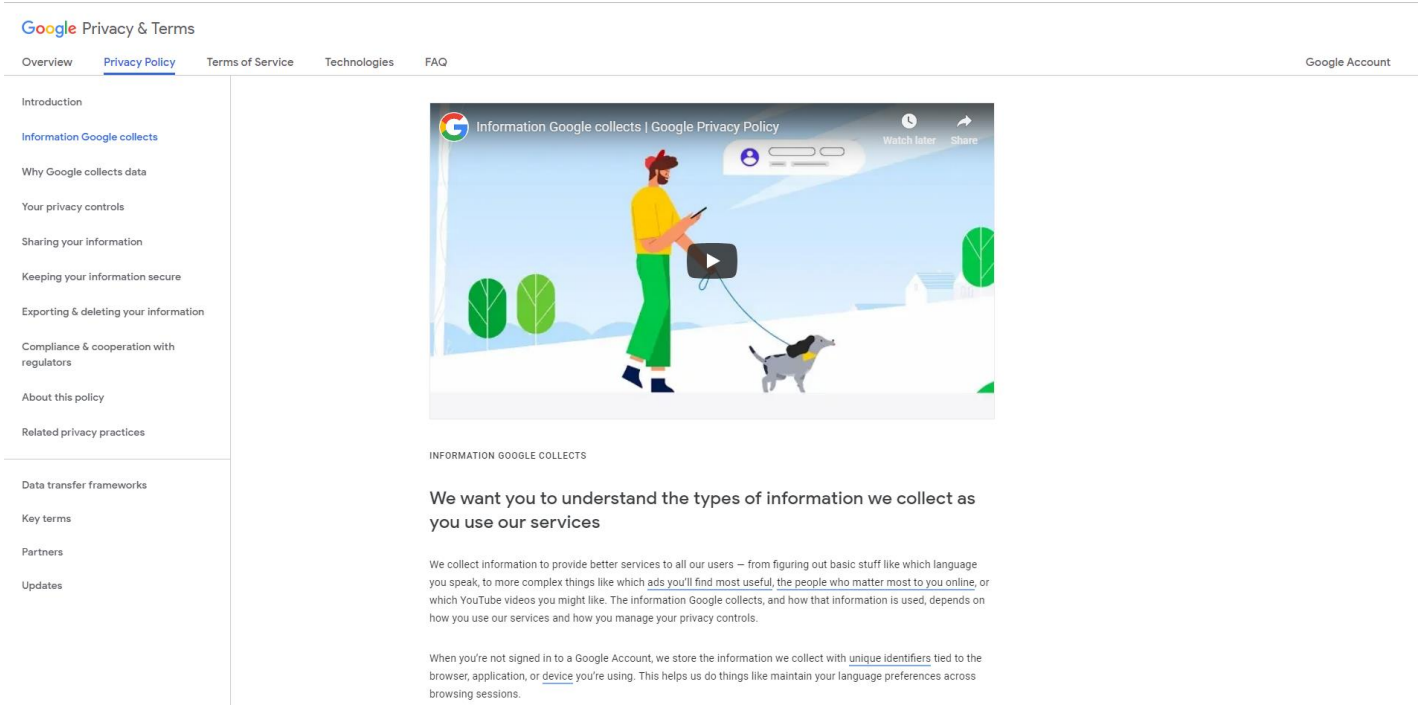
The company needs to chose p*rivacy leaders* in its entities and key departments.



II – Awareness

IF IT ISN'T DOCUMENTED,
IT ISN'T DONE.

Example of Privacy Policy



III – Training

A CREDIBLE AND EFFECTIVE CORPORATE GLOBAL COMPLIANCE PROGRAM INCLUDES AN ONGOING TRAINING COMPONENT FOCUSING ON COMPLIANCE ISSUES FOR STAFF AT ALL LEVELS

An efficient data governance shall involve everyone

The **key players** in corporate governance must:

- **train** data subjects within the company (board of directors, employees, etc.)
- and **raise awareness** among people outside the company (customers, partners, suppliers) of good practices and obligations regarding data protection.

Good practice re training

- Training should be **mandatory** for all persons involved in the collection and processing of personal data. e-Learning methods are preferable.

- International entities should be able to offer accessible training in **several languages.**

- **Employees' knowledge** of personal data protection policies and procedures within the company should be regularly **tested**.

IV – The implementation of measurement indicators

ANYTHING THAT CAN BE DONE CAN BE MEASURED
AND THAT WHICH GETS MEASURED GETS DONE

Implementing measurement indicators

- The company must **implement indicators** to monitor, evaluate and process internal developments within the company (new processing, new organisation, acquisition, etc.), but also changes in personal data protection requirements (new internal IT system, new decree, new guidelines, etc.).

- This requires the definition of baseline measures to determine the **effectiveness of governance** and the **risks associated** with it.

- The monitoring of these indicators over time makes it possible to measure the **evolution** (progress, stagnation, regression) of the company's maturity in terms of data governance.

V – Incident management

ESTABLISH A FORMAL POLICY AND CENTRALIZED PROCESS FOR HANDLING PRIVACY INCIDENTS AND BREACHES.

Companies should ensure to draft SOPs

- Standard Operating Procedures should be drafted in order to hlp document vulnerabilities that require notification

    - Since the entry into force of the GDPR, some personal data breaches require a rapid response from the company (within **72 hours**).

    - The company must give employees the right reflexes. **This involves automating processes**: who reports what information? to whom? how? in what way? in how long? how the information that reports is processed?

    - You need to document the vulnerabilities.

VI – Transparency

Make publicly available the main principles governing privacy compliance, the policies and the role and responsibilities of the bodies in charge of handling privacy matters within the organization

Transparency: the ultimate principle?

- Transparency must be **an essential objective** for the company. However, this requires a high degree of maturity in terms of data protection.

- The company must be able to **engage in substantial interactions** with **regulators** and **civil society.** This commitment is different from lobbying. Such an outward orientation is essential to guide the company's internal behaviour and prove its accountability.

How to be transparent ?

- **Publicly disclose** (e.g. website) at a **higher level** the **governance structure in place**, including the name of the DPO and his or her hierarchical position within the company.

- **Publicly disclose all codes of conduct, privacy policies and relevant documents** relating to the company's privacy policy in order to demonstrate the company's ambitions in terms of personal data protection.

- **Publicly** and periodically **disclose the monitoring of the governance indicators** put in place.

- **NOTE**: transparency is not without risks and requires that the company really be at the level of its ambitions.

QUESTIONS?