Privacy protection: legal issues and GDPR

Privacy legislation: many sources

Various sources

- European Convention on Human Rights
- Treaty on the Functioning of the European Union (TFEU)
- Charter of Fundamental Rights of the EU
- National (constitutional) legislation (per country)

Many aspects

- Customers, users: collect information, user profiling,
- Privacy at work in the EU: Telephone calls E-mail / Use of Internet and online technology
- National laws implement privacy at work differently

1. Privacy by Design
2. EU regulations: GDPR
3. Data Protection Officer (DPO)
4. Italy regulations
5. Complications: BYOD

Privacy by design (PbD)

Privacy by Design is an approach to system engineering which promotes privacy throghout the whole engineering process

- take human values into account in a well-defined manner throughout the whole process
- is not about data protection but designing so data doesn't need protection
- the root principle is based on enabling service without data control transfer from the citizen to the system

Privacy by design (PbD)

Privacy by Design

- Proactive vs. Reactive (plan in advance not wait for the problem)
- Privacy as a Default Setting
- Privacy Embedded into Design (a requirement in the specification of the system)
- Full Functionality and Life Cycle Protection
- Visibility and Transparency
- Respect for User (user friendly not cryptic)

Privacy by design (PbD)

1995: PbD originates in a joint report by researchers in Canada and Netherlands

2010: regulators from around the world unanimously passed a resolution recognizing Privacy by Design as an essential component of fundamental privacy protection

2012: US Federal Trade comm: PbD one of the three recommended practices for protecting online privacy in the report “Protecting user privacy in an era of rapid change”

2012: adoption from the EU parliament (vague); more precisely regulations in 2016 that are effective starting May 2018

Privacy by Design:
The 7 Foundational Principles

1. ***Proactive*** not ***Reactive:*** Preventative, not Remedial;
2. Privacy as the ***Default*** setting;
3. Privacy ***Embedded*** into Design;
4. **Full** Functionality: Positive-Sum, not Zero-Sum;
5. End-to-End **Security**: **Full** Lifecycle Protection;
6. Visibility **and** Transparency: Keep it **Open**;
7. Respect for User Privacy: Keep it **User-Centric**.

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Data Minimization

According to Privacy by design supporters

- Data minimization is the most important safeguard in protecting personally identifiable information;
- The use of cryptography, de-identification techniques, data aggregation, are absolutely critical.

Claim: Pseudoanonimity and Security (mainly Cryptography) allow to maintain anonimity

"Re-Identification concerns are over-stated … anonymized data can, in many circumstances be used without fear of re-identification."

Data Minimization & De-identification

- De-identification techniques are intended to remove identifying information from a dataset while retaining some utility in the remaining data.
- De-identification can be used within an organization to minimize the privacy risk associated with data use or storage.
- De-identification can also be used prior to sharing or release of a dataset. In some cases, de-identified data can be released without further controls, while in others it is necessary to additional protection measures such as data use agreements that administratively restrict what recipients of the data can do with it.

De-identification: problems

The de-identified data can be re-identified (data can be matched back up with the original data)

- Disclosure of private facts affects the individuals whose data were re-identified.
- Damage to reputation affects the organization that performed the de-identification.

Many of those re-identified individuals were public figures (public figures are inherently easier to re-identify than private figures: more information about public figures is available in the public domain).

NOTE: the cost of de-identification should be considered

De-identification: problems

There is no agreement regarding the meaning of re- identification risk.

- the term is taken to mean the percentage of de-identified records that can be re-identified. In these cases, re-identification risk can be directly measured by performing a re-identification attack.
- Others consider it as the probability of record re-identification in the future. In this case, the risk must be estimated but is ultimately impossible to quantify.
- Another issue concerns whether the re-identification risk may also be estimated as the probability that any record can be re-identified or some record

De-identification: problems

Organizations must consider employing a combination of several approaches. These include

- removing quasi-identifiers and other kinds of information that might be used to re-identify the data subjects;
- continuously surveying for data that could be linked to the de-identified information that they are sharing;
- controls on the de-identified data, such as data use agreements and click-through agreements that prohibit re-identification, linking to other data, or sharing with others;
- technical controls that limit the activities of data recipients.

De-identification: conclusions

After more than a decade of research, there is comparatively little known about the underlying science of de-identification:

- Many of the current techniques and procedures in use, such as the HIPAA Privacy Rule's Safe Harbor de-identification standard, are not firmly rooted in theory.
- There are no widely accepted standards for testing the effectiveness of a de-identification process or gauging the utility lost as a result of de-identification.

Conclusions: there is a clear need for standards and assessment techniques that can measurably address the breadth of data and risks

Data Minimization

Therefore the following claim

Claim: Pseudoanonimity and Security (mainly Cryptography) allow to maintain anonimity

"Re-Identification concerns are over-stated … anonymized data can, in many circumstances be used without fear of re-identification."

Correct ???

Privacy by design: criticisms

- Privacy by Design in the meaning of "Foundational" has been critiqued as "vague" and leaving "many open questions about their application when engineering systems.
- It has also been pointed out that Privacy by Design is similar to voluntary compliance (a form of corporate social responsability: it is in a company's own interest to behave socially responsibly and that in pursuit of good public image)

Privacy by design: criticisms

- Technology evolution: evolutionary approach will come at the cost of privacy infringements because evolution implies also letting privacy invading products utilizable until they are proven unfit for privacy
- Certain business models are built around customer surveillance and data manipulation and therefore voluntary compliance is unlikely

Privacy by design: criticisms

- Current definitions of privacy by design do not address the methodological aspect of system engineering, such as using decent system engineering methods, e.g., which cover the complete system and data life cycle.
- The concept also does not focus on the role of the actual data holder, but on that of the system designer. This role is not known in privacy law, so the concept of Privacy by Design is not based in law. This in turn undermines the trust by data subjects, data holders and policy makers.

1. Privacy by Design
2. EU regulations: GDPR
3. Data Protection Officer (DPO)
4. Italy regulations
5. Complications: BYOD

European regulations: GDPR

January 2012: the European Commission presented a proposal to ensure a coherent framework and a harmonized system in EU matters. It consists of two different tools:

- a proposal for a Regulation concerning "*the protection of individuals with regard to the processing of personal data and the free movement of such data*", aimed at regulating the processing of personal data in both the private and public sector, and intended to replace the 95/46
- a proposal for a *Directive addressed to the regulation of prevention, conflict and repression of crimes, and to the enforcement of criminal penalties*; it will replace Framework Decision 977/2008 / EC on the protection of personal data exchanged by the authorities of police and justice (which Italy has not, however, yet implemented).

European regulations: GDPR

Very, very long process to arrive a final decision

- April 14, 2016, the plenary of the European Parliament adopted at second reading the texts and Regulations (260 pages) Directive (120 pages). This step concludes the legislative process
- It will be enforced starting 25th of May 2018
- **EDPS mobile app**
  https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package

a free app for mobile devices from the EDPS. It allows you to compare the latest proposed texts for the forthcoming General Data Protection Regulation from the European Commission, the European Parliament and the Council of the European Union.

General Data Protection Regulations

- Chapter 1 – General Provisions
- Chapter 2 – Principles
- Chapter 3 – Rights of the Data Subject
- Chapter 4 – Controller and Processor
- Chapter 5 – Transfer of Personal Data to other Countries or International Organizations
- Chapter 6 – Independent Supervisory Authorities
- Chapter 7 – Cooperation and Consistency
- Chapter 8 – Remedies, Liability and Penalties
- Chapter 9 – Provisions Relating to Specific Processing Situations
- Chapter 10 – Delegated Acts and Implementing Acts
- Chapter 11 – Final Provisions

GDPR: Global Data Protection Regulation

Applies to **processing of personal data** by data controllers and processors

Regulation: directly effective in Member States (no local law required)

The GDPR will apply in all Member States as from **25th of May 2018**

Why is GDPR important

Data processing must comply with the **6 general GDPR principles**

- **Lawfulness, fairness and transparency**
- **Purpose limitation:** personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- **Retention**: personal data must be kept in an identifiable format no longer than necessary
- **Integrity and confidentiality:** personal data must be kept secure
- **Data minimization:** personal data must be adequate, relevant and limited to the purpose
- **Accuracy:** personal data must be accurate and up to date

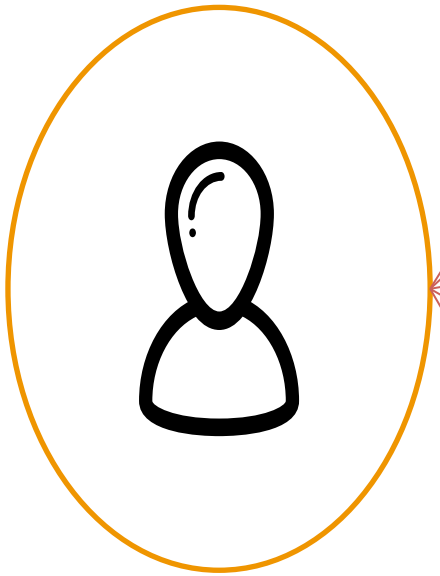
The Global Data Protection Regulation

Data processing must satisfy at least one **processing condition**

- Consent: the individual has given clear consent (much stricter rules under GDPR)
- Necessary for the performance of a contract
- Legal obligation: ex. Hotel registration for police
- Vital interests: ex. You are unconscious in a hospital
- Public functions
- Legitimate interests

Personal data

Any information relating to the identification, directly or indirectly, of natural persons



Name

Identification number

Location data

Online identifier

Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity

Personal data

Broader definition of personal data under GDPR:

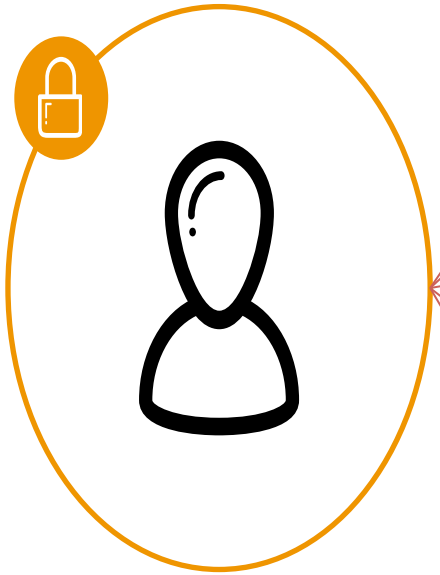
- Obvious identifiers: names, addresses etc.
- Less obvious identifiers: physical, psychological, economic, cultural features, location data or online identifiers

If data is anonymised, GDPR does not apply

If data is pseudonymised, GDPR *does* apply

Sensitive Personal data

Personal data revealing:



- Racial or ethnic origin
- Political opinions, religious or philosophical beliefs
- Trade union membership
- Data concerning health or sex life and sexual orientation
- Genetic data or biometric data

Sensitive Personal data

Explicit consent (or another specific legal basis) required to process these:

- Racial Origin
- Political Opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic Data (e.g. biological samples) NEW
- Biometric Data (e.g. fingerprints) NEW
- Data concerning Health
- Data concerning a person's sex life or sexual orientation
- Also separate rules for criminal convictions/ offences data (although not special category)

Data controller and Data Processor

Data controller

The person or body that, alone or jointly with others, determines the purpose and means of the processing of personal data

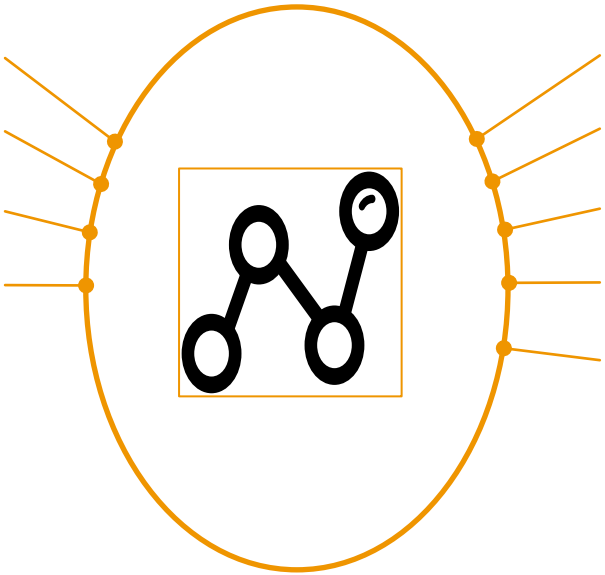
Data processor

A natural/legal person or body which processes personal data on behalf of the controller

Data processing

Any (automatic) operation which is performed on personal data

Collection, recording
Organization, structuring
Storage
Alteration, alignment or combination



Retrieval, consultation
Use
Disclosure by transmission
Making available, restriction
Erasure or destruction

Data processing

Under GDPR, DP Notices must contain much more information, including details of:

- Who is collecting the data
- Why it is being collected
- What legal basis is being relied upon to process the data
- How it will be processed
- How long it will be kept for
- Who it will be disclosed to
- Individuals' rights (access, erasure, restrict processing)
- The name and contact details of the Data Protection Officer
- The right to lodge a complaint with the DPC
- The existence of automated decision making, including profiling

Purpose limitation

Only use personal data for the purpose that it was originally collected for

- Be clear about why you are collecting personal data
- Make sure that data subjects are also clear about the purpose(s) for which you are collecting/ holding their data and what they might be contacted about
- Cannot expand purpose without reverting to individual

Data accuracy

Keep all personal data accurate and, where necessary, up-to-date

- The longer personal data is held, the more likely it will be inaccurate / out-of-date.
- Individuals have the right to have errors rectified.
- Staff must ensure that local procedures are in place to ensure high levels of data accuracy, including periodic review and audit.

Data minimisation

Only ask for the minimum amount of data that you need: If you don't need it, don't ask for it

Personal data must be:

- Adequate
- Relevant
- Limited to the **minimum** amount of personal data from data subjects which you need to achieve your purpose.

Carry out periodic reviews of data being sought and data already held.

Data retention (in time)

Keep personal data only for as long as necessary

- Be clear about length of time data will be kept and reason for same.
- **Data should never be kept "just in case"!** Decide how long data should be kept for before you collect it.
- If you no longer need it, dispose of it in line with the UCC records management policy.

Security

Keep personal data safe and secure

- Take appropriate security measures when processing personal data
- Keep all personal data secure and in such a way that it does not permit unauthorised access, intentionally or accidentally.
- Adhere to UCC's Information policies at all times.

Example

- Keep personal data locked away, Encrypt laptops
- Dispose of personal data as confidential waste
- Don't disclose to 3rd parties without permission
- Don't share passwords

Tools and techniques

- GDPR requires businesses to implement "*technical and organizational measures to provide appropriate protection to the personal data they hold*."
- This requires to secure the Personal Identifiable Information (PII) & Personal Health Information (PHI) to Prevent Unauthorized Access and, in the event of unauthorized access … the data they get is unintelligible.

Tools and techniques:

Encryption *In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as* ***encryption****.*

Security *Those measures should* ***ensure an appropriate level of security****, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.*

Tools and techniques

GDPR expressly states that such measures include:

1. The **pseudonymization** and **encryption** of personal data
2. Measures to ensure resilience of systems and services processing data
3. Measures that allow businesses to restore the availability and access to the data in the event of a breach
4. Frequent testing of the effectiveness of the security measures

Tools and techniques

- When encrypting personal data, in accordance with Article 4 No. 5 GDPR, the encryption key is the "additional information" which is "kept separately" and "subject to technical and organizational measures".
- Hence safety measures such as a secure key management and the respective encryption method used by the controller have to be used "*to ensure that the personal data are not attributed to an identified or identifiable natural person*". Therefore, because of its existing assignment rule encryption is an example of pseudonymisation.

Encryption

According to Mozilla's statistics, an encryption milestone was met in early 2017 when the average volume of encrypted traffic on the internet surpassed the average volume of unencrypted traffic.

2017 DBIR report: the percentage of hacking related breaches involving the misuse of stolen or weak credentials has reached 81%. No other attacker technique detailed comes close to this number.

Important: credential misuse is an epidemic and is rapidly getting worse.

Tools and techniques

GDPR includes a definition of “pseudonymisation”. According to Article 4 No. 5 GDPR, pseudonymisation:

- “*means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*”.
- pseudonymisation shall, like encryption, be one of the “appropriate safeguards” of Article 6 Par. 4 (e) GDPR.

Key Implications of the GDPR

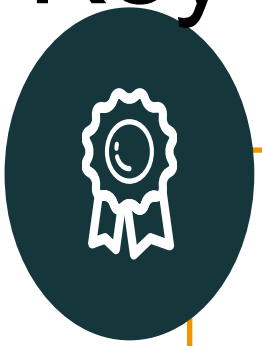
Increased fines

1

- Regulators can impose fines of **up to 4% of annual turnover** or **€20.000.000** (whichever is highest)
- Regulator may perform **audits**, issue **warnings** or a (temporary) **ban** on processing
- Individuals may sue for compensation to recover (non-)material damages

2

Key Implications of the GDPR



Proof of compliance

2

Organizations must **demonstrate** they are compliant by:

- Evidencing that they comply with the 6 GDPR principles and processing conditions
- Documenting suitable policies that set out how you process personal data
- Performing Privacy Impact Assessments
- Implementing technical security measures

3

Key Implications of the GDPR

New rights

- Right to access and rectify personal data within 30 days
- Right to be forgotten
- Right to data portability
- Right to challenge profiling and automated decisions
- Right to object to direct marketing

3

4

Key Implications of the GDPR

Privacy by Design, Privacy by Default

4

Mandatory to implement **Privacy by Design**

- Ensure privacy and data protection is a key consideration during the entire lifecycle of any project

Privacy by Default:

- Privacy as the default setting and embedded into design

5

Key Implications of the GDPR

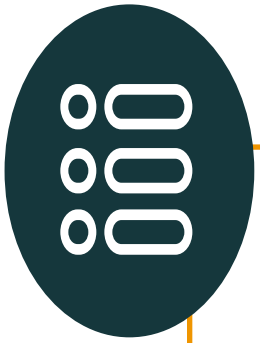
Data Protection Officers (DPO)

- Mandatory appointment in certain cases
- Report to highest levels of management, may not be dismissed or penalized

5

6

Key Implications of the GDPR



Privacy Impact Assessments

- Mandatory for “high” risk personal data processing
- In some cases consulting the Supervisory Authority is required

6

7

Key Implications of the GDPR

Privacy Notices

- Increase of **mandatory** amount of **information** included in privacy notices
- Supplied to the individual at the time they provide personal data
  - If processing is for a new purpose, prior notification must be given
- Must be “concise, transparent, intelligible and easily accessible”
  - Translation into local languages

Key Implications of the GDPR

Consent

- Consent must be freely given, specifc, informed and unambiguous
- Consent may be withdrawn at any time
- Consent must be explicit for sensitive personal data and for data transfers outside the EU

Key Implications of the GDPR

Mandatory breach notifications

Mandatory record keeping of all security breaches, regardless of whether they need to be notified to the supervisory authority

9

10

Key Implications of the GDPR

Obligations for data processors

- New obligations specifically for data processors: more responsibility, higher liability
- Data sub-processors fall into the same scope

Key Implications of the GDPR

Extra-territorial scope

The GDPR applies to data controllers and processors established in the EU and organizations that target EU citizens

Key Implications of the GDPR

New key aspects: individuals

- **easier access to your own data**: individuals will have more information on how their data is processed and this information should be available in a clear and understandable way;
- **a right to data portability**: it will be easier to transfer your personal data between service providers;
- **a "right to be forgotten"**: when you no longer want your data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted;
- **the right to know when your data has been hacked:** companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible so that users can take appropriate measures

Key aspects: individuals

- **Data protection by design and by default**: 'Data protection by design' and 'Data protection by default' are now essential elements in EU data protection rules. *Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.*
- **Stronger enforcement of the rules**: data protection authorities will be able to fine companies who do not comply with EU rules up to 4% of their global annual turnover.

Key aspects: individuals

Right to be forgotten: How will it work?

- The Directive gives individuals a possibility to have their data deleted, in particular when the data is no longer necessary.
- *For example, if an individual has given her or his consent to processing for a specific purpose, e.g. display on a social networking site, and does not want this service anymore, than there is no reason to keep the data in the system*.
- In particular, when children have made data about themselves accessible, often without fully understanding the consequences, they must not be stuck with the consequences of that choice for the rest of their lives.

Key aspects: individuals

Right to be forgotten: How will it work?

- This does not mean that on each request of an individual all his personal data are to be deleted at once and forever.
- Example: if the retention of the data is necessary for the performance of a contract or for compliance with a legal obligation, the data can be kept as long as necessary for that purpose.
- The proposed provisions on the "right to be forgotten" are very clear: **freedom of expression,** as well as historical and scientific **research are safeguarded**.
- For example, no politician will be able to have their earlier remarks deleted from the web. This will allow news websites to continue operating on the basis of the same principles.

Key aspects: individuals

Data breach notification duty

- Today may be imposed by supervisory authorities
- Notification to supervisory authorities: Detailed information without undue delay (e.g. at the latest within 24 hours after becoming aware of the breach);
- Standard format of document data breach for verification purposes
- Notification to data subjects
- Likelihood of adversely impacting a data subject
- Encryption may provide exemption

Key aspects: individuals

Example *an Italian Facebook member had turned to the Privacy Authority after consultation with the social network and have received an unsatisfactory answer.*

- The member complained of being the victim of extortion attempts by another Facebook user, who, after having obtained his "friendship" would initially entertained a confidential correspondence, which has resulted in crime attempts.
- After the other user created a “fake”account, using his personal data and the photograph posted on his profile, from which he sent to all Facebook contacts concerned montages of photographs and videos gravely offend the honor as well as its public and private image.

Key aspects: individuals

Example *Facebook continued*

- The individual then applied to Facebook Ireland for cancellation and the fake account lockout, as well as the communication of its data in a clear, even to those in the fake.
- Facebook Irl. replied with incomplete data member; moreoever not all fake information were cancelled
- The individual had turned to the Italian Privacy Authority
- The Ital. Privacy Auth. asked Facebook that replied that has "*already taken steps to delete the fake account (...) reported by the applicant through the (...) reporting tool*"
- The Privacy auth. ordered Facebook to act immediately to answer the user requests; otherwise a civil action will start in Italy

Key aspects: business

New business opportunity and favor innovation:

- **One continent, one law**: The regulation will establish one single set of rules which for companies to do business in the EU
- **One-stop-shop**: businesses will only have to deal with one single supervisory authority (estimated to save €2.3 billion/year)
- Within a single market for data, identical rules on paper are not enough. The rules must be applied in the same way everywhere. The 'one-stop-shop' will favor cooperation between the data protection authorities on issues of interest for all of Europe. Companies will only have to deal with one authority, not 28.
- Businesses will profit from faster decisions, from one single interlocutor (eliminating multiple contact points), and from less red tape.

Key aspects: business

New business opportunity and favor innovation:

- **European rules on European soil–** companies outside of Europe will have to apply the same rules when offering services in EU.
- **Risk-based approach:** the rules will avoid a "one-size-fits-all" obligation and rather tailor them to the respective risks.
- **Rules fit for innovation:** Data protection by design: will guarantee that data protection safeguards are built into products and services from the earliest stage of development. Privacy-friendly techniques such as pseudonomysation will be encouraged.

Key aspects: business

New rules will save cost for about **€2.3 billion per year** (UE source)

- ***Example:*** *A chain of shops has its head office in France and shops in other EU countries. Each shop collects data relating to clients and transfers it to the head office for further processing.*
- ***With the current rules:*** *France's data protection laws would apply to the processing done by head office, but individual shops would still have to report to their national data protection authority: the company's head office would have to consult local lawyers for all its branches to ensure compliance with the law.*
- ***With the Data Protection Reform:*** The data protection law across all EU countries will be the same – one European Union – one law. This will eliminate the need to consult with local lawyers to ensure local compliance for the shops. The result is direct cost savings and legal certainty.

Key aspects: business

How will the Data Protection Reform encourage innovation and use of big data?

- According to some estimates, the value of European citizens' personal data could grow to nearly €1 trillion annually by 2020.
- **'Data protection by design and by default'** will become an essential principle. It will incentivise businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. The Regulation promotes techniques such as **anonymisation**, **pseudonymisation** (replacing personally identifiable material with artificial identifiers), and **encryption**.
- This will encourage the use of "big data" analytics, which can done using anonymised or pseudonymised data.

Key aspects: business

Use of "big data" analytics

- Key principle: when personal data is collected for one or more purposes it should not be further processed in a way that is incompatible with the original purposes.
- This does not prohibit processing for a different purpose or restrict 'raw data' for use in analytics.
- A key factor in deciding whether a new purpose is incompatible with the original purpose is whether it is fair. Fairness will consider factors such as; the effects on the privacy of individuals (e.g. specific and targeted decisions about identified persons) and whether an individual has a reasonable expectation that their personal data will be used in the new way.

Key aspects: business

Example: *Current car technology requires important data flows, including the exchange of personal data. In case of a crash, cars equipped with eCall emergency call system can automatically call the nearest emergency centre.*

Advantages with the new rules,

- one rule for Europe: the function of eCall will become easier, simpler and more efficient in terms of data protection
- raw data can be used to analyse where the most accidents take place and how future accidents could be avoided. It can also be used to analyse traffic flows
- providing individuals with clear, effective information will help build trust in analytics and innovation. The information to be provided is the purpose for which it will be processed.

Key aspects: business

Example: Google maps - an online navigation and mapping system across Europe collects images of all private and public buildings, and may also take pictures of individuals.

- ***With the current rules:*** *in Germany, the deployment of this service led to a major public and political outcry. The company offered additional to the individuals residing in that State after negotiation with the competent DPA; however the company refused to commit to offer the same additional guarantees to individuals in other Member States.*
- ***With the new rules*** *will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Any company - regardless of whether it is established in the EU or not - will have to apply EU data protection law.*

1. Privacy by Design
2. EU regulations: GDPR
3. Data Protection Officer (DPO)
4. Italy regulations
5. Complications: BYOD

Key organizational issues

Key principle: accountability

- Ensure and be able to demonstrate compliance: Adopt policies and Implement appropriate measures, Documentation
- Nominate the **Head of the Protection of Personal Data** (**Data Protection Officer**)
- Performing data protection impact assessment
- Prior authorization or consultation (where required) Implement mechanisms to verify effectiveness
- Verification by independent internal or external auditors, where proportionate

Head of the Personal Data Protection

The Head of the Personal Data Protection will have to :

1. adequate knowledge of legislation and the data management practices personal ;

2. carry out its functions in full independence and in the absence of conflicts of interest ;

3. operate in the employ of the owner or responsible or on the basis of a service contract

The owner or manager of the treatment will have to make available to the head of the personal data protection (DPO) human and financial resources necessary to perform its tasks .

DPO: Tasks

The Data Protection Manager will:

- **inform and advise** the owner of the treatment about their obligations under the European Regulation
- **check the implementation and application of the Regulations**, **provide opinions** on the assessment of the impact on data protection
- act as a contact point about any issue related to the processing of their data or the exercise of their rights;
- act as a contact point for the Authority for the protection of personal data or, where appropriate, refer to the Guarantor at its own initiative.

DPO: in what crcumstances?

Must compulsorily appoint a Head of protection of personal data :

a) government departments and agencies, with the exception of judicial authorities;

b) all persons whose main business consists of treatments which , by their nature , their object or their purposes , require regular and systematic monitoring of those concerned ;

c) all persons whose main business is processing , large-scale , sensitive data concerning health or sex life , genetic , judicial and biometrics .

You can still designate a security manager

of personal data even in cases other than those mentioned above

A group of companies or public entities can appoint a unique DPO

Data breach

Prevent Data Security Breaches. Examples:

- Disclosure of confidential data to unauthorised individuals
- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use of information
- Hacking, viruses or other security attacks on IT equipment / systems / networks
- Emails containing personal data sent in error to wrong recipient
- Emails sent to mailing list not using the BCC field

Applies to paper **and** electronic records
Consequences: Fines, reputational damage, legal action, harm to individuals

Data breach notification duty

When data breachs occur:

- Notification to supervisory authorities
  - Detailed information
  - Without undue delay and at the latest within 24 hours after becoming aware of the breach
  - If not within 24 hours, reasoned justification for the delay, maximum 72 hours
  - Standard format is likely
  - Document data breach for verification purposes
- Notification to data subjects
  - Likelihood of adversely impacting a data subject
  - Encryption may provide exemption and may be imposed

Accountability

Maintain a record of processing activities

- It is mandatory to maintain records of processing activities in order to demonstrate how data protection principles are observed and clearly document:
- What personal data is processed
- Why it is conserved
- How it was obtained
- The legal basis for processing
- Where/how it is stored
- Security measures in place
- Who can access it
- How long we retain it

  - Register of Personal Data
  - Data Privacy Impact Assessments

Rights of data subject

All requests to be directed to Information Compliance Manager

- Right of access (copy to be provided within 1 month)
- Right to erasure (Right to be forgotten) - individuals can request that their
- details be deleted in certain circumstances
- Right to restrict and object to processing
- Right to data portability
- Right not to be subject to a decision based solely on automated processing

1. Privacy by Design
2. EU regulations: GDPR
3. Data Protection Officer (DPO)
4. Italy regulations
5. Complications: BYOD

Key Aspects in US

Data privacy is not highly legislated or regulated in the US

- Partial regulations exist but there is no all-encompassing law regulating acquisition, storage, use of personal data in the US
- Access to prvate data can be sought when seeking for emplyment, medical care, housing, etc. In general whoever owns the data has the right to store and use even if data is obtained withot permission unless there are laws and specific regulations
- Examples of specific regulations:
  - HIPAA: Health Insurance Portability and Accountability Act
  - Children Online Protection ACT
- The Supreme Court interpreted the Constitution to grant a right of privacy to individuals
- Few states, however, recognize an individual's right to privacy, a notable exception being California

Key aspects in Italy

1. Anyone has the right to protection of personal data concerning him
2. the processing of personal data will be respect for human rights and fundamental freedoms and dignity, with particular reference to privacy, and the right to identity the protection of personal data
3. The information systems and programs are configured to **minimize** the use of personal data and identification data, in order to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or mechanisms permitting the identification of the individual only in case of need

Two types of personal data

- **Sensitive data**: personal data revealing racial or ethnic origin, religious beliefs , philosophical or other beliefs, political opinions , membership of parties , unions, associations or organizations of a religious , philosophical, political or trade union, as well as personal data disclosing health and sex life

- **Judicial data** : personal data relating to criminal records, the register of offense-related administrative sanctions and the relevant current charges , or as an accused or suspected person of the criminal procedure code

Rights of individual

- **The right of access** to personal data, including the right to obtain confirmation of the existence of data concerning him, the right to have their communication in intelligible form
- **The updating, correction or the integration of data**
- **The cancellation, anonymization or blocking of data** processed in violation of the law
- **The right to oppose**
  - For legitimate and documented reasons to the treatment , even if carried out in a legitimate way
  - If the processing carried out for the purpose of sending advertising materials or direct selling or for carrying out market research . In this case, you do not need motivation.

Key roles

- **Holder of data**: The person, legal person, public administration or any other body , organization that is competent (example: the owner, the Administrative board)
- **Person in charge of data**: any natural person, legal person, public administration or any other body, association or body appointed by the holder to the processing of personal data; responsible is designated by the Holder
- **The operator of data**: persons authorized to perform processing operations by the holder of the respoor manager
- *The processing operations can be carried out by staff who operate under the direct authority of the owner or manager, by following the instructions given.*

Authority (Garante)

- The Authority is a collegial body composed of four members , elected by Parliament

Obligations towards the Authority,

- Communicate data processing
- Preliminary consent of specific actions,
  - use of detection systems of biometric (e.g. graphometric signature or access to through fingerprint) or use of intelligent video surveillance systems, *which are able to automatically detect abnormal behaviors or events , report them*
  - data processed with the help of electronic instruments to define the profile or personality , or to analyze habits or consumption choices

Obligations to individuals

Information disclosed to individuals

- **external**: potential customers, active and potential suppliers , users of business services , visitors at the company's offices , Internet surfer accessing corporate sites
- **Internal**: employees and related workers and directors,
- **Mandatory collection of consent** from individuals; not generic consent but specific in relation to the processed data and with communication of guaranteed rights
- **Consent should be given before collecting data** possibly oral (phone marketing) or advice (videosurveillance in offices)
- **Limited number of cases** when it is not requested (e.g. risk of death, police etc.)

Obligations to individuals

- **Mandatory collection of consent** from individuals; not generic consent but specific in relation to the processed data and with communication of guaranteed rights
- **Consent should be given before collecting data** possibly oral (phone marketing) or advice (videosurveillance in offices)
- **Limited number of cases** when it is not requested (e.g. risk of death, police etc.)

Obligations to individuals

Right of access (Italy); upon request it is mandatory provide

- Confirmation of the existence of personal data and their communication in an intelligible form if requested
- Indication about the data source, purpose of treatment, the specific treatment, the identity of the holder, subjects or categories of persons to whom the data may be communicated or who can learn about them as managers or agents
- The updating, the correction or integration of data
- Cancellation, transformation into anonymous form or blocking of data that do not require conservation
- Quick answer: 15 days

Thing to consider -1

- If PII is used in the test environment, it is required to be protected at the same level that it is protected in the production environment, which can add significantly to the time and expense of testing the system.
- Explain why?

Thing to consider -2

If you are simulating a live environment, how does the IT department do that? The simple answer is that it grabs a bunch of data (technically, a sample) from its production database and runs that through the testing process. This isn't an issue if the application is concerned with stock control but it is an issue if the application deals with individuals, as in a consumer sales application or a

human resources application.

Explain why?

Thing to consider -2

If you are simulating a live environment, how does the IT department do that? The simple answer is that it grabs a bunch of data (technically, a sample) from its production database and runs that through the testing process. This isn't an issue if the application is concerned with stock control but it is an issue if the application deals with individuals, as in a consumer sales application or a human resources application.

Explain why?

In these cases, unless you have formal consent from the people whose data you are using, then simply sampling the production system for test data is illegal: you are using the data for purposes for which it was not provided and you are making that information

1. Privacy by Design
2. EU regulations: GDPR
3. Data Protection Officer (DPO)
4. Italy regulations
5. Complications: BYOD

More complications

BYOD (Bring Your Own Device)

BYOD & BYOT

'Bring your own device' (BYOD) and 'Bring your own technology' (BYOT)

- Private device used for professional purposes vs. corporate device used for private purposes
- Legal issues
  - Privacy and data protection
  - Electronic communications
  - Intellectual property rights / data ownership and recovery
  - Cybercrime
  - Tax law issues
  - Insurance

BYOD: new problems

- Legal ownership of the device is generally not relevant for data protection purposes
  - Controller: determination of purpose and means
  - Devices owned by third parties can be used
  - Technology used and ownership thereof can have impact on security obligations
- Security assessment is much more complicated
  - Proliferation of devices and data
  - Data recovery
  - Less security in case of private devices?
  - Loss of control?

BYOD: new problems

Data loss is a serious risk in most cases of BYOD

- theft and loss of portable devices is very common
- Security is generally less advanced on personal devices in comparison with corporate devices
- Compared with (a limited number of) routine back-up tapes, the risk is higher as a result of the higher number of devices

The risk related to the absence of adequate security measures

- Stolen or lost portable devices are generally re-used, rather than stolen for their data contents
- The absence of encryption of the tapes was envisaged in the decision, not the loss as such

BYOD: possible costs

Non-BYOD precedents provide guidance for BYOD

- Fine of 2.275.000 £ imposed by FSA on a UK company due to data loss by service provider (outsourced data processing)
  - Data loss related to 46.000 clients due to an unencrypted backup tape
  - No evidence that the data had been misused or compromised, but it was clear that there were no effective data protection systems in place or systems to manage the risks to the security of customer data resulting from the outsourcing arrangement

BYOD: possible costs

Fines for illegal screening and monitoring of employees:

- Fine of 1.100.000 EUR imposed by Berlin DPA on a German company
- Screening of employee and supplier data to combat corruption and Monitoring communication sent via external e-mail accounts by employees
  - Combined fine of approx. 1.500.000 EUR imposed by twelve German state DPAs on a German company for 'spying' on employees
- Monitoring employees is regulated in a different manner in the EU member states

BYOD: solutions

Any monitoring of employees should be implemented in accordance with applicable law

- Policies are a paramount instrument
  - Raise awareness of emplyees (instruct)
  - Ensure policy enforceability (enforce)
- Monitoring is particularly sensitive in case of BYOD, as the devices have a dual purpose (professional / private)
  - Monitoring, if any, should be restricted to use of the device within the employment context
  - Monitoring use of the device outside the employment context is disproportional
- Rights and obligations of the parties involved: During contract and upon and after termination (data!)