The Roadmap to GDPR Compliance in e-Healthcare services

ICT Legal Consulting

Prof Dr Paolo Balboni – Founding Partner
paolo.balboni@ictlegalconsulting.com

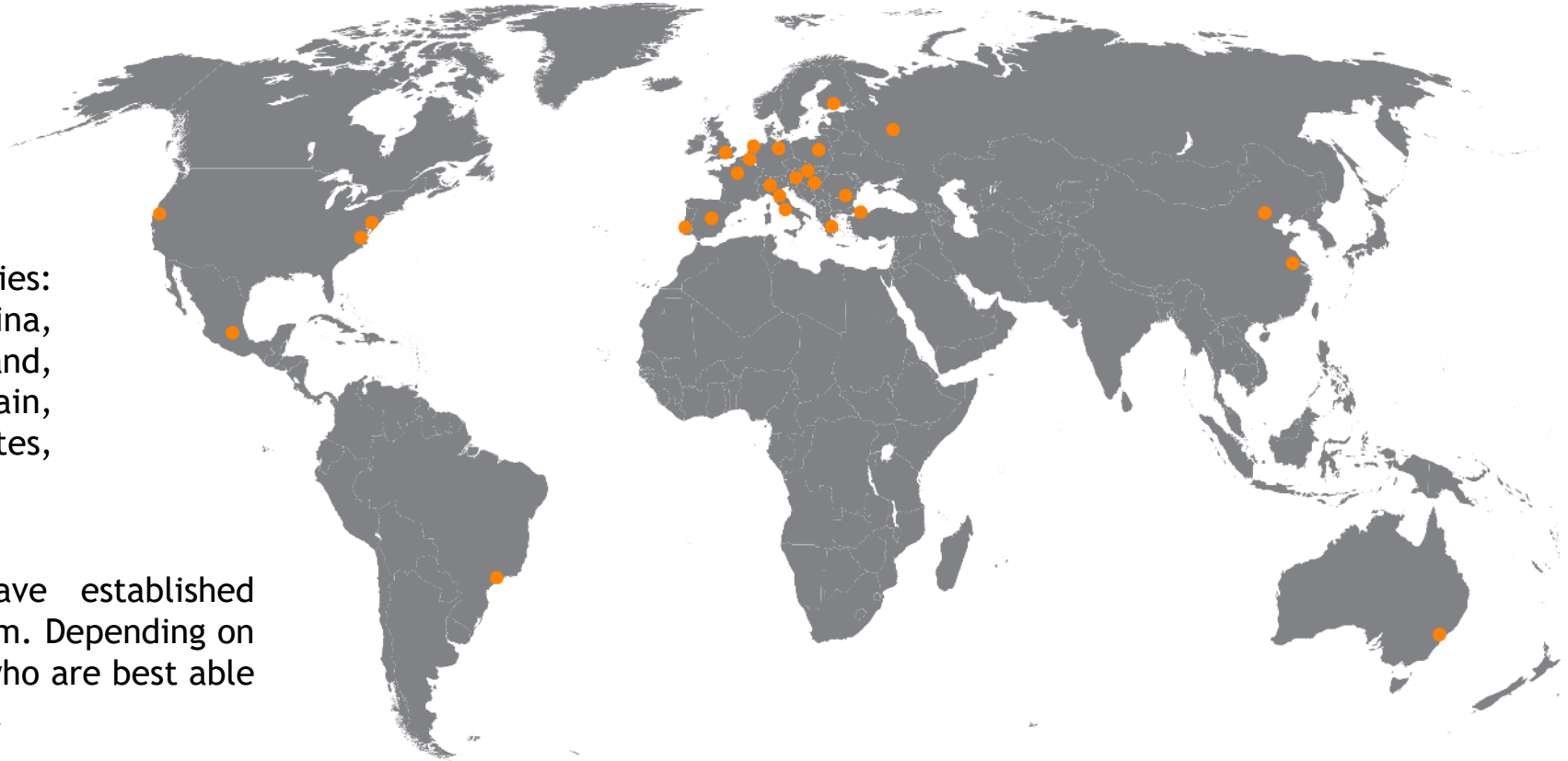
Anastasia Botsi - Associate
anastasia.botsi@ictlegalconsulting.com

ICT LEGAL CONSULTING

cyberwatching.eu
The European watch on cybersecurity & privacy

The Firm

ICT Legal Consulting is an Italian law firm with offices in Milan, Bologna, Rome and Amsterdam.



The firm is present in 19 other countries: Australia, Austria, Belgium, Brazil, China, France, Germany, Greece, Mexico, Poland, Portugal, Romania, Russia, Slovakia, Spain, the United Kingdom the United States, Turkey and Hungary.

In each of these countries we have established partnerships with more than one law firm. Depending on the task, we contact the professionals who are best able to meet the specific needs of customers.

In Detail

ICT Legal Consulting is an international law firm. It was established by Paolo Balboni and Luca Bolognini, who have successfully assembled a network of trusted, highly-skilled lawyers and cyber security advisors specialized in the fields of Information and Communication Technology, Privacy, Data Protection/Security and Intellectual Property.

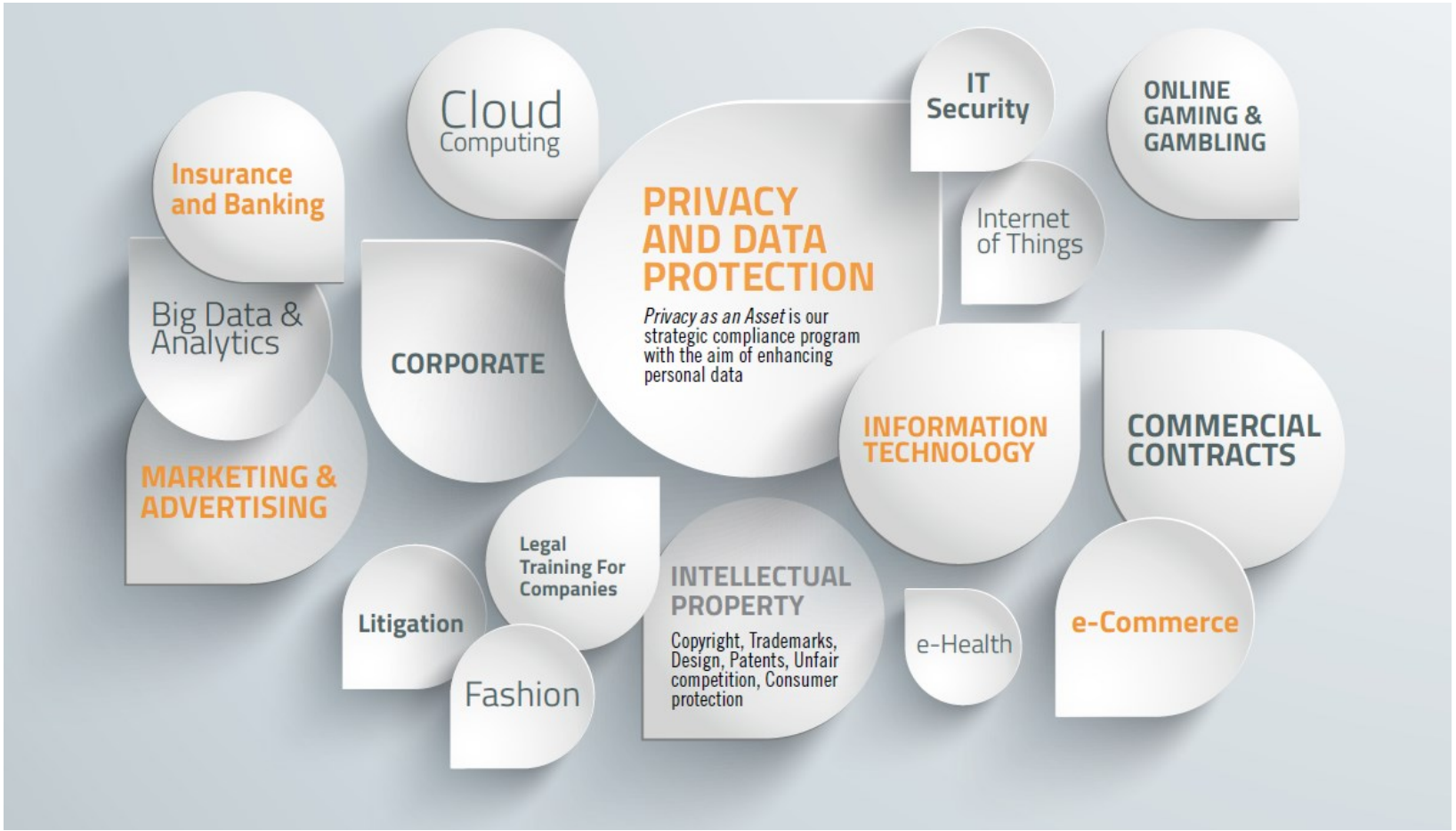
We have developed significant expertise working with multinationals and companies in the communications, media & entertainment, IT, healthcare, pharmaceutical, fashion, food & beverage, energetic and smart grids, banking/financial services, automotive, industrial manufacturing and eGovernment sectors.

In more detail, we provide complete assistance in the fields of personal data protection, IT contracts, eHealth, eCommerce, eMarketing, advertising, cloud computing, web 2.0 service provider liability, internet and mobile content, online gambling, online gaming, electronic signatures, digital document retention and online storage, renewable energy and administrative responsibility and corporate liability.

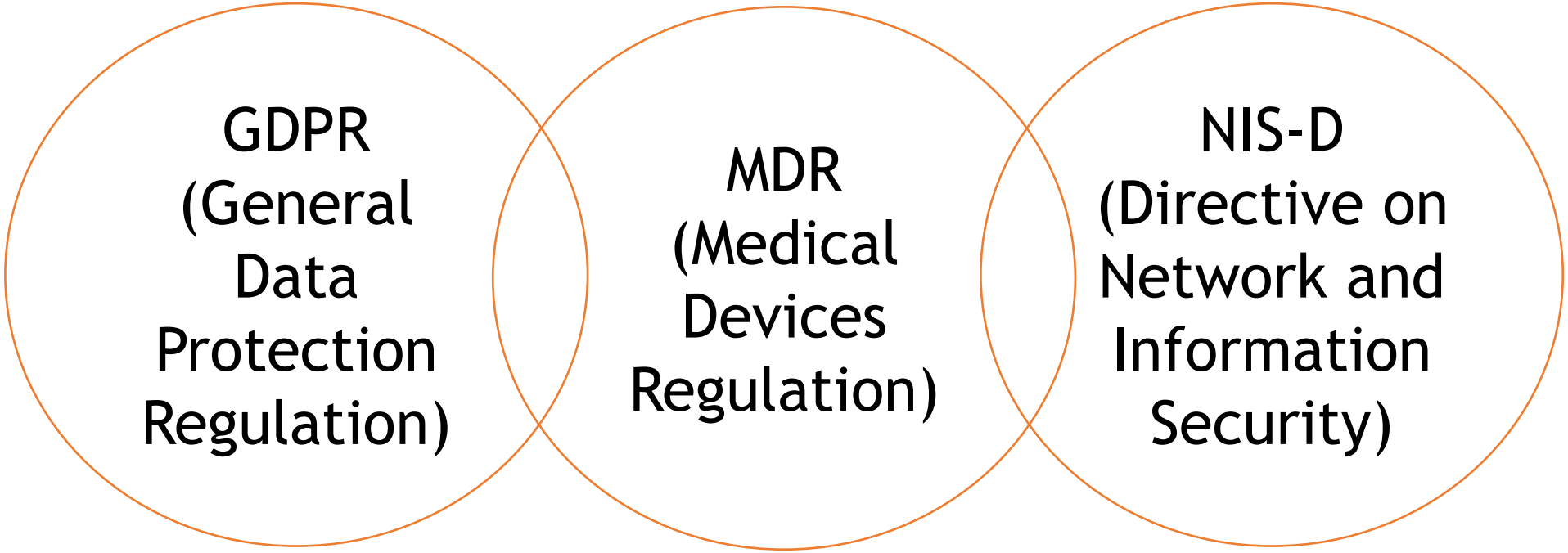
We also deal with the protection and management of intellectual property and competition rights: copyright, design, patents, unfair competition, consumer protection and media law, unfair commercial practices, misleading and comparative advertising, the labeling and sale of foodstuffs.

Our professionals regularly advise multinational companies on legal and technical issues, offering a strategic and holistic approach. Our goal is to turn legal advice into a competitive advantage for our clients.

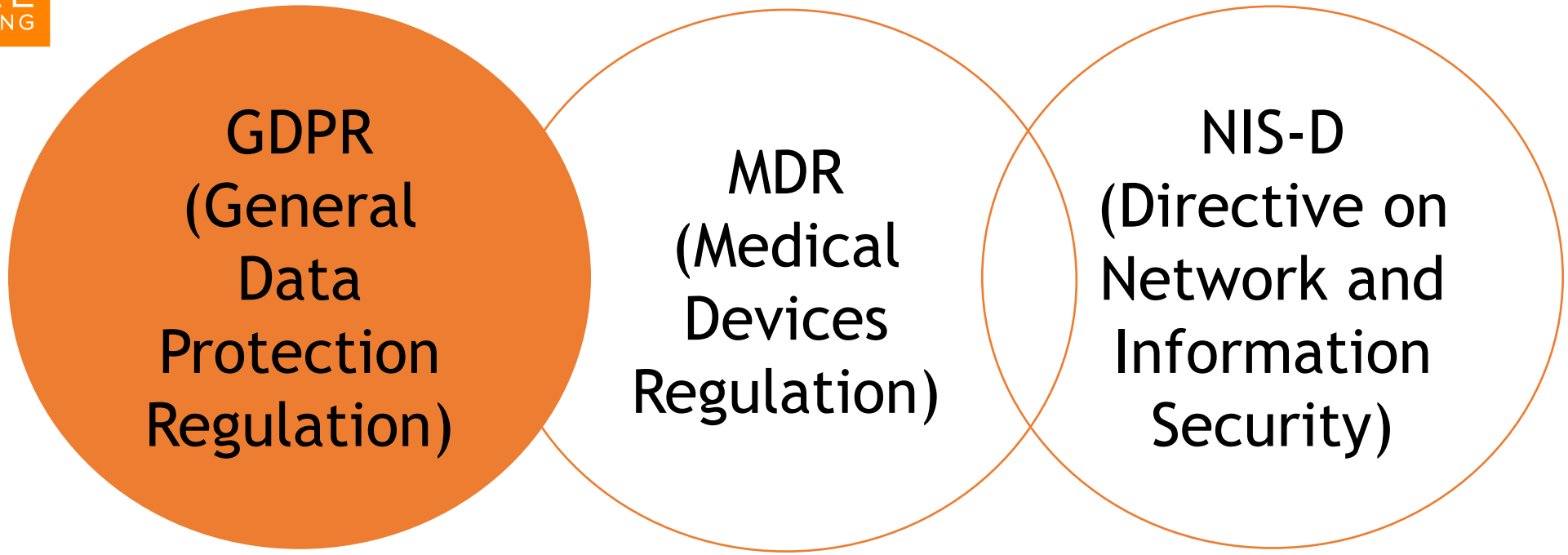
Main Practice Areas



Applicable Legal Framework



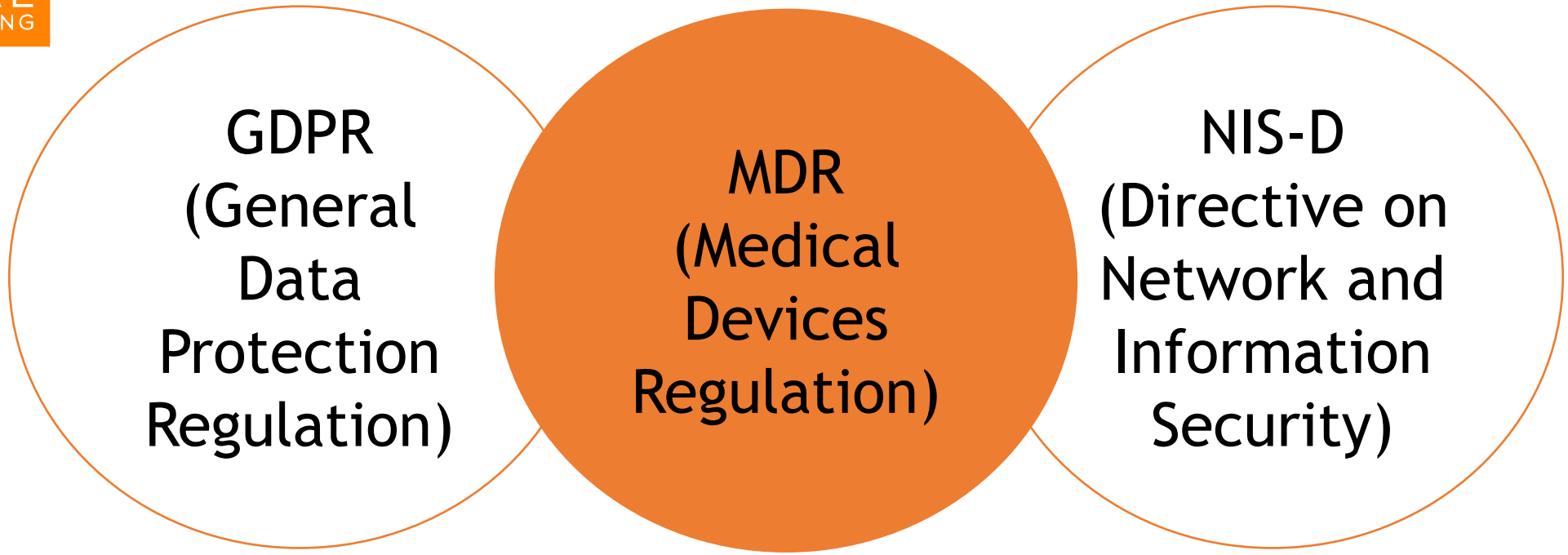
Applicable Legal Framework



Indicates principles and obligations relating to the protection of rights and freedoms of data subjects, e.g.:

- Data protection by design and by default, and principles of lawfulness, fairness and transparency
- Data Protection Impact Assessments, and security measures

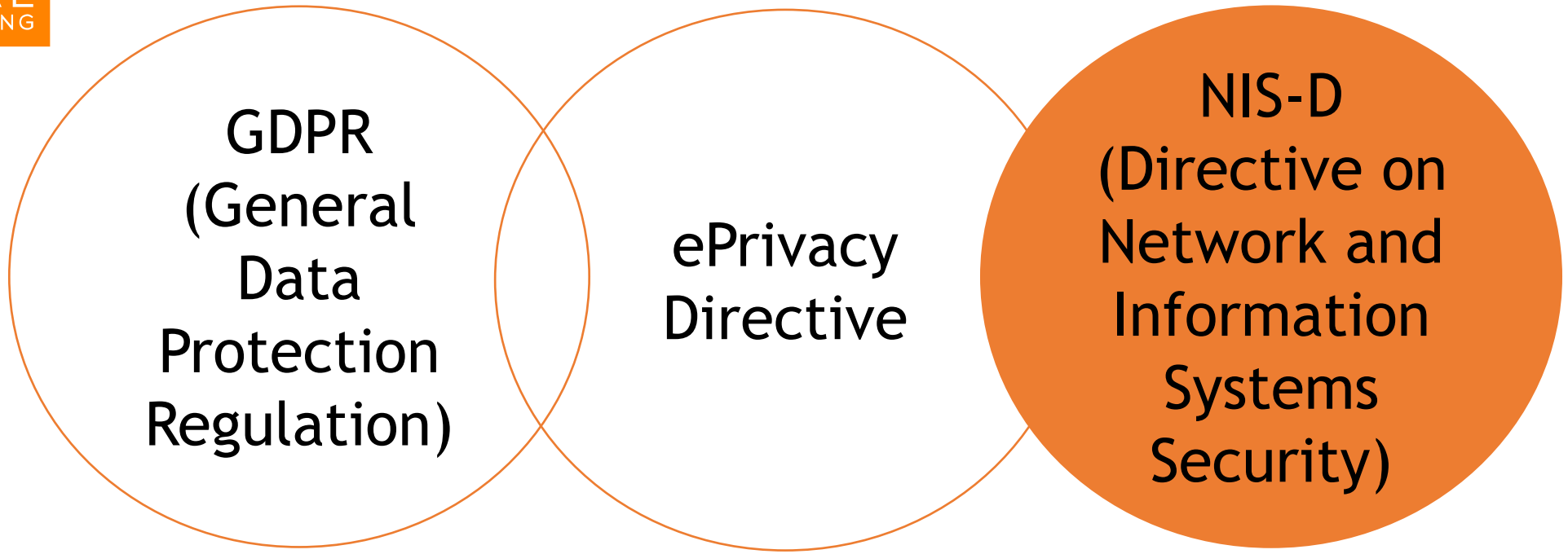
Applicable Legal Framework



Ensure a consistent high level of health and safety protection for EU citizens for using medical devices:

- Defining devices in the healthcare sector and classifying them
- Designing and manufacturing medical devices
- Making available or putting into service medical devices for human use and placing them on the market

Applicable Legal Framework



Establishes a common level of security for network and information systems focusing on Essential Service Providers and Digital Service Providers, e.g.:

- Security requirements and,
- Incident notifications and coordination of Computer Incident Response Teams

The General Data Protection Regulation

Personal Data: Any information relating to an identified **or** identifiable natural person ("data subject").

An **identifiable natural person** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Special Categories of Personal Data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership

- ✓ **Data concerning health** means personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- ✓ **Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- ✓ **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

The General Data Protection Regulation

Accountability: The controller shall be responsible for, and be able to demonstrate compliance with the GDPR (Art. 5 (2) and Art. 24 GDPR)

Data Controller: the company or public authority / agency which, determines the **purposes** (the why) and the means (the what and how) of the processing (Art. 4 (7) GDPR).

Data Processor: the company or public authority / agency, which processes personal data on behalf of the controller, per instructions of the controller (Art. 4 (8) GDPR).

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The General Data Protection Regulation

The objectives:

1. Protect individuals' personal data

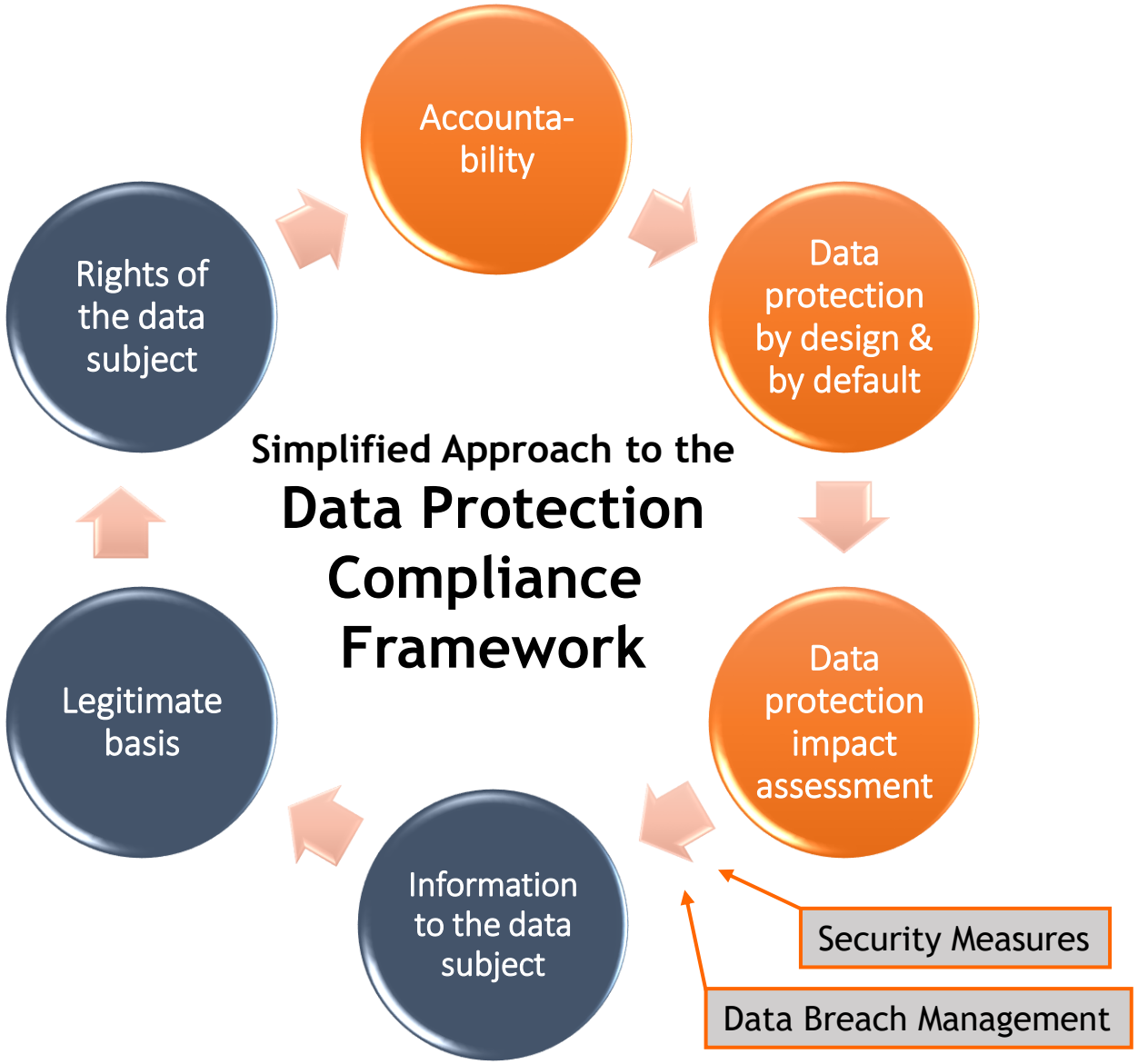
2. Ensure the free movement of personal data within the Union

The territorial scope:

- ✓ **Criterion 1**: The GDPR applies where processing takes place "in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not."
- ✓ **Criterion 2**: The GDPR applies to controllers or processors not established in the Union, where the processing activities relate to:
  - ✓the offering of goods or services to data subjects in the Union; OR
  - ✓the monitoring of the behaviour of data subjects in the Union.

The GDPR reiterates Data Protection by Design and by Default

- Accountability
- Data Protection Impact Assessments
- Security Measures



Accountability under the GDPR means…

The responsibility of Data Controllers when processing personal data is:

- To ensure, and **to be able to demonstrate**, compliance with the GDPR, implementing appropriate:
  - Technical measures
  - Organisational measures (i.e. data protection policies, complying with approved codes of conduct or certification mechanisms)

[Art. 24 GDPR: Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. Those measures shall be reviewed and updated where necessary.]

Data Protection by Design and by Default: GDPR

- **Data protection by design and by default** raises concerns in terms of the guarantees that e-healthcare platforms may offer (intrusive nature)

- According to the characteristics of the platform, the data subjects should be protected **by design** and **by default**

- **Producers of products, services and applications** should take into account the right to data protection in the development & design stages to ensure that controllers and processors are able to fulfil their data protection obligations

- Conducting a **Data Protection Impact Assessment** to make sure that from the designing of the e-healthcare platform /tool, privacy is taken into consideration

Data Protection by Design and by Default: GDPR

The CNIL offers a software to **conduct a Privacy Impact Assessment:**

- ✓ A **legal and technical knowledge** base
- ✓ A modular tool: **customisable content** based on the specific needs
- ✓ **Portable** and **web versions**

Security by Design: MDR

- Electronic programmable systems shall be **developed and manufactured in accordance with the state of the art** (e.g., principles of development life cycle, risk management, information security, verification and validation)
- Manufacturers shall set out **minimum requirements** concerning **hardware, IT networks characteristics** and **IT security measures**, (e.g., protection against unauthorised access, necessary to run the software as intended).
- PANACEA's **Security-by-Design Framework (SbDF)**

Security Measures

The responsibility of the controller to **ensure** and **demonstrate** compliance is challenging:

- Risk-based approach in security: **assessing the risk** of the processing activities; and implementing **security and organisational measures**
  - Physical / technical separation of personal data and encrypted data
  - Pseudonymisation is crucial in clinical trials
  - Respect access rights protocols (i.e., **do not** share credentials)
  - Securely sharing health data (in encrypted forms)
  - Follow **confidentiality** obligations

Security Measures

The CNIL has created a practical Guide listing the **basic precautions** that should be implemented **systematically**:

1. Listing the processing activities (of personal data)
2. Assessing the risks (generated by each processing)
3. Implementing the planned security measures
4. Carrying out periodical security audits

Provides 17 Factsheets on security measures, such as:

- Authenticating Users (N° 2)
- Access Management (N° 3)
- Securing servers (N° 8) and websites (N° 9)
- Managing data processors (N° 13)
- Encrypting, Guaranteeing Integrity and signing (N° 17)

ENISA's Mapping of OES Security Requirements to Specific Sectors

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27799	HIPAA
Part 1 – Governance and Ecosystem				
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	5.1 Management direction for information security 6.1 Internal organization	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility Risk analysis Risk management
		Information system security policy	5.1 Management direction for information security 6.1 Internal organization	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility
		Information system security accreditation	5.1 Management direction for information security 6.1 Internal organization 8.1 Responsibility for assets 8.2 Information classification	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility Risk analysis Risk management
		Information system security indicators	5.1 Management direction for information security 6.1 Internal organization 18.1 Compliance with legal and contractual requirements 18.2 Information security reviews	Assigned Security Responsibility
		Information system security audit	5.1 Management direction for information security 6.1 Internal organization 7.1 Prior to employment 7.2 During employment 7.3 Termination and change of employment	
Part 2 – Protection				
2.1	**IT Security Architecture**	Systems configuration	13.1 Network security management 13.2 Information transfer	–
		System segregation	13.1 Network security management 13.2 Information transfer	–
		Traffic filtering	13.1 Network security management 13.2 Information transfer	–
		Cryptography	13.1 Network security management	–

THE EU CYBERSECURITY AGENCY

➢ Also see the Procurement Guidelines for Cybersecurity in Hospitals

Security measures during COVID-19 pandemic
ENISA's Cybersecurity advice to healthcare sector

- Arrange **clear communication channels and information** within the healthcare staff (e.g., raise awareness internally)
- If systems are compromised:
  - Freeze any activity in the system – disconnecting the infected machines from others and from medical device
  - Go off-line from the network
  - Immediately contact the national Computer Security Incident Response Teams (CSIRTs)
- Ensure **business continuity** through effective backup and restore procedures
  - The role of e-health provider must be well-defined when failure of a system disrupts the hospital's core services, i.e., Data Processing Agreements
- In case **of impact to medical devices**, incident response should be coordinated with the device manufacturers
- A preventative measure is **network segmentation** – network traffic can be isolated and / or filtered to limit and / or prevent access between network zones

Security Measures: Data Breach Management

The responsibility of the controller to **ensure** and **demonstrate** compliance is challenging:

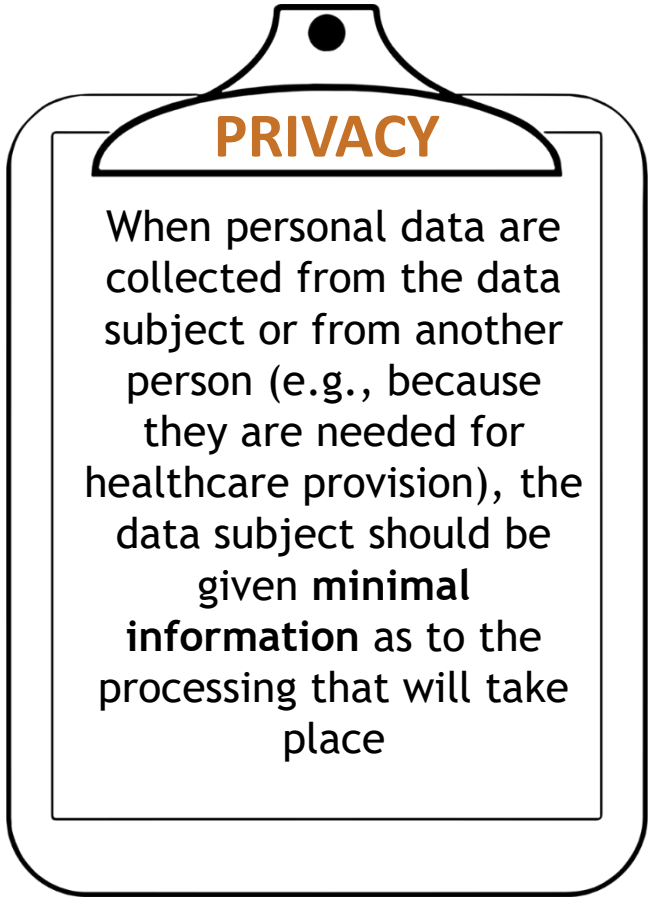
- Data breach management (Art. 33-34 GDPR): organisations have **72 hours** from when they became aware of an incident to communicate it to the relevant supervisory authority, and in some cases, to the data subject involved
- **Communication** is key, be aware of **who** should be contacted and **what** information is required from you

Network and Information Security Directive

Directive (EU) 2016/1148 on Security of Network and of Information Systems

- Healthcare is one of the sectors identified as **Operators of Essential Services** (OES) under the NISD
- Identified OES must:
  - take appropriate security measures to secure their network and information systems
  - take appropriate security measures prevent and minimize the impact of security incidents to ensure service continuity
  - **notify serious cyber incidents** (those having significant impact on service continuity) to the relevant national authority without undue delay

Principle of Transparency

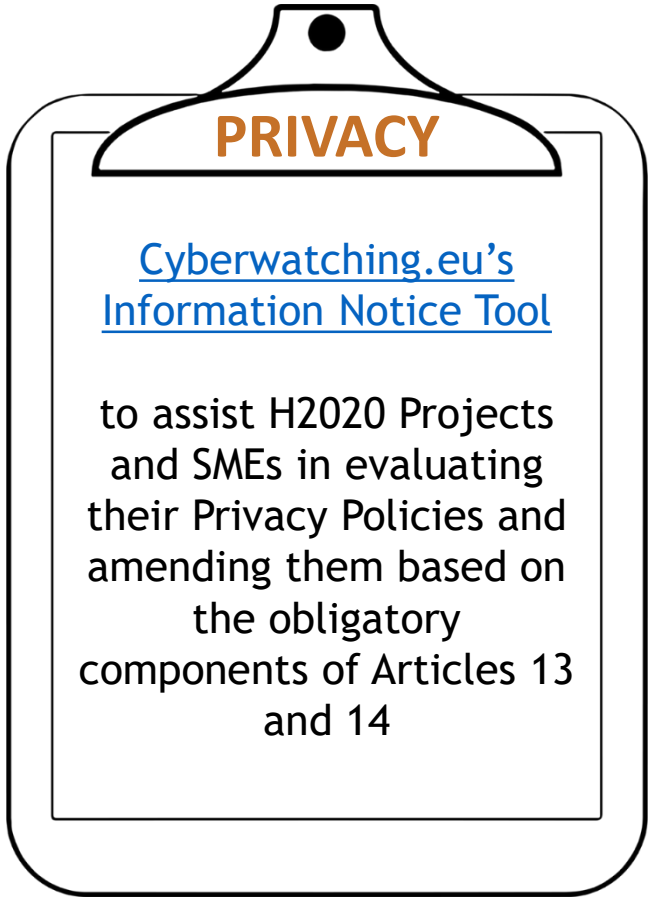


Information that must be disclosed to the Data Subject:

- ❑ Identity and contact details of **data controller**
- ❑ Contact details of **the data protection officer** (where applicable)
- ❑ The **purposes** of processing their personal data
- ❑ The **recipients** of the personal data
- ❑ The **legal basis** of the processing
- ❑ The existence of and the how to freely exercise their **data subject rights**

[Artt. 13, 14 GDPR]

Principle of Transparency



Information that must be disclosed to the Data Subject:

- ✓ Identity and contact details of **data controller**
- ✓ Contact details of **the data protection officer** (where applicable)
- ✓ The **purposes** of processing their personal data
- ✓ The **recipients** of the personal data
- ✓ The **legal basis** of the processing
- ✓ The existence of and the how to freely exercise their **data subject rights**

[Artt. 13, 14 GDPR]

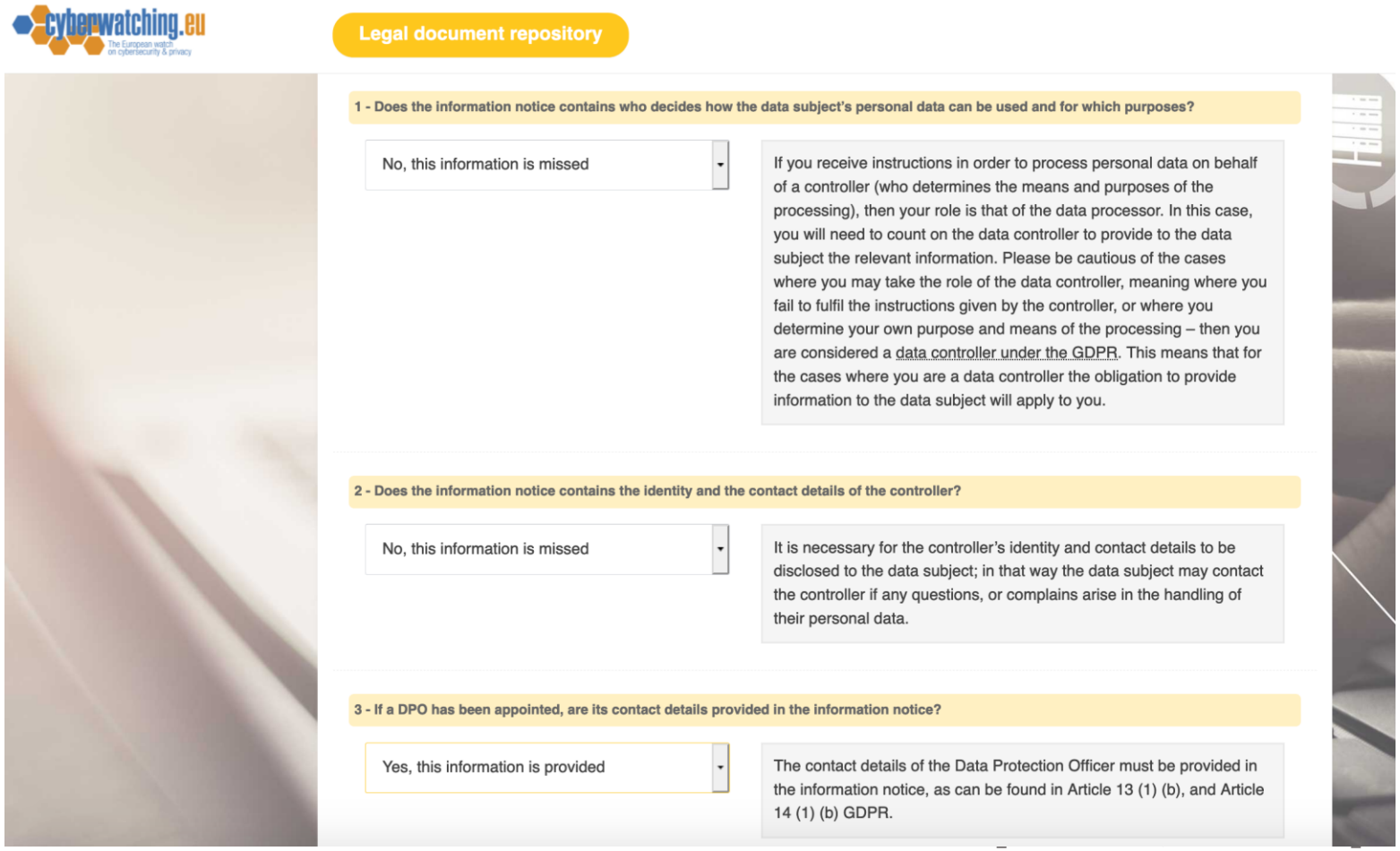
Principle of Transparency

cyberwatching.eu INFORMATION NOTICE TOOL

PRIVACY

[Cyberwatching.eu's Information Notice Tool]

to assist H2020 Projects and SMEs in evaluating their Privacy Policies and amending them based on the obligatory components of Articles 13 and 14



Principle of Transparency

Informed Consent: clinical investigations

PRIVACY

When personal data are collected from the data subject or from another person (e.g., because they are needed for healthcare provision), the data subject should be given **minimal information** as to the processing that will take place

A data subject can provide informed consent after having been duly informed of:

- ❑ the nature, objectives, benefits, implications, risks and inconveniences of the clinical investigations
- ❑ The **data subject's rights and guarantees** (right to refuse to participate and withdraw from clinical investigation)
- ❑ The conditions of the clinical investigation
- ❑ The possible treatment alternatives

Data Subject Rights

- Any organisation that processes personal data must ensure that data subjects are **informed** about their rights and how to **freely exercise** them:
  - ❑ Right of **access** (Art. 15 GDPR): By what means can the persons concerned obtain the information relating to them.
  - ❑ Right to **rectification** (Art. 16 GDPR): How to complete incomplete / inaccurate data.
  - ❑ Right to **erasure** (Art. 17 GDPR): Allowing the deletion of any data relating to the data subject.
  - ❑ Right to **restrict the processing** (Art. 18 GDPR): Under certain conditions, the data subject may request for the organisation to restrict its processing

Data Subject Rights

- Any organisation that processes personal data must ensure that data subjects are **informed** about their rights and how to **freely exercise** them:

  - ❑ Right to **data portability** (Art. 20 GDPR): The ability to transfer the data in a structured, commonly-used and machine-readable format to the data subject.

  - ❑ Right to **object to processing** (Art. 21 GDPR): The data subject may object to the processing if the controller relies on the performance of a task carried out in the public interest, or on the legitimate interest of the organisation.

  - ❑ Right not to be subject to a **decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Art. 22 GPDR).

Principle of Lawfulness

Choosing the **correct legal basis** for the processing activities of **personal data** (e.g. name, DOB, contact details):

- **Performance of contract:** The personal data collected from patients must be necessary for the provision of the contract;
- **Consent:** For processing beyond the provision of healthcare, consent can be relied upon (e.g., marketing. It must be clearly distinguishable, intelligible and easy to access, in clear and plain language as per Art.9 GDPR);
- **Legal obligation:** A regulation or law obliges the healthcare organisation to collect or retain data;
- **Legitimate interest:** The organisation has an interest which is not overridden by the interests or rights of the data subject;
- **Vital interests** of the data subject: The organisation is faced with the life-or-death of the data subject at hand and the data subject is physically or legally incapable of giving consent;
- **Public interest.**

[Art. 6 GDPR]

Principle of Lawfulness

Choosing the **correct legal basis** for the processing activities of **special categories** **of personal data**:

- **Explicit Consent:** For processing beyond the provision of healthcare, consent can be relied upon. It must be clearly distinguishable, intelligible and easy to access, in clear and plain language (Art.9 GDPR);
- **Vital interests** of the data subject: The organisation is faced with the life-or-death of the data subject at hand and the data subject is physically or legally incapable of giving consent.
- **Preventative or occupational medicine:** Processing is necessary for the medical diagnosis, provision of health / social care / treatment, or the management of health or social care systems and services.
- **Public interest in the area of public health:** The organisation must protect the society against serious cross-border threats to health, or to ensure high standards of quality and safety of health care and medicinal products / devices.
- **Archiving purposes in the public interest, scientific or historical research purposes:** The organisation must be carrying out scientific research, as defined in the European Data Protection Supervisor Preliminary Opinion on data protection and scientific research

Principle of Purpose Limitation

The personal data must be collected for **specified**, **explicit** and **legitimate** purposes.

No further processing may occur if it is **incompatible with those purposes.**

Principle of Purpose Limitation

The personal data must be collected for **specified**, **explicit** and **legitimate** purposes.

No further processing may occur if it is **incompatible with those purposes.**

Compatibility test between initial and later purpose, takes into account:

- A **link** between purposes;
- The **context of collection** of personal data;
- The nature of personal data (e.g., special categories of personal data);
- Possible **consequences** of the further processing to the data subjects;
- Existence of appropriate **safeguards** (e.g. encryption / pseudonymisation).

[Art. 5(1(b)) GDPR]

Principle of Data Minimisation

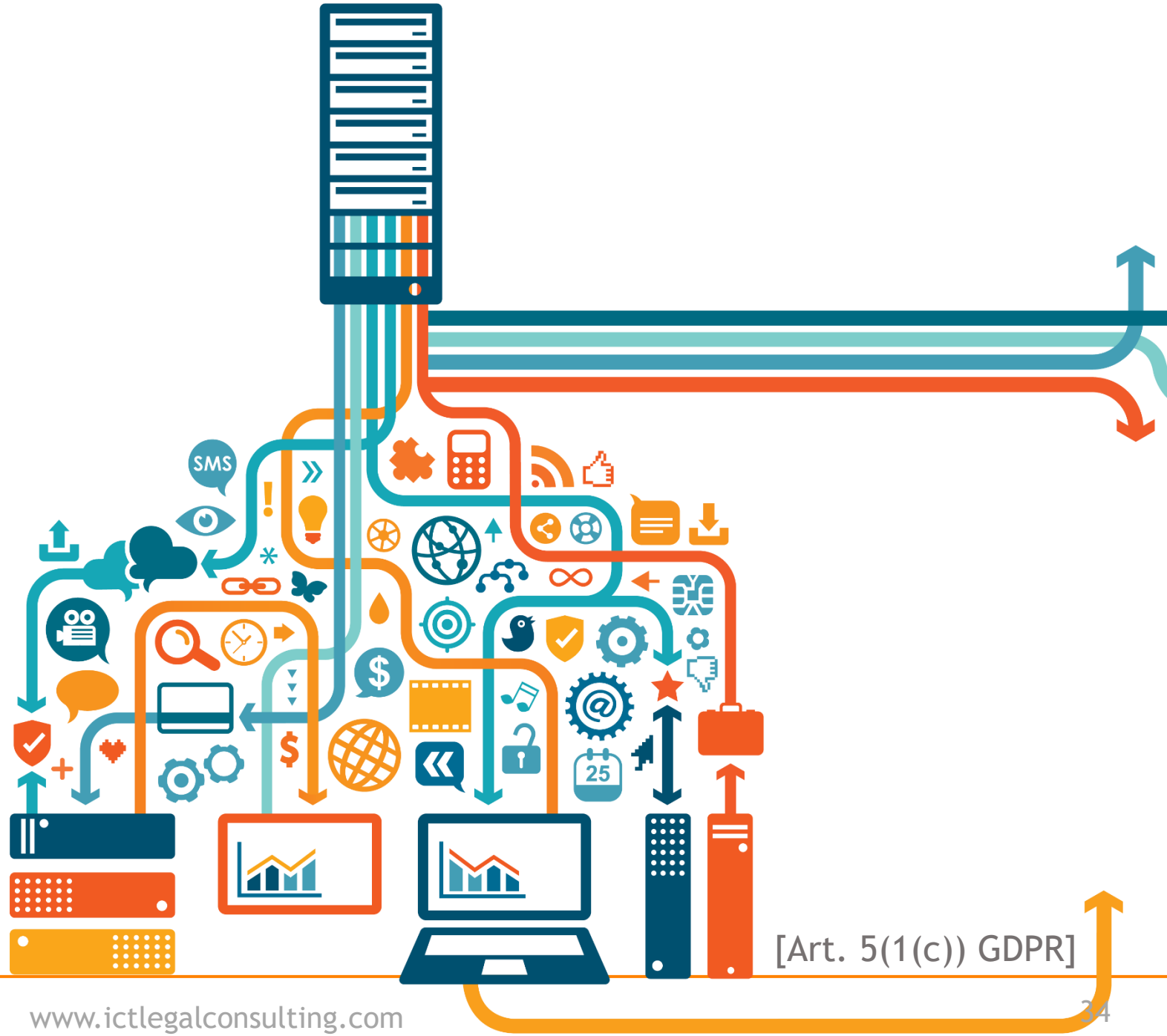
Personal data collected must be

✓ **adequate**,

✓ **relevant**, and

✓ **limited to what is necessary**

in relation to the purposes



[Art. 5(1(c)) GDPR]

Processing Health Data

Member States can introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

[Art. 9(4) GDPR]

Council of Europe Recommendation on the protection of health-related data

Set of principles to protect health-related data, including:

- "Personal data protection principles should be taken into account **by default (privacy by default)** and incorporated right from the design of information systems which process health-related data (privacy by design). Compliance with these principles should be **regularly reviewed** throughout the life cycle of the processing. The controller should carry out, before commencing the processing and at regular intervals, an **assessment of the potential impact** of the foreseen processing of data in terms of data protection and respect for privacy, including of the measures aimed at mitigating the risk." [Recommendation 4.2]
- ***Protecting health-related data flows*** "Transborder data flows may only take place where an appropriate level of data protection is secured in accordance with the safeguards provided for in Convention 108" [Recommendation 17]

Sanctions and enforcement

- Up to the greater of 2% of an undertaking's total annual worldwide turnover or €10 million for a large number of violations
- Up to the greater of **4% of an undertaking's total annual worldwide turnover** or €20 million for a more limited set of violations, including
  - ➢ *violation of data subjects' rights*
  - ➢ *violation of basic principles for processing (legal basis, new consent rules, **special categories of personal data**)*
  - ➢ *violation of the rules on data transfers*

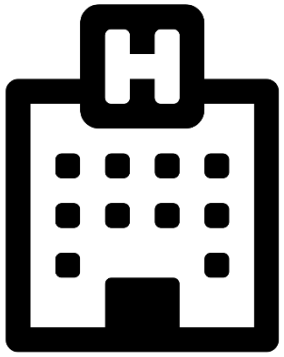
Fines

- Right to **lodge a complaint** with a Supervisory Authority for processing of their data in violation with the GDPR
- Right to **start legal action:**
  - ➢ against a Supervisory Authority for failure to investigate a complaint or keeping the data subject informed
  - ➢ against a controller or processor for processing of their data in violation with the GDPR (courts where controller or processor is established/courts of place of residence of data subject)
- Right to **obtain compensation** for material or immaterial damage
  - ➢ joint liability of controllers and processors for the entire damage
- **Class actions**
  - ➢ certain not-for-profit organizations can be mandated by data subjects to lodge complaints and claim compensation on their behalf
  - ➢ Member States may also mandate organizations to act on behalf of data subjects

Data subjects' right to remedies

Relevance: Recent Fines

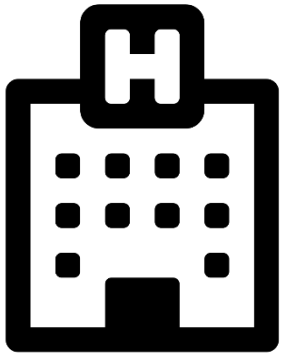
Hospitale do Bareiro



- over 980 doctors, psychologists, technicians, staff and dietitians which **could freely access** patient data, without having been properly authorised to do so,
- Lack of internal policies for access rights,
- Failure to remove access rights of terminated employees.

Relevance: Recent Fines

Hospitale do Bareiro



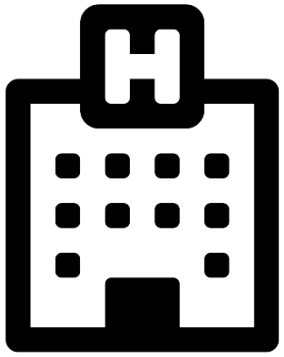
- over 980 doctors, psychologists, technicians, staff and dietitians which **could freely access** patient data, without having been properly authorised to do so,
- Lack of internal policies for access rights,
- Failure to remove access rights of terminated employees.

The Portuguese Data Protection Authority fined the hospital **400,000 EUR**

150,000.00 EUR for a breach of the **principle of integrity**;
150,000.00 EUR for a breach of the **principle of confidentiality**;
100,000.00 EUR for a breach of the **principle of data minimisation;**

Relevance: Recent Fines

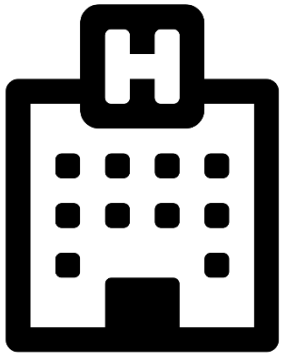
Haga Hospital



- Dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person.
- Insufficient security measures in 2 areas:
  1. Hospital must regularly check who consults patient records;
  2. Good security requires authentication with at least two factors (i.e., password and staff pass).

Relevance: Recent Fines

Haga Hospital



- Dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person.
- Insufficient security measures in 2 areas:
  1. Hospital must regularly check who consults patient records;
  2. Good security requires authentication with at least two factors (i.e., password and staff pass).

The Dutch Data Protection Authority fined the hospital **460,000 EUR**

and **simultaneously** imposed an order subject to a penalty

*If the Haga Hospital has not improved security before 2nd of October 2019, the hospital must pay **100,000 EUR every two weeks**, with a maximum of 300,000 EUR.*

Awards

Balboni
Bolognini
& Partners

Thank you for your attention!

Prof Dr Paolo Balboni – Founding Partner

paolo.balboni@ictlegalconsulting.com

Anastasia Botsi – Associate, LL.B.

anastasia.botsi@ictlegalconsulting.com