



Balboni
Bolognini
& Partners



A Novice's Guide to build a solid GDPR Data Protection Compliance Framework: a focus on the healthcare sector

ICT Legal Consulting

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

Anastasia Botsi - Associate
anastasia.botsi@ictlegalconsulting.com

Milan - Bologna - Rome - Amsterdam

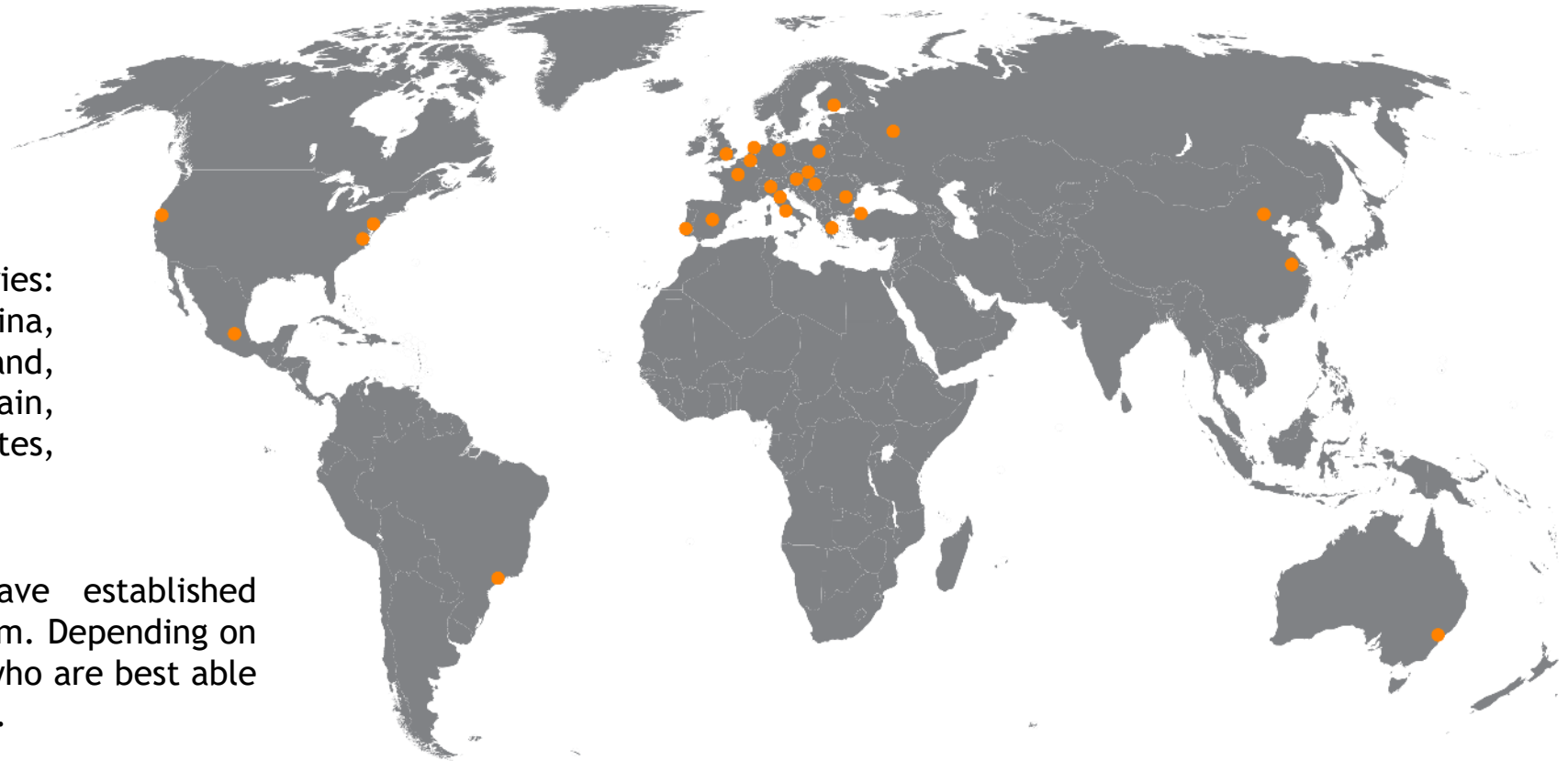


The Firm

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.

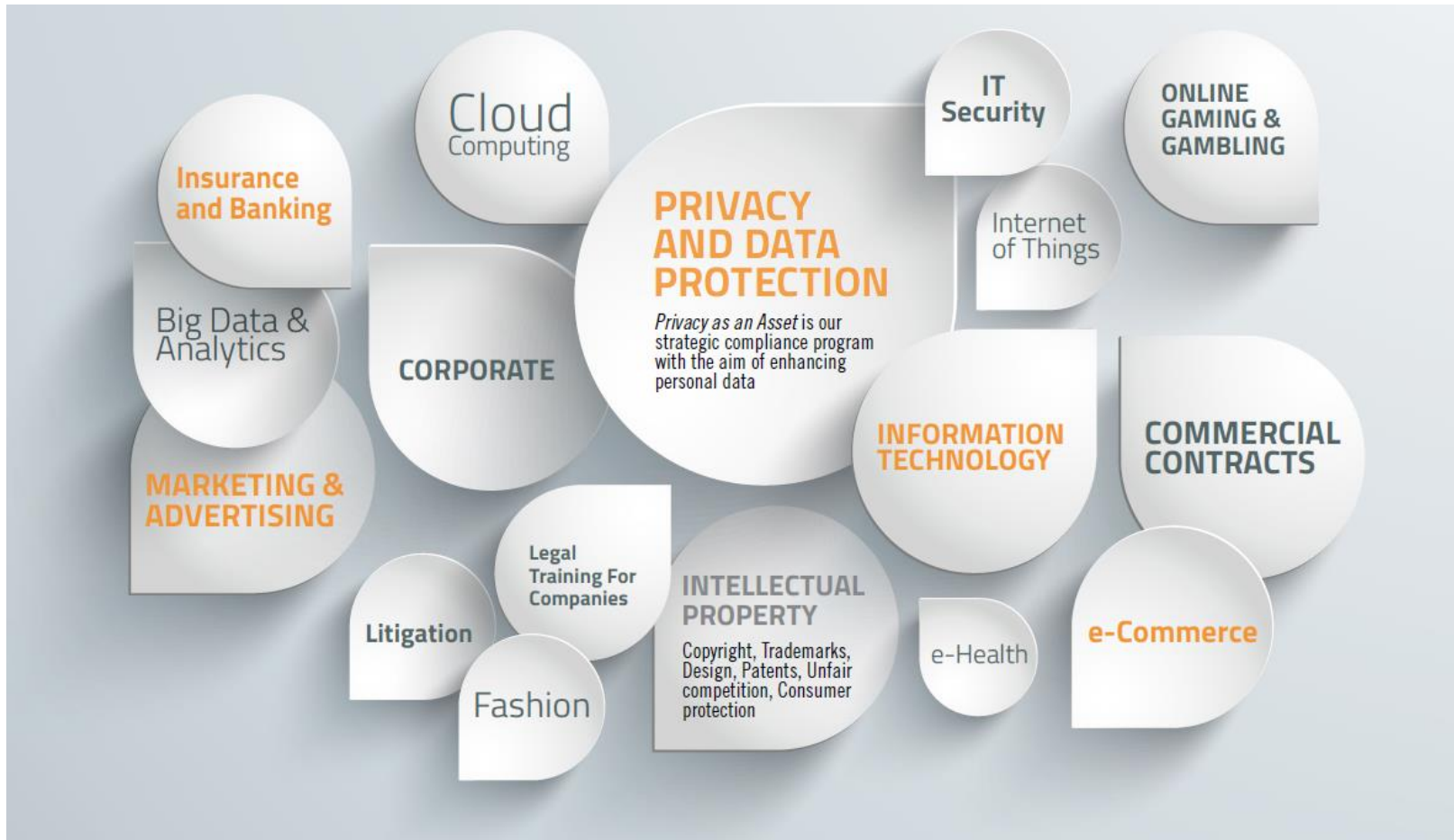
We have developed significant expertise working with multinationals and companies in the communications, media & entertainment, IT, healthcare, pharmaceutical, fashion, food & beverage, energetic and smart grids, banking/financial services, automotive, industrial manufacturing and eGovernment sectors.

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





The Team



PAOLO BALBONI, Prof. Dr. - Founding Partner

Prof. Dr. Paolo Balboni is a top-tier ICT, privacy & data protection lawyer and Founding Partner of ICT Legal Consulting. Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity within the Maastricht University Faculty of Law. Lead Auditor BS ISO/IEC 27001:2013 (IRCA Certified).



AVV. LAURA SENATORE - Partner

Laura joined ICT Legal Consulting in 2017 and is now a Partner of the firm. Fellow of the Italian Institute for Privacy, graduated cum laude in law at the University of Salerno. She worked as a trainee at the Italian Data Protection Authority (*Garante per la protezione dei dati personali*).



ANASTASIA BOTSI - Associate , LL.B.

Anastasia joined ICT Legal Consulting in 2018 and is now an Associate of the firm. Professionally certified DPO by the European Center of Cybersecurity and Privacy, and a sponsored researcher of the Dutch Science Foundation, to analyse the legislative management of cybersecurity risks and trained in European Law.

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

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

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

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

The **objectives**:

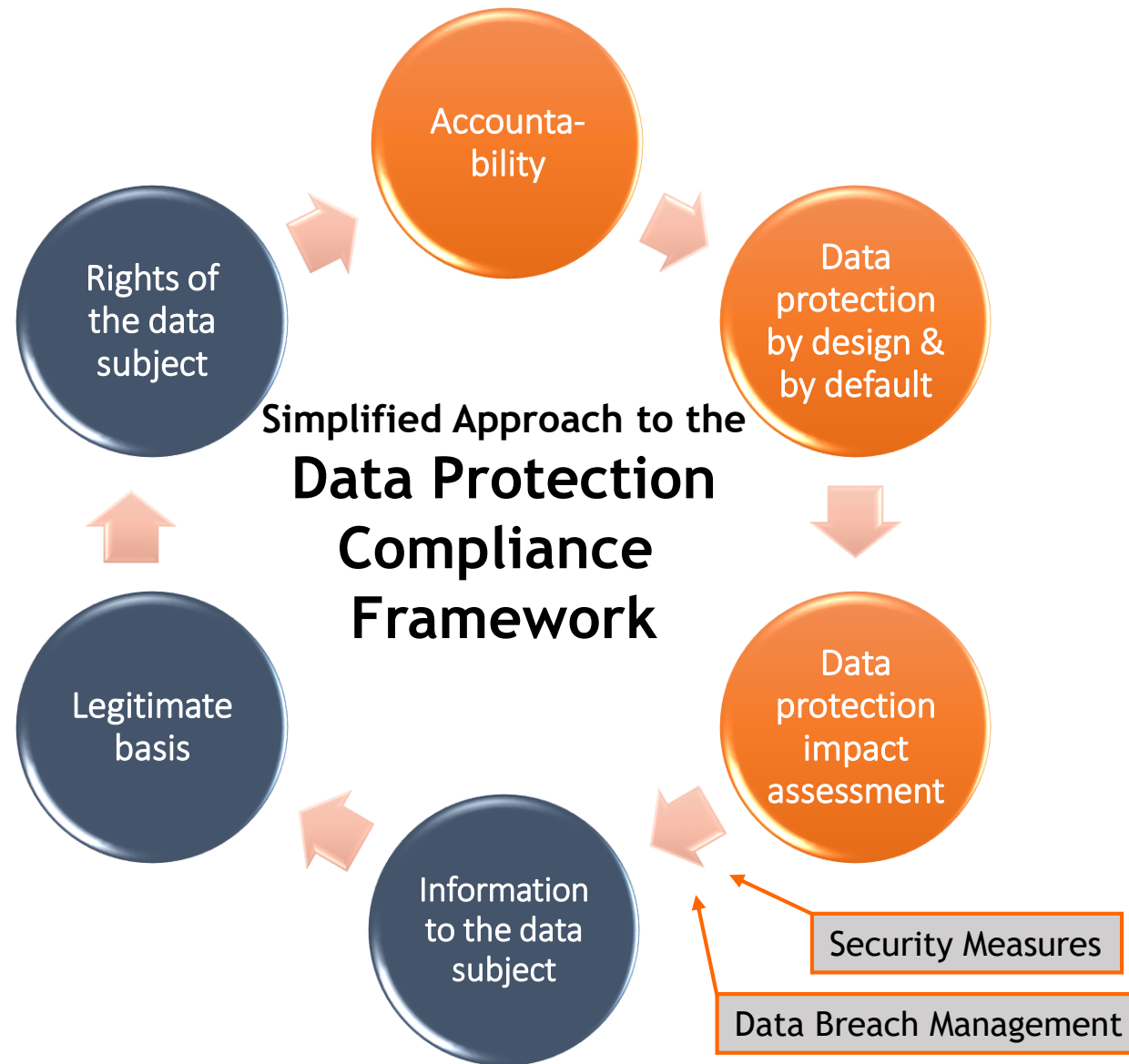
1. Protect individuals' personal data
2. Ensure the free movement of personal data within the Union

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 is a Game Changer for Privacy

- Accountability
- 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.]

Security

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
 - Respect access rights protocols (i.e., **do not** share credentials)
 - Securely sharing health data (in encrypted forms)
 - Follow **confidentiality** obligations



Security

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



Principle of Transparency

PRIVACY

When personal data are collected from the data subject or from another person (e.g., because they are provided by a third party, or collected from a pre-existing record), the data subject should be given **minimal information** as to the processing that will take place

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**



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 GDPR).

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.

Art. 9 GDPR

CAUTION

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.



THIS IS SPARTA



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).

Sanctions and enforcement

➤ Fines

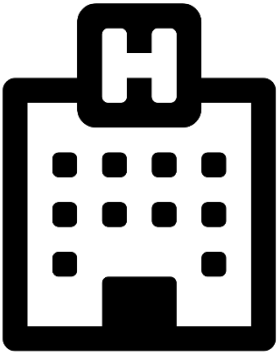
- Up to the greater of 2% of an undertaking's total annual worldwide turnover or €10 million for a large number of violations
- Up to the greater of **4% of an undertaking's total annual worldwide turnover** or €20 million for a more limited set of violations, including
 - *violation of data subjects'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

➤ Data subjects' right to remedies

- Right to **lodge a complaint**
 - with a Supervisory Authority for processing of data in violation of the GDPR.
- Right to **start legal action**
 - against a Supervisory Authority for failure to investigate a complaint or failure to keep the data subject informed;
 - against a controller or processor for processing of data in violation of the GDPR (courts where the controller or processor are 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.

Relevance: Recent Fine

Hospitale do Bareiro



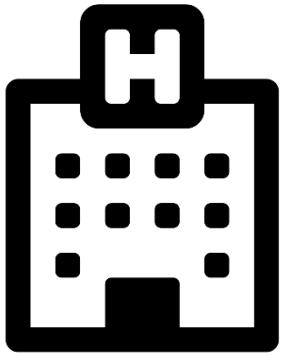
- over 980 doctors, psychologists, technicians, staff and dietitians which **could freely access** patient data, without having been properly authorised to do so.
- Lack of internal policies for access rights
- Failure to remove access rights of terminated employees

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 Fine

Haga Hospital



- The investigation revealed that 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)

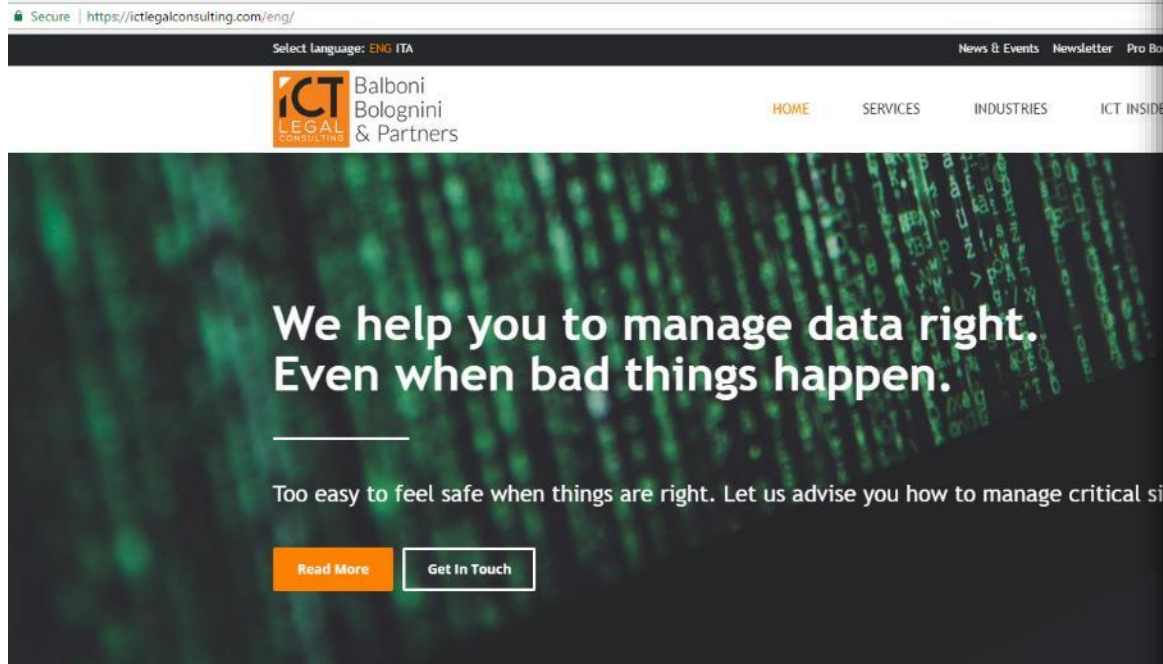
The Dutch Data Protection Authority fined the hospital **460,000 EUR**

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

*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.*

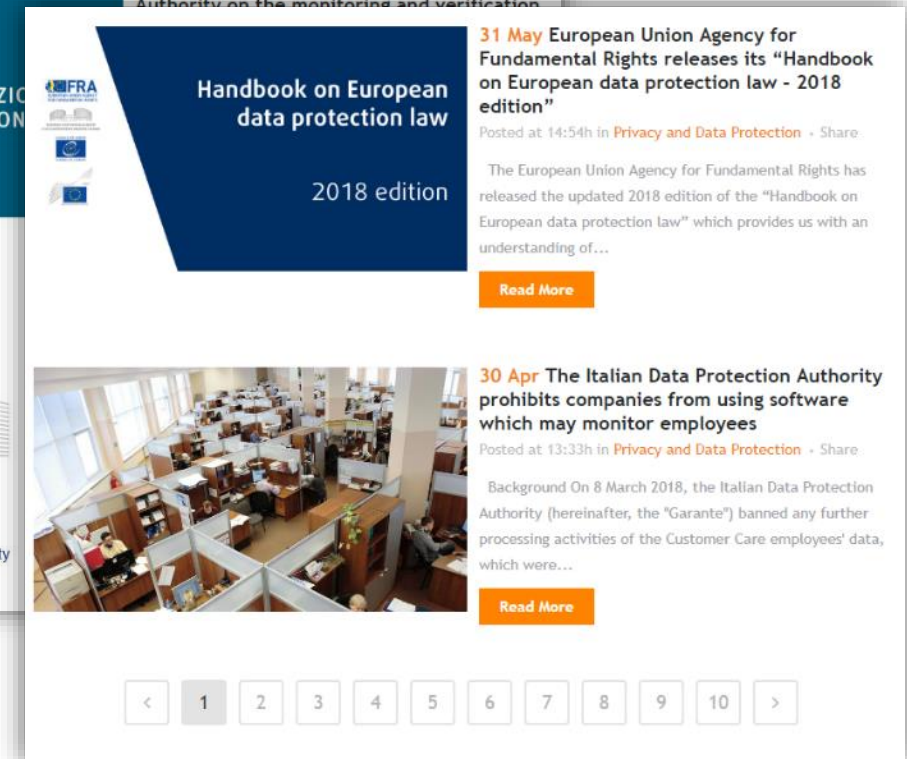


Website & Publications



Stay updated!

ictlegalconsulting.com/eng/newsletter/



Awards





Balboni
Bolognini
& Partners

Thank you for your attention!

Anastasia Botsi - Associate, LL.B.

anastasia.botsi@ictlegalconsulting.com

© 2019 ICT Legal Consulting - All rights reserved. This document or any portion thereof may not be reproduced, used or otherwise made available in any manner whatsoever without the express written permission of ICT Legal Consulting, except for the use permitted under applicable laws

info@ictlegalconsulting.com - www.ictlegalconsulting.com

“Excellence is not an act but a habit” Aristotle