ICT LEGAL CONSULTING

cyberwatching.eu
The European watch
on cybersecurity & privacy

ICTLC - ICT Legal Consulting

Laura Senatore– Senior Associate

laura.senatore@ictlegalconsulting.com

Presents

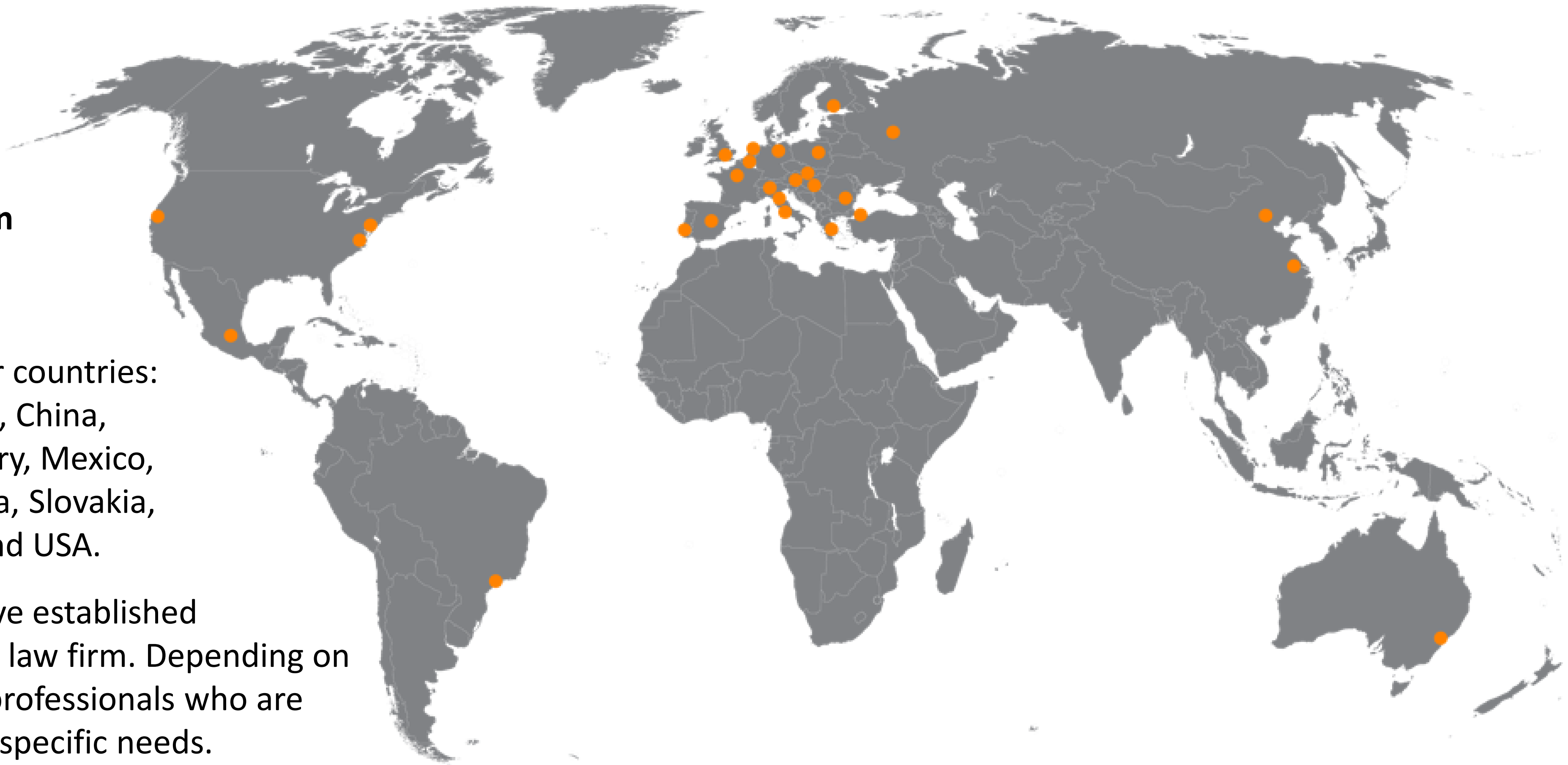
GDPR and recent EU directives and laws

The Firm – Global Presence

ICT Legal Consulting is an international law firm founded in 2011 with offices in Amsterdam, Milan, Bologna, and Rome.

We are present in nineteen other countries: Australia, Austria, Belgium, Brazil, China, France, Germany, Greece, Hungary, Mexico, Poland, Portugal, Romania, Russia, Slovakia, Spain, Turkey, United Kingdom and USA.

In each of these countries we have established partnerships with more than one law firm. Depending on the assignment, we contact the professionals who are most capable of meeting clients' specific needs.



The Expertise

Avv. Laura Senatore - Senior Associate

Laura joined ICT Legal Consulting in 2017 and he is now Senior Associate 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*).

She provides legal advice to multinationals and start-ups on privacy and personal data protection, with special reference to GDPR compliance. In addition, she participates to several H2020 European Projects on privacy and cybersecurity. Lawyer admitted at the Salerno Bar (Italy), she speaks fluent English and French.

GDPR and recent EU directives and laws

❖ **General Data Protection Regulation (“GDPR”):** Regulation UE 2016/679 on the protection of natural persons with regard to the processing of personal data

- ➢ adopted on 14 April 2016
- ➢ became enforceable in all european Member States on 25 May 2018
- ➢ aims to bring a <u>single standard for data protection among all member states in the EU</u>
- ➢ applies to entities that operate in the EU or deal with the data of any resident of the EU

❖ **NIS Directive:** Directive (EU) 2016/1148 on Security of Network and of Information Systems

- ➢ adopted by the European Parliament on 6 July 2016
- ➢ entered into force in August 2016
- ➢ Member States had to <u>transpose the Directive into their national laws</u> by 9 May 2018
- ➢ Member States have to identify operators of essential services by 9 November 2018
- ➢ aims to create <u>an overall higher level of cybersecurity in the EU</u>
- ➢ affects digital service providers (DSPs) and operators of essential services (OESs)

A Focus on GDPR

Applicable Law

- **Broader territorial reach, when compared to current framework (Directive 95/46/EC)**
  - ✓ **Criterion 1**: The GDPR applies where processing takes place “in the context of the activities of an establishment of a controller <u>or processor</u> in the Union, <u>regardless of whether the processing takes place in the Union or not</u>.”
  - ✓ **Criterion 2**: The GDPR applies to controllers <u>or processors</u> not established in the Union, where the processing activities relate to:
    - ✓ the offering of goods or services to <u>data subjects in the Union</u>; OR
    - ✓ the monitoring of the behavior of data subjects <u>in the Union</u>.

ICT LEGAL CONSULTING

The challenges of the GDPR

- ➢ Accountability
- ➢ Security Measures

Accountability under the GDPR means..

Entities that process personal data have:

➢ To ensure, and **to be able to demonstrate**, compliance with the GDPR – implementing appropriate:

- Technical measures
- Organisational measures

[Art. 24 GDPR]

Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk,**
including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

[Art. 32 GDPR]

ICT LEGAL CONSULTING

A risk-based approach under the GDPR..

Before the GDPR

- ➢ Legislators accepted standard security measures (checklist of security measures)

Data Security since the GDPR

- ➢ Enhanced obligations both for controllers and processors
  - o Assessing processing activities and finding relevant organizational and technical measures

- ➢ There is no list of possible types of security measures, a RISK- BASED APPROACH is needed

- ➢ A challenge for SMEs, since there is less resources

How can this approach be implemented?

✓ **Defining appropriate technical measures**

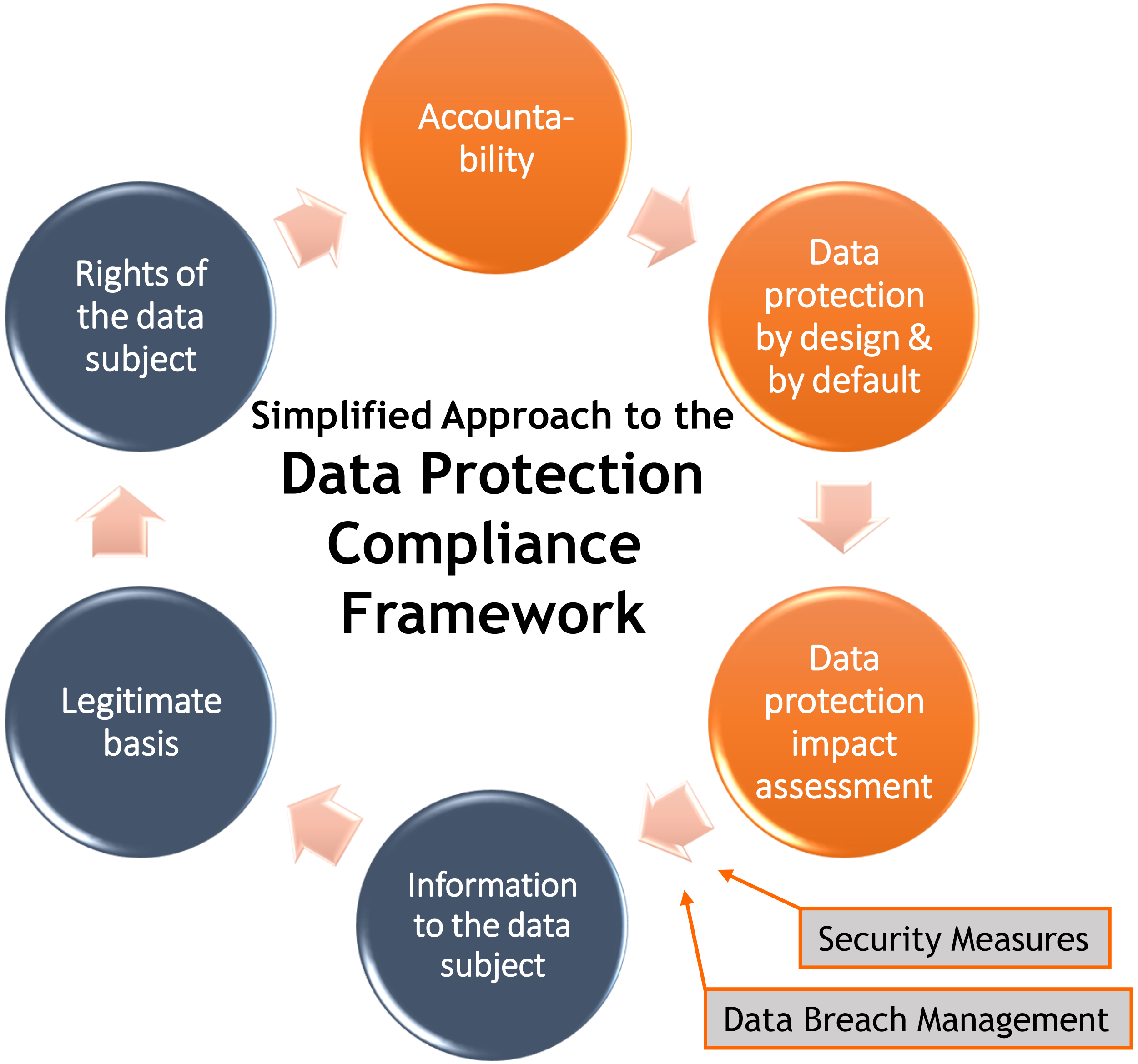
- Each entity processing personal data shall define its own relevant technical measures and describe them in a document (attached to the Record of Processing)

✓ **Annex in Data Processing Agreement (technical measures)**

- Defining the relevant security measures prior to the processing activities
- Having a mandate to implement these security measures with the Data Processor

✓ **Data Protection Compliance Framework (organisational measures)**

- Defining the organisational measures taken in form of Policies, Procedures, Guidelines and Records



Simplified Approach to the Data Protection Compliance Framework

Accounta-bility

Data protection by design & by default

Data protection impact assessment

Information to the data subject

Legitimate basis

Rights of the data subject

Security Measures

Data Breach Management

How can this approach be implemented?

- ✓ Choosing measures based on Principles of Data Protection by Design and by Default
- ✓ Describing security measures in the Record of Processing Activities and attaching them to the Data Processing agreements
- ✓ Conducting a Data Protection Impact Assessment for risky processing activities, and finding the relevant security measures
- ✓ Adopting Data Breach Management Policies
- ✓ Adhering to relevant Certifications to demonstrate compliance

Certifications under GDPR

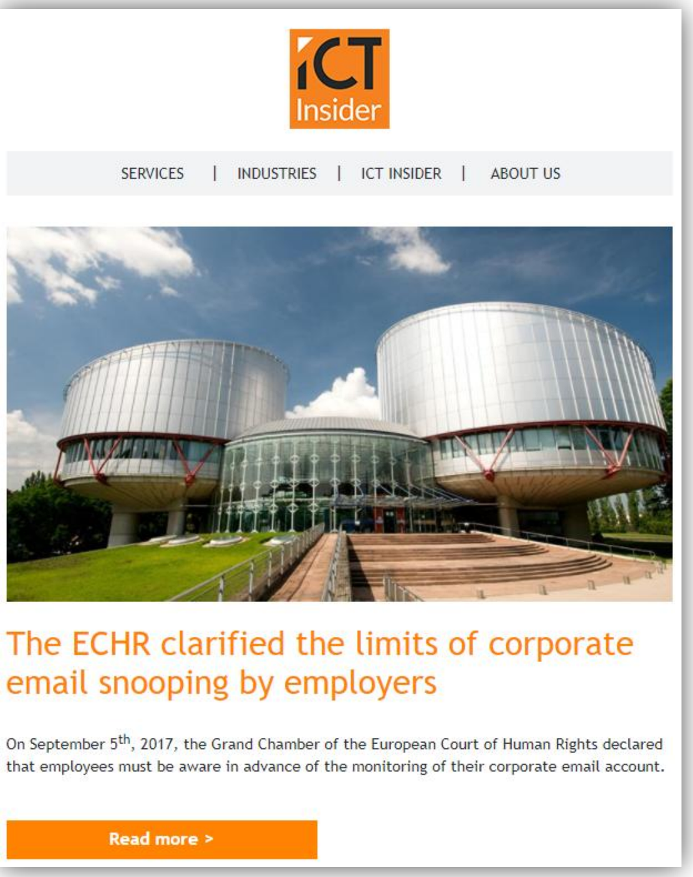
Why could a business be interested in getting a certification according to the GDPR?

- Accountability: certification is an element to demonstrate **compliance**
  - **Art. 24 (3)**: “Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.”

- Transparency: can be ensured
  - **Recital 100:** “In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services"

Stay updated!

ictlegalconsulting.com/eng/newsletter/



The ECHR clarified the limits of corporate email snooping by employers

On September 5th, 2017, the Grand Chamber of the European Court of Human Rights declared that employees must be aware in advance of the monitoring of their corporate email account.

Thank you for your attention!

Laura Senatore– Senior Associate

laura.senatore@ictlegalconsulting.com