Balboni Bolognini & Partners

ICT Legal Consulting

on

GDPR: the possible value of certification in data protection compliance and accountability

Prof. Dr. Paolo Balboni – Founding Partner

Professor of Privacy, Cybersecurity, and IT Contract Law

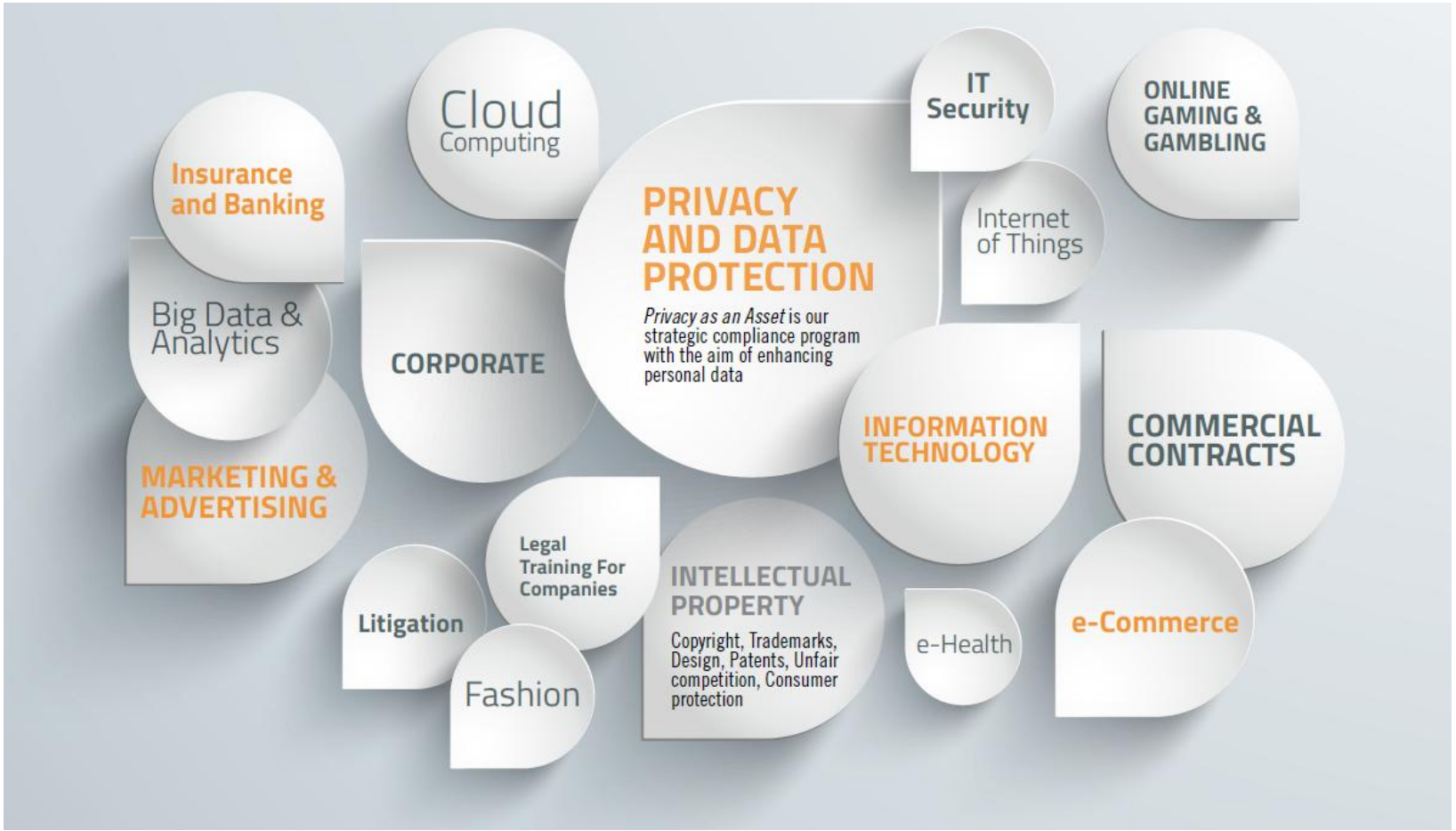
paolo.balboni@ictlegalconsulting.com

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.

Main Practice Areas



The expertise

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. President of the European Privacy Association. Lead Auditor BS ISO/IEC 27001:2013 (IRCA Certified).

Paolo Balboni (qualified lawyer admitted to the Milan Bar) is a Founding Partner of ICT Legal Consulting (ICTLC), a law firm with offices in Milan, Bologna, Rome, an International Desk in Amsterdam, and multiple Partner Law Firms around the world. Together with his team he advises clients in the fields of Personal Data Protection, also acting as Data Protection Officer in outsourcing, Data Security, Information and Communication Technology (ICT) and Intellectual Property Law. Paolo has considerable experience in Information Technologies including Cloud Computing, Big Data, Analytics and the Internet of Things, Media and Entertainment, Healthcare, Fashion, Automotive, Insurance, Banking, Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT).

Paolo is Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law, President of the European Privacy Association based in Brussels and Cloud Computing Sector Director and Responsible for Foreign Affairs at the Italian Institute for Privacy in Rome, Italy. He is involved in European Commission studies on new technologies and participated in the revision of the EU Commission proposal for a General Data Protection Regulation.

He co-chairs the Privacy Level Agreement (PLA) Working Group of Cloud Security Alliance and has acted as the legal counsel for the European Network and Information Security Agency (ENISA) projects on 'Cloud Computing Risk Assessment', 'Security and Resilience in Governmental Clouds', and 'Procure Secure: A guide to monitoring of security service levels in cloud contracts'.

Paolo is the author of the book Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers (T.M.C Asser Press), and of numerous journal articles published in leading European Law reviews.

Graduated in Law at the University of Bologna (Italy) in 2001, Paolo Balboni completed his Ph.D. in Comparative Technology Law at Tilburg University (The Netherlands) in 2008. He speaks Italian, English and Dutch fluently and has good knowledge of French, Spanish, and German.

The General Data Protection Regulation

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)

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

Certification: The establishment of data protection certification mechanisms and of data protection seals and marks, for demonstrating compliance with the GDPR, through a voluntary and transparent process (Art. 42 GDPR)

Certification Bodies: certification bodies which have an appropriate level of expertise in relation to data protection, with ensured accreditations by either a Supervisory Authority and/or a National Accreditation body (according to Reg 765/2008) (Art. 43 GDPR):

- ✓ Independence
- ✓ Established procedures for issuing, periodic review and withdrawal of data protection certification, seals and marks
- ✓ Established procedures for handling complaints about infringements of the certification
- ✓ No conflict of interests

The General Data Protection Regulation

What are the **steps** towards getting a certification?

1. Find an existing certification mechanism that fits the business size and needs (Art. 42(1) GDPR) (the Board will publish a register that collates all certification mechanisms and data protection seals and marks);
2. Submit (either as a Data Controller or Data Processor) the business' processing activities to the certification mechanism, providing all information about the processing activities which are necessary to conduct the certification procedure;
3. Wait for approval by a Supervisory Authority or a Certification Body (depending on type of certification)
4. Certification is issued for a maximum period of three years, after which it may be renewed, under the same conditions

The General Data Protection Regulation

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"

The General Data Protection Regulation

Who are the certifications for?

- **Data Controllers:** in order to have a mechanisms standardized to implement technical and organizational measures (Art. 24 GDPR)

- **Data Processors:** in order to demonstrate sufficient guarantees of compliance with the Data Controller's instructions (Art. 28 (5) GDPR)

Privacy by Design and by Default

"An approved certification mechanism pursuant to art. 42 GDPR may be used as an element to demonstrate compliance with the principles of **Privacy by design and by default**" (Art. 25 GDPR)

- **Privacy by design:** is an approach to projects that promotes privacy and data protection compliance **from the start**

- **Privacy by default:** is an approach of a maximum degree of privacy by ensuring that personal data are **automatically protected** in any given IT system of business practice.

Transfers based on Certifications

- Principle for transfers

"A controller or processor may transfer personal data to a third country only if the controller or processor has provided **appropriate safeguards**" (Art. 46 GDPR)

- Transfers and certifications

" An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to **apply the appropriate safeguards**, the transfer is compliant to the GDPR." (Art. 46 (2) (f) GDPR)

The Challenges of Certification Mechanisms

- Certification can be issued **maximum for three years**, after which **renewal** is needed (art. 42 (7) GDPR)
- Despite having a mechanism to demonstrate GDPR compliance, a certification **does not** reduce responsibility to comply with the GDPR (Art. 42 (4) GDPR)
- The specific **needs of SMEs** need to be taken into account as well (Art. 42 (1) GDPR)
- **Businesses operating across the EU** can certify to a particular scheme but it is **uncertain** that it will apply in each jurisdiction
  - ✓ Supervisory Authorities need to adopt a common approach and mutual recognition
  - ✓ European Data Protection Board to create a European Data Protection Seal

Balboni
Bolognini
& Partners

Thank you for your attention!

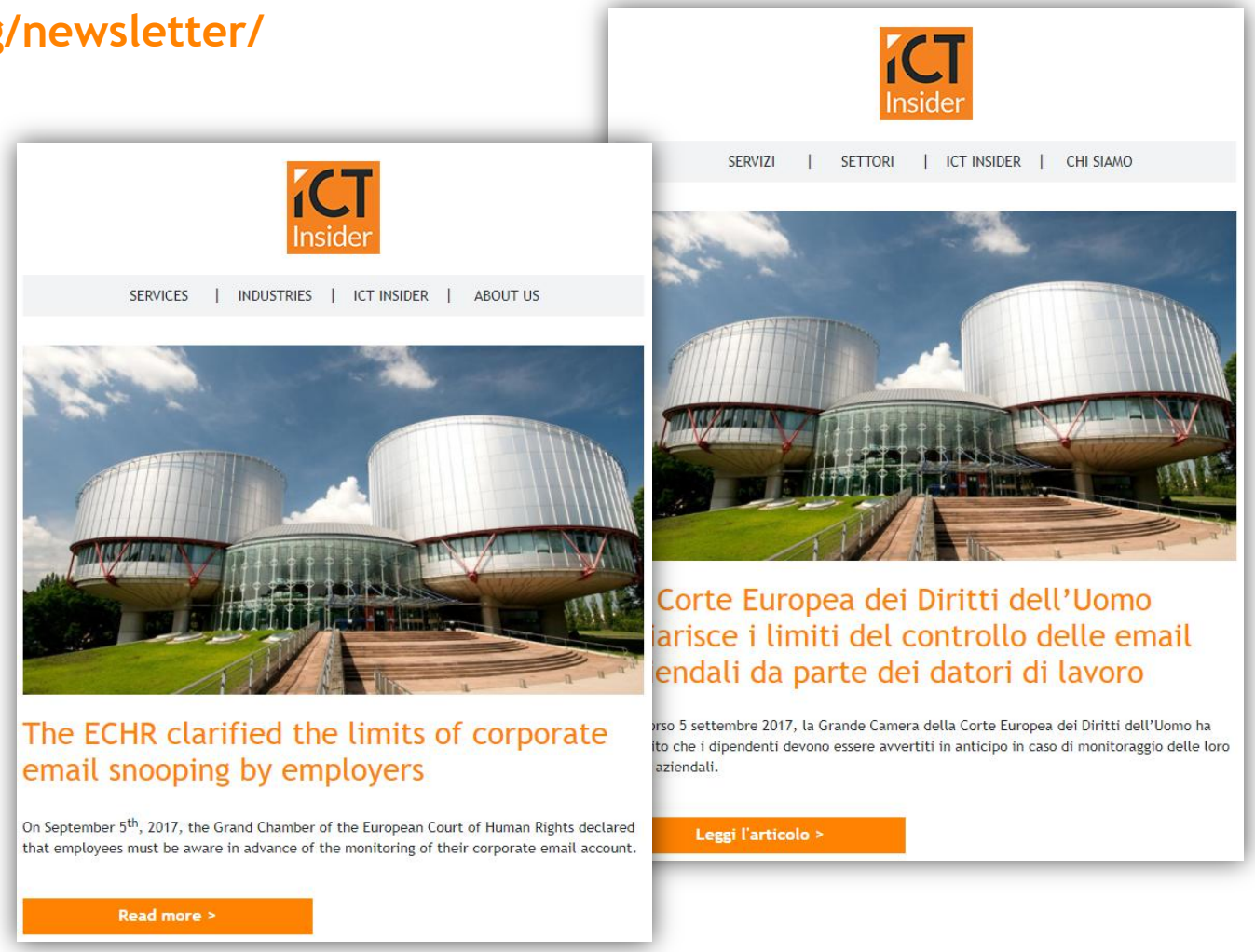
Prof. Dr. Paolo Balboni – Founding Partner

Professor of Privacy, Cybersecurity, and IT Contract Law

paolo.balboni@ictlegalconsulting.com

Newsletter, to stay updated…

ictlegalconsulting.com/eng/newsletter/



- The following slides are for informative purposes, including the relevant GDPR Articles -

Article 24 Responsibility of the controller

1. *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 this Regulation. Those measures shall be reviewed and updated where necessary.*

2. *Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*

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.*

Article 42 Certification

1. *The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.*

2. *In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.*

3. *The certification shall be voluntary and available via a process that is transparent.*

4. *A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.*

5. *A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.*

6. *The controller or processor which submits its processing to the certification mechanism shall provide the certifi- cation body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.*

7. *Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.*

8. *The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.*

Article 43 Certification Bodies

1. *Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:*

   a) *the supervisory authority which is competent pursuant to Article 55 or 56;*

   b) *the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (1) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.*

2. *Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:*

   a) *demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;*

   b) *undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;*

   c) *established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;*

   d) *established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and*

   e) *demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.*

Article 43 Certification Bodies

3. *The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.*

4. *The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.*

5. *The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.*

6. *The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.*

7. *Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.*

8. *The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).*

9. *The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).*