# GDPR and SMEs:
# A practical look at the main duties and obligations and how to comply with them

**15th June 2018 - Brussels**

**Avv. Laura Senatore**

Laura.senatore@ictlegalconsulting.com

Senior Associate at ICT Legal Consulting

Fellow of the Italian Institute for Privacy

Partner at Cyberwatching.eu

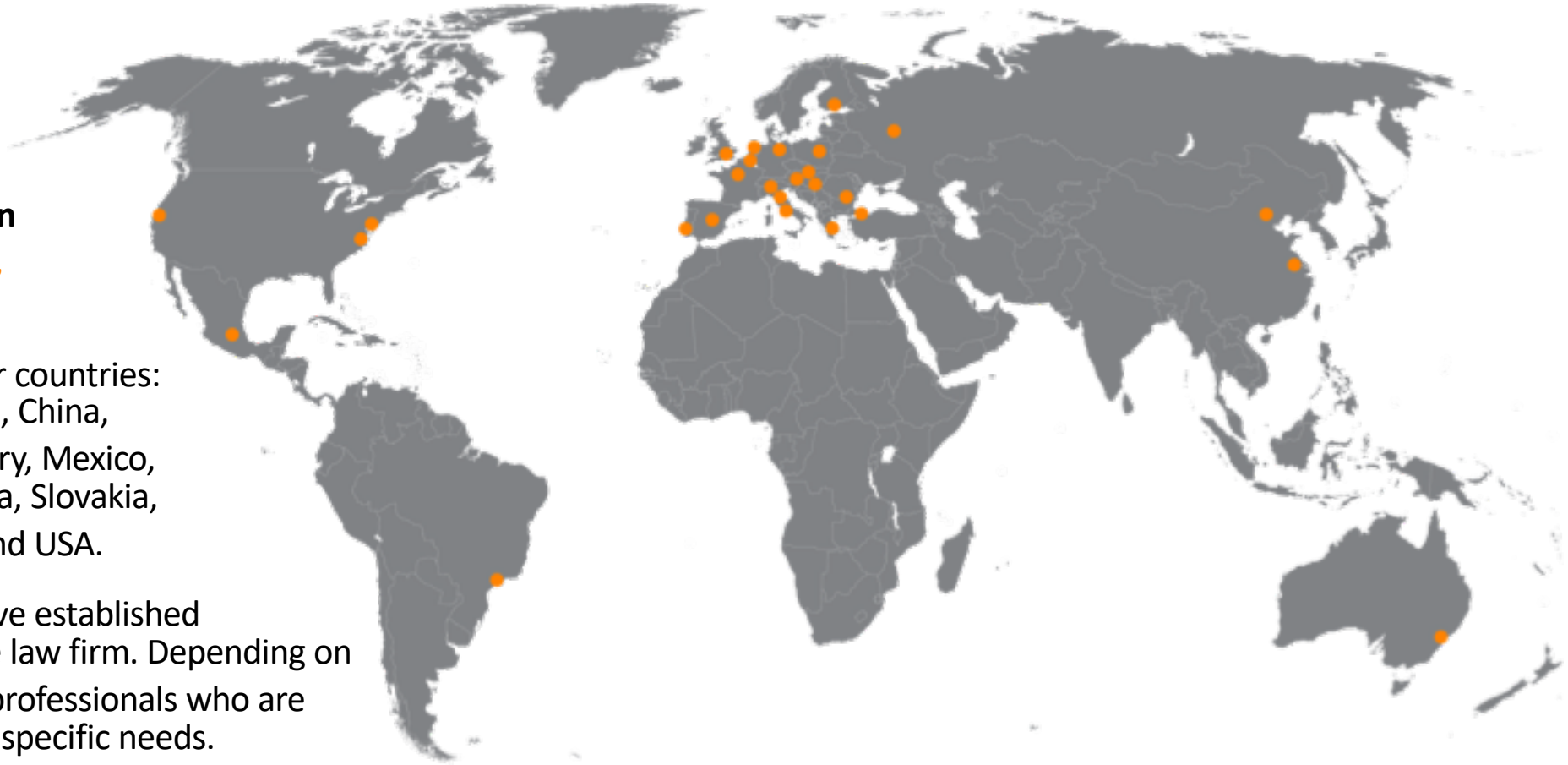
Milan - Bologna - Rome - Amsterdam

# 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.



# AGENDA

## 1. Game Changers

GDPR and key definitions

## 2. Main duties and obligations: how to comply with them

Lawfulness, fairness and transparency
Information notice
Data Processing Agreements
Authorization to the processing of personal data

# Introduction to the GDPR

**2012**

- *Start of reform process, aiming to align the data protection laws of the EU's 28 Member States, and update rules for the digital age*

**April 2016**

- *GDPR is enacted, after years of difficult negotiations*

**May 4 2016**

- Text published in the OJEU - enters into force 20 days after publication

**May 25 2018**

- *GDPR applies throughout the EU after a 2-year transition period*

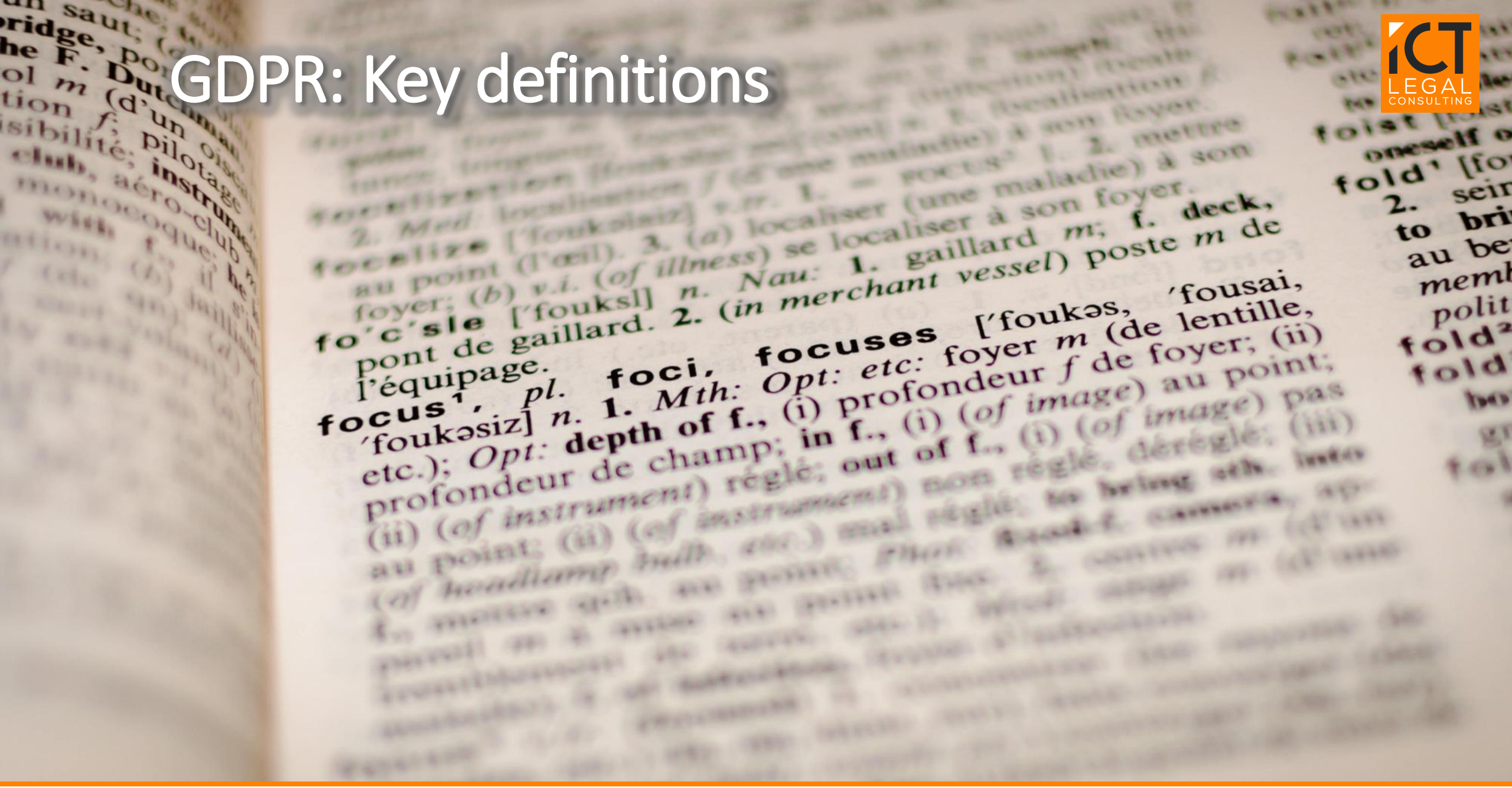
The previous legal framework was based on Directive 95/46/EC, which created an inconsistent patchwork of national laws.

**GDPR objectives:** high level of protection (maintains data protection principles), modernization, harmonization, more effective implementation

# 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 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 behavior of data subjects in the Union.

# GDPR: Key definitions



# Key Definitions (1)

## 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.

## 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.

## Controller

- natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**.

## Processor

- natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

# Key Definitions (2)

## Special Categories of Personal Data

- **data concerning health** means personal data related 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;

.

# GDPR: Game Changers

# GDPR: Game Changers

- **Principle of Accountability (Art. 24 GDPR)**
- **Data Subjects' rights**
- **Enforcement, Sanctions and Remedies**

# Accountability

# Accountability (1)

- **Controllers' responsibility:**
  - To ensure, and **to be able to demonstrate**, compliance with the GDPR
    - This may include having appropriate data protection policies in place, complying with approved codes of conduct or certification mechanisms

*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. (Art. 24 GDPR)*

# Accountability (2)

## ➢ Record of processing activities (Art. 30 GDPR)

- ➢ Required for organization with less than 250 employees when:
  - ➢ the processing it carries out **is likely to result in a risk to the rights and freedoms of data subjects**,
  - ➢ the processing is **not occasional**, or
  - ➢ the processing includes **special categories of data** as referred to in Article 9(1) or **personal data relating to criminal convictions and offences** referred to in Article 10

- ➢ That record shall contain:
  - ➢ the name and contact details of the **controller and the data protection officer**;
  - ➢ the **purposes of the processing;**
  - ➢ a description of the **categories of data subjects** and of the **categories of personal data;**
  - ➢ the categories of **recipients** to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
  - ➢ where applicable, **transfers of personal data to a third country or an international organisa**tion, including the identification of that third country or international organisation andthe documentation of suitable safeguards;
  - ➢ where possible, the envisaged time **limits for erasure** of the different categories of data;
  - ➢ where possible, a general **description of the technical and organisational security measures** referred to in Article 32(1).

# Accountability (3)

## ➢ Data Protection Officer ("DPO") (Artt. 37-39 GDPR)

- ➢ Required when:
  - ➢ core activities consist of processing operations which require **regular and systematic monitoring of data subjects on a large scale**
  - ➢ core activities refers to "processing on a large **scale of special categories of data** pursuant to Article 9"

- ➢ Significant powers and independence of DPOs
  - ➢ Must be involved, properly and in a timely manner, in all issues related to personal data protection
  - ➢ All data subjects may contact the DPO directly with any issues regarding their personal data and rights under the GDPR
  - ➢ DPO bound by secrecy and confidentiality concerning the performance of his/her tasks
  - ➢ Must inform and advise on obligations under the GDPR and other applicable data protection provisions, and monitor compliance with those provisions
  - ➢ Must be consulted on DPIAs, and monitor their performance
  - ➢ Contact point for Supervisory Authorities

# Accountability (4)

## Data Security

- Enhanced obligations both for controllers and processors
- There is no list of possible types of security measures: **RISK- BASED APPROACH**

***Security of processing (Art. 32 GDPR)***

*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 .***

# Data Subjects' Rights

# Data Subjects' Rights

- **Right of access (Art. 15 GDPR)**
- **Right to rectification (Art. 16 GDPR)**
- **Right to restriction of processing (Art. 18 GDPR)**
- **Right to object (Art. 21 GDPR)**
- **Right to erasure, "Right to be forgotten" (Art. 17 GDPR)**
- **Right to data portability (Art. 20 GDPR – NEW!)**

# Sanctions and enforcement

# 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 an SA for processing of their data in violation with the GDPR
  - Right to **start legal action**
  - - against an SA 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

# How to face compliance: 4 basic steps

- Lawfulness, fairness and transparency
- Information Notice
- Data Processing Agreements
- Authorisation to processing

# Lawfulness, fairness and transparency

- You must identify valid grounds under the GDPR (known as a ‘lawful basis’) for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

# Checklist (Lawfulness, fairness and transparency)

**Lawfulness**

- ✓ You Have identified an appropriate lawful basis (or bases) for our processing.
- ✓ If you are processing special category data or criminal offence data, you have identified a condition for processing this type of data.
- ✓ You don't do anything generally unlawful with personal data

**Fairness**

- ✓ You have considered how the processing may affect the individuals concerned and can justify any adverse impact.
- ✓ You only handle people's data in ways they would reasonably expect, or you can explain why any unexpected processing is justified.
- ✓ You do not deceive or mislead people when we collect their personal data.

**Transparency**

- ✓ You are open and honest, and comply with the transparency obligations of the right to be informed.

# Information notice to data subjects – Art. 13 GDPR (1)

When collecting personal data, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the **controller** and, where applicable, of the controller's representative;
- (b) the contact details of the **data protection officer**, where applicable;
- (c) the **purposes of the processing** for which the personal data are intended as well as the **legal basis** for the processing;
  (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the **recipients** or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to **transfer personal** data to a third country or international;

# Information notice to data subjects- Art. 13 GDPR (2)

In addition to this, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- the **period** for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller **access to and rectification or erasure of personal data or restriction** of processing concerning the data subject or to **object** to processing as well as the **right to data portability**;
- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to **withdraw consent** at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to **lodge a complaint** with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the **existence of automated decision-making, including pro**filing, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

# Data Processing Agreement (Art. 28 GDPR)

- Whenever a controller uses a processor it needs to have a written contract in place
- The contract is important so that both parties understand their responsibilities and liabilities.
- The GDPR sets out what needs to be included in the contract (Art. 28 GDPR).
- Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide **'sufficient guarantees'** that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.
- Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

# Checklist (Data Processing Agreement)

The Data Processing Agreement shall include the following compulsory details:

- ✓ the subject matter and duration of the processing;
- ✓ the nature and purpose of the processing;
- ✓ the type of personal data and categories of data subject; and
- ✓ the obligations and rights of the controller.

# Checklist (Data Processing Agreement)

The Data Processing Agreement shall include the following compulsory terms:

- ✓ the processor must only act on the **written instructions** of the controller (unless required by law to act without such instructions);
- ✓ the processor must ensure that people **processing the data are subject to a duty of confidence**;
- ✓ the processor must take appropriate measures to ensure the **security** of processing;
- ✓ the processor must only engage a sub-processor with the **prior consent of the data controller and a written contract**;
- ✓ the processor must **assist the data controller in providing subject access and allowing data subjects to exercise their rights** under the GDPR;
- ✓ the processor must **assist the data controller in meeting its GDPR obligations** in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- ✓ the processor must **delete or return** all personal data to the controller as requested at the end of the contract; and
- ✓ the processor must submit to **audits and inspections**, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

# Authorisation to processing (Art. 29 GDPR)

The processor and any person acting under the authority of the controller or of the processor (i.e. employees), who has access to personal data, **shall not process those data except on instructions frm the controller**, unless required to do so by Union or Member State law.

## Checklist

- ✓ Provide your employees with **instructions** on how to process personal data

# Thank you for your attention!
# Q&A

**Avv. Laura Senatore**

Laura.senatore@ictlegalconsulting.com

Senior Associate at ICT Legal Consulting

Fellow of the Italian Institute for Privacy

Partner at Cyberwatching.eu



Milan - Bologna - Rome - Amsterdam

# The Firm

**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.

# Awards






# Contacts


**Milano**
Via Cappuccini, 19
20122 - Milan - Italy
Phone: +39 02 84247194
Fax: +39 02 700512101

**Bologna**
Via Ugo Bassi, 3
40121 - Bologna - Italy
Phone: +39 051 272036
Fax: +39 051 272036

**Roma**
Piazza di San Salvatore in Lauro, 13
00186 - Roma - Italy
Phone: +39 06 97842491
Fax: +39 06 23328983

**Amsterdam**
Piet Heinkade 55 (11th floor)
1019 GM - Amsterdam – The Netherlands
Phone: +31 (0)20 894 6338
Fax: +31 (0)20 808 5050


**ICTLC** | **ICT Legal Consulting** is present in 19 other countries:
Australia, Austria, Belgium, Brazil, China, France, Germany, Greece, Mexico, Poland, Portugal, United Kingdom, Romania, Russia, Slovakia, Spain, United States, Turkey, Hungary

Follow us on:


**Email contact**
info@ictlegalconsulting.com

**Skype contact**
Ict.legal.consulting