

# cyberwatching.eu

The European watch  
on cybersecurity & privacy

## Legal Aspects: the GDPR & IoT

Anastasia Botsi - Associate  
[anastasia.botsi@ictlegalconsulting.com](mailto:anastasia.botsi@ictlegalconsulting.com)



Balboni  
Bolognini  
& Partners

Funded by the European Commission  
Horizon 2020 – Grant # 740129



# 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.



# The General Data Protection Regulation: 101 Terminology

**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.

**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;

# GDPR is a Game Changer for Businesses

---

- Accountability
- Security Measures

A close-up photograph of a person's hands holding a newspaper. The person is wearing a dark suit jacket and a watch with a blue and orange face. The newspaper is open to a page with financial news. The word "business" is printed in large blue letters. Below it, there are sections for "Currencies", "Commodities", and "News". The "Currencies" section shows the Euro (€) rate at 1.5314 and the Pound (£) rate at 1.3628. The "Commodities" section shows Gold at \$1146.06 and Brent Crude at \$52.14. The "News" section has a headline about Tesco. At the bottom of the page, there is a headline about a new global crisis warning from the IMF.

business

## Currencies

FTSE 100	6960.22
FTSE All Share	2477.20
FTSE All Share Yield	3.00
FTSE Europe 500	2854.00
Nikkei 225	21616.40
DAX European 30	1220.90
S&P 500	1980.90
Nasdaq	4760.00

€  
Rate  
**1.5314**  
Change  
-4.03c

£  
Rate  
**1.3628**  
Change  
-1.23c

## Commodities

Gold  
AU 999.9  
**\$1146.06**  
(£748)  
-0.94 (-0.08pc)

Brent Crude  
AU 75.00  
**\$52.14**  
(November)  
-0.54 (-1.04pc)

## News

Long haul  
for Tesco  
Company  
halts sales  
spiral but  
profits fall

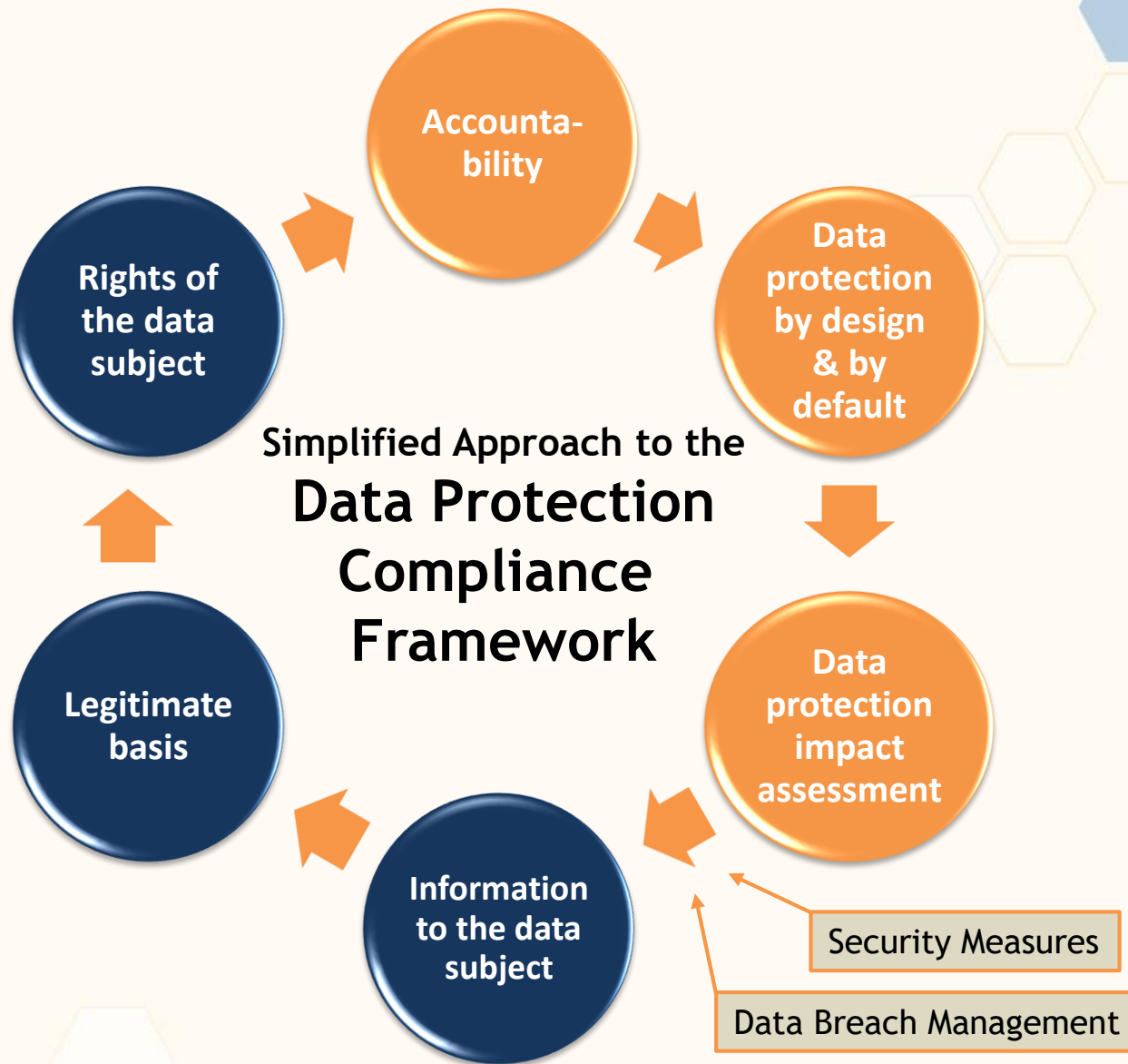
...the new global crisis, warns IMF

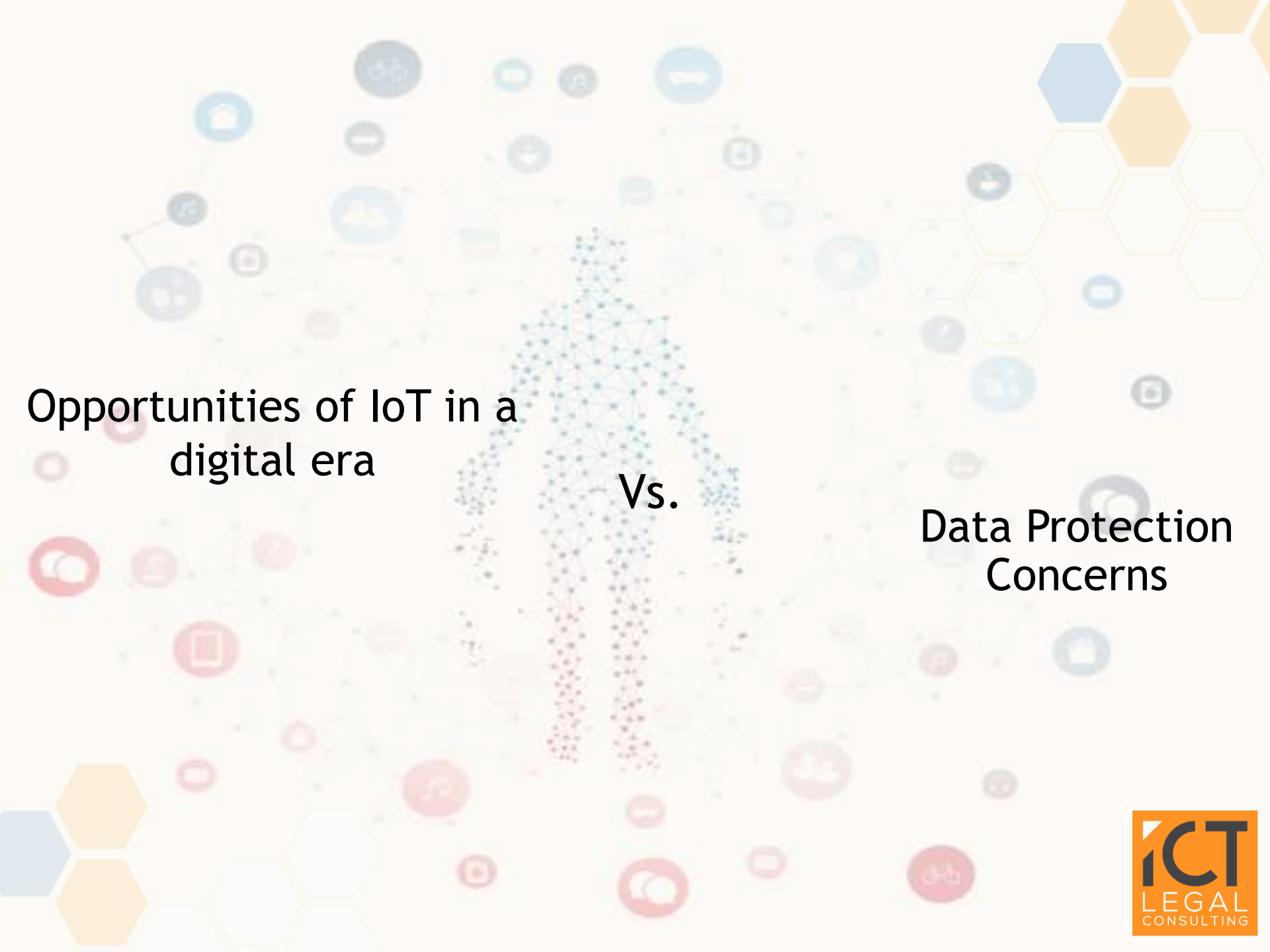
# Accountability under the GDPR means..

## Data Controllers responsibility 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.]*





Opportunities of IoT in a  
digital era

Vs.

Data Protection  
Concerns

# Internet of Things: Opportunities

- A growing paradigm with technical, social, and economic significance
- A wide ecosystem of interconnected services and devices (i.e., sensors, consumer products and everyday smart home objects, cars, and industrial and health components)
- Technologies collect, exchange and process data in order to dynamically adapt to a specific context, transforming the business world and the way we live as a whole
- Gartner predicts that by 2020 the number of connected devices will reach **20 billion**





# Internet of Things: Data Protection Concerns



- **Data protection by design and by default** raises concerns in terms of the guarantees that IoT may offer (intrusive nature)
- According to the characteristics of the device, the data subjects should be protected **by design** and **by default**
- Conducting a **Data Protection Impact Assessment** to make sure that from the designing of an IoT device, privacy is taken into consideration

# IoT: Data Protection Concerns

- An average 127 new things are connected to the Internet per second, or 328 million things connected every month, meaning that IoT has immense ability to scale globally.
- The responsibility of the controller to **ensure** and **demonstrate** compliance is challenging:
  - ❑ Risk-based approach in security (art. 24 and 32 GDPR): **assessing the risk** of a large volume of IoT devices deployed around the world is tricky, and uncertain; and **security and organisational measures** to be implemented may be disproportionate to the risk (the impact of threats / risks on IoT deployments is much larger than other Information Society services)
  - ❑ Data breach management (art. 33-34 GDPR): companies 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

# IoT: Data Protection Concerns

- IoT devices by their nature do not tend to rely on graphical user interfaces (i.e., phone or laptop)
- Informing a customer is not as straightforward
- The principle of lawfulness, fairness and transparency, (art. 5.1(a) GDPR) is challenged:
  - ❑ Which means may be used by the controller to **inform** the IoT user about the relevant elements of the processing of their personal data ?
  - ❑ How can the IoT user be properly **alerted** about changes that will occur in the handling of their personal data?

Want to know what to include in your information notice to your data subjects? Check articles 13 and 14 GDPR.



# IoT: Data Protection Concerns

- The reliance on data processing and analytics in the cloud exponentially increases the interactions between the device and the data, **involving numerous parties**
- The data controller shall be accountable for all the parties that may be involved in the processing, storage, alteration, decision-making, etc. of the connected IoT device or service
  - ❑ It is not always simple / possible to determine whether parties involved are a controller or a processor
  - ❑ Legally binding all processors may be overwhelming, but the GDPR requires that a contract or other instrument is signed between the controller and the processor (art. 28 (3) GDPR)

# IoT: Data Protection Concerns

- **Defining** and **implementing** appropriate security measures for IoT is complex, especially due to the diversity of application areas for IoT
  - ❑ Striking a balance between the particularities of each domain is essential and accordingly it is important to consider the differences in apportioning risk to distinct environments.
    - ✓ [ENISA's Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures](#) cover major vertical application areas of IoT relating to critical information infrastructures (i.e., smart homes, smart cities, smart cars, etc.)



# 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



# Conclusions

- The GDPR presents serious challenges for IoT
- Opportunity for manufacturers and network operators to work together to build privacy into the design of IoT (according to **principles of data protection by design and by default**)
- Risk-assessment can be conducted according to ENISA's definition of baseline **security measures**
- Conducting a **Data Protection Impact Assessment** for risky processing activities, and finding the relevant security measures
- Adopting **Data Breach Management Policies**
- Finding a way to **adequately inform** data subjects of the processing of their personal data by means of IoT devices
- Adhering to relevant **Certifications** to demonstrate compliance

## Useful Sources:

- ✓ Data Protection Self Assessment Toolkit
  - ❖ Data Controller and Data Processor's checklist
  - ❖ Record of Processing Activities assessment
  - ❖ Direct Marketing assessment
- ✓ Cyberwatching.eu Deliverable on the Cybersecurity legal and policy aspects: preliminary recommendations and road ahead



# Check your temperature !

## The **GDPR Temperature Tool**

Improving the GDPR compliance posture of SMEs

A free online tool helping small businesses understand their risk of GDPR-related sanctions



**20**

Questions



**15**

Minutes of your  
time



**1**

Recommendations  
report

Visit  
[cyberwatching.eu](https://cyberwatching.eu)

Download your  
customised action plan



Answer the **GDPR-sanction**  
related questions

Act and implement change in  
your organisation

\*The GDPR sanction tool is not an attempt nor is it supposed to be replaced by the risk assessment that should be conducted by SMEs. Rather it is merely an indication of their risk to sanctions, according to their responses which provide a basis of their processing activities.





# **Thank you for your attention!**

---

**Anastasia Botsi - Associate, LL.B.**

**[anastasia.botsi@ictlegalconsulting.com](mailto:anastasia.botsi@ictlegalconsulting.com)**

**+31 621335013**

© 2018 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](mailto:info@ictlegalconsulting.com) - [www.ictlegalconsulting.com](http://www.ictlegalconsulting.com)



“Excellence is not an act but a habit” Aristotle