LEGAL ASPECTS OF BLOCKCHAIN TECHNOLOGY:

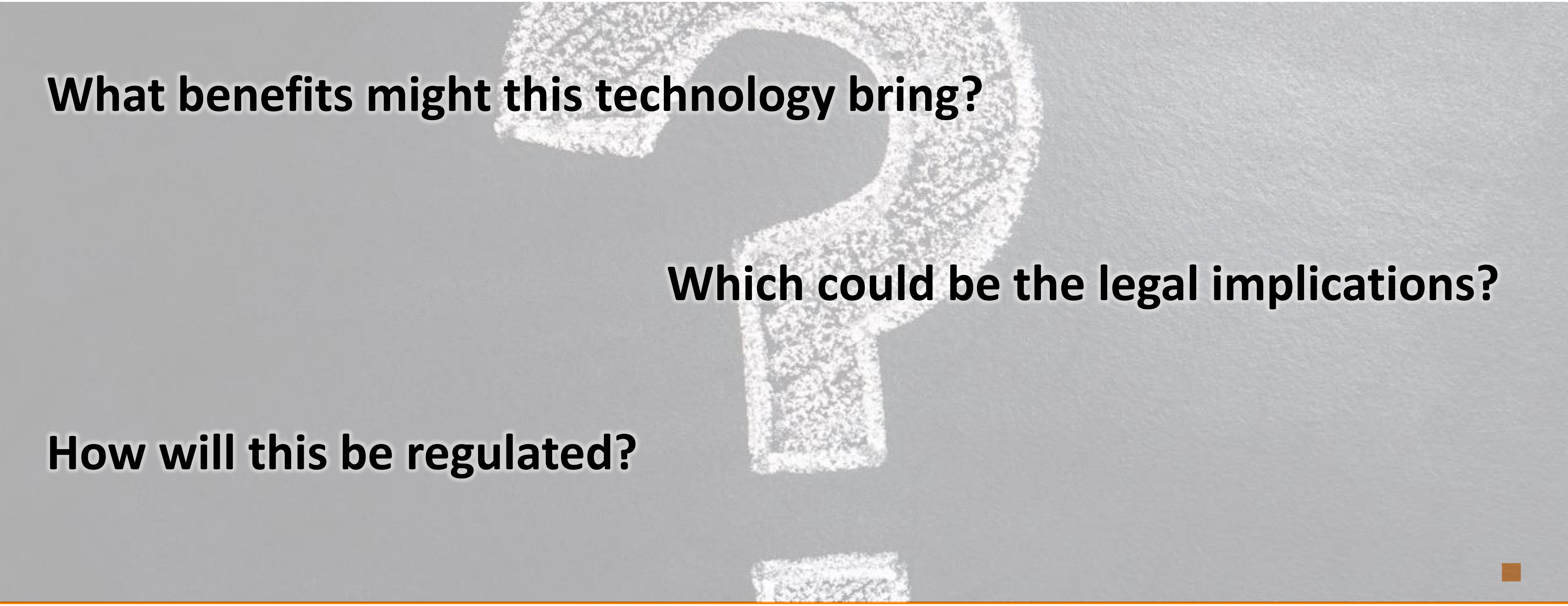
GDPR and its implications on Blockchain Technology

Anastasia Botsi
Associate at ICT Legal Consulting
anastasia.botsi@ictlegalconsulting.com

Milan - Bologna - Rome - Amsterdam

Blockchain: Multi-application overview and opportunities, 19 November 2019

Fundamental legal questions



What benefits might this technology bring?

Which could be the legal implications?

How will this be regulated?

Personal Data

Blockchain and **Personal Data.**

“Personal Data”: very broad definition under Regulation (EU) 2016/679 (the General Data Protection Regulation, or ”GDPR”)

*“**any information** relating to an **identified** or **identifiable** natural person (data subject)”.*

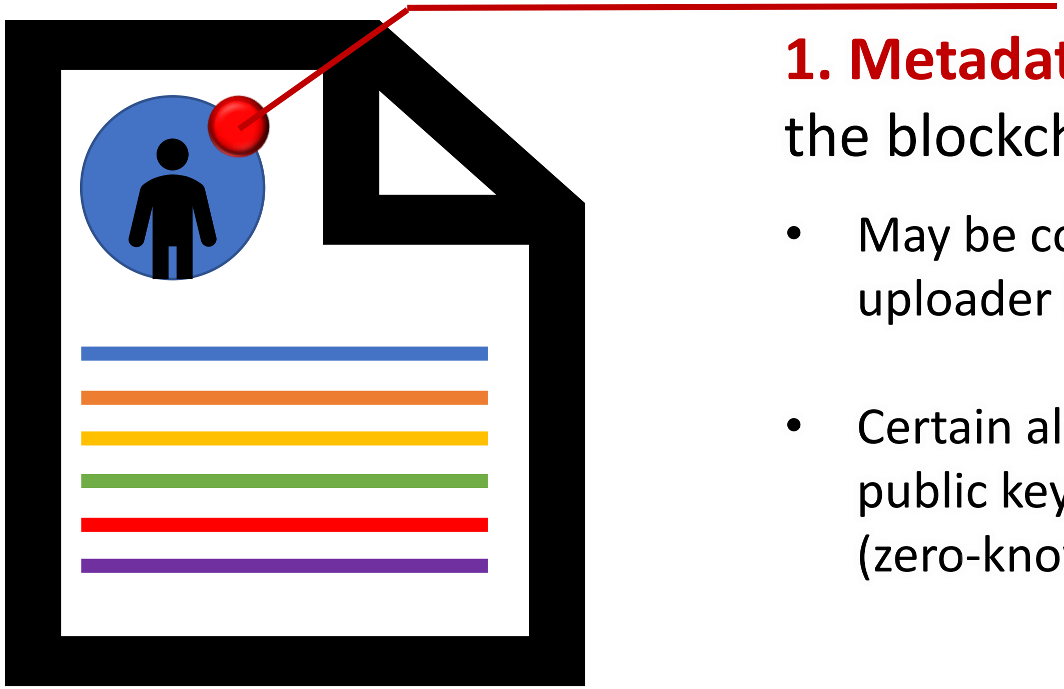
Includes details which can identify individuals (e.g., names, national ID numbers), as well as **<u>any</u>** information linked to an individual who is identified (e.g., contact details, orders made, location).

Even if information is encrypted, if it relates to an individual and the encryption can be reversed, it is **still** personal data!

As it will still be information relating to an **identifiable** individual...

Blockchain and **Personal Data.**

There are, essentially, **two types of data** which may be stored on a blockchain:

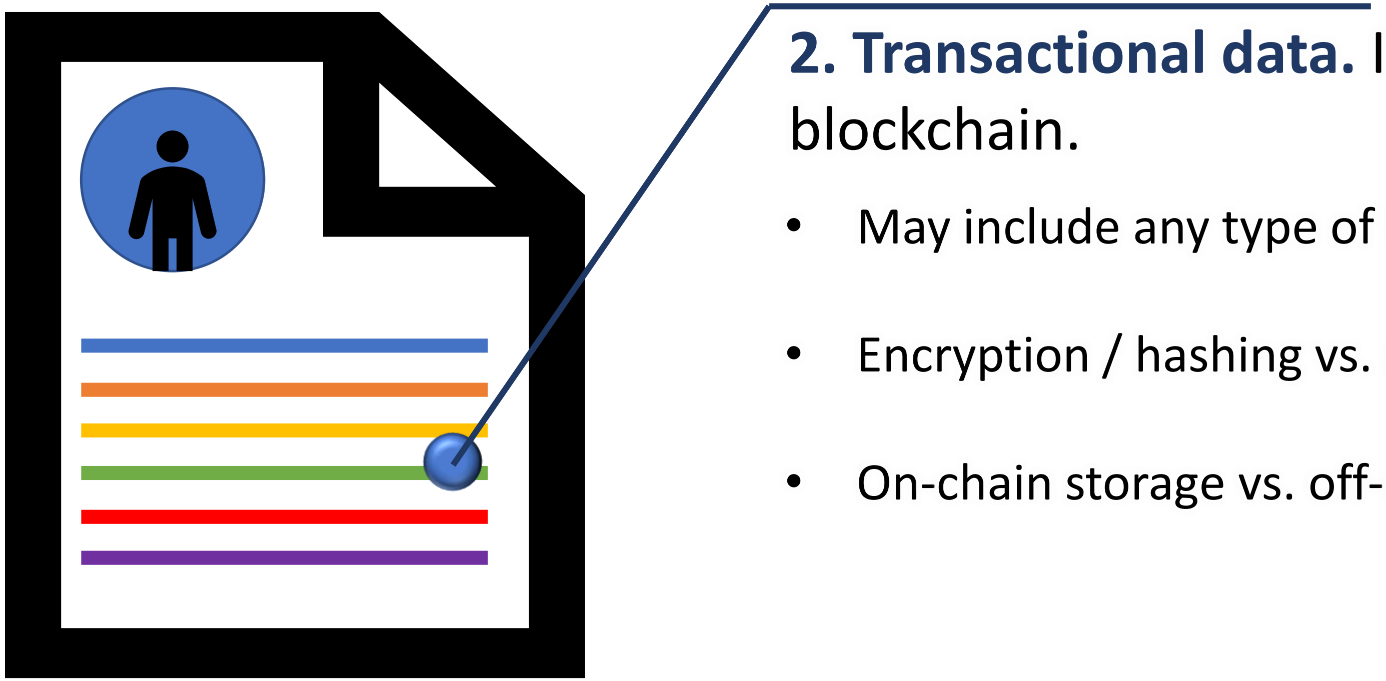


1. Metadata. Information related to an upload made onto the blockchain.

- May be considered personal data, if it is possible to identify the uploader lawfully and through not particularly complex means.
- Certain alternatives have been suggested in an attempt to render public keys anonymous, to avoid their qualification as personal data (zero-knowledge proofs, noise).

Blockchain and Personal Data.

There are, essentially, **two types of data** which may be stored on a blockchain:



2. Transactional data. Information uploaded onto the blockchain.

- May include any type of information, including personal data.
- Encryption / hashing vs. anonymous data
- On-chain storage vs. off-chain storage

Blockchain and **Personal Data.**

Data Protection Principles:

PRINCIPLE NO. 1.1: Lawfulness

- Generally, the handling of personal data via a blockchain-based system is **not a purpose** in itself, but rather **a means to achieve a given purpose**.

- It is important to identify **the reason for which personal data are handled via a blockchain system**, so that a legal basis for that reason can be properly selected.

- It is possible to conceive of situations where individual’s consent can be leveraged, but also the need to perform a contract with an individual, to comply with applicable law, or to pursue legitimate interests.

Blockchain and **Personal Data.**

Data Protection Principles:

PRINCIPLE NO. 1.2: Fairness

- Blockchain systems meant to handle personal data should be **carefully designed** in order to ensure that the privacy, autonomy and integrity of individuals is not unreasonably harmed.
- The same goes for organisations wishing to make use of blockchain systems to process personal data – **carrying out a Data Protection Impact Assessment** (DPIA), when not legally required, is nonetheless strongly recommended to allow this assessment to be made.
- The **way** in which individuals are **informed** as to how their data may be affected by use via blockchain must be carefully thought out.

Blockchain and Personal Data.

Data Protection Principles:

PRINCIPLE NO. 1.3: Transparency

- It is **not always easy** to identify the information required by the GDPR, particularly for public blockchains (e.g., recipients, retention periods, international transfers).
- Nonetheless, the key is to provide meaningful information to data subjects, meaning **information which is relevant to them**, to the greatest extent possible.
- This is not as much of a problem with **private blockchains.**

Blockchain and Personal Data.

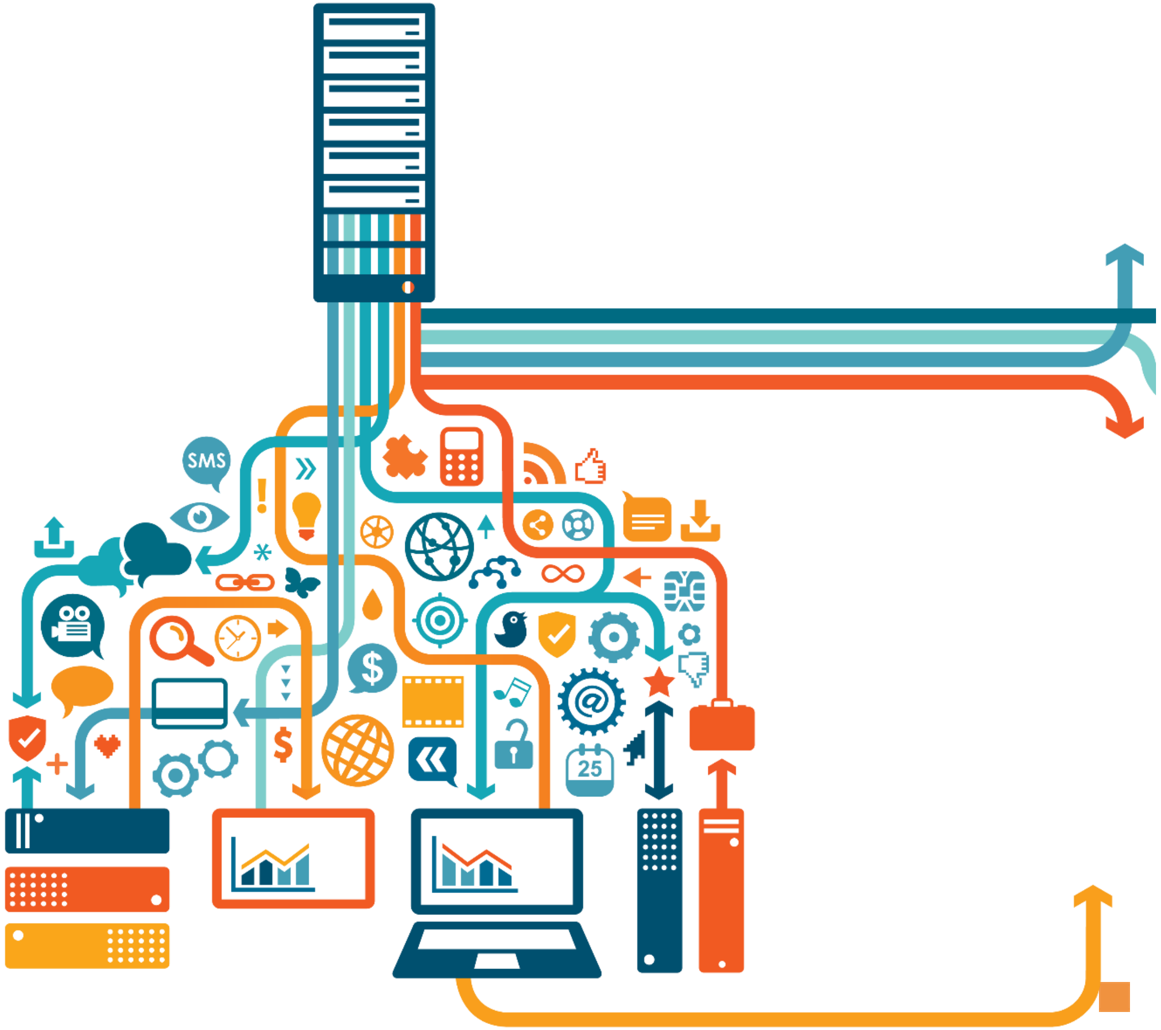
Data Protection Principles:

PRINCIPLE NO. 2: Purpose Limitation

- Organisations need to **map the purposes** for which they collected personal data, and avoid the reuse, combination or repurposing of those data for **incompatible purposes**.

- The use of blockchain does not necessarily collide with this principle, as it is but a **means to achieve a given purpose** (or purposes).

- Storage of personal data, collected for an initial purpose, on blockchain for further archiving purposes, may be justified under the GDPR insofar as those **archiving purposes are carried out in the pubic interest**.

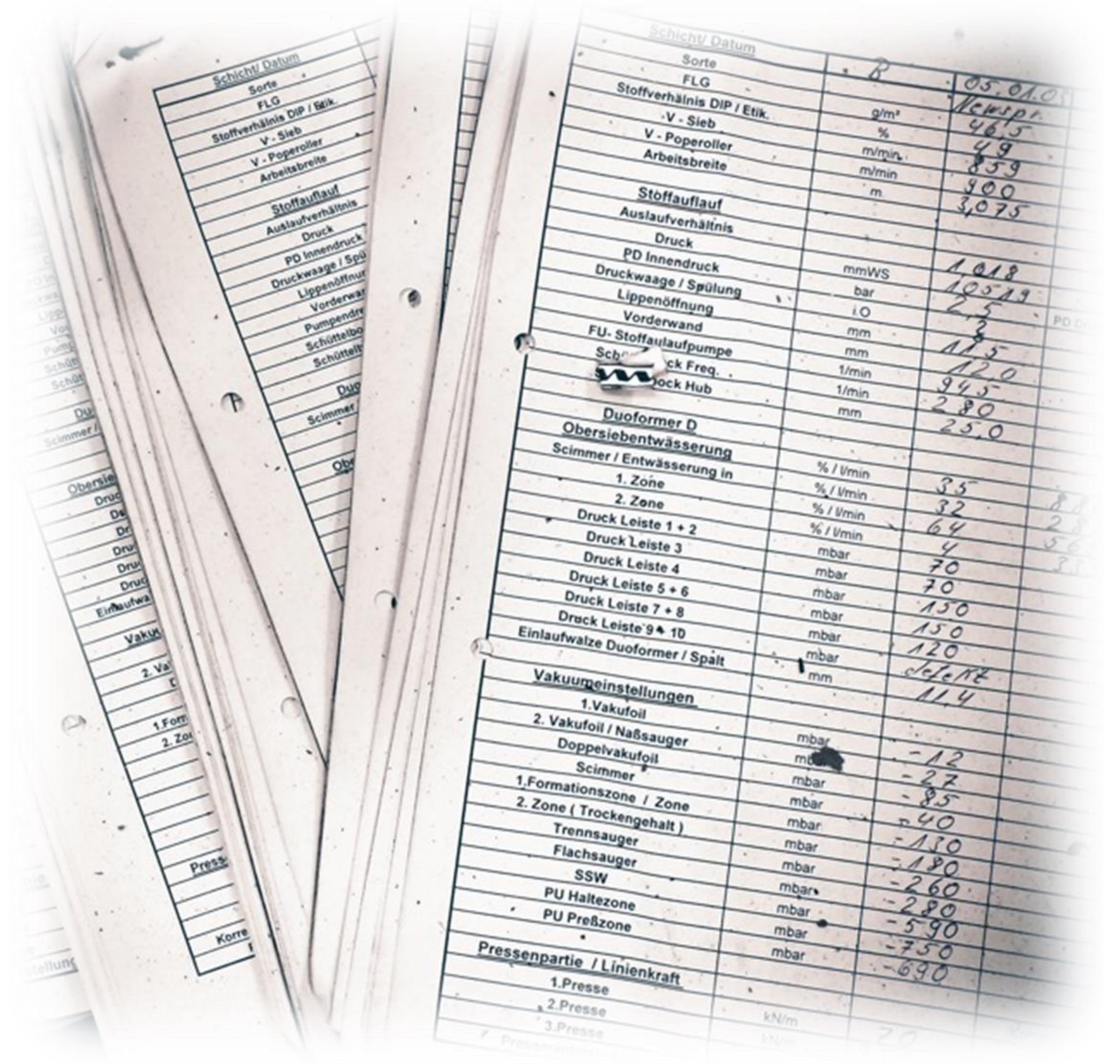


Blockchain and Personal Data.

Data Protection Principles:

PRINCIPLE NO. 3: Data Minimisation

- This principle is a potential major obstacle to blockchain use under the GDPR.
- Blockchain should only be used to handle personal data if this is **necessary** (i.e., there are no less privacy-intrusive alternatives available).
- On-chain storage may be inherently at odds with this principle. Off-chain storage therefore seems to be a preferable approach.



Blockchain and **Personal Data.**

Data Protection Principles:

PRINCIPLE NO. 4: Accuracy

- Data on a blockchain cannot, in principle, be retroactively amended.
- Amendments could be carried out by additing supplemental data to the blockchain.
- Off-chain storage appears to be the best way to ensure compliance with this principle.

Blockchain and Personal Data.

Data Protection Principles:

PRINCIPLE NO. 5: Storage Limitation

- The tendentially immutable nature of blockchain systems is in conflict with this principle.
- While it may not be possible to erase data on-chain, disabling read/write access of others (except for the data subject) could achieve an equivalent end result.
- While transactional data can be kept off-chain, public keys cannot.

Blockchain and Personal Data.

Data Protection Principles:

PRINCIPLE NO. 6: Integrity and Confidentiality

- Those wishing to resort to blockchain to process personal data must consider if the system in question **offers sufficient security measures**.
- This requires an in-depth analysis of that system, to ensure that a reasonable level of security is afforded.

Blockchain and Personal Data.

Data Protection Principles:

PRINCIPLE NO. 7: Accountability

- Blockchain-based systems may be able to keep records of all operations carried out with certain types of personal data

- Blockchain could potentially be **leveraged as an accountability tool**, either complementing or (if the complexity of information which can be stored on the blockchain allows it) even assuming the role of records of processing activities (as required by GDPR).

Blockchain and Personal Data.

Data Protection by Design; Fairness by Design:

Data Protection by Design:
Implement appropriate technical and organisational measures to ensure that your systems/activities involving the processing of personal data respect the **data protection principles.**

1. Processing of personal data via IT systems should be the outcome of a **design project**.

2. Measures to ensure **effective protection** of personal data should be carefully selected and implemented.

3. The measures chosen must be appropriate and effective in **ensuring and demonstrating compliance**.

4. All measures identified must be **effectively integrated** into the processing system/activities foreseen.

European Data Protection Supervisor, *Opinion 5/2018 – Preliminary Opinion on privacy by design*
https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

Blockchain and Personal Data.

Data Protection by Design; Fairness by Design:

DATA PROTECTION IMPACT ASSESSMENT

- **Users of blockchain systems** (whether just to upload personal data, or to access uploaded personal data) must also consider the principle of data protection by design.

- **DPIA =** A thorough assessment of an intended processing activity, in order to identify and mitigate potential risks to the rights and freedoms of data subjects concerned, which should be documented for accountability purposes.

1 **Describe processing operations and purposes**

2 **Assess necessity and proportionality**

3 **Assess risks to data subjects**

4 **Identify measures to address risks**

Blockchain and Personal Data.

Data Protection by Design; Fairness by Design:

Fairness by Design
A further specification of the principle of Data Protection by Design.

The processing of personal data must be balanced and proportionate towards data subjects.

- Data subjects' **interests and reasonable expectations of privacy** must be considered from the design stage = any systems intended to process personal data must be configured so as to **respect individuals' privacy, autonomy and integrity**.

- Algorithms used to make decisions regarding individuals should be **regularly controlled against bias and discriminatory results**.

- Data subjects should be **empowered and afforded control over their data** to the greatest extent possible.

Personal Data + Blockchain

Conclusions

- Blockchain and data protection principles do not necessarily see eye-to-eye; in particular the principles of **data minimisation**, **storage limitation**, and the **rights of data subjects**.

- There are significant issues in assigning **data processing roles** to blockchain participants and identifying **international transfers of data**, in particular where the GDPR's formal requirements regarding these topics are concerned.

- **Off-chain storage of personal data** (keeping only references to the data on-chain) appears to be an effective workaround for many of the issues described.

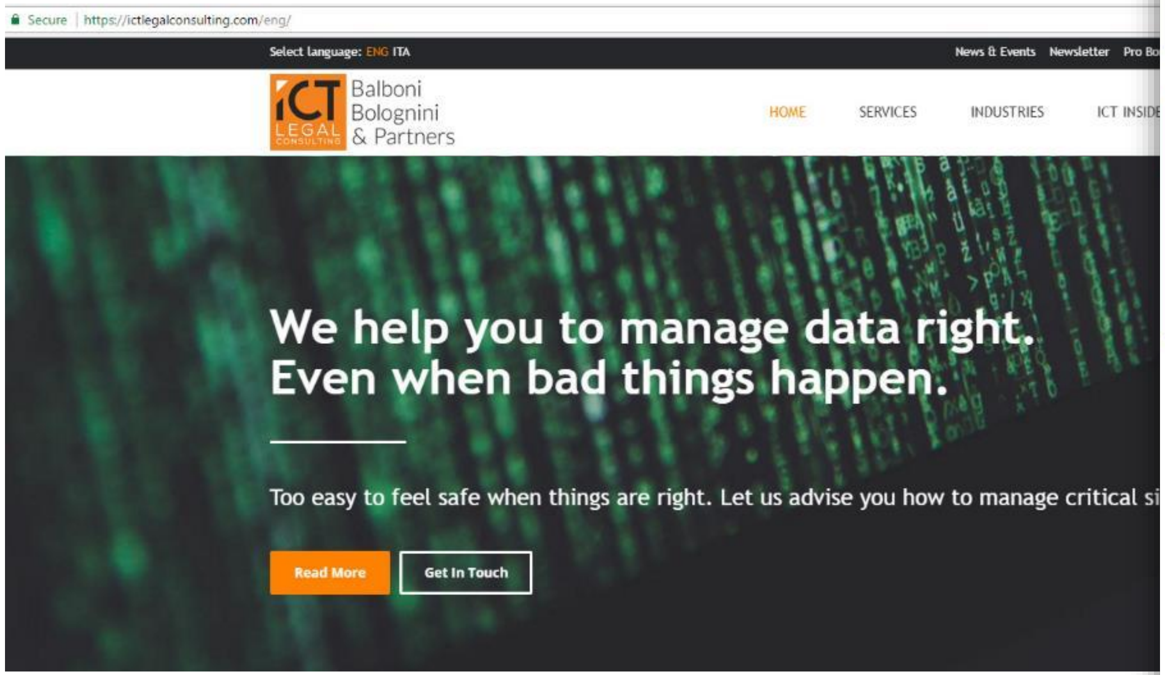
- While blockchain systems have the potential to empower data subjects, **data protection principles must be considered from their design phase** in order to ensure that they are crafted in a manner compliant with the GDPR.

Thank you for your attention!
Q&A

Anastasia Botsi
Associate at ICT Legal Consulting
anastasia.botsi@ictlegalconsulting.com

Amsterdam - Milan - Bologna - Rome - Helsinki

Website & Publications



🔒 Secure | https://ictlegalconsulting.com/eng/

Select language: ENG ITA

News & Events Newsletter Pro Bo

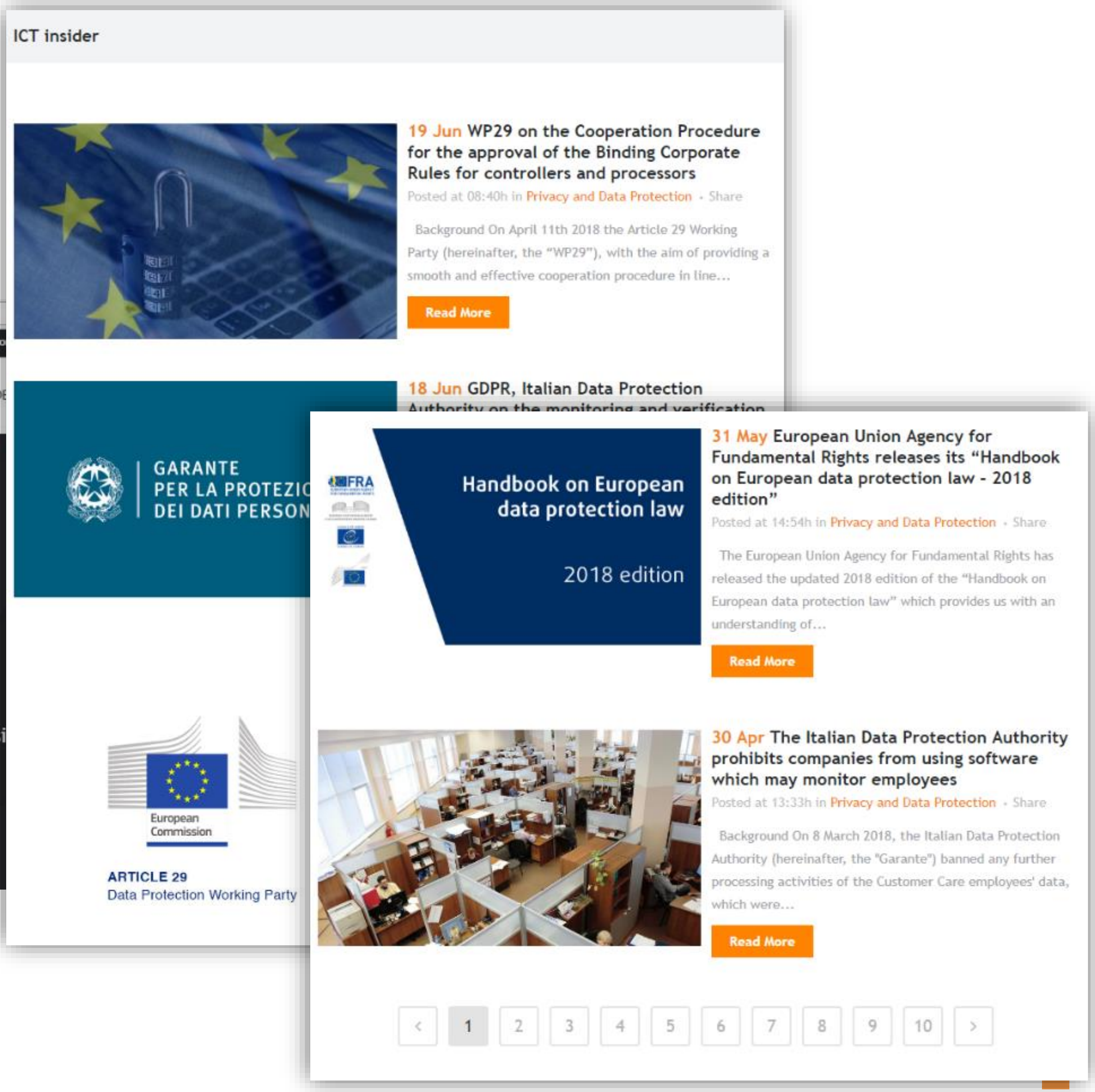
ICT LEGAL CONSULTING Balboni Bolognini & Partners

HOME SERVICES INDUSTRIES ICT INSIDE

We help you to manage data right. Even when bad things happen.

Too easy to feel safe when things are right. Let us advise you how to manage critical si

Read More Get In Touch



ICT insider

19 Jun WP29 on the Cooperation Procedure for the approval of the Binding Corporate Rules for controllers and processors

Posted at 08:40h in Privacy and Data Protection · Share

Background On April 11th 2018 the Article 29 Working Party (hereinafter, the "WP29"), with the aim of providing a smooth and effective cooperation procedure in line…

Read More

18 Jun GDPR, Italian Data Protection Authority on the monitoring and verification

GARANTE PER LA PROTEZIO DEI DATI PERSON
European Commission
ARTICLE 29 Data Protection Working Party
FRA
Handbook on European data protection law
2018 edition

31 May European Union Agency for Fundamental Rights releases its "Handbook on European data protection law - 2018 edition"

Posted at 14:54h in Privacy and Data Protection · Share

The European Union Agency for Fundamental Rights has released the updated 2018 edition of the "Handbook on European data protection law" which provides us with an understanding of…

Read More

30 Apr The Italian Data Protection Authority prohibits companies from using software which may monitor employees

Posted at 13:33h in Privacy and Data Protection · Share

Background On 8 March 2018, the Italian Data Protection Authority (hereinafter, the "Garante") banned any further processing activities of the Customer Care employees' data, which were…

Read More

‹ 1 2 3 4 5 6 7 8 9 10 ›

Stay updated!

ictlegalconsulting.com/eng/newsletter/