# A GDPR Code of Conduct for Blockchain

Silvan Jongerius - Managing Partner

Tech GDPR

**Silvan Jongerius / @silvanjongerius / @techgdpr / silvan@techgdpr.com**

# Key problems of Blockchain under GDPR

1. The definition of personal data is unclear
2. The GDPR roles in decentralised environments are unclear
3. Deletion and rectification obligations under BC/DLT are unclear
4. Transfers of personal data outside of the EEA

# Codes of Conduct (Article 40 GDPR)

- Compliance instruments approved by data protection authorities
- Enabling specific sectors to own and resolve key data protection challenges in their sector in accordance with the GDPR.
- "regulated self-regulation”
- Providing a detailed description of what is the most appropriate, legal and ethical set of behaviours.

**codes are**

„voluntary accountability tools which set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of what is the most **appropriate**, **legal** and **ethical** set of behaviours of a sector.“

# A code of conduct may define

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection and pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals’ rights, in particular the right to erasure (‘right to be forgotten’);
- technical and organisational measures, including data protection by design and by default as well as security measures;
- the transfer of personal data to third countries or international organisations; or
- dispute resolution procedures.

# Key goals

- Achieve best practices
- Protecting from liability risks
- Earn trust and confidence
- Provide legal certainty

# Code of conduct: scope

- Territorial scope: national/transnational
- Material scope: BC/DLT "*refer to many different forms of distributed databases that present much variation in their technical and governance arrangements and complexity*"[1],
  - Codes should specify or define what types or versions of BC/DLT technologies are covered.

[1] Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?; publication of the Scientific Foresight Unit (STOA), European Parliamentary Research Service; Download link: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf .

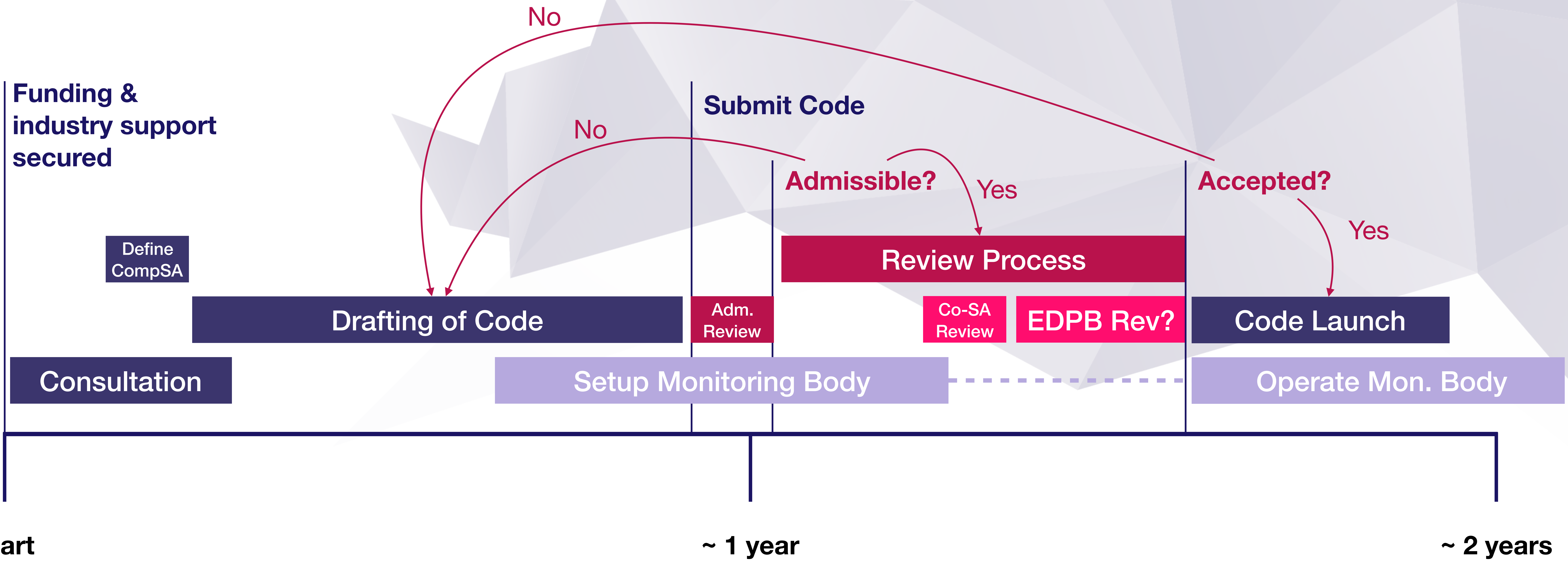
# A BC/DLT code of conduct could:

- Define what is personal data, pseudonymisation, anonymisation
- Define roles and responsibilities
- Define how data protection by design and default can be implemented
- Define how privacy notices can be provided
- Define which TOMs are appropriate
- Assist with defining when a DPIA must be carried out
- Enable international transfers
- Define how dispute resolution takes place

# Process (tbc)

Code Owner

CompSA/EDPB



Funding & industry support secured

Define CompSA

Consultation

Drafting of Code

No

No

Submit Code

Adm. Review

Admissible?

Yes

Review Process

Co-SA Review

EDPB Rev?

Accepted?

Yes

Code Launch

Setup Monitoring Body

Operate Mon. Body

Start

~ 1 year

~ 2 years

@techgdpr

# Requirements

**Draft should demonstrate**

- meets a particular need of that sector or processing activity, facilitates the application of the GDPR,
- specifies the application of the GDPR,
- provides sufficient safeguards, and
- provides effective mechanisms for monitoring compliance with a code.

# Requirements

**Approval Requires**

- codes must have regulatory character and not just re-state the wording of the law,
- codes must not replace the provisions of the GDPR, but rather contribute to its application for the BC/DLT sector by specifying the GDPR provisions,
- codes must provide safeguards for the protection of personal data, appropriate to the type of data processed [the more sensitive the data are, the stricter the safeguards must be].

# INATBA Privacy WG - discussion

1. Which problems can a CoC solve? Which does it not solve?
2. Is this the best instrument we can use?
   - Approved certification
   - Binding ‘network' rules
3. Is there sufficient alignment within the industry to propose this?
4. Which bodies could be Code Owner and Monitoring Body?
5. Would INATBA be an appropriate organisation for these roles?
6. Any other points related to compliance instruments

Silvan Jongerius / @silvanjongerius / @techgdpr / silvan@techgdpr.com

Tech GDPR

DPO Service - GDPR Assessment - Privacy by Design
Data Protection Impact Assessment

for Blockchain, AI & IoT