change
the rules.

How far can a Contract Serve as a Justification for Permanent Storage on a Blockchain?

Philipp Quiel

Agenda

➢ General scope of the legal basis in Art. 6 (1) b GDPR

➢ Possibilities of concluding contracts in blockchain systems

➢ Applying Art. 6 (1) b GDPR to data processing with blockchain

  technology

➢ What happens if some terminates a contract?

Scope of Art. 6 (1) b GDPR

Scope

"(…) processing is **necessary** for the **performance of a contract** to which the

data subject is party; or in order to take **steps at the request of the data**

subject prior to entering into a contract"

▶ There must be a contract or a request prior to entering into a contract

▶ Data subjects must be party to a contract

▶ The person processing data does not have to be identical with the person who

has a contractual relationship with the data subject

Scope

What does "necessary" mean?

▶ 2 different approaches: core contract view vs. concrete objective approach

▶ Concrete objective approach: Engeler ZD 2018, 55 ff. PinG 2019, 149 ff.

▶ General idea: what data processing is necessary should be determined by

concrete provisions of a contract and from an objective perspective

▶ Core contract view: EDPB guidelines on Art. 6 (1) b GDPR

▶ General idea: only the "core" of a contract can be covered by Art. 6 (1) b GDPR

Scope

Core contract view (EDPB)

▶ "Identification of the "**core contract**" should be done from a "more abstract point of **view based on the general expectations of consumers**""

▶ "Assessing what is 'necessary' involves a combined, fact-based assessment of the processing for the objective pursued and of whether it is **less intrusive compared to other options for achieving the same goal**. **If there are realistic, less intrusive alternatives, the processing is not 'necessary'**.""

Scope

Weaknesses of the core contract view

▶ Art. 6 (1) b GDPR is lacking openness and is always binary

▶ What should "core of a contract" mean? Where is this written in provisions of

the GDPR? Why should DPAs determine what part of a contract is "core"?

▶ Marginal 36 of EDPB's guidelines: „within the boundaries of **contractual law**,

and if applicable, **consumer law**, **controllers are free to design their**

business, services and contracts."

▶ There are good arguments against the EDPB's core contract view

Scope

Concrete objective approach (Malte Engeler)

▶ "As long as contractual provisions are **neither immoral nor contrary to good faith**, and

as long as they **pass a general terms and conditions check**, the data protection

assessment must accept the **concrete contractual provisions** that have been effectively

agreed and consequently come to the conclusion that the **data processing operations**

required to fulfil these agreements are justified by Art. 6 (1) b GDPR."

▶ A link between the processing of data and the contractual rights and obligations is needed

and the agreed clauses of contracts determine what is necessary

▶ Purpose of data processing = fulfillment of contractual obligation *A* or exercising right *B*

out of contract *X*

Scope

<u>Strengths of the concrete objective approach</u>

▶ Contractual freedom remains as it is governed in civil law

▶ Data subjects are not free of protection but remain protected by consumer

protection and contract law and data protection law

▶ Higher Court of Munich: "Contractual parties **must be able to process contract-**

relevant information. Contracts are always the result of **privately autonomous**

decisions. Data processing pursuant to Art. 6 (1) b GDPR is **necessary** if it is

carried out and **required for the fulfilment of obligations** or the **exercise of**

rights arising from a contract."

Possibilities of concluding contracts

Possibilities

Permissionless blockchain systems

▶ Possibility of concluding a contract with everyone part of the blockchain system that is

  processing data?

▶ Civil law of member states might not allow a conclusion of contracts with an undefined

  number of parties ---> transparency

▶ Who is the controller?

▶ <u>Not</u> the key question – data processing can be carried out by other parties than the

  controller ("*contract to which the data subject is party*")

▶ One party has to take the responsibility of concluding contracts with data subjects

▶ Integration of automatized conclusion of contracts should be possible

Possibilities

Permissioned blockchain systems

▶ Central entity that administrates permissions

▶ Concluding contracts with central entity should be more easy

▶ Contractual provisions must be neither immoral nor contrary to good faith and

 pass a general terms and conditions check

▶ It is (in general) possible to conclude blockchain technology specific contracts

Applying Art. 6 (1) b GDPR to data processing with blockchain technology

Application

▶ "Core contract view" would set borders where *"less intrusive compared to other options for achieving the same goal (fulfilling the core of a contract)"* would be available

▶ Core contract view would complicate concluding contracts in permissionless blockchain systems

▶ Concrete objective approach leaves much room for customization

▶ Anything that can be agreed upon within the boundaries of consumer and contract law can be justified under the legal basis in Art. 6 (1) b GDPR

▶ Agreeing on processing of data with blockchain technology possible

Termination of contracts

Termination

Problem of data no longer being necessary?

▶ Legal basis remains: data remains necessary for fulfillment of the contracts with other parties

Problems with deletion because data is hypothetically no longer "necessary"?

Permissionless blockchain systems:

▶ Art. 11 (2) GDPR: If the purposes for which a controller processes personal data **do not or do no longer require the identification** of a data subject by the controller **Articles 15 to 20 shall not apply**

Permissioned blockchain systems:

▶ Art. 17 (3) e GDPR: "*shall not apply to the extent that processing is necessary for the establishment, exercise or defense of legal claims*"

▶ Art. 6 (1) f GDPR might apply

Thank you for your attention

twitter.com/philippquiel

linkedin.com/in/philippquiel

Philipp Quiel

![reuschlaw Legal Consultants]

Berlin

Joachimsthaler Str. 34
10719 Berlin

T > +49 30 / 233 28 95 0
F > +49 30 / 233 28 95 11
E > info@reuschlaw.de

Saarbrücken

Hochstraße 63
66115 Saarbrücken

T > +49 681 / 85 91 60 0
F > +49 681 / 85 91 60 11
E > info@reuschlaw.de

Social Media

https://twitter.com/reuschlaw

https://www.xing.com/companies/reuschrechtsanwälte

https://www.linkedin.com/company/7371939/

www.reuschlaw.de

DEUTSCHLANDS
BESTE
ANWÄLTE
2018
Philipp Reusch
Produkthaftung
Handelsblatt
Handelsblatt · 13.07.2018
Eine Kooperation mit
Best Lawyers

The
LEGAL 500
DEUTSCHLAND
FÜHRENDE KANZLEI
2019

WirtschaftsWoche
TOP Kanzlei
Datenschutzrecht
2019
reuschlaw
Legal Consultants
In Kooperation mit:
Handelsblatt Research Institute
Ausgabe 34/2019

REUSCHLAW LEGAL CONSULTANTS   2019
RECOGNIZED BY
Best Lawyers