



Vortrag IT-Rechtstag 2021

Dr. Rainer Knyrim

2021 ist ein schwieriges Jahr...

WIRTSCHAFT

Budget: Corona-Krise sorgt für Rekord-Defizit von 33,2 Mrd. Euro

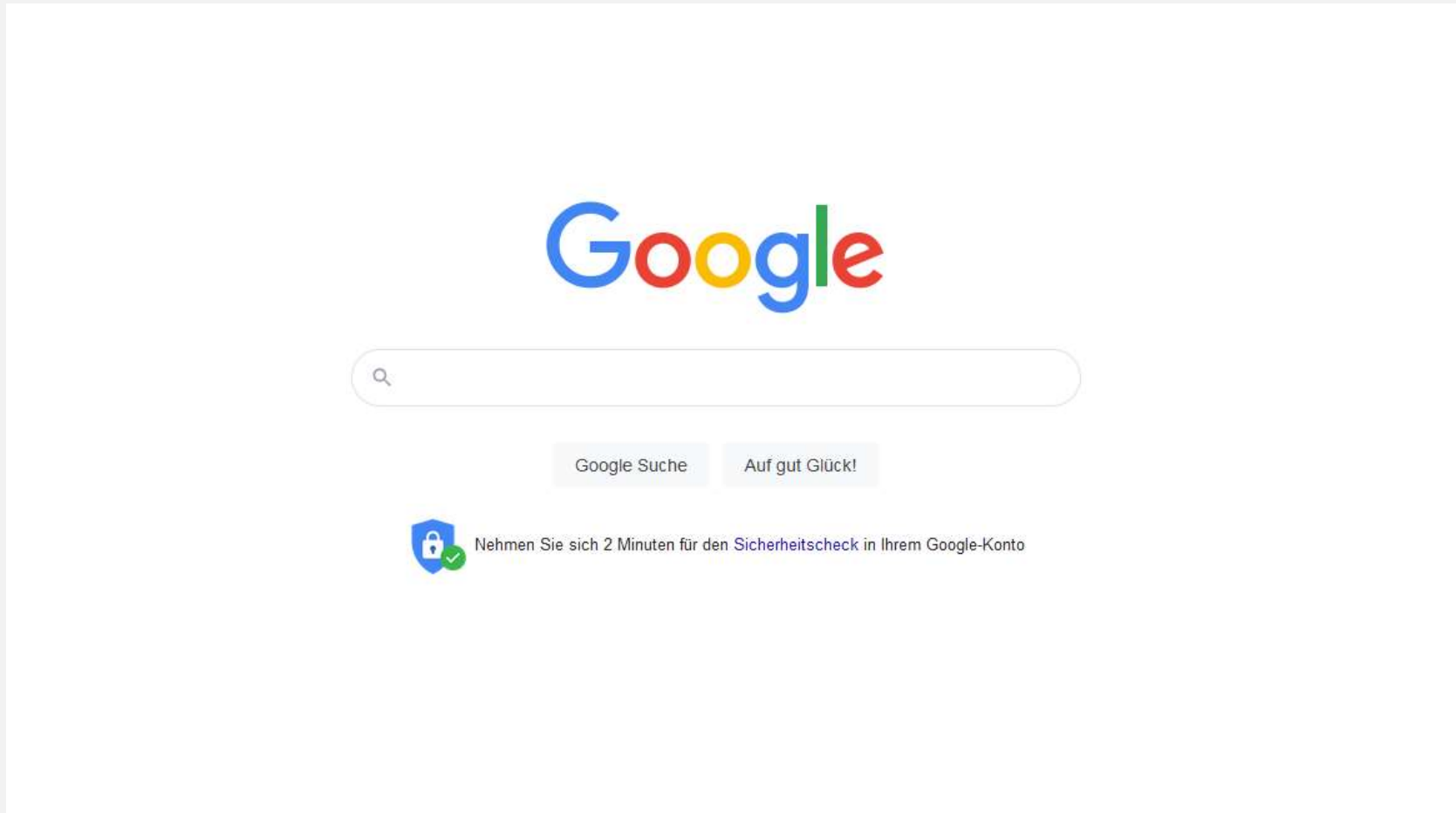
5 KOMMENTARE

1.04.2021 09:32 (Akt. 1.04.2021 14:37)

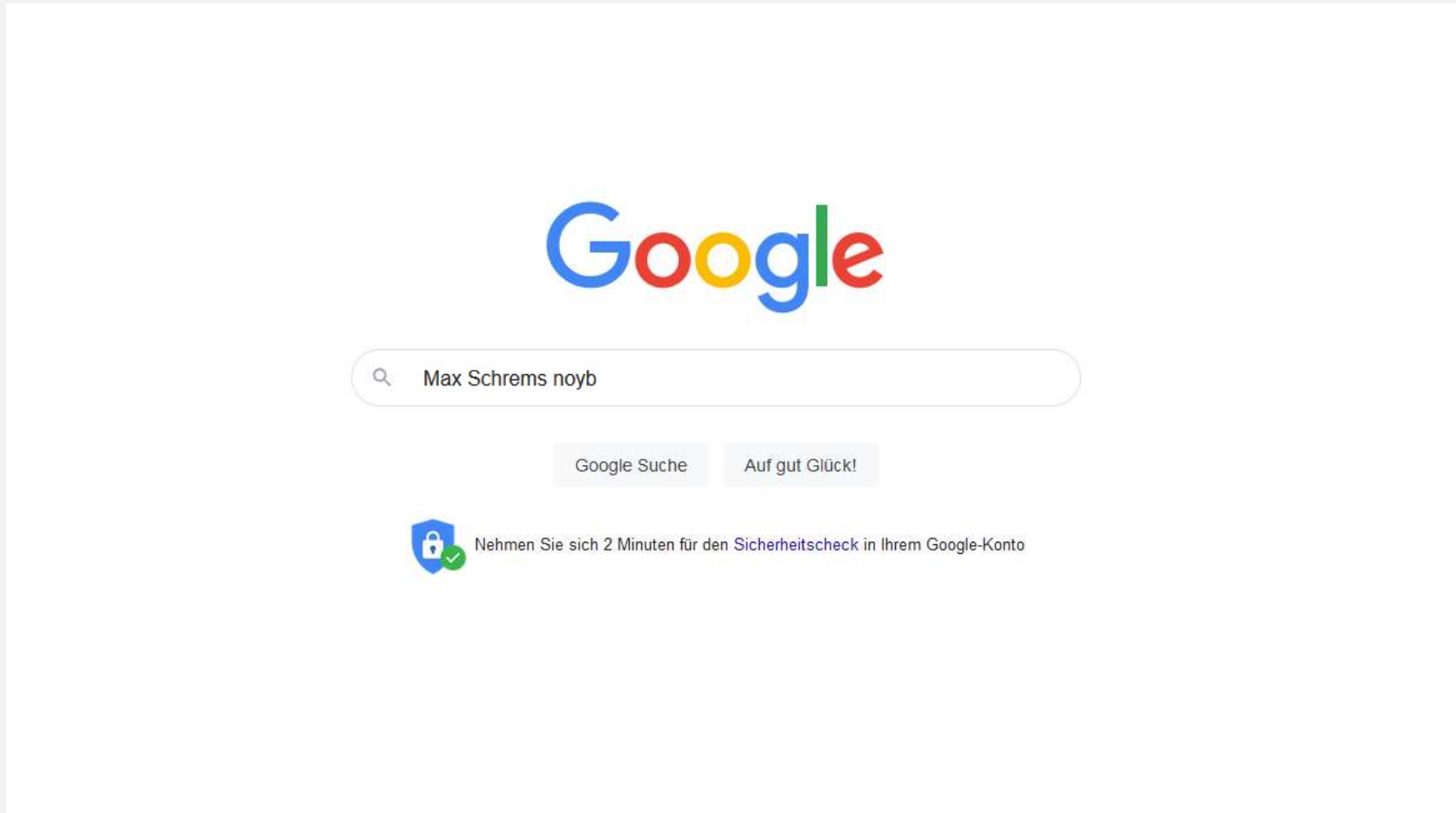


Wer soll das bezahlen?

Someone has to pay the pandemic!



Someone has to pay the pandemic!



Max Schrems, 6.5.2021

Penalty of more than € 6 billion possible. Since the complaint targets Google LLC which operates separately from its European subsidiary (Google Ireland Ltd) any data protection authority in the EU can impose a penalty under the GDPR. In this specific case, the Austrian Data Protection Authority (DPA) can impose 4% of Google LLC's global turnover - a record sum of just over €6 billion.

"It is a unique opportunity to do something for the protection of fundamental rights and for a county's budget simultaneously. Under the GDPR, there is even an obligation for authorities to issue appropriate penalties and Google really fulfills every condition to make full use of the penalty range."
– Max Schrems, Honorary Chairman of *noyb.eu*

Schrems: Eine „einzigartige Gelegenheit“ zwei Fliegen mit einer Klappe schlagen: öst. Datenschutzbehörde soll EUR 6 Milliarden Strafe gegen Google verhängen und kann damit gleichzeitig etwas für die Grundrechte und unser Budget tun.

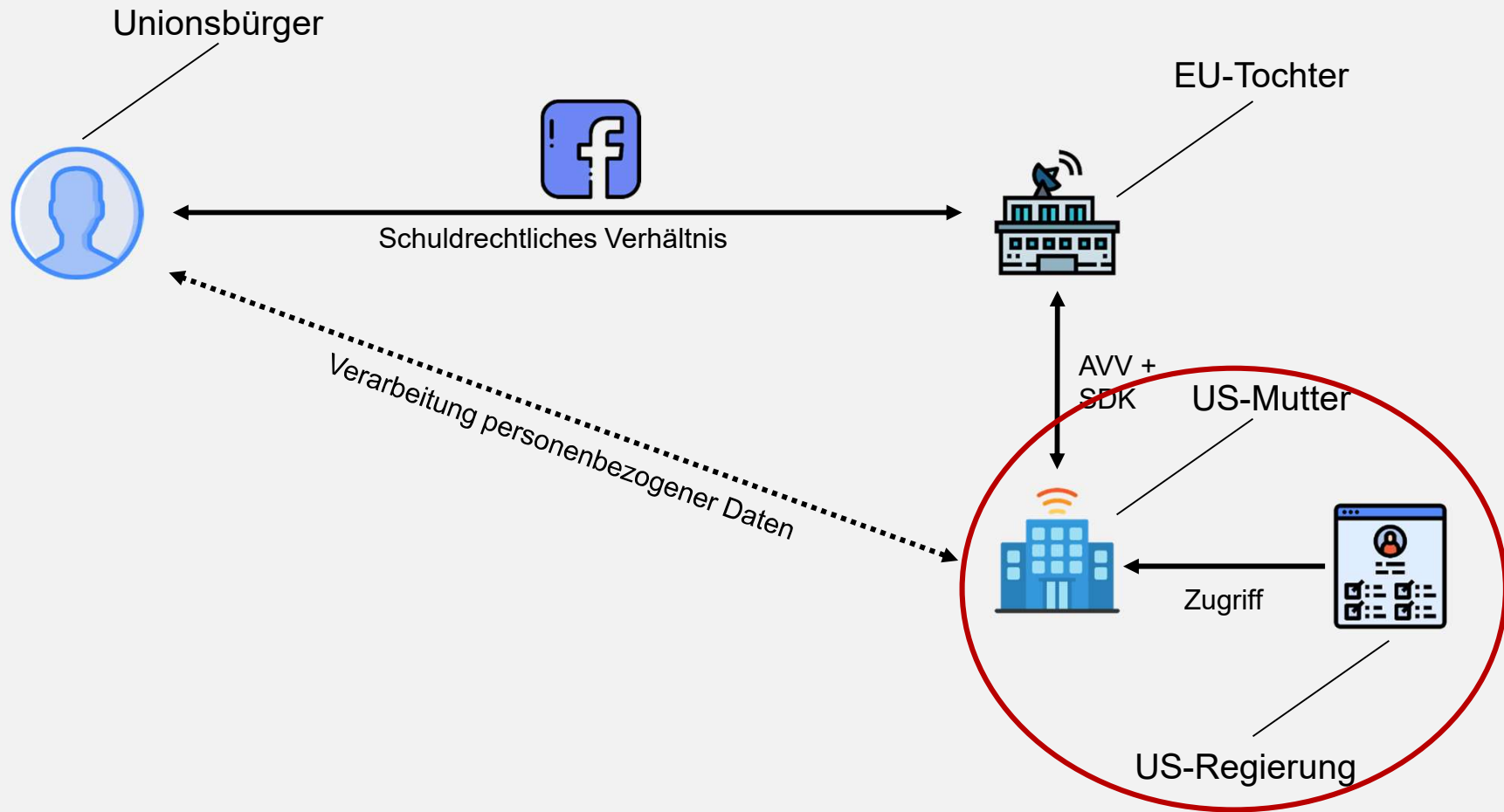
Aber lassen Sie uns ganz von vorne beginnen:

Willkommen zu meinem Vortrag am heurigen IT-Rechtstag:

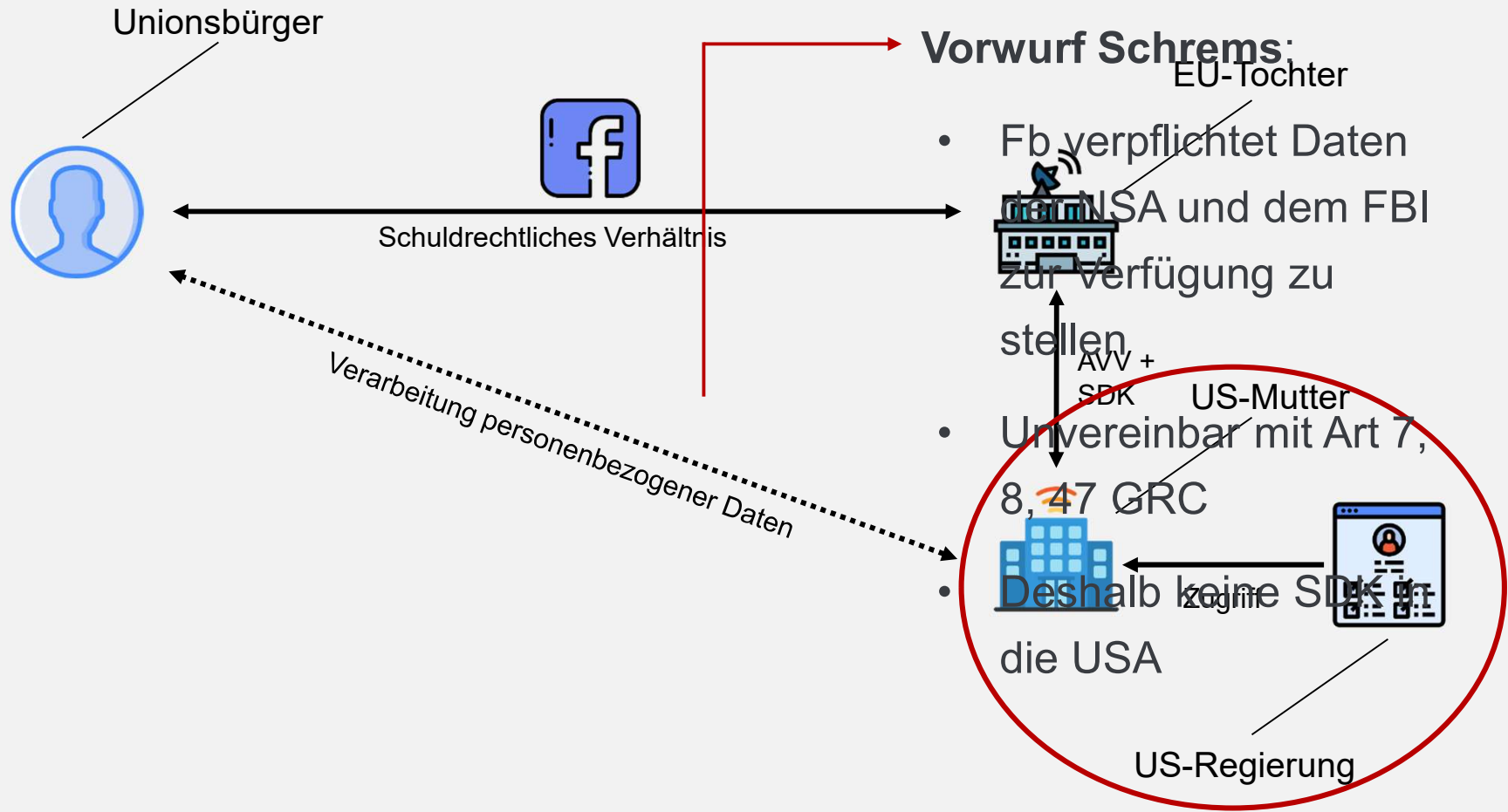
Schrems II – Bewältigung der Folgen

Teil 1: Was bisher geschah

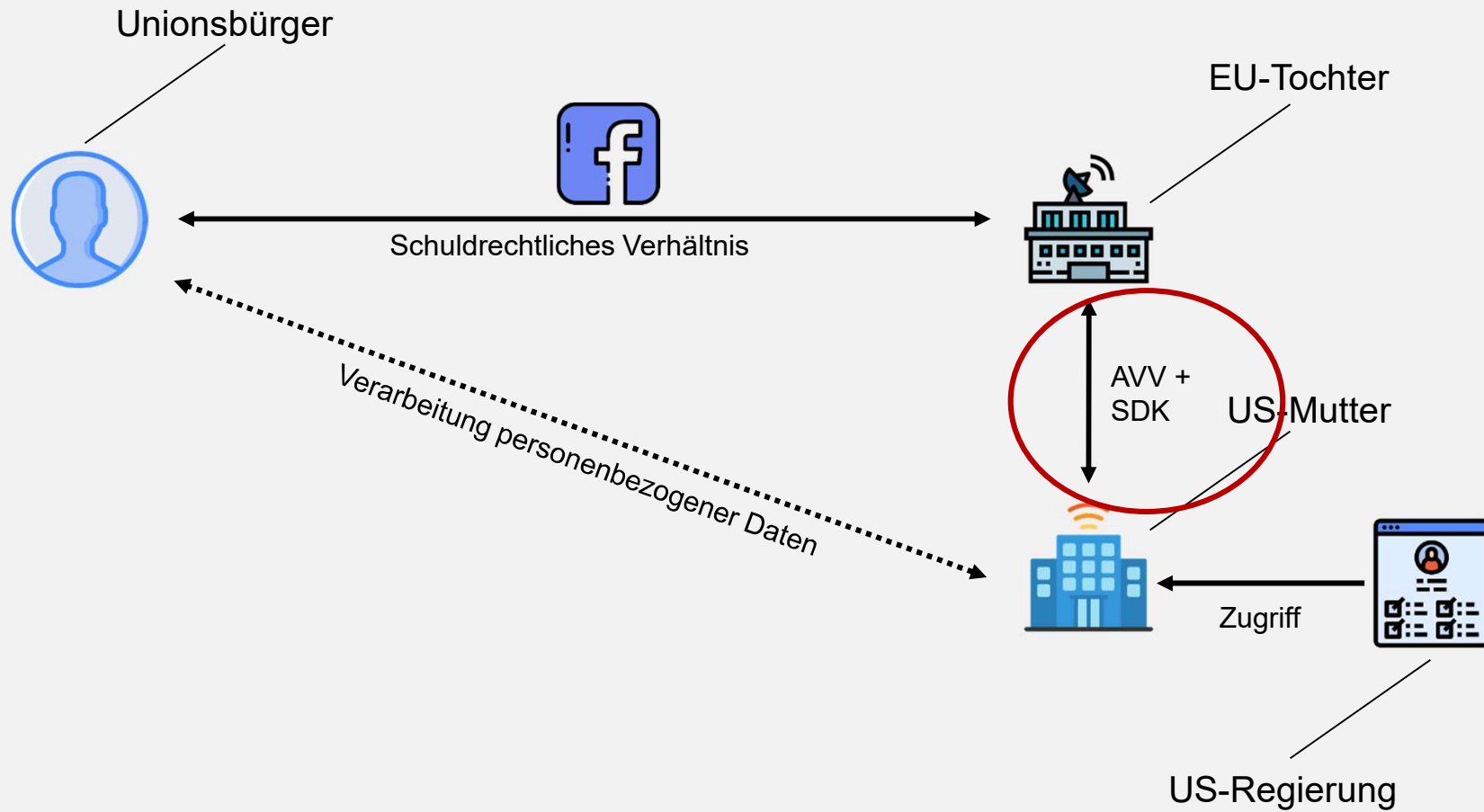
Ausgangssituation



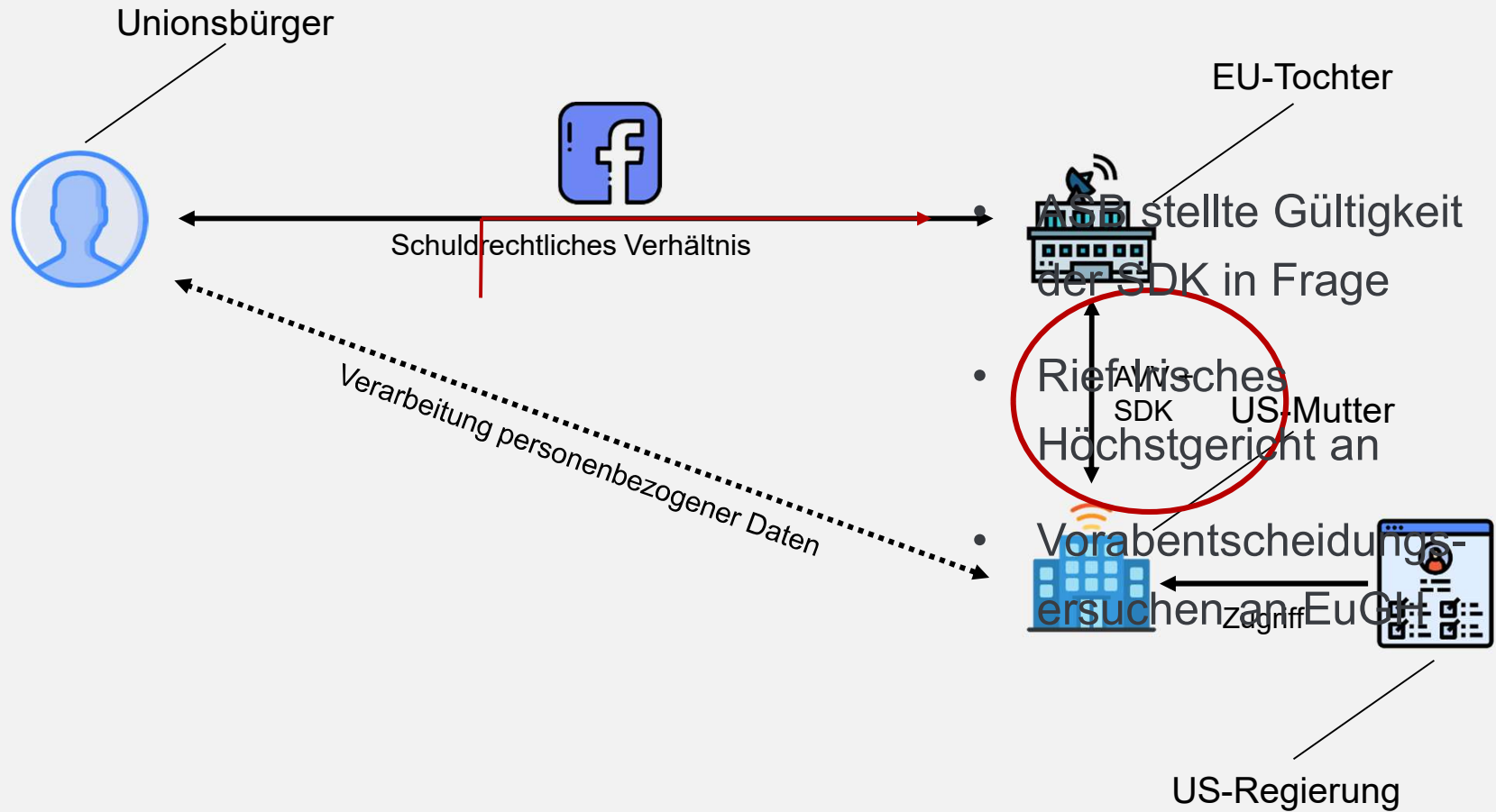
Ausgangssituation



Ausgangssituation



Ausgangssituation



EuGH Schrems II



**Angemessenes
Schutzniveau**

Beurteilungsmaßstab

Elemente des Art 45 Abs 2
DSGVO, **durchsetzbare
Rechte und wirksame
Rechtsbehelfe** müssen
gegeben sein



**Standardvertragsklauseln
nur mit zusätzlichen
Maßnahmen weiter
einsetzbar**

Wegen etwaigem Zugriff von
Behörden im Drittland sind
**Datentransfers in Länder
mit nicht angemessenem
Schutzniveau auf Basis
Standardvertragsklauseln
nur mehr mit zusätzlichen
technisch-
organisatorischen
Maßnahmen (TOMs)
zulässig**



**Standardvertragsklauseln
Drittlandsübermittlungen
sind von**

**Datenschutzbehörde bei
Zweifeln auszusetzen oder zu
untersagen. Datenexporteur
hat Meldepflicht** bei
Datenschutzbehörde wenn er
trotz fehlendem Schutzniveau
weiter übermittelt



Privacy Shield aufgehoben

**USA nicht mehr im Kreis
jener Staaten mit
angemessenem
Datenschutzniveau – Privacy
Shield aufgehoben**, Problem
daher nun auch bei US-
Datentransfers mit
Standardvertragsklauseln

Datentransfers in Drittländer – Art 44ff DSGVO

Drittland: = alle Nicht-EWR - Staaten

Angemessenheitsbeschluss


Art 45 DSGVO

- ~~Privacy Shield~~
- Gleichgestellte Drittstaaten

Geeignete Garantien
Art 46, 47 DSGVO

Ausnahmen für bestimmte Fälle
Art 49 DSGVO

Gleichgestellte Drittstaaten

- Andorra
 - Argentinien
 - Kanada
 - Färöer Inseln
 - Guernsey
 - Isle of Man
 - Israel
 - Jersey
 - Japan
 - Neuseeland
 - Uruguay
 - Schweiz
-  Wie geht es nach dem Brexit weiter?

Datentransfer generell

Angemessenheitsbeschluss
Art 45 DSGVO

Geeignete Garantien

Art 46, 47 DSGVO

- *Verbindliche interne Datenschutzvorschriften*
- *Standarddatenschutzklauseln (EU, national)*
- *Genehmigte Verhaltensregeln*
- *Genehmigte Zertifizierungen*
- *Vertragsklauseln*

Ausnahmen für bestimmte Fälle
Art 49 DSGVO

Datentransfer in die USA – zusätzliche Maßnahmen?

Angemessenheitsbeschluss
Art 45 DSGVO

Geeignete Garantien Art 46, 47 DSGVO

- Verbindliche interne Datenschutzvorschriften
- Standarddatenschutzklauseln (EU-Kommission)
- Genehmigte Verhaltensregeln
- Genehmigte Zertifizierungen
- Vertragsklauseln

Ausnahmen für bestimmte Fälle
Art 49 DSGVO

Standarddatenschutzklauseln (SDK)

Vertragliche Regelungen zwischen Datenexporteur und –importeur. Neue SDK im Entwurf von EU-Kommission publiziert.

Datenschutzniveau in den USA trotz SDK **nicht angemessen**

Zusätzliche Maßnahmen erforderlich (vgl. EuGH, EDSA)

Prüfpflicht des Datenexporteurs vor **jeder** Übermittlung

→ **Kein Verlassen auf einmal Prüfung des Status Quo bei Vertragsabschluss möglich**

Datentransfer generell

Angemessenheitsbeschluss
Art 45 DSGVO

Geeignete Garantien
Art 46, 47 DSGVO

Ausnahmen für bestimmte Fälle

Art 49 DSGVO

- *Einwilligung der betroffenen Person*
- *Vertragsanbahnung und –erfüllung*
- *Wichtige Gründe öffentlichen Interesses*
- *Geltendmachung, Ausübung, Verteidigung von Rechtsansprüchen*
- *Schutz lebenswichtiger Interessen*
- *Übermittlung aus Registern*
- *Zwingende berechnigte Interessen*

Übermittlung an Drittländer – Ausnahmen gem. Art 49 DSGVO

- Beispiel „Interviews“:
 - Selbständige, freie Wissenschaftlerin
 - Werkvertrag mit NGO/NPO in USA (einzelnes, zeitlich begrenztes Projekt)
 - Inhalt: Durchführung und Auswertung von Interviews und Berichterstellung (Interviewpartner werden von Wissenschaftlerin selbst ausgesucht und kontaktiert)
 - In Interviews geht es auch um politische Meinungen (Art 9-Daten!)

Übermittlung an Drittländer – Ausnahmen gem. Art 49 DSGVO

- Beispiel „Interviews“:
 - **Lösung**: ausdrückliche Einwilligung gemäß Art 49 Abs 1 lit a
 - Kommt nur für gelegentliche und nicht wiederholte Übermittlungen in Betracht!
 - Ausdrückliche Einwilligung nachdem die betroffenen Personen über die Risiken derartiger Datenübermittlungen informiert wurden und vor tatsächlicher Datenübermittlung

Teil II

Teil II

Bewältigung der Folgen von Schrems II:

Auf der Suche nach den zusätzlichen Maßnahmen

Bewältigung der Folgen von Schrems II: Welche zusätzliche Maßnahmen müssen getroffen werden?

Antworten gibt der Europäischen Datenschutzausschuss in seinen Empfehlungen:

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Adopted on 10 November 2020

Empfehlungen EDSA 1/2020

Providing for the contractual obligation to use specific technical measures

Depending on the specific circumstances of the transfers, the contract may need to provide that for transfers to take place, specific technical measures would have to be put in place (see supra the technical measures suggested).

Google – zusätzliche Maßnahme?



Austrian DPA has option to fine Google up to €6 billion

May 06, 2021



Project

[EU-US Data Transfers](#)

Support us!

[noyb funding goal](#)

67 %

INVEST IN PRIVACY!

Follow us!

Sie haben 6 entgangene An

Empfehlungen EDSA 1/2020

The exporter could reinforce its power to conduct audits⁸² or inspections of the data processing facilities of the importer, on-site and/or remotely, to verify if data was disclosed to public authorities and under which conditions (access not beyond what is necessary and proportionate in a democratic society), for instance by providing for a short notice and mechanisms ensuring the rapid intervention of inspection bodies and reinforcing the autonomy of the exporter in selecting the inspection bodies.

AWS

AWS GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) supplements the AWS Customer Agreement available at <http://aws.amazon.com/agreement>, as updated from time to time between Customer and AWS, or other agreement between Customer and AWS governing Customer’s use of the Service Offerings (the “**Agreement**”) when the GDPR applies to your use of the AWS Services to process Customer Data. This DPA is an agreement between you and the entity you represent (“**Customer**”, “**you**” or “**your**”) and the applicable Amazon Web Services contracting entity under the Agreement (“**AWS**”). Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this DPA will have the meanings given to them in Section 17 of this DPA.

AWS

SUPPLEMENTARY ADDENDUM TO AWS GDPR DATA PROCESSING ADDENDUM

The purpose of this supplementary addendum (this “**Addendum**”) is to outline supplemental measures that AWS takes to protect Customer Data. This Addendum supplements, but does not modify, the AWS GDPR Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf, or other agreement between Customer and AWS governing the processing of Customer Data pursuant to the GDPR (the “**AWS GDPR DPA**”). Unless otherwise defined in this Addendum, all capitalised terms used in this Addendum will have the meanings given to them in the AWS GDPR DPA.

AWS

- 11. Customer Audits.** Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing AWS to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement. If AWS declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

AWS

Clause 5

Obligations of the data importer¹

- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

AWS: Vetorecht gegen Subverarbeiter? Art 28 DSGVO?

6. Sub-processing.

6.1 **Authorised Sub-processors.** Customer agrees that AWS may use sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services. The AWS website (currently posted at <https://aws.amazon.com/compliance/sub-processors/>) lists sub-processors that are currently engaged by AWS to carry out processing activities on Customer Data on behalf of Customer. At least 30 days before AWS engages any new sub-processor to carry out processing activities on Customer Data on behalf of Customer, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer objects to a new sub-processor, then without prejudice to any termination rights Customer has under the Agreement and subject to the applicable terms and conditions, Customer may move the relevant Customer Data to another AWS Region where the new sub-processor to whom Customer objects, is not engaged by AWS as a sub-processor. Customer consents to AWS's use of sub-processors as described in this Section. Except as set forth in this Section, or as Customer may otherwise authorise, AWS will not permit any sub-processor to carry out processing activities on Customer Data on behalf of Customer.

Empfehlungen EDSA 1/2020

The contract could oblige the importer and/or the exporter to notify promptly the data subject of the request or order received from the public authorities of the third country, or of the importer's inability to comply with the contractual commitments, to enable the data subject to seek information and an effective redress (e.g. by lodging a claim with his/her competent supervisory authority and/or judicial authority and demonstrate his/her standing in the courts of the third country).

Empfehlungen EDSA 1/2020

The importer could commit to reviewing, under the law of the country of destination, the legality of any order to disclose data, notably whether it remains within the powers granted to the requesting public authority, and to challenge the order if, after a careful assessment, it concludes that there are grounds under the law of the country of destination to do so. When challenging an order, the data importer should seek interim measures to suspend the effects of the order until the court has decided on the merits. The importer would have the obligation not to disclose the personal data requested until required to do so under the applicable procedural rules. The data importer would also commit to providing the minimum amount of information permissible when responding to the order, based on a reasonable interpretation of the order.

AWS

AWS and EU data transfers: strengthened commitments to protect customer data

Our strengthened contractual commitments include:

- **Challenging law enforcement requests:** We will challenge law enforcement requests for customer data from governmental bodies, whether inside or outside the EEA, where the request conflicts with EU law, is overbroad, or where we otherwise have any appropriate grounds to do so.
- **Disclosing the minimum amount necessary:** We also commit that if, despite our challenges, we are ever compelled by a valid and binding legal request to disclose customer data, we will disclose only the *minimum amount* of customer data necessary to satisfy the request.

These strengthened commitments to our customers build on our long track record of challenging law enforcement requests. AWS rigorously limits – or rejects outright – law enforcement requests for data coming from any country, including the United States, where they are overly broad or we have any appropriate grounds to do so.

Salesforce



Salesforce's Principles for Government Requests for Customer Data

Published: July 2020

Salesforce

We notify an affected customer of any request for its Customer Data unless we are explicitly prohibited from doing so by law

Trust starts with transparency. Unless prohibited by law, Salesforce always notifies a customer when it receives a request for that customer's Customer Data, including a government request, as further set out in the "Compelled Disclosure" section of our Master Subscription Agreement.

Salesforce

Salesforce's Processor Binding Corporate Rules contain specific requirements regarding our handling of government requests for EU Personal Data

If we receive a government request for Personal Data governed by [Salesforce's Processor Binding Corporate Rules](#) ('BCRs'), and we are prohibited by law from notifying the affected customer, we use best efforts to request that the confidentiality requirement be waived in order for us to notify the appropriate EU data protection authorities. Our commitment to this approach is described in Section 10 of our BCRs, which are legally binding on Salesforce and have been reviewed and approved by all EU data protection authorities.

Salesforce

Publiziert als Prinzip auf Homepage, aber nicht Vertragsbestandteil der BCRs von Salesforce:

We do not disclose Customer Data to government agencies unless compelled by law and we challenge unlawful requests

We review each government request for Customer Data on a case-by-case basis and only comply if and to the extent we determine the request is lawful. When reviewing the lawfulness of a government request, we take into account all applicable laws, including the laws of other jurisdictions, where applicable. We require governmental agencies to follow the required legal process under applicable laws, such as issuing their request via a subpoena, court order, or search warrant. Where we believe a government request for Customer Data is invalid or unlawful, we try to challenge it.

Empfehlungen EDSA 1/2020 – digitaler „Totmannknopf“!

Insofar as allowed by national law in the third country, the contract could reinforce the transparency obligations of the importer by providing for a “Warrant Canary” method, whereby the importer commits to regularly publish (e.g. at least every 24 hours) a cryptographically signed message informing the exporter that as of a certain date and time it has received no order to disclose personal data or the like. The absence of an update of this notification will indicate to the exporter that the importer may have received an order.

Empfehlungen EDSA 1/2020 –

Furcht des EDSA vor Herausgabepflicht des Verschlüsselungsschlüssels:

As an example, US data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible.

Empfehlungen EDSA 1/2020 – Use Cases

Use Case 1: Data storage for backup and other purposes that do not require access to data in the clear

A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes.

If

1. the personal data is processed using strong encryption before transmission,
2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
3. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,
4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
5. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and
6. the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,

then the EDPB considers that the encryption performed provides an effective supplementary measure.

Empfehlungen EDSA 1/2020 – Use Cases

Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear

A data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country.

If

1. a controller transfers data to a cloud service provider or other processor,
2. the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,⁷¹

then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.

In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.



Entscheidung Conseil d'Etat

COUNCIL OF STATE
adjudicating on the dispute
N° 450163

ASSOCIATION INTERHOP and others

Order of 12 March 2021
FRENCH REPUBLIC
IN THE NAME OF THE FRENCH PEOPLE
THE INTERIM RELIEF JUDGE

Entscheidung Conseil d'Etat

Datenspeicherung von Covid-Impfdaten in AWS Cloud zulässig, da Verschlüsselungsverfahren auf Basis einer vertrauenswürdigen Dritten mit Sitz in Frankreich eingerichtet war:

the contestation of any general request or one that does not comply with European regulations. Doctolib has also set up a security system for data hosted by AWS through an encryption procedure based on a trusted third party located in France in order to prevent the reading of data by third parties. Having regard to those safeguards and to the data concerned, the level of protection of the data relating to appointments made in the context of the Covid-19 vaccination campaign cannot be regarded as manifestly inadequate in the light of the risk of infringement of the General Data Protection Regulation invoked by the applicants. Although the applicant association also invoked the

<https://www.youtube.com/watch?v=uhXalpNzPU4>
Encryption and Key Management in AWS -

AWS Summit

Client-Side Encryption with S3

Amazon S3 Encryption Client with AWS SDKs

The diagram illustrates the architecture for Client-Side Encryption with S3. It is divided into two main sections: 'Your applications in your data center' and 'AWS'.

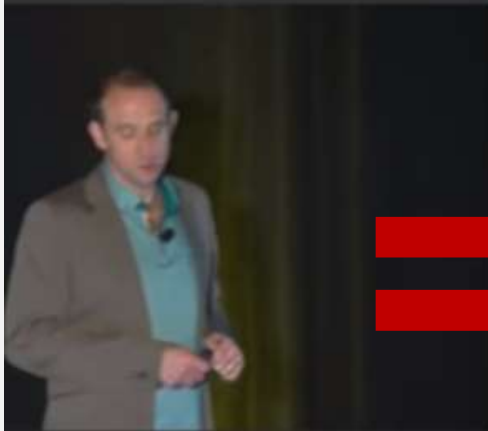
- Your applications in your data center:** This section shows data being processed by 'Your key management infrastructure' and then sent to 'AWS SDK with S3 Encryption Client'.
- AWS:** This section shows 'Your application in Amazon EC2' and 'Your key management infrastructure in EC2'. The application in EC2 sends data to the key management infrastructure in EC2, which then encrypts the data. The encrypted data is then stored in 'Your Encrypted Data in Amazon S3'.

A red arrow points to the 'Your key management infrastructure in EC2' component, indicating its role in the encryption process.

nd Key
in AWS



AWS Summit



and Key
t in AWS



Comparison of Key Management

	On-Premises HSM	AWS CloudHSM	AWS Key Management Service
Where keys are generated and stored	Your network	AWS	AWS
Where keys are used	Your network or your EC2 instance	AWS + your network	AWS
How to use keys	Customer code	Customer code + Safenet APIs	Management Console, AWS SDKs
Performance/Scale/HA responsibility	You	You	AWS
Integration with AWS services?	No	Redshift	Yes
Price	\$\$\$\$	\$\$	\$
Who controls access to keys	Only You	Only You	You + AWS

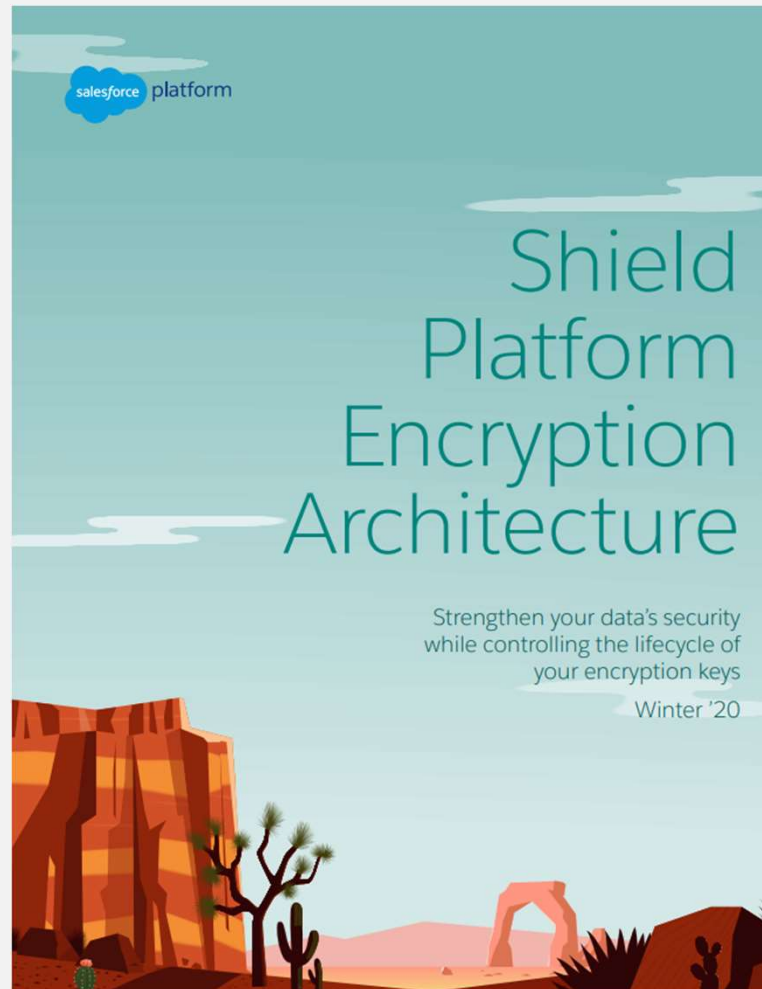
AWS Summit

AWS CloudHSM

- You receive **dedicated access** to HSM appliances
- HSMs are located in AWS datacenters
- Managed & monitored by AWS
- **Only you have access to your keys and operations on the keys**
- HSMs are inside your VPC – isolated from the rest of the network
- Uses SafeNet Luna SA HSM appliances



Salesforce



Salesforce

Sie haben vier Optionen zum Einrichten Ihres Schlüsselmaterials.

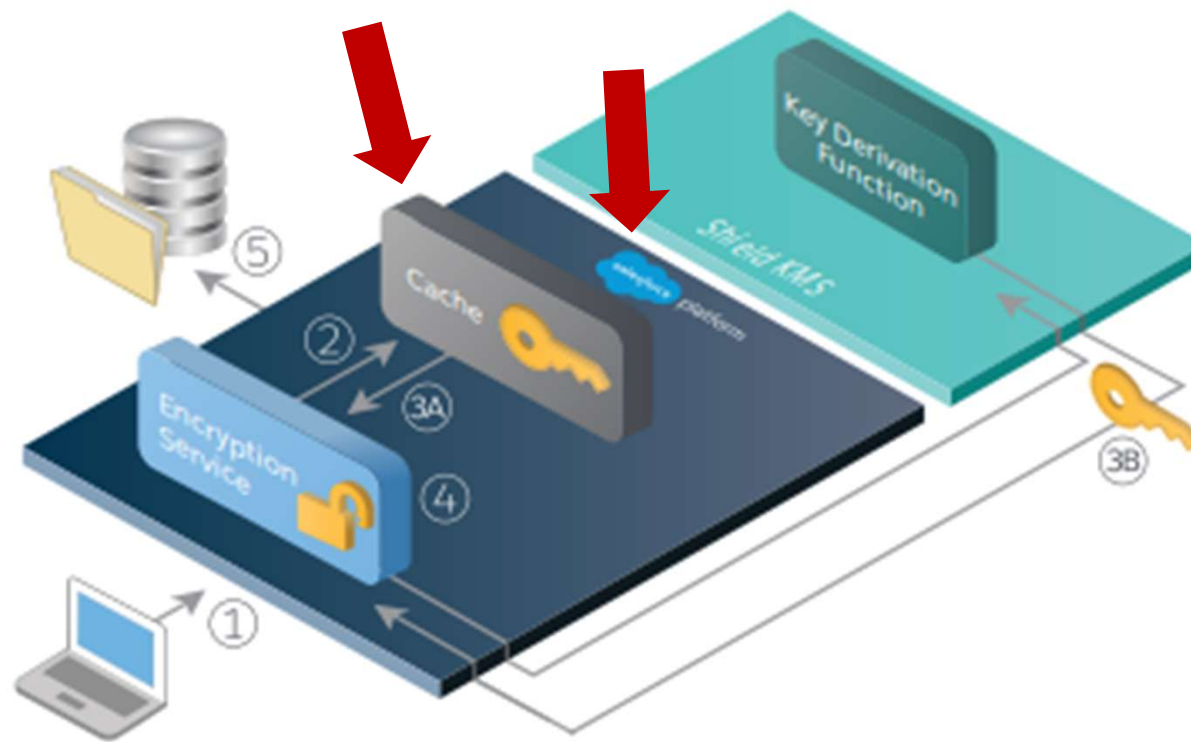
- Verwenden Sie den Shield-Service für die Schlüsselverwaltung (Key Management Service, KMS), damit Ihr organisationsspezifisches Mandantengeheimnis für Sie generiert wird.
- Verwenden Sie eine Infrastruktur Ihrer Wahl, beispielsweise ein lokales Hardware-Sicherheitsmodul, um das Mandantengeheimnis außerhalb von Salesforce zu generieren und zu verwalten. Laden Sie dieses Mandantengeheimnis anschließend in die Salesforce-KMS hoch. Diese Option wird allgemein als "Bring Your Own Key" bezeichnet, auch wenn das Element, das Sie tatsächlich "mitbringen", das Mandantengeheimnis ist, von dem der Schlüssel abgeleitet wird.
- Deaktivieren Sie den Ableitungsvorgang des Shield-Service für die Schlüsselverwaltung mit dem Service "Bring Your Own Key". Verwenden Sie die gewünschte Infrastruktur, um anstelle eines Mandantengeheimnisses einen Datenverschlüsselungsschlüssel zu erstellen. Laden Sie diesen Datenverschlüsselungsschlüssel anschließend in den Shield-Service für die Schlüsselverwaltung hoch. Wenn Sie die Ableitung auf Schlüssel-für-Schlüssel-Basis deaktivieren, umgeht der Shield-Service für die Schlüsselverwaltung den Ableitungsvorgang und verwendet dieses Schlüsselmaterial als Ihren endgültigen Datenverschlüsselungsschlüssel. Sie können vom Kunden bereitgestellte Datenverschlüsselungsschlüssel so rotieren, wie Sie ein vom Kunden bereitgestelltes Mandantengeheimnis rotieren würden.
- Generieren und speichern Sie Ihr Schlüsselmaterial außerhalb von Salesforce. Verwenden Sie dazu den gewünschten Schlüsselservice und den Salesforce-Service für nur zwischengespeicherte Schlüssel, um Ihr Schlüsselmaterial nach Bedarf abzurufen. Ihr Schlüsselservice überträgt Ihr Schlüsselmaterial über einen sicheren Kanal, der von Ihnen konfiguriert wird. Anschließend wird es im Cache für sofortige Verschlüsselungs- und Entschlüsselungsvorgänge verschlüsselt und gespeichert.



Salesforce

HOW SHIELD PLATFORM ENCRYPTION WORKS

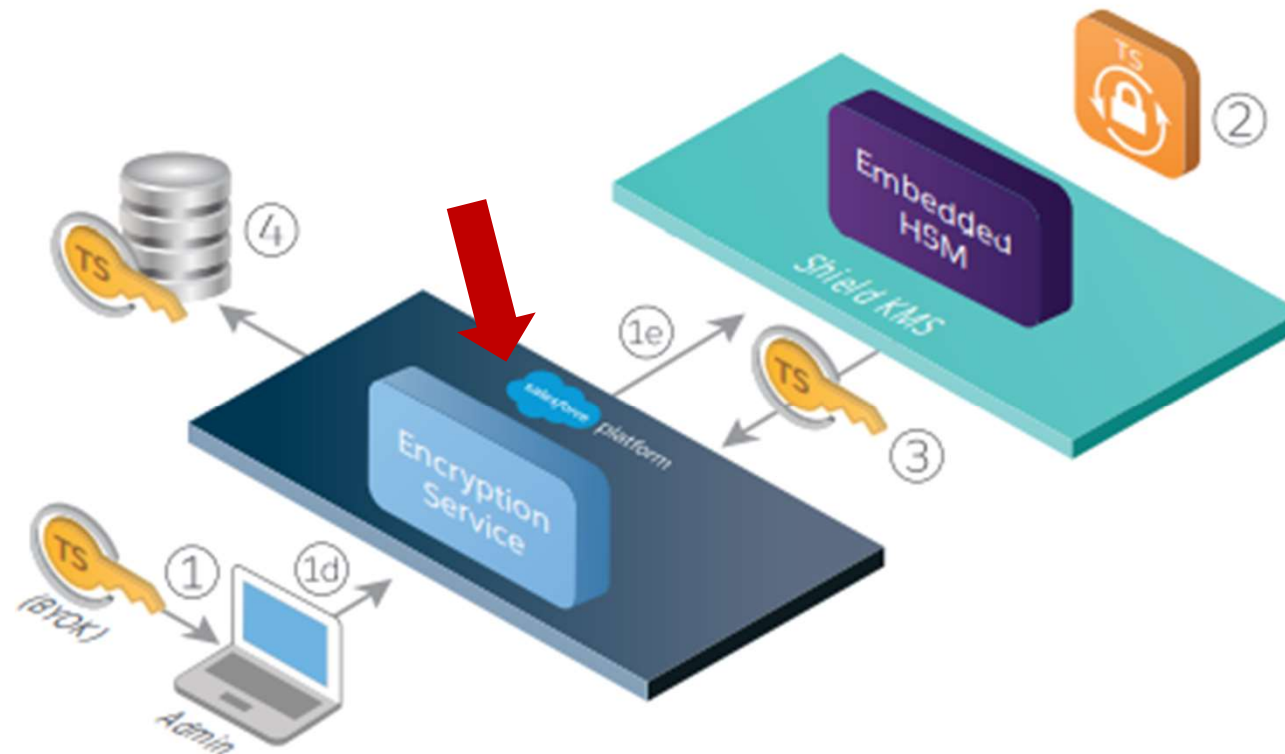
Shield Platform Encryption process flow



Salesforce

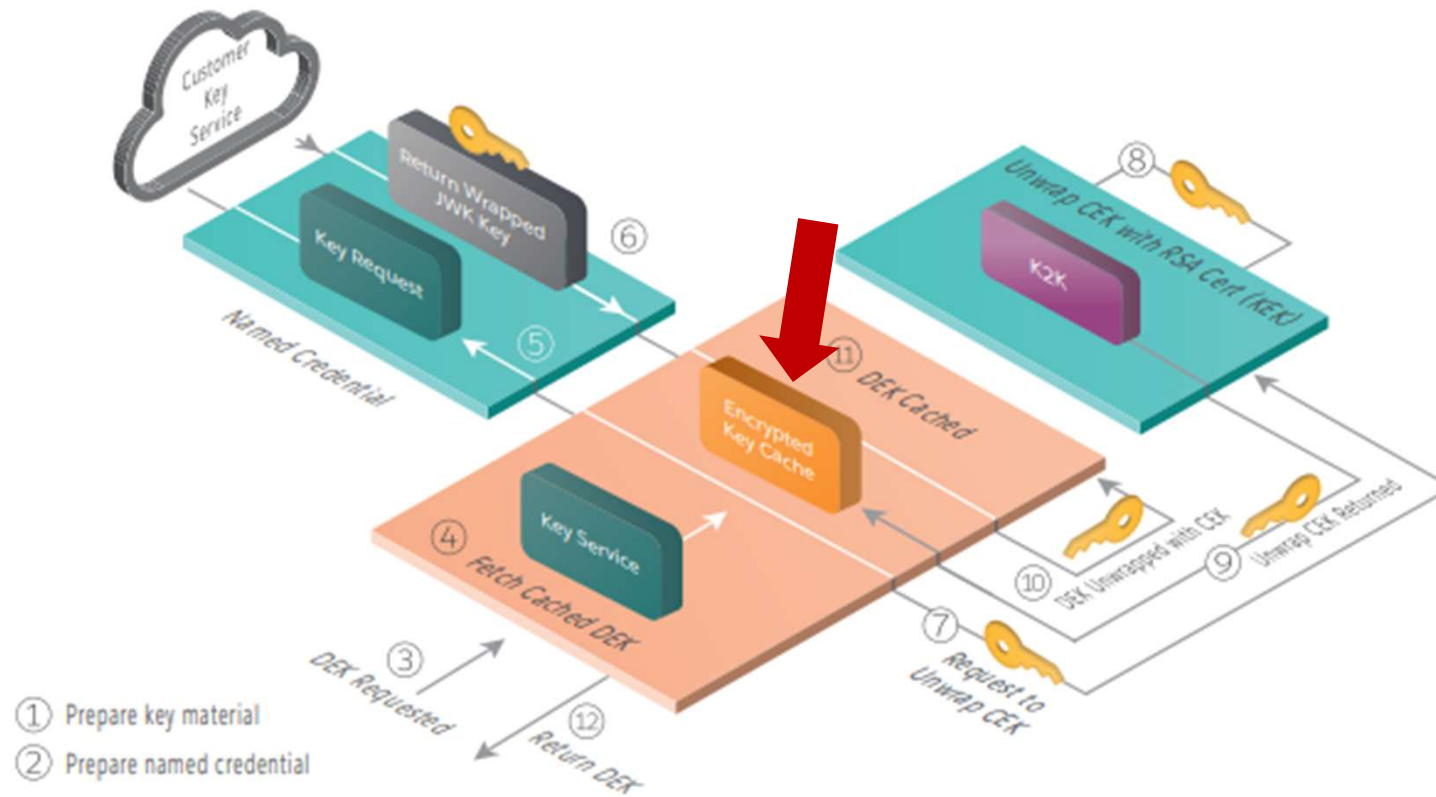
KEY DERIVATION ARCHITECTURE

Customer-supplied tenant secret flow



Salesforce

KEY DERIVATION ARCHITECTURE Cache-only key flow



Praxiserfahrung Verschlüsselungsschlüssel

As an example, US data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible.

Praxiserfahrung: IT-Sicherheits- und Kryptographiearchitekten sind zT sehr fokussiert auf die Absicherung gegen Angriffe von außen, allenfalls auch noch gegen böswillige Mitarbeiter. Der Fall, dass Behörden legaler Weise den Schlüssel herausverlangen können ist oft nicht in ihrem Scope, Schrems II wird daher von den Technikern nicht immer richtig verstanden und muss von den Juristen erst übersetzt werden.

Fraglich ist, ob es technisch möglich ist, ein System so zu gestalten, dass die Daten niemand mehr beim Auftragsverarbeiter selbst entschlüsseln kann und damit dazu auch nicht (erfolgreich) gezwungen werden kann?

Fraglich ist dann aber auch, ob im jeweiligen Land die IT-Systeme von den Anbietern vorsätzlich so konstruiert werden dürfen, dass Überwachungsgesetze nicht mehr umgesetzt werden können?

Was tun, wenn Verschlüsselungslösung das Schrems II - Problem nicht löst? Pseudonymisieren – EDSA Use Case 2

Use Case 2: Transfer of pseudonymised Data

A data exporter first pseudonymises data it holds, and then transfers it to a third country for analysis, e.g., for purposes of research.

If

1. a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information⁶⁹,
2. that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,
3. disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and
4. the controller has established by means of a thorough analysis of the data in question taking into account any information that the public authorities of the recipient country may possess that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

then the EDPB considers that the pseudonymisation performed provides an effective supplementary measure.

Was tun, wenn auch das nicht funktioniert?

- Alternativenanbieter in der EU suchen. Insbesondere bei Webseite-Analysetools, Mailprogrammen gibt es brauchbare Alternativen in der EU.



The screenshot shows the heise online website interface. At the top, there is a navigation bar with the heise online logo and a search icon. Below the navigation bar, there are several menu items: IT, Wissen, Mobiles, Security, Developer, Entertainment, Netzpolitik, and W. Underneath the menu items, there is a section for TOPTHEMEN with tags for EXCHANGE, BITCOIN, AMAZON, CORONA, E-AUTO, and PODCASTS. The main content area displays a news article with the headline "Microsoft: Daten europäischer Unternehmen und Behörden bleiben auf EU-Servern". The article text begins with "Datenverkehr mit den USA hat keine Rechtsgrundlage. Microsoft verspricht, Daten von EU-Unternehmen und der Verwaltung nur auf Servern in der EU zu verarbeiten."

Was tun, wenn auch das nicht funktioniert?

- Wenn keine Alternative:
 - DSFA machen.
 - Zusätzliche Maßnahmen vereinbaren, wenn möglich aushandeln.
 - Mögliche Datenschutzeinstellungen im System aktivieren.
 - Gesamten Prozess dokumentieren.
 - Risiko abschätzen, Management Entscheidung treffen lassen.



Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg



Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 - 40 59 Zentrale - 40 40
E-Fax: 040 - 428 54 - 4000
Ansprechpartner: [REDACTED]

E-Mail: [REDACTED]

Az.: W / 3090/2020

Hamburg, 16. Oktober 2020



KNYRIM.TRIEB
RECHTSANWÄLTE

Drittstaatenübermittlung mittels Office 365 *Hier vorliegende Beschwerde*

Sehr geehrte geehrter Herr [REDACTED],

wir haben einen Hinweis darauf erhalten, dass in Ihrem Unternehmen Office 365 eingesetzt wird und dass dabei personenbezogene Daten in die USA übermittelt werden. Vor dem Hintergrund der Entscheidung des Europäischen Gerichtshofs vom 16.07.2020, Rs. C-311/18 – Schrems II – bitten wir Ihr Unternehmen um Mitteilung, wie Sie diese Praktik mit den unionsrechtlichen Vorgaben in Einklang bringen. Bitte nehmen Sie bzw. das Unternehmen Stellung zu dem uns zugetragenen Hinweis und gehen Sie dabei insbesondere auf die folgenden Punkte ein:

1. Nutzt Ihr Unternehmen Office 365?
2. Welche personenbezogenen Daten werden dort eingefügt?
3. Zu welchen Zwecken geschieht die Nutzung von Office 365?
4. Aufgrund welcher Rechtsgrundlage (erster Stufe) geschieht die Nutzung von Office 365?
5. Seit wann werden diese Verarbeitungen vorgenommen?
6. Werden die Daten nach Ziff. 2 in die USA oder andere Staaten außerhalb des Europäischen Wirtschaftsraums übermittelt?
7. Auf welche rechtlichen Vorkehrungen im Sinne des Kapitel V der DSGVO werden die Drittstaatenübermittlungen nach Ziff. 5 gestützt?

8. Für den Fall, dass die Standardvertragsklauseln der Europäischen Kommission genutzt werden: Welche zusätzlichen Maßnahmen im Sinne der o.g. Entscheidung des Europäischen Gerichtshofs haben Sie unternommen?
9. Bitte nennen Sie auch vorbereitende Schritte im Hinblick auf ggfs. noch nicht vollständig umgesetzte Maßnahmen nach Ziff. 7.
10. Für den Fall, dass die Umstellung auf andere Systeme geplant ist, teilen Sie uns bitte die erwogenen Lösungen und den Stand der Umsetzung mit.
11. Bitte lassen Sie uns die den Einsatz von Office 365 betreffenden Teile Ihres Verzeichnisses der Verarbeitungstätigkeiten zukommen.

Der Stellungnahme Ihres Unternehmens sehen wir entgegen bis zum 15.11.2020.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kontrolliert als Aufsichtsbehörde über die nicht-öffentlichen Stellen gemäß § 40 des Bundesdatenschutzgesetzes (BDSG) die Ausführung der Vorschriften über den Datenschutz im Bereich der Privatwirtschaft. Alle der Kontrolle unterliegenden Stellen haben dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit auf Verlangen die für die Erfüllung seiner Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Für Amtshandlungen, die der Kontrolle durch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit nach § 40 BDSG dienen, werden nach § 34 des Hamburgischen Datenschutzgesetzes (HmbDSG) Gebühren erhoben.

Mit freundlichen Grüßen
im Auftrag



München und Ansbach, den 20.11.2020

Pressemitteilung

Stärkung der Nutzer-Rechte: Microsoft ergänzt Standardvertragsklauseln

Bayerische Datenschutzbehörden begrüßen Initiative
zur Absicherung internationaler Datentransfers

Die neuen Vertragsklauseln von Microsoft enthalten Regelungen über

- die Information der betroffenen Person, wenn Microsoft durch eine staatliche Anordnung rechtlich bindend dazu verpflichtet wurde, Daten an US-Sicherheitsbehörden herauszugeben;
- die Verpflichtung von Microsoft, den Rechtsweg zu beschreiten und die US-Gerichte anzurufen, um die behördliche Anordnung zur Herausgabe der Daten anzufechten;
- den Anspruch auf Schadensersatz für die betroffene Person, deren Daten unrechtmäßig verarbeitet wurden und die dadurch einen materiellen oder immateriellen Schaden erlitten hat

Damit sei, so die gemeinsame Bewertung der beteiligten Datenschutzaufsichtsbehörden, zwar die Transferproblematik in die USA nicht generell gelöst – denn eine Ergänzung der Standardvertragsklauseln könne eben nicht dazu führen, dass der vom Europäischen Gerichtshof als unverhältnismäßig beanstandete Zugriff der US-amerikanischen Geheimdienste auf die Daten unterbunden werde.

noyb gg. Netdokter und Google wg. Google Analytics

Complainant:

████████████████████
████████████████████

Represented pursuant to
Article 80(1) of the GDPR by:

noyb - European Centre for Digital Rights
Goldschlagstr. 172/4/3/2, 1140 Vienna

Respondent to the first
complaint

netdokter.at GmbH
Heiligenstädter Lände 29 / Top 5
1190 Vienna

3. Question 3 - Contract between netdokter.at GmbH and Google LLC

3.1. General remark


Google LLC's answer to this question is conditional and not conclusive. Google LLC describes possible scenarios but does not answer

- whether netdokter.at GmbH uses the free Google Analytics version or the paid version "Google Analytics 360";
- whether netdokter.at GmbH has negotiated or attempted to negotiate the terms of the contract in relation to Google LLC;
- whether netdokter.at GmbH has activated the "data sharing setting" and thus, in the opinion of Google LLC, there is (also) a data protection responsibility of Google LLC and/or Google Ireland Ltd.

Werden Sie aktiv, damit es für Sie als Verantwortlichem nicht so endet, wie noyb fordert....

(2) gemäß Artikel 58(2)(d), (f) und (j) DSGVO unverzüglich ein Verbot oder eine Aussetzung jeglicher Datenübermittlungen vom Verantwortlichen an Google LLC in den Vereinigten Staaten von Amerika verhängt und die Rückgabe dieser Daten an die EU/EWR oder ein anderes Land, das einen angemessenen Schutz gewährleistet, anordnet;

(3) eine wirksame, verhältnismäßige und abschreckende Geldbuße gegen den Verantwortlichen und Google gemäß Artikel 83(5)(c) DSGVO verhängt, wobei zu berücksichtigen ist, dass



Ausblick: Entwurf neue Standarddatenschutzklauseln (Klausel 2)

- (a) The Parties warrant that they have no reason to believe that the laws in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Clauses.
- (b) The Parties declare that in providing the warranty in paragraph a, they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred;
 - (ii) the laws of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards;
 - (iii) any safeguards in addition to those under these Clauses, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination.



Ende

Fragen?

RA Dr. Rainer Knyrim,
Knyrim Trieb Rechtsanwälte OG
1060 Wien, Mariahilfer Straße 89a
Tel. +43/1/9093070, Email ky@kt.at
www.kt.at

Anmeldung zum kostenloser Datenschutz-Newsletter:

<https://www.kt.at/newsletter/>