Privacy Shield ade, was nun?

Referent: Patric Rudtke

VINTIN
make IT unique

Patric Rudtke

Diplom-Betriebswirt (FH)

Manager Team Datenschutz
Senior Consultant für Datenschutz
Externer Datenschutzbeauftragter
Manager IT-Service Management (ITIL)
ISMS Specialist & Lead Auditor ISO 27001

patric.rudtke@vintin.de
09721 / 675 94 167

VINTIN
make IT unique

heise online heise+

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal

TOPTHEMEN: IPHONE 12 E-AUTO SECURITY WINDOWS 10 CORONAVIRUS HOMEOFFICE

FAQ: Das Ende des Privacy Shields

Der EuGH hat den Datenschutzbeschluss "Privacy Shield" für nichtig erklärt. Gibt es jetzt noch eine Rechtsgrundlage, um Daten legal in die USA zu transferieren?

Lesezeit: 4 Min. In Pocket speichern

Rechtsprechung

EuGH, 16.07.2020 - C-311/18

Volltextveröffentlichungen (7)

- Europäischer Gerichtshof
  Facebook Ireland und Schrems
  Vorlage zur Vorabentscheidung - Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten - Charta der Grundrechte der Europäischen Union - Art. 7, 8 und 47 - Verordnung (EU) 2016/679 - Art. 2 Abs. 2 - Anwendungsbereich - Übermittlungen personenbezogener Daten ...
- kanzlei.biz
  Privacy-Shield-Vereinbarung ungültig
- Betriebs-Berater
  Facebook vs. Schrems - Ungültigkeit des EU-US-Privacy-Shield-Abkommens
- WM Zeitschrift für Wirtschafts- und Bankrecht (Abodienst; oder: Einzelerwerb Volltext 12,79 €)
  Zur Frage der Zulässigkeit der Übermittlung personenbezogener Daten einer natürlichen Person

Kurzfassungen/Presse (16)

- Europäischer Gerichtshof (Pressemitteilung)
  Rechtsangleichung - Der Gerichtshof erklärt den Beschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig
- damm-legal.de (Kurzinformation)
  Privacy-Shield-Abkommen ist auf Grund von uferloser US-amerikanischer Überwachung unwirksam

20.11.2020

Ausschnitt aus betroffenen Diensten/ Programmen/ Services/ Unternehmen

- Analyse (Netz, Security, User)
- Chat
- Cloudspeicher
- Cloudservices
- CRM
- Collaboration
- E-Learning
- ERP
- Videokonferenz
- Virtualisierung

Sicheres Datenschutzniveau

D = EU-DSGVO und BDSG und LDSG
EU = EU-DSGVO
Sichere Drittländer z. B. durch Gesetzgebung mit angemessenen Betroffenenrechten (Art 45)
Unsichere Drittländer haben auf Grund fehlender oder nicht ausreichender Gesetze kein angemessenes Datenschutzniveau

2-stufige Prüfung bei Auslandstransfer

Artikel 44 Einhaltung der Bestimmungen des DS-GVO

Art. 45	Art. 47	Art. 46 (2) c und d	Art. 40 (3)	Art. 42	Art. 46 (3) a
Drittland bietet angemessenes Schutzniveau	Binding Corporate Rules	Standard-vertragsklauseln *Standard-datenschutzklauseln*	Genehmigte Verhaltensregeln	Genehmigte Zertifikate	Genehmigte individuelle Vertragsklauseln
	Art. 46 Geeignete Garantien sowie durchsetzbare Rechte und wirksame Rechtsbehelfe für den Betroffenen				

Privacy Shield

1. Stufe sicheres Datenschutzniveau im „Drittland“
    1. Sicheres Drittland
    2. Binding Corporate Rules
    3. Standardvertragsklauseln
    4. USA mit Privacy Shield (vormals Safe Harbour) als sicheres Drittland für bestimmte Unternehmen Art. 45 DSGVO

(nicht mehr anwendbar seit 10/2015)

2. Rechtmäßigkeit der Datenverarbeitung (Erlaubnisvorbehalt)

(nicht mehr anwendbar seit Juli /2020)

My Privacy is None of Your Business

#InvestInPrivacy

noyb

News Projekte Ressourcen Jetzt Unterstützen! Über uns DE

STARTSEITE > NEWS > 101 BESCHWERDEN ZU EU-US-TRANSFERS EINGEREICHT

101 Beschwerden zu EU-US-Transfers eingereicht

17 Aug 2020

Projekt

EU-US-Datenübertragungen

Unterstütze uns!

noyb Fundingziel

67 %

JETZT UNTERSTÜTZEN

Folge uns!

Nächste Schritte für EU-Unternehmen & FAQs

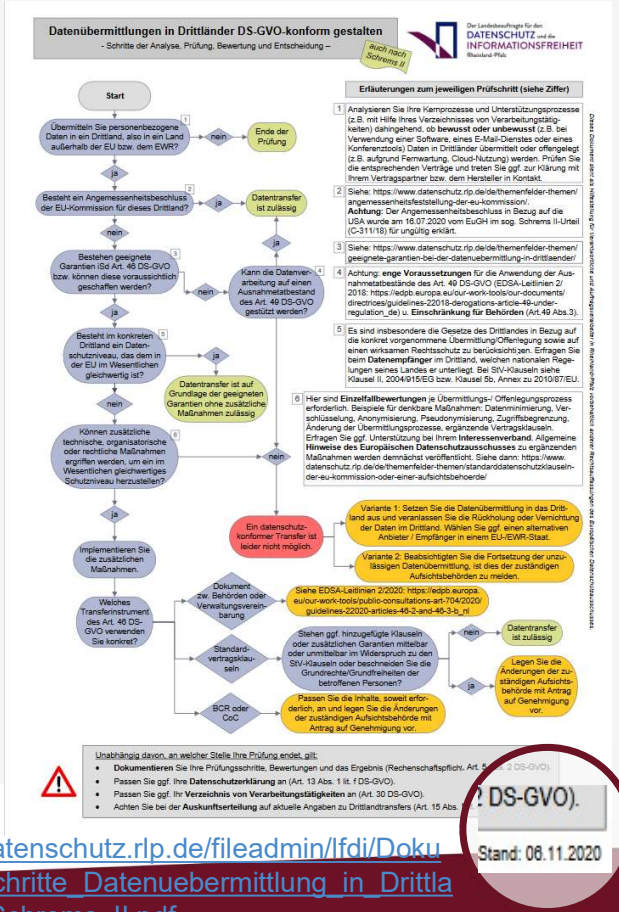
20 Jul 2020

Wir haben die nächsten Schritte nach dem EuGH-Urteil über EU-US-Datentransfers für EU-Unternehmen zusammengefasst und Musteranträge veröffentlicht, die Sie an Ihre Nicht-EU/EWR-Anbieter senden können.

Mehr lesen

3

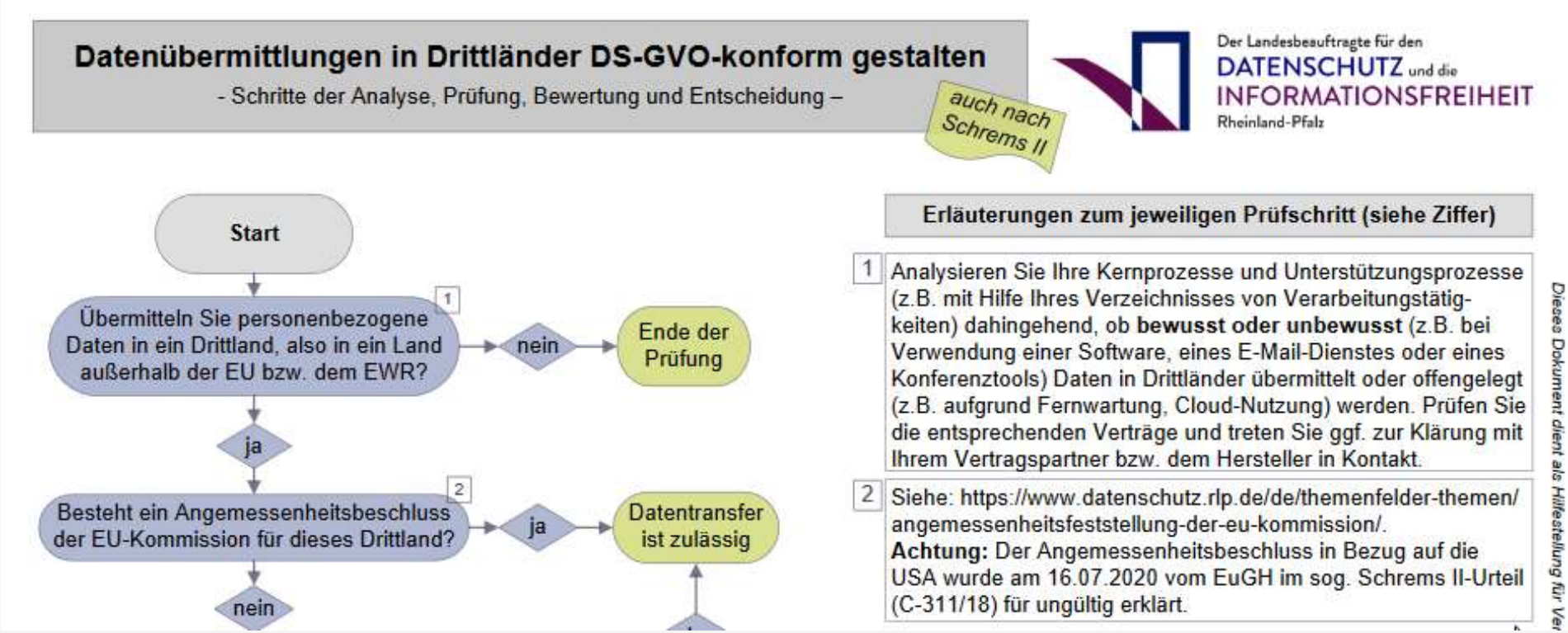
Empfehlungen für Verantwortliche



https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf

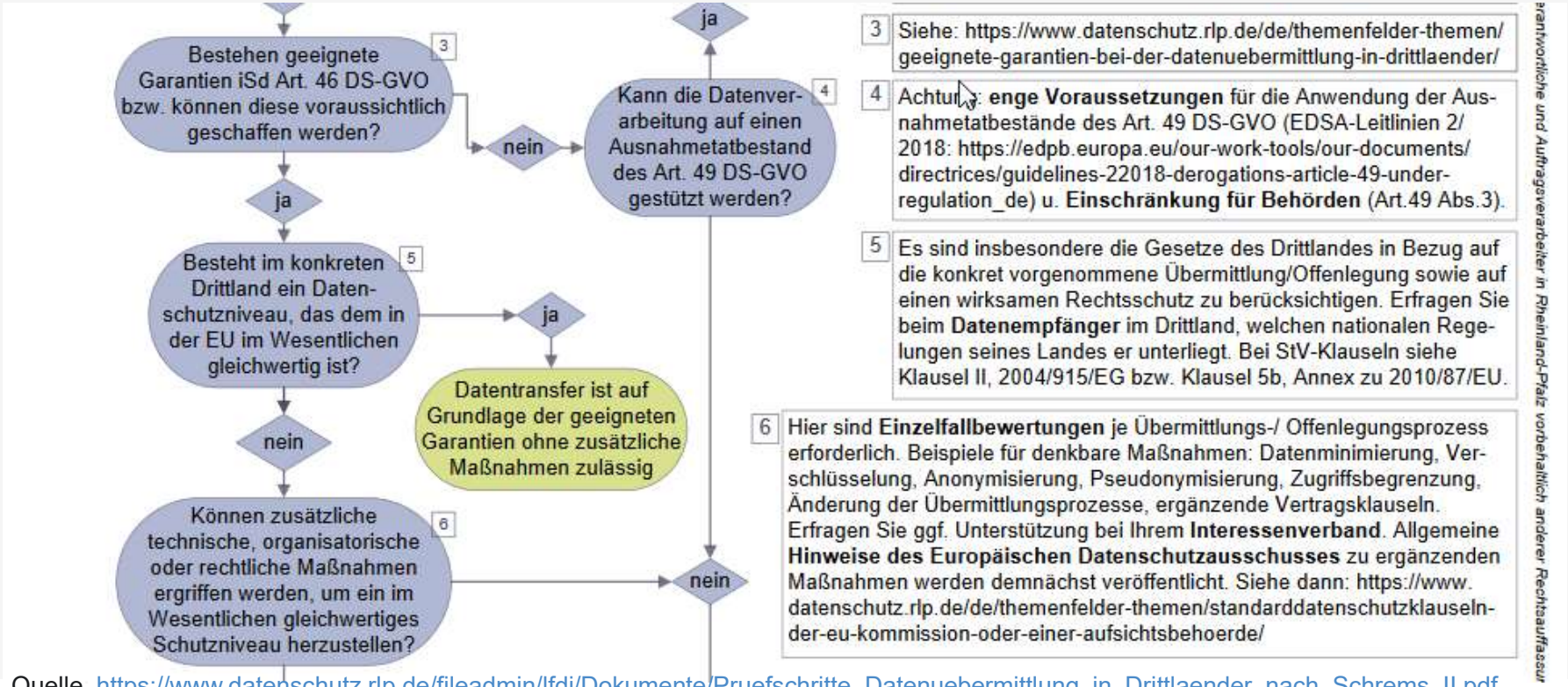
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Prüfschritte nach LDI-Rheinland-Pfalz (1)



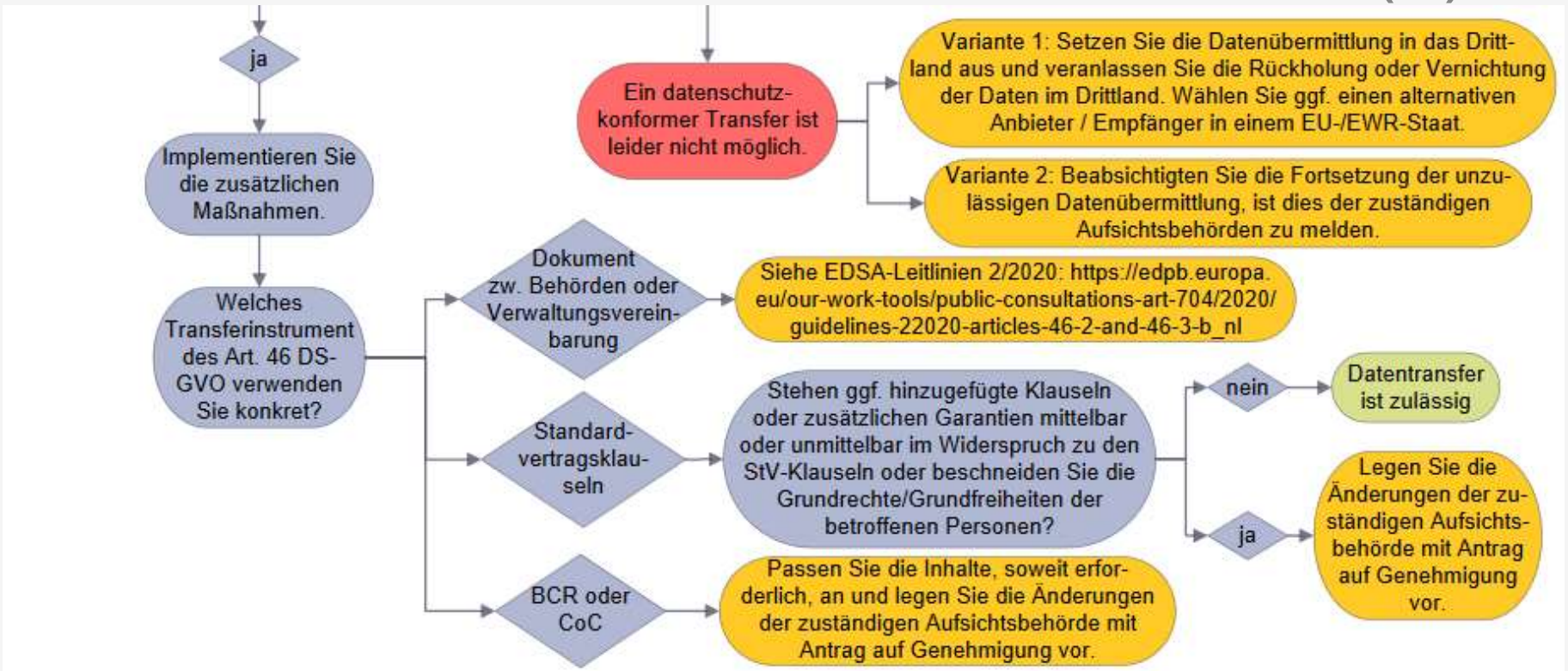
Quelle https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf

Prüfschritte nach LDI-Rheinland-Pfalz (2)



Quelle https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf

Prüfschritte nach LDI-Rheinland-Pfalz (3)



Quelle https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf

Empfehlungen des Europäischen Datenschutzausschusses (EDA)

Quelle: 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

Die sechs Empfehlungen/ Schritte des EDA

1. Ermitteln Sie alle Übermittlungen in Drittländer
2. Ermitteln Sie das jeweilige Rechtsmittel für das erforderliche Datenschutzniveau im jeweiligen Drittland
3. Ermitteln Sie mögliche Beeinträchtigungen des vereinbarten Datenschutzniveaus
4. Ermitteln und ergreifen Sie zusätzliche Maßnahmen zur Sicherung des Schutzniveaus
5. Dokumentieren Sie alle diesbezüglich durchgeführten Maßnahmen
6. Reviewen Sie regelmäßig, hinsichtlich Veränderungen

©https://pixabay.com/ peggy_marco

Quelle: 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

4. Ergreifen zusätzlicher Maßnahmen

- technisch
  - Anonymisierung und Pseudonymisierung
  - Verschlüsselung
- organisatorisch
  - Länge und Komplexität der Verarbeitung ändern
  - Verringerung der beteiligten Akteure
  - Bildung eines Expertenteams (IT-Security, Legal Counsel, DSB)
- vertraglich
  - Transparenz beim Verarbeiter im „unsicheren“ Drittland

Anwendungsfall 1:
Datenspeicherung für Backup- und andere Zwecke, die keinen Zugriff auf offene Daten benötigen

- Starke Verschlüsselung noch vor der Übermittlung
- Aktueller Stand der Technik
- Gilt auch für die geplante Speicherdauer
- Ordnungsgemäße Technik
- Korrekte Schlüsselverwaltung
- Schlüssel liegt beim Verantwortlichen im EWR/ sicheren Drittland

©https://pixabay.com/ peggy_marco

=> wirksame ergänzende Maßnahmen

Quelle: 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

Anwendungsfall 2:
Übertragung pseudonymisierter Daten

- Beim Empfänger
  - keiner bestimmten Person zuordenbar
  - Keine bestimmte Person identifizierbar
- Zusätzliche Informationen zur Repseudonymisierung sind
  - nur beim Exporteur,
  - in EWR oder sicherem Drittland
  - durch angemessene TOM gesichert
- Explizite Prüfung durch Exporteur, dass im Empfängerland keine Repseudonymisierung, auch unter Zuhilfenahme weiterer Informationen, ausgefeilter Technik oder hoher Rechenleistung möglich ist

=> wirksame ergänzende Maßnahmen

©https://pixabay.com/ peggy_marco

Quelle: 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

Anwendungsfall 6:
Übermittlung an einen Cloud-Dienstanbieter oder Verarbeiter, die zur Erbringung des Dienstes Zugriff auf die Daten benötigen

- Verantwortlicher übermittelt an Verarbeiter in „unsicherem“ Drittland
- Verarbeiter benötigt Zugriff auf die Daten
- Transportverschlüsselung ist im Einsatz
- Ruhedaten sind angemessen verschlüsselt

©https://pixabay.com/ peggy_marco

=> Keine ausreichend wirksamen ergänzenden Maßnahmen

Quelle: 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

Anwendungsfall 7:
Remotezugriff auf Daten für geschäftliche Zwecke

- Verantwortlicher stellt Daten Dritten in „unsicherem“ Drittland für gemeinsame Geschäftszwecke zur Verfügung:
  - Globale HR-Services für Unternehmensgruppe
  - Globales CRM-System
- Empfänger hat Direktzugriff auf die Daten
- Transportverschlüsselung ist im Einsatz
- Ruhedaten sind angemessen verschlüsselt

©https://pixabay.com/ peggy_marco

=> Keine ausreichend wirksamen ergänzenden Maßnahmen

Quelle: 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

Mögliche vertragliche Verpflichtungen eines Empfängers in einem unsicheren Drittland (1)

- Benennung der gesetzlichen Offenbarungspflichten im Drittland
- Statistische Zahlen zu bisherigen Offenbarungen im Drittland
- Zu ergreifende Maßnahmen zur Abwehr dieser Ansprüche
- Explizite Informationen zu allen eingehenden Offenbarungsverfahren
- Benennung unter welchen Voraussetzung er einer Verschwiegenheit hinsichtlich Offenbarungen an Behörden unterliegt

©https://pixabay.com/ peggy_marco

Quelle: 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

Mögliche vertragliche Verpflichtungen eines Empfängers in einem unsicheren Drittland (2)

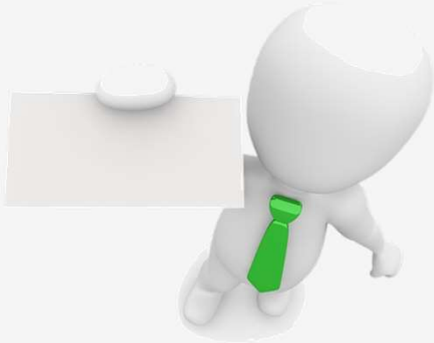
- Zusage über die Nichtexistenz von „Backdoors“
- Zusage darüber, dass Prozesse nicht dahingehend geändert werden um Dritten den Zugriff auf die Daten zu ermöglichen/ erleichtern
- Sanktions- und Sonderkündigungsrechte, wenn diese Zusagen nicht eingehalten werden

©https://pixabay.com/ peggy_marco

Quelle: 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

Mögliche vertragliche Verpflichtungen eines Empfängers in einem unsicheren Drittland (3)

- Vereinbarung von Audits durch Verantwortlichen oder beauftragte Dritte auf Einhaltung von TOM und getroffener Vereinbarungen
- Audits sind kurzfristig Ansetzbar
- Verantwortlicher entscheidet über zu prüfenden Ort, zu prüfendes System, etc.
- Voraussetzung sind entsprechende Logs, die die Feststellung solch eines Zugriffs/ solch eine Übermittlung ermöglichen



©https://pixabay.com/ peggy_marco

Quelle: 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

Mögliche vertragliche Verpflichtungen eines Empfängers in einem unsicheren Drittland (4)

- Regelmäßige Bestätigung des Importeurs (z. B. alle 24 Stunden), dass bislang keine Offenbarungspflichten gegenüber Behörden vorliegen. (Warrant Canary)
  - Digital signierte Nachricht
  - Darf nicht durch Gesetzgebung des „unsicheren“ Drittlandes ausgeschlossen sein

© www.pixabay.com iirliinnaa

Quelle: 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

Mögliche vertragliche Verpflichtungen eines Empfängers in einem unsicheren Drittland (5)

- Bei Erhalt einer Offenbarungsanordnung:
  - Prüfung auf Rechtskonformität
  - Nutzung aller Anfechtungs- und Widerspruchsmöglichkeiten
  - Erwirkung einer Aussetzung bei Anfechtung und Widerspruch
  - Befolgung der Anordnung nur wenn erforderlich
  - Beschränkung der Offenbarung auf erforderlichen Umfang

© https://pixabay.com/de/ mohamed_hassan

Quelle: 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

Mögliche vertragliche Verpflichtungen eines Empfängers in einem unsicheren Drittland (6)

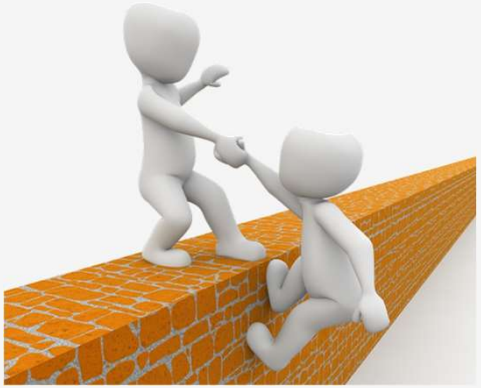
- Information der ersuchenden Behörde über Unvereinbarkeit der Offenbarung mit den vertraglichen Verpflichtungen.
- Zugleich Information des Verantwortlichen/ Exporteurs sowie der zuständigen Aufsichtsbehörde über die erhaltene Offenbarungsverpflichtung

©https://pixabay.com/ peggy_marco

Quelle: 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

Mögliche vertragliche Verpflichtungen eines Empfängers in einem unsicheren Drittland (7)

- Unverzügliche Information des Betroffenen über Offenbarungsanfragen
- Unterstützung des Betroffenen bei der Ausübung von (Schutz-)Rechten



©https://pixabay.com/ peggy_marco

Quelle: 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

Und schon umgesetzt.

New Steps to Defend Your Data

Nov 19, 2020 | Julie Brill - Corporate Vice President for Global Privacy and Regulatory Affairs and Chief Privacy Officer

With today's announcement, we are moving to be the first company to respond to the EDPB's guidance with new commitments that demonstrate the strength of our conviction to defend our customers' data. Microsoft has already demonstrated that we provide strong protections for our customers' data, we are transparent about our practices and we defend our customers' data. We believe the new steps we're announcing today go beyond the law and the EDPB draft recommendations, and we hope these additional steps will give our customers added confidence about their data.

- First, we are committing that we will challenge every government request for public sector or enterprise customer data – from any government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.
- Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure.

We call these protections Defending Your Data, and we will begin adding them to our contracts with public sector and enterprise customers immediately.

Defending Your Data makes a substantial addition to our foundational privacy promises, and builds on the strong protections we already offer customers.

- **We use strong encryption:** We encrypt customer data with a high standard of encryption both when it is in transit and at rest. Encryption is a critical point in the draft EDPB recommendations. We do not provide any government with our encryption keys or any other way to break our encryption.
- **We stand up for customer rights:** We do not provide any government with direct, unfettered access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with demands when we are clearly compelled to do so. Our first step is always to attempt to re-direct such orders to customers or to inform them, and we routinely deny or challenge orders when we believe they are not legal.
- **We are transparent**: We have, for many years, published information about government demands for customer data. We sued the U.S. government over the ability to disclose more data about the national security orders we receive seeking customer data and reached a settlement enabling us to do so. As a result, twice a year, we disclose more detailed information about these national security orders across all our businesses (consumer, enterprise, and public sector), in addition to our regular Law Enforcement Request Report.
- **We have a track record of legal success.** We have more experience than any other company going to court to establish the limits of government surveillance orders, and we have even taken one case to the U.S. Supreme Court. Our efforts have provided customers with greater transparency and stronger protections. No commitment to challenge access orders can assure victory, but we feel good about our record of success to date.

Quelle https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

©https://pixabay.com/ peggy_marco

VINTIN
make IT unique

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

VINTIN GmbH
Felix-Wankel-Straße 4
D-97526 Sennfeld

+49 (0) 9721 / 67594-10
info@vintin.de
Facebook | Twitter | Xing | LinkedIN | YouTube