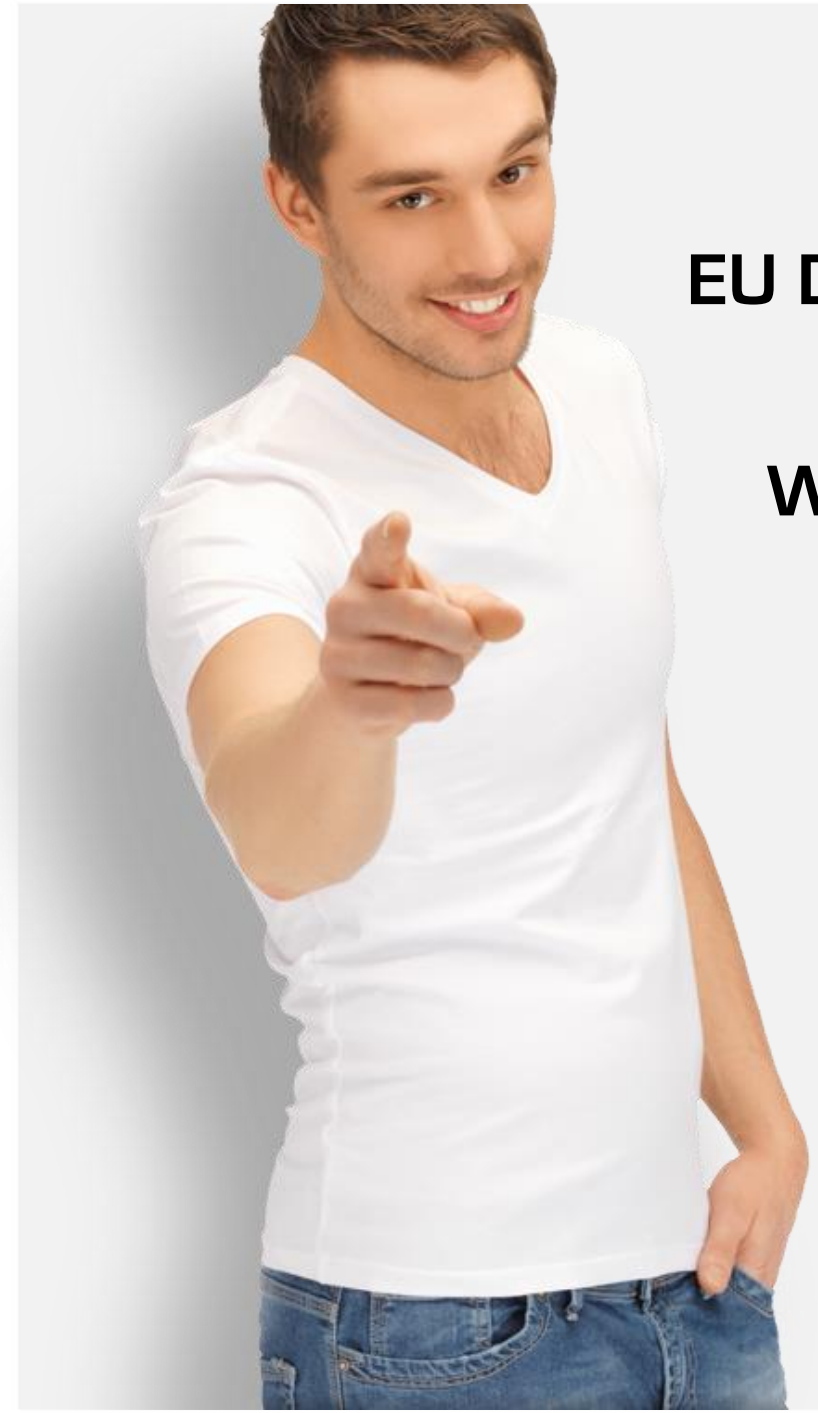


EU Datenschutzgrundverordnung (DSGVO)

Was bedeutet das für mich? Teil 2

Referent: Eric Drissler

Verantwortlicher & Auftragsverarbeiter:

Datenschutz-Folgeabschätzung - Art. 35 DSGVO

„hat eine **Form der Verarbeitung**, insbesondere bei **Verwendung neuer Technologien**, aufgrund der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der Verantwortliche **vorab eine Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden. … erforderlich für“

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen…
- …Verarbeitung besonderer Kategorien von personenbezogenen Daten…
- …Verarbeitung personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten…
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche → bspw. Kameraüberwachung

Verantwortlicher & Auftragsverarbeiter:

Datenschutz-Folgeabschätzung - Art. 35 DSGVO

Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Richtung ist bereits bekannt (noch nicht rechtsverbindlich):

- Daten zur Bewertung, zum Scoring oder zum Profiling, insbesondere in den Bereichen Arbeit, **wirtschaftliche Situation**, Gesundheit, persönliche Vorlieben und Interessen, **Bonität**, Verhaltensweisen, Aufenthaltsort; → Mieterselbstauskunft!
- Formen **automatisierter Entscheidungsfindung** mit rechtlichen Folgen; → Scoring, Vorabfilterung von Mietern
- Verarbeitung **sensibler Daten** wie beispielsweise Gesundheitsdaten;
- umfangreiche Verarbeitungsvorgänge;
- zusammengeführte oder kombinierte Datensätze;
- Daten **schutzbedürftiger Personen** wie Kindern, älteren Menschen, Patienten oder Mitarbeitern; → Beschäftigtendatenschutz

Verantwortlicher & Auftragsverarbeiter:

Datenschutz-Folgeabschätzung - Art. 35 DSGVO

- Nutzung neuer Technologien wie IoT-Entwicklungen;
- **Datentransfers außerhalb der EU**; → US Dienste wie Google bspw.
- **Datenverarbeitung kann dazu führen, dass ein Betroffener ein Recht nicht ausüben oder einen Vertrag nicht schließen kann** (bspw. Prüfung auf Kreditwürdigkeit); → Mieterselbstauskunft

Ähnlich der bisherigen Vorabkontrolle, wobei noch nicht klar ist ob die Pflicht sofort besteht oder erst wenn zwei Kriterien erfüllt sind → sicherer zunächst direkt ausführen!

Auch negative Bewertungen sind zu dokumentieren.

Verantwortlicher & Auftragsverarbeiter:

Datenschutz-Folgeabschätzung - Art. 35 DSGVO

Die Datenschutzfolgeabschätzung enthält zumindest Folgendes:

- eine **systematische Beschreibung der geplanten Verarbeitungsvorgänge** und der **Zwecke der Verarbeitung**, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten **berechtigten Interessen**;
- eine **Bewertung der Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine **Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen** gemäß Absatz 1 und
- die zur **Bewältigung der Risiken geplanten Abhilfemaßnahmen**, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Verantwortlicher & Auftragsverarbeiter:

Datenschutz-Folgeabschätzung - Art. 36 DSGVO

Zwingende Einbeziehung der Datenschutzaufsichtsbehörde

Verbleibt trotz Abhilfemaßnahmen bei einer Datenschutz-Folgenabschätzung ein hohes Risiko, dann ist eine vorherige Konsultation bei zuständiger Aufsichtsbehörde vorzunehmen	Aufsichtsbehörde wird prüfen, ob Verarbeitung mit Verordnung im Einklang steht, insbesondere wenn Risiko nicht ausreichend ermittelt wurde, schriftliche Empfehlungen unterbreiten oder Befugnisse nach	Reaktionszeit der Aufsichtsbehörde: innerhalb von 8 Wochen mit Verlängerungs-möglichkeit um weitere 6 Wochen bei Komplexität	bei Verstoß: Sanktionsrahmen bis 10 Mio. EUR bzw. die 2 % des Vorjahresumsatzes (je nachdem was höher ist)

Verantwortlicher & Auftragsverarbeiter:

Datenschutzbeauftragter - Art. 37 - 39 DSGVO, § 38 BDSG n. F.

- Bestellpflicht nach BDSG n.F.: „soweit sie in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“ → Personen, nicht mehr Beschäftigte!
- Sonderfälle direkte Bestellung: öffentliche Stellen / Behörden, bei Kerntätigkeit Überwachungsmaßnahmen, bei Kerntätigkeit besondere Kategorien von Daten oder pbD über strafrechtliche Verurteilungen und Straftaten
- **interner DSB und externer DSB weiterhin zulässig**
- **ab 25.05.2018** muss der **DSB der zuständigen Aufsichtsbehörde gemeldet werden** mit Kontaktdaten → erst dann
- nach wie vor darf es **keine Interessenskonflikte** geben

Verantwortlicher & Auftragsverarbeiter:

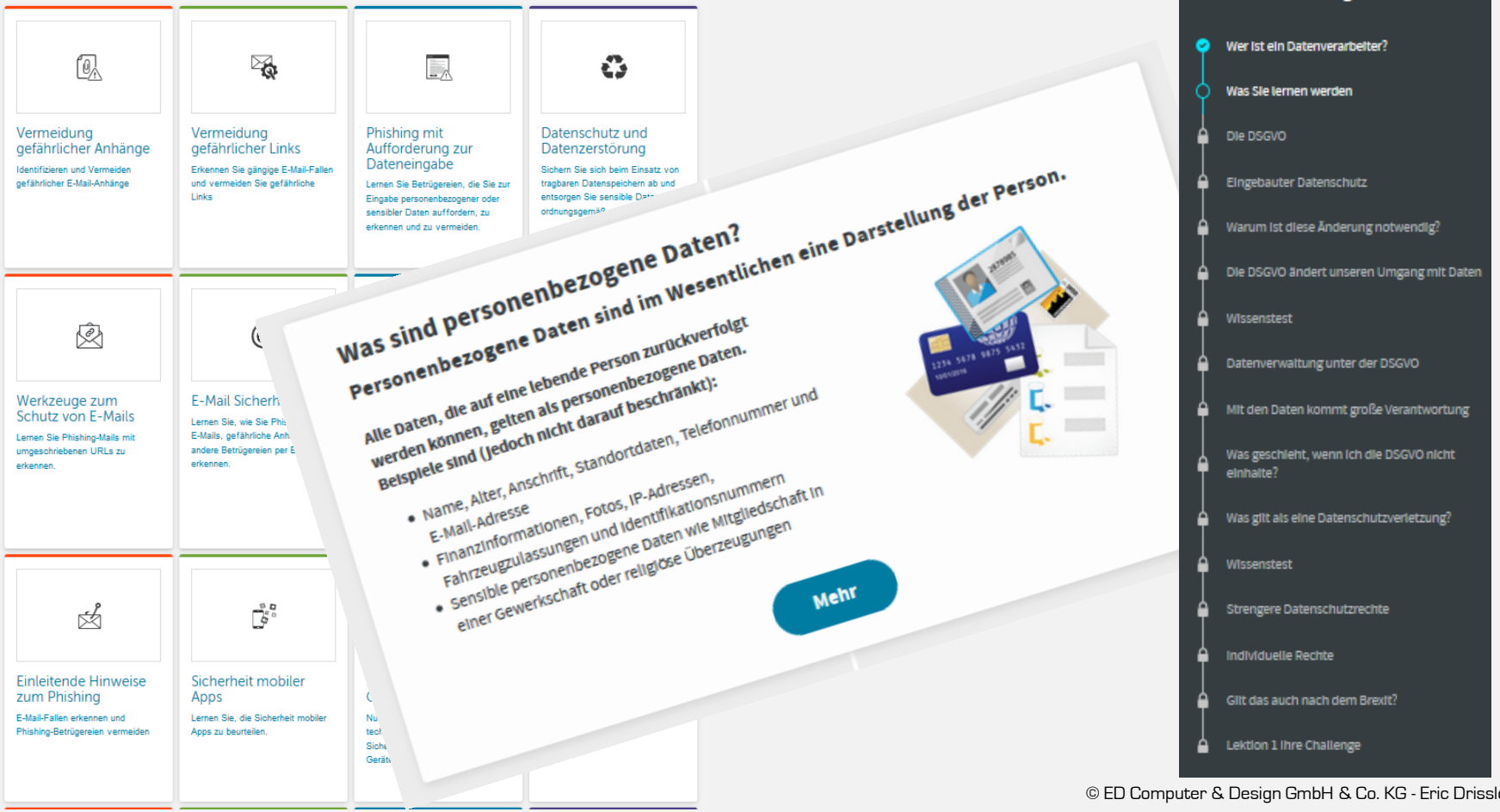
Datenschutzbeauftragter - Art. 37 - 39 DSGVO, § 38 BDSG n. F.

- **Unterrichtung und Beratung** des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten … **hinsichtlich ihrer Pflichten** nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften
- **Überwachung der Einhaltung** dieser Verordnung, anderer Datenschutzvorschriften … sowie der **Strategien** des Verantwortlichen oder des Auftragsverarbeiters für den **Schutz personenbezogener Daten** einschließlich der **Zuweisung von Zuständigkeiten**, der **Sensibilisierung und Schulung** der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen **Überprüfungen**
- **Beratung** – auf Anfrage – im Zusammenhang mit der **Datenschutz-Folgenabschätzung** und **Überwachung ihrer Durchführung**
- **Zusammenarbeit mit der Aufsichtsbehörde**
- Tätigkeit als **Anlaufstelle für die Aufsichtsbehörde**

Verantwortlicher & Auftragsverarbeiter:

Datenschutzbeauftragter - Art. 37 - 39 DSGVO, § 38 BDSG n. F.

Tipp für Sensibilisierung, Schulung und Überprüfung: zusätzlich zu Präsenzschulungen mit Ihrem DSB bieten sich Trainingsplattformen mit Maßnahmen und Fragen zum Nachweis an → meist schon so für 50 € pro User/Jahr möglich



Verantwortlicher & Auftragsverarbeiter:

Zertifizierung - Art. 42 DSGVO

- Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von **datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen**, **die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird**. Den **besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen**.
- Die **Zertifizierung** muss **freiwillig** und über ein **transparentes Verfahren** zugänglich sein.
- Eine **Zertifizierung** gemäß diesem Artikel **mindert nicht** die **Verantwortung** des Verantwortlichen oder des Auftragsverarbeiters für die **Einhaltung dieser Verordnung** und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden ....
- Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von **drei Jahren** erteilt und kann unter **denselben Bedingungen verlängert werden**, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

„unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der Art, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete **technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Das heißt Sie müssen die Maßnahmen nicht nur dokumentieren, sondern Eintrittswahrscheinlichkeit und Schwere des Risikos bewerten vgl. Risikoanalyse

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

„Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob **unbeabsichtigt** oder **unrechtmäßig**, oder **unbefugte Offenlegung** von beziehungsweise **unbefugten Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.“

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

Technische und organisatorische Maßnahmen (TOM) gemäß §9 BDSG alt,

- Zutrittskontrolle → physikalischer Zutritt in Büros, Serverräume etc.
- Zugangskontrolle → logischer Zugang zu den EDV-Systemen, mit dem personenbezogene Daten verarbeitet werden
- Zugriffskontrolle → Zugriff auf personenbezogene Daten
- Weitergabekontrolle → Weitergabe von personenbezogenen Daten
- Eingabekontrolle → Eingabe, Veränderung oder Entfernung personenbezogener Daten
- Auftragskontrolle → Verarbeitung durch einen Dritten im Auftrag
- Verfügbarkeitskontrolle → Schutz vor Verlust und Zerstörung
- Trennungskontrolle → Zweckbindung der Datenverarbeitung

Tipp: gut beschreiben beschrieben auch in Teil 3 §64 BDSG neu (der eigentlich nur für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen gilt)

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

„der **Verantwortliche** und der Auftragsverarbeiter **unternehmen Schritte**, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu **personenbezogenen Daten** haben, diese **nur auf Anweisung des Verantwortlichen verarbeiten** ..“

Übermittlung pbD an Drittländer oder int. Organisationen:

Grundsätze - Art. 44 DSGVO

Jedwede **Übermittlung personenbezogener Daten**, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein **Drittland** oder eine **internationale Organisation** verarbeitet werden sollen, ist **nur zulässig**, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem **Kapitel (Art. 44 bis Art. 50) niedergelegten Bedingungen einhalten** und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

- **Sicherer Drittstaaat** mit **Angemessenheit des gebotenen Schutzniveaus**
- **Standarddatenschutzklauseln**, die von der **Kommission** .... erlassen werden (EU Standartvertragsklauseln)
- von einer **Aufsichtsbehörde** angenommenen **Standarddatenschutzklauseln** (Corporate Binding Rules)

Rechtsbehelfe, Haftung und Sanktionen:

Haftung und Recht auf Schadenersatz - Art. 82 DSGVO

Jede Person, der wegen eines **Verstoßes gegen diese Verordnung** ein **materieller** oder **immaterieller Schaden** entstanden ist, hat **Anspruch auf Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Rechtsbehelfe, Haftung und Sanktionen:

Sanktionen - Art. 83 & 84 DSGVO

Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen ... in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Beachtet werden:

- **Art, Schwere und Dauer** des Verstoßes sowie **Ausmaß**;
- **Vorsätzlichkeit oder Fahrlässigkeit** des Verstoßes
- jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter **getroffenen Maßnahmen** zur Minderung des den betroffenen Personen entstandenen Schadens;
- Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen ... **getroffenen technischen und organisatorischen Maßnahmen**;
- etwaige einschlägige **frühere Verstöße** des Verantwortlichen oder des Auftragsverarbeiters;
- Umfang der **Zusammenarbeit mit der Aufsichtsbehörde**, ...
- **Kategorien personenbezogener Daten**, die von dem Verstoß betroffen sind;
- **Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde**, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
- .....

Rechtsbehelfe, Haftung und Sanktionen:

Sanktionen - Art. 83 & 84 DSGVO

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu **10 Mio. EUR** oder im Fall eines Unternehmens von bis **zu 2** % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
- ....

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu **20 Mio. EUR** oder im Fall eines Unternehmens von bis zu **4** % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
- die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
- die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
- ....

Rechtsbehelfe, Haftung und Sanktionen:

Strafvorschriften - § 42 BDSG n. F.

Mit **Freiheitsstrafe bis zu drei Jahren** oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

- einem Dritten übermittelt oder
- auf andere Art und Weise zugänglich macht → Konzern/Unternehmensgruppenzugriffe ohne Regelung

und hierbei gewerbsmäßig handelt.

Mit **Freiheitsstrafe bis zu zwei Jahren** oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

- ohne hierzu berechtigt zu sein, verarbeitet oder
- durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Zusammenfassung?

- Kümmern Sie sich um Ihre Verpflichtungserklärungen
- Erstellen Sie das Verzeichnis der Verarbeitungstätigkeiten
- denken Sie an die Informationspflichten
- neue Verarbeitungsvorgänge? Prüfen ob eine Datenschutzfolgeabschätzung erforderlich ist; Ergänzung des Verzeichnis der Verarbeitungstätigkeiten;
- direkte Prüfung von Privacy by Design und Default
- Erstellen Sie Policies und Richtlinien
- Beachten Sie die Meldepflicht
- Bestellen Sie Ihren DSB wenn erforderlich und melden diesen nach 25.05.2018 der zuständigen Datenschutzaufsichtsbehörde
- Überprüfen Sie Ihre bestehenden Auftragsdatenverarbeitungsverträge und überführen Sie diese zu Auftragsverarbeitungsverträge
- Sorgen Sie für ausreichende Sicherheit der Verarbeitung und dokumentieren diese

Fragen?

Hilfe und Unterstützung?

Webinare zu einzelnen Fachthemen:

https://immobilienprofi.edudip.com/academy/eric.drissler

alle Workshops / Seminare / Webinare:

https://www.edcud.de/EDdatenschutz-Schulungen

Beratung, Datenschutz-Audit, Mitarbeiter Schulungen, externer DSB:

ED Computer & Design GmbH & Co. KG

Lina-Bommer-Weg 4

51149 Köln

Telefon +49 (0) 221 28 88 77 66

Telefax +49 (0) 221 28 88 77 67

E-Mail datenschutz@edcud.de Internet www.edcud.de