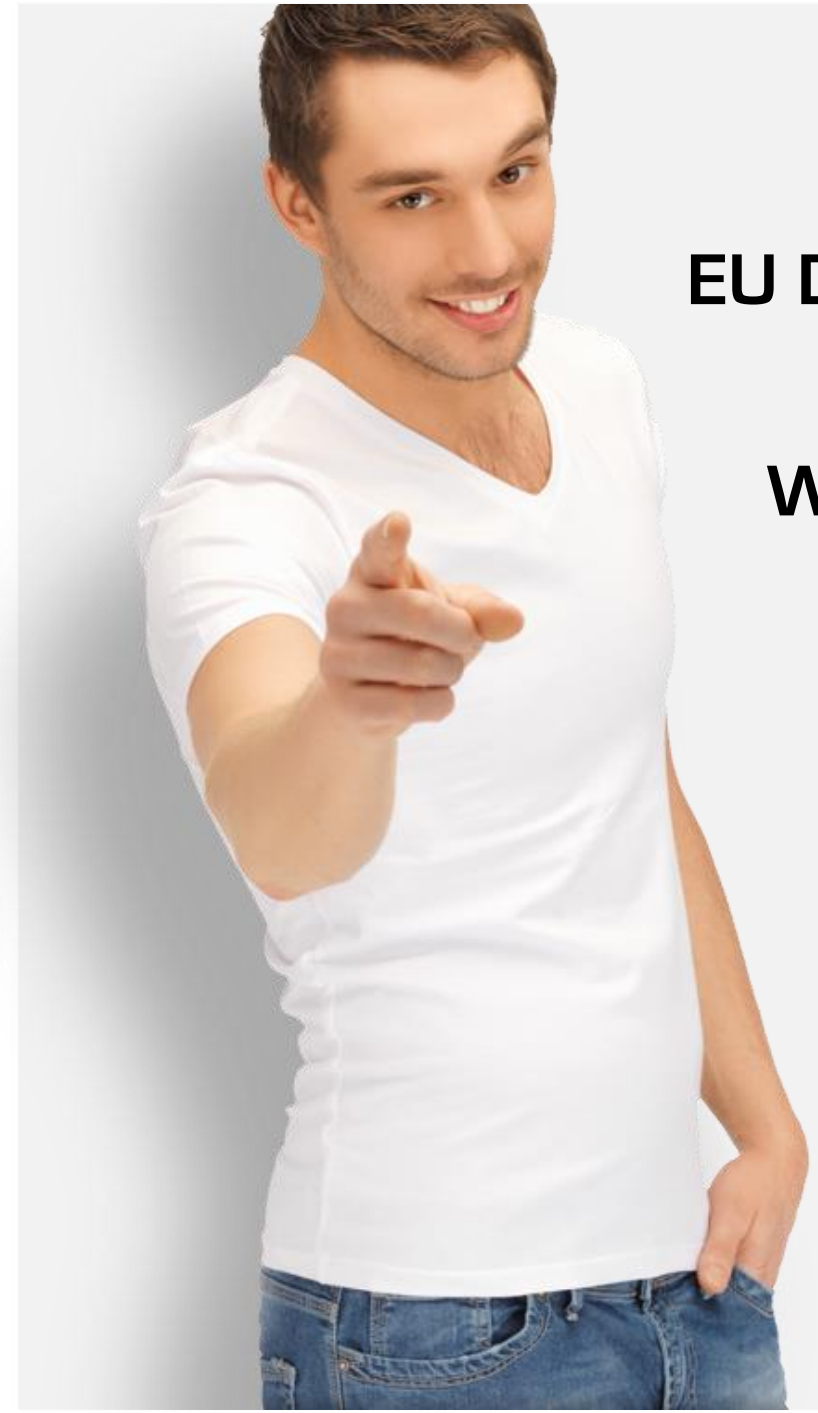

EU Datenschutzgrundverordnung (DSGVO)

Was bedeutet das für mich? Teil 1

Referent: Eric Drissler

Wer ist ED Computer & Design?

- 1998 gegründet
- herstellerneutrales bundesweites IT-Dienstleistungsunternehmen (Systemhaus)
- Unternehmenssitz: Köln
- Geschäftsbereiche:
  - EDit ➔ IT-Consulting, Hard- und Software, Netzwerke, Security
  - EDcom ➔ ITK-Consulting, Telekommunikation, Unified Communication, SoundSolution
  - EDmoiis ➔ EDmoiis immo, EDmoiis crm
  - EDweb ➔ Webentwicklungen, Webdesign, Webhosting
  - EDdesign ➔ Designkonzepte, Grafikdesign für Digital und Print
  - EDdatenschutz ➔ Stellung eDSB, Datenschutz-Audits, Schulungen
- Mitarbeiter: 12+1
- Ausbildungsbetrieb für IT-Systemkaufleute & Fachinformatiker
- seit 2001 mit Schwerpunkt in der Immobilienwirtschaft
- Partnerschaft mit allen IVD-Regionalverbänden

Allianz für Cyber-Sicherheit

Über mich

- Ausbildung in der Informationstechnik
- ITIL V2 Foundation Certificate 2008
- ITIL V3 Foundation Bridge Certificate 2009
- Datenschutzbeauftragter (TÜV)
- Datenschutzmanager (TÜV)
- externer Datenschutzbeauftragter (TÜV)
- Datenschutzauditor (TÜV)
- Extern bestellter Datenschutzbeauftragter für div. Mandaten
- Prozessbeteiligt bei der Zertifizierung gemäß ISO 27001 bei einem Hoster

EU DSGVO

- EU Datenschutzgrundverordnung (DSGVO), ist eine Verordnung damit verbindlich in allen Mitgliedsstaaten der EU und muss nicht in nationales Recht umgesetzt werden
- es gibt 99 Artikel, die Hintergründe werden in 173 Erwägungsgründen beschrieben
- Teilweise sind sogenannte „Öffnungsklauseln“ enthalten, so dass die nationalen Staaten dies eigenständig regeln bzw. ergänzen können – in Deutschland ist das BDSG n. F.
- BDSG n.F. mit weiteren 84 Paragraphen → Teil 2 + Teil 3 für nicht öffentliche Stellen

- Stichtag ist der 25. Mai 2018, ohne Übergangsfrist
- bereits jetzt nach EU DSGVO ausrichten ist zulässig

Räumliche Anwendung

- Sitzlandprinzip
- Marktortprinzip → Unternehmen müssen nicht mehr in der EU einen Sitz haben, damit die Verordnung greift
- Beobachten des Verhaltens innerhalb der EU bzw. betroffene der EU
- ob entgeltlich oder unentgeltlich ist unerheblich

Grundsätze:

Grundsätze für die Verarbeitung personenbezogener Daten - Art. 5 DSGVO

- **rechtmäßige Weise**, nach **Treu und Glauben** und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden → Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und **dürfen nicht** in einer mit diesen Zwecken **nicht zu vereinbarenden Weise weiterverarbeitet werden** ....
- dem **Zweck angemessen** und erheblich sowie auf das für die Zwecke der Verarbeitung **notwendige Maß beschränkt** → Datenminimierung
- **sachlich richtig** und erforderlichenfalls auf dem **neuesten Stand** sein... → Richtigkeit
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen **nur so lange ermöglicht**, wie es **für** die Zwecke, für die sie **verarbeitet werden, erforderlich ist**... → Speicherbegrenzung
- in einer Weise verarbeitet werden, die eine **angemessene Sicherheit**... gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und **vor unbeabsichtigtem Verlust**, **unbeabsichtigter Zerstörung** oder **unbeabsichtigter Schädigung** ... → Integrität und Vertraulichkeit

Grundsätze:

Rechtmäßigkeit der Datenverarbeitung - Art. 6 DSGVO

„Die **Verarbeitung** ist **nur rechtmäßig**, wenn **mindestens eine** der nachstehenden **Bedingungen erfüllt** ist: “

- die betroffene Person hat ihre Einwilligung zu der Verarbeitung … gegeben
- die Verarbeitung ist für die Erfüllung eines Vertrags, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen → Exposeanfragen, Kaufvertrag usw.
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt → bspw. Geldwäschegesetz
- .....

Grundsätze:

Einwilligung - Art. 7 DSGVO

„**Beruht** die **Verarbeitung auf** einer **Einwilligung**, muss der Verantwortliche **nachweisen können**, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten **eingewilligt hat**. “

- in verständlicher und leicht zugänglicher
- in einer klaren und einfachen Sprache
- betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen → bis dahin bleibt erhalten; Widerruf muss gleich einfach wie die Einwilligung sein

Grundsätze:

Verarbeitung besonderer Kategorien von personenbezogenen Daten - Art. 9 DSGVO

Strenge Vorgaben und der Umgang mit dieser Art von Daten:

- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- die Gewerkschaftszugehörigkeit
- genetischen Daten zur eindeutigen Identifizierung einer natürlichen Person
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Rechte der betroffenen Person:

Transparenz und Informationspflichten - Art. 13 DSGVO

„Werden **personenbezogene Daten** bei der betroffenen Person erhoben, so **teilt der Verantwortliche** der betroffenen Person **zum Zeitpunkt der Erhebung** dieser Daten Folgendes **mit**: “

- Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission .....

und weitere ....

Rechte der betroffenen Person:

Auskunftsrechte - Art. 15 DSGVO

„Die **betroffene Person** hat das **Recht**, von dem Verantwortlichen eine **Bestätigung darüber zu verlang**en, ob sie betreffende **personenbezogene Daten verarbeitet werden**; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf folgende Informationen: “

- Verarbeitungszwecke
- Kategorien personenbezogener Daten
- Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen
- Aufbewahrungsdauer bzw. Kriterien für die Festlegung dieser Dauer
- das Bestehen eines Rechts auf Berichtigung oder Löschung … Widerspruchsrecht
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling …

Ergo müssen die Daten sauber erfasst werden inkl. Übermittlungsziele

Rechte der betroffenen Person:

Rechte zur Berichtigung - Art. 16 DSGVO

„Die **betroffene Person** hat das **Recht**, von dem Verantwortlichen **unverzüglich** die **Berichtigung** sie betreffender **unrichtiger personenbezogener Daten zu verlangen**. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. “

Rechte der betroffenen Person:

Rechte auf Vergessenwerden = Löschen - Art. 17 DSGVO

„Die **betroffene Person** hat das **Recht**, von dem Verantwortlichen zu verlangen, dass sie betreffende **personenbezogene Daten unverzüglich gelöscht** werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten **unverzüglich zu löschen**, sofern einer der folgenden Gründe zutrifft: ....“

- personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig
- ...betroffene Person widerruft ihre Einwilligung ... und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung ....
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft ... erhoben.

Ausnahme besteht, wenn eine Aufbewahrungspflicht entgegen steht!

Rechte der betroffenen Person:

Rechte auf Datenübertragbarkeit - Art. 20 DSGVO

„Die **betroffene Person** hat das **Recht**, die **sie betreffenden personenbezogenen Daten**, die sie einem Verantwortlichen bereitgestellt hat, in einem **strukturierten, gängigen und maschinenlesbaren Format zu erhalten**, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln....“

Beispiele:

- vollständige Übertragung von Unterlagen von Makler zu Makler
- vollständige Übertragung von WEG zu WEG Verwaltung

Technisch jedoch noch nicht definiert und nicht einfach realisierbar!

Verantwortlicher & Auftragsverarbeiter:

Privacy by Design - Art. 25 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** der mit der Verarbeitung **verbundenen Risiken** für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl **zum Zeitpunkt der Festlegung** der Mittel für die Verarbeitung als auch zum **Zeitpunkt der eigentlichen Verarbeitung** geeignete **technische und organisatorische Maßnahmen**....“

Beispiele:

- HTTPS Verschlüsslung auf Webseite
- minimale Pflichtfelder; Selbstauskunft reduziert

Verantwortlicher & Auftragsverarbeiter:

Privacy by Default - Art. 25 DSGVO

„Der Verantwortliche trifft **geeignete technische und organisatorische Maßnahmen**, die sicherstellen, dass **durch Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck **erforderlich ist**, verarbeitet werden....“

Beispiele:

- Haken muss bewusst gesetzt werden

Verantwortlicher & Auftragsverarbeiter:

Auftragsverarbeiter - Art. 28 DSGVO

- ersetzt die Auftragsdatenverarbeitung
- „legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche**. Sie legen in einer Vereinbarung in **transparenter Form** fest, **wer** von ihnen **welche Verpflichtung** gemäß dieser Verordnung erfüllt, insbesondere was **die Wahrnehmung der Rechte** der betroffenen Person angeht, und **wer welchen Informationspflichten ...**nachkommt..“
- Haftung endlich beidseitig – bisher nur Auftraggeber!

Verantwortlicher & Auftragsverarbeiter:

Auftragsverarbeiter - Art. 28 DSGVO

Grundsatz der Privilegierung bleibt erhalten, **Auftragsverarbeiter ist kein Dritter**

Verantwortlicher nach wie vor für die Verarbeitung **bleibt verantwortlich**

- Pflichtinhalte bei der Beauftragung
- Angemessenheit der Schutzmaßnahmen
- Nachweis der ausreichenden Schutzmaßnahmen, auch über Verhaltensregeln oder Zertifizierung möglich
- Einbindung von Subunternehmern formalisierter geregelt

Was ändert sich?

- **geänderte inhaltliche Anforderungen an Vereinbarung**
- **gemeinsame Haftung** nach Art. 28 des Auftraggebers und des Auftragnehmers

Das heißt es besteht ein zwingender Überprüfungsbedarf bestehender Auftragsdatenverarbeitungsverträge.

Verantwortlicher & Auftragsverarbeiter:

Verzeichnis der Verarbeitungstätigkeiten - Art. 30 DSGVO

„Jeder **Verantwortliche** und gegebenenfalls sein Vertreter führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben..:“

- Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation ....
- vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Verantwortlicher & Auftragsverarbeiter:

Verzeichnis der Verarbeitungstätigkeiten - Art. 30 DSGVO

Liste der üblichen Verfahren in der Immobilienwirtschaft (nicht abschließend):

- Rekrutierung von Mitarbeitern, Auszubildenden und Praktikanten
- Durchführung eines Arbeitsverhältnisses oder Ausbildungsverhältnisses
- Nachweis und/oder Vermittlung des Abschluss eines Mietvertrags
- Nachweis und/oder Vermittlung des Abschluss eines Kaufvertrags
- Nachweis und/oder Vermittlung des Abschluss eines Kaufvertrags im Rahmen eines Gemeinschafts- oder Tippgeschäfts
- Verwaltung von Mieteinheiten
- Verwaltung des gemeinschaftlichen Eigentums (WEG-Verwaltung)
- Bewertung von bebauten und unbebauten Grundstücken
- Verwaltung der Kontaktdaten von Lieferanten und Dienstleistern zur Beauftragung von Leistungen

Das bisherige öffentliche Verfahrensverzeichnis entfällt, dafür müssen fast alle Bestandteile im Rahmen der Informationspflichten vor Erhebung an den Betroffenen gegeben werden, damit noch transparenter!

Tipp: Je Verarbeitungstätigkeit ein einzelnes Dokument, alle zusammen bilden das Verzeichnis

Verantwortlicher & Auftragsverarbeiter:

Verzeichnis der Verarbeitungstätigkeiten - Art. 30 DSGVO

Aufbau und Inhalt des Templates

- **Namen und Kontaktdaten des Verantwortlichen** und gegebenenfalls des **gemeinsam mit ihm Verantwortlichen**, des Vertreters des Verantwortlichen sowie eines etwaigen **Datenschutzbeauftragten**
- **Zweck der Verarbeitung**
- Beschreibung der **Kategorien betroffener Personen** und der **Kategorien personenbezogener Daten**
- **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich **Empfänger in Drittländern oder internationalen Organisationen**
- **Übermittlungen** von personenbezogenen Daten **an ein Drittland** oder an **eine internationale Organisation**, einschließlich der Angabe des **betreffenden Drittlands** oder der betreffenden **internationalen Organisation**, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- vorgesehene **Fristen für die Löschung** der verschiedenen Datenkategorien
- allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen** gemäß Artikel 32 Absatz 1

Verantwortlicher & Auftragsverarbeiter:

Verzeichnis der Verarbeitungstätigkeiten - Art. 30 DSGVO

Verzeichnis von Verarbeitungstätigkeiten

Artikel 30 DSGVO

Name der Verarbeitungstätigkeit: <Tätigkeit>

Stand: <Datum>

betrachtet am: <Datum>

Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	Verantwortlicher: <Firmenname> Vertreten durch die Geschäftsführer: <Namen der vertretungsberechtigten Organe (Geschäftsführer)> <Geschäftsadresse> <Telefonnummer> <E-Mail> Gemeinsam verantwortliche Auftragsverarbeiter (Partnerunternehmen, z.B. ISTA, Freiberufler...): <Firmenname> Vertreten durch die Geschäftsführer: <Namen der vertretungsberechtigten Organe (Geschäftsführer)> <Geschäftsadresse> <Telefonnummer> <E-Mail> <Teilleistung> Datenschutzbeauftragter: <Name> <Geschäftsadresse> <Telefonnummer> <E-Mail>
Zweck der Verarbeitung	<Zweck>
Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	<Auflistung: welche Personengruppen sind betroffen> <pro Personengruppe: welche personenbezogenen Daten werden erhoben?>
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen	<Auflistung: wer erhält personenbezogene Daten?> <pro Empfänger: welche personenbezogenen Daten von wem erhält er?> <Drittland: In der Regel kein Drittland, keine internationale Weitergabe, es sei denn, der <entsprechende Personengruppe> befindet sich in einem solchen>
Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien	<Drittland: In der Regel kein Drittland, keine internationale Weitergabe, es sei denn, der <entsprechende Personengruppe> befindet sich in einem solchen>
vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien	<Fristen der Löschung> Sonst: nach Entfall der Notwendigkeit und gesetzlichen Aufbewahrungsfrist
allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.	TOMs sind als Anlage beigefügt (für jeden Betrieb eigene TOMs |beinhaltet Zutritt, Zugang, Zugriff, Eingabekontrolle, Weitergabekontrolle, Verfügbarkeitskontrolle, Auftragskontrolle, Trennungsgebot)

Hinweis: Aus Gründen verbesserter Lesbarkeit wurde in der Regel die männliche Schreibweise verwendet. Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sowohl die männliche, als auch die weibliche Schreibweise gemeint sind.

Verantwortlicher & Auftragsverarbeiter:

Meldepflicht bei Datenschutzverletzungen - Art. 33 DSGVO

„im Falle einer **Verletzung des Schutzes personenbezogener Daten** meldet der Verantwortliche **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, **es sei denn**, dass die **Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten** natürlicher Personen führt…“

- Beschreibung der Art der Verletzung
- Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen bzw. Datensätze
- Namen und die Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten

  ….

Fragen?

weiter geht's mit
Teil 2
um 12:00 Uhr