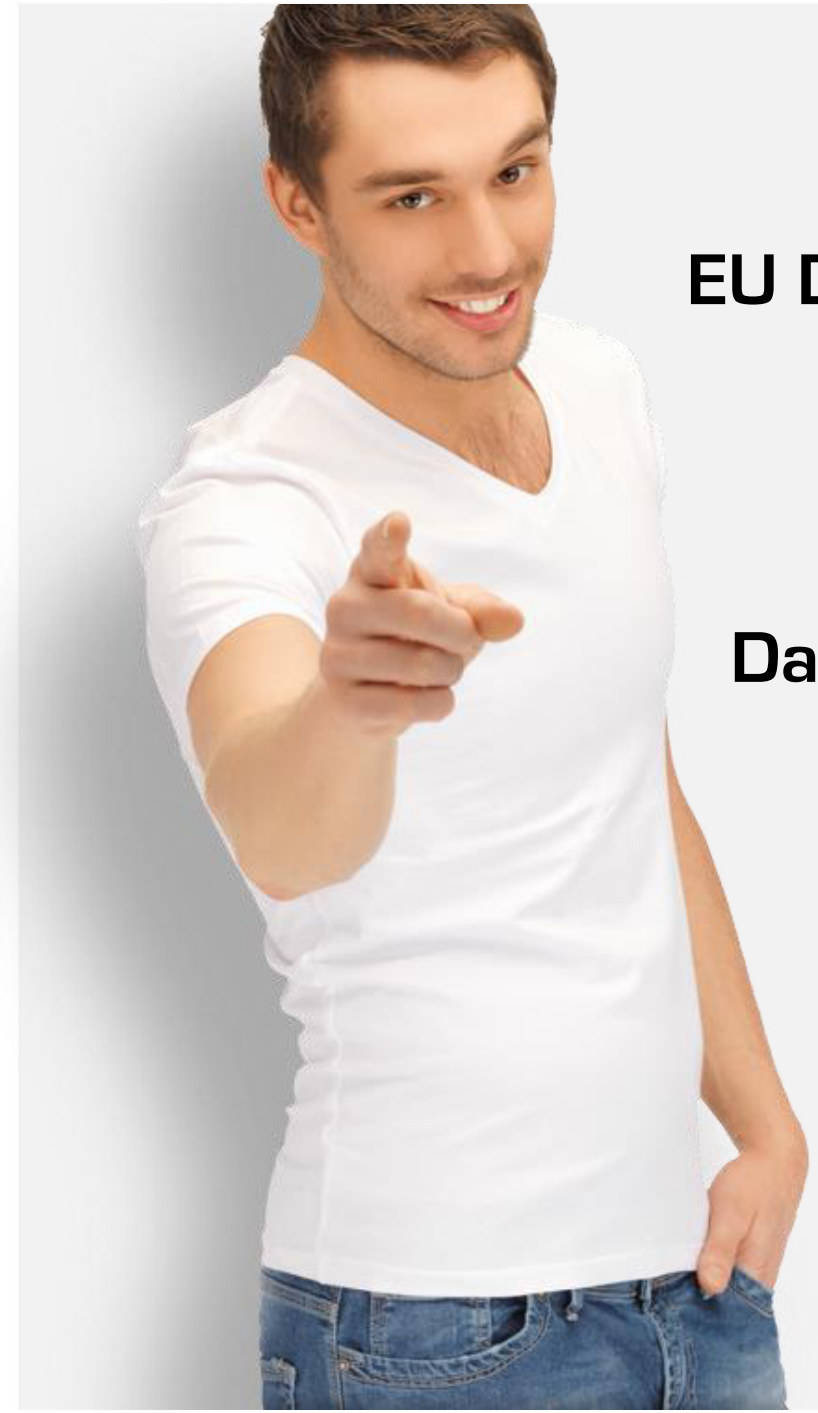


EU Datenschutzgrundverordnung (DSGVO)

Workshop Teil:

Auftragsverarbeitung, Datenschutzfolgeabschätzung, Policies und mehr

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

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,** sozusagen die „verlängerte Werkbank des Maklers“

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:

Auftragsverarbeiter - Art. 28 DSGVO

Wer sind Auftragsverarbeiter klassisch in der Immobilienwirtschaft?

- Lohn & Gehaltsabrechner
- online Maklersoftwareanbieter
- 360 Grad Tour Anbieter
- Aktenvernichter
- IT-Dienstleister
- Webhoster (zumindest bei shared Systemen)
- Heizkostenabrechner
- ....

Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

[Stand: Mai 2017]

Vereinbarung

zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

.....]

Hinweis

„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.“

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/..... vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ..... (Definition der Aufgaben)

(2) Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom .....

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: .....

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in ……..

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: ……. (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)

- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ ...

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung

einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
   - ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
   - ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
   - ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen

Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

c) ☐ Die Auslagerung auf Unterauftragnehmer oder

☐ der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer

- ☐ ist nicht gestattet;
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

.....	.....
Ort / Datum	Ort / Datum
.....	.....
Unterschrift vom Auftraggeber	Unterschrift vom Auftragnehmer

Anlage – Technisch-organisatorische Maßnahmen des Auftragsverarbeiters

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

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

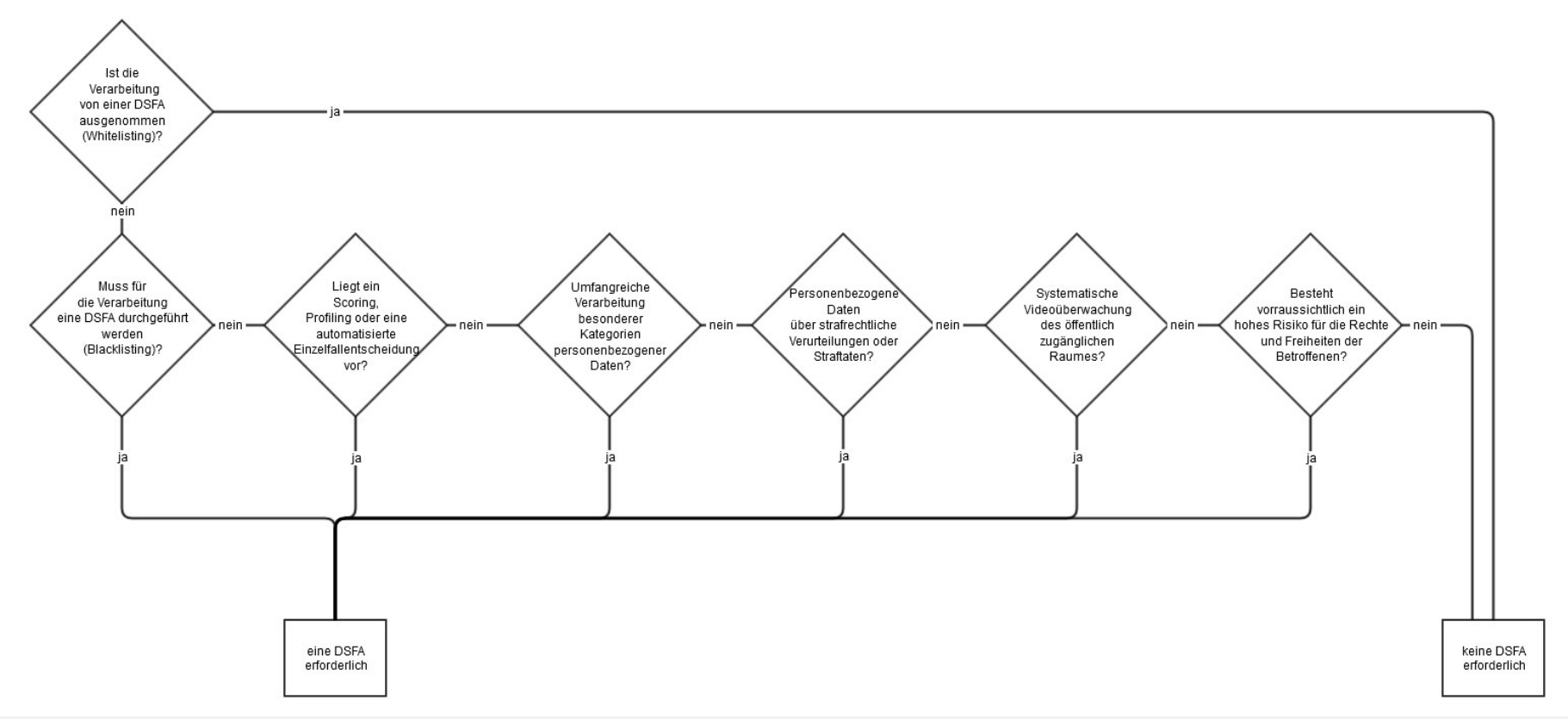
Ähnlich der bisherigen Vorabkontrolle, wobei noch nicht klar ist ob die Pflicht sofort besteht oder erst wenn zwei Kriterien erfüllt sind → sicherer zunächst direkt ausführen!

Auch negative Bewertungen sind zu dokumentieren.

Verantwortlicher & Auftragsverarbeiter:

Datenschutz-Folgeabschätzung - Art. 36 DSGVO

Ist eine Datenschutzfolgeabschätzung erforderlich?



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)

Datenschutzfolgeabschätzung

Artikel 35 DSGVO

Name der Folgeabschätzung: <Name des geplanten Verarbeitungsvorgangs>

erstellt am: <Datum der Erstellung>

betrachtet am: <Datum des letzten jährlichen Reviews – zur Fortschreibung>

Namen und Kontaktdaten des Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	<u>Verantwortlicher</u>: <Firmenname> Vertreten durch die Geschäftsführer: <Namen der vertretungsberechtigten Organe (Geschäftsführer)> <Geschäftsadresse> <Telefonnummer> <E-Mail> <u>Datenschutzbeauftragter</u>: (immer eine natürliche Person) <Name> <Geschäftsadresse> <Telefonnummer> <E-Mail>
Beteiligte an dieser Datenschutzfolgeabschätzung	<Vor- und Nachname> <Position>
systematische Beschreibung des geplanten Verarbeitungsvorgangs inkl. der Datenflüsse	<Beschreibung>
Kategorien betroffener Personengruppen	<Wer ist von diesem Verarbeitungsvorgang betroffen?>
Kategorien von Daten	<Welche Daten sollen verarbeitet Werden?>
Zweck der Verarbeitung	<Wieso soll dieser Verarbeitungsvorgang eingeführt werden?>
berechtigtes Interesse des Verantwortlichen einschließlich der Rechtsgrundlage	<Beschreibung des berechtigten Interesses inkl. der Rechtsgrundlage>

Bewertung der Notwendigkeit und Verhältnismäßigkeit	<objektive Bewertung mit Begründung ob diese Verarbeitung wirklich notwendig ist und verhältnismäßig ist>
Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (ohne Abhilfemaßnahmen) – Risikobewertung unter Berücksichtigung a) möglicher physischer, materieller und immaterieller Schäden, b) deren Schwere sowie c) Eintrittswahrscheinlichkeit	<Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen in Bezug auf Schutzklasse, Eintrittswahrscheinlichkeit, Schwere und Folgen, Vertraulichkeit, Integrität, Verfügbarkeit inkl. Begründung ohne Abhilfemaßnahmen>
geplanten Abhilfemaßnahmen zur Bewältigung der Risiken einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren – dies sind u.a. technische und organisatorische Maßnahmen; Wirksamkeitsprüfungen benennen; Restrisiken sind ebenfalls zu benennen	<alle konkrete geplanten Maßnahmen, Sicherheitsmaßnahmen, Garantien und Verfahren zur Reduzierung der Risiken für die Rechte und Freiheiten betroffener Personen inkl. der Wirksamkeitsprüfungen sowie evtl. Restrisiken>
Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (mit Abhilfemaßnahmen) – Risikobewertung unter Berücksichtigung a) möglicher physischer, materieller und immaterieller Schäden, b) deren Schwere sowie c) Eintrittswahrscheinlichkeit	<Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen in Bezug auf Schutzklasse, Eintrittswahrscheinlichkeit, Schwere und Folgen, Vertraulichkeit, Integrität, Verfügbarkeit inkl. Begründung unter Beachtung der getroffenen Maßnahmen>
Freigabe des Verarbeitungsvorgang	<Kann die Freigabe erfolgen? Sind Auflagen vorhanden die zuerst erledigt sein müssen vor einer Erneutbewertung? Freigabe der Aufsichtsbehörde erforderlich?>

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:

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

nicht alle Maßnahmen müssen und können technisch geregelt werden, **organisatorische Maßnahmen** sind auch zulässig – hier eine Übersicht für mögliche Policies:

- Arbeitsplatz / IT-Policy beinhaltet bspw. CleanDesk Regelung inkl. Bildschirmsprerre, Passwort-Regelungen, Umgang mit Wechseldatenträgern, Nutzung und Installation von Software/Diensten, Vernichtung von Papier/Datenträgern
- Mobile Device Policy beinhaltet bspw. Verschlüsslung, erforderlichen Passwortschutz, Meldepflicht bei Verlust, keine Weitergabe an Dritte, keine sensiblen Telefonate/Datennutzung in der Öffentlichkeit
- E-Mail Policy → dienstlicher E-Mail Account, nur dienstlich!
- Internet-Policy
- Meldepflicht bei Datenpannen Policy
- HomeOffice Policy
- .....

Was technisch umgesetzt werden kann, ist meist besser sichergestellt bspw. jährlich verpflichtende Passwortänderung, die Einhaltung der organistatorische Maßnahmen müssen auch geprüft werden!

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** ..“

Das heißt am besten verpflichten Sie Ihre Mitarbeiter/innen entsprechend darauf.

Verpflichtung auf die Vertraulichkeit personenbezogener Daten, des Fernmeldegeheimnisses gemäß § 88 Telekommunikationsgesetz (TKG) und zur Wahrung von Geschäftsgeheimnissen

Verpflichtung auf die Vertraulichkeit personenbezogener Daten

Es ist mir untersagt, personenbezogene Daten, zu denen ich dienstlich Zugang habe, unbefugt zu erheben, zu verarbeiten oder zu nutzen. Dies gilt sowohl für die dienstliche Tätigkeit innerhalb wie auch außerhalb (z.B. bei Kunden und Interessenten) des Unternehmens. Dieses Verbot besteht auch nach der Beendigung meiner Tätigkeit fort..

Verpflichtung auf das Fernmeldegeheimnis nach § 88 TKG

Ich bin zur Wahrung des Fernmeldegeheimnisses verpflichtet, soweit ich im Rahmen meiner Tätigkeit bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirke.

Verpflichtung auf Wahrung von Geschäftsgeheimnissen

Über alle Angelegenheiten des Unternehmens, beispielsweise Einzelheiten der Organisation, Geschäftsvorgänge und Zahlen des internen Rechnungswesens, ist von mir Verschwiegenheit zu wahren, sofern sie nicht allgemein öffentlich bekannt geworden sind. Hierunter fallen auch Vorgänge von Drittunternehmen, mit denen ich befasst bin. Auf die gesetzlichen Bestimmungen über den unlauteren Wettbewerb wurde ich besonders hingewiesen.

Alle Aufzeichnungen, Abschriften, Geschäftsunterlagen, Ablichtungen dienstlicher oder geschäftlicher Vorgänge, die mir dienstlich überlassen oder von mir angefertigt werden, sind vor der Einsichtnahme durch Unbefugte zu schützen.

Von diesen Verpflichtungen habe ich Kenntnis genommen. Die Pflicht zur Wahrung Vertraulichkeit personenbezogener Daten und der genannten Geheimnisse gilt zeitlich unbegrenzt auch über die Beendigung des Arbeitsverhältnisses hinaus. Ich bin mir bewusst, dass die Verletzung der Vertraulichkeit personenbezogener Daten, des Fernmeldegeheimnisses oder von Geschäftsgeheimnissen strafbar sein kann, insbesondere nach §§ 41 bis 43 BDSG (neu), § 206 StGB und nach § 17 UWG. Das Merkblatt zur Verpflichtungserklärung mit den Abschriften aller genannten Vorschriften habe ich erhalten.

Datenschutzbeauftragte/r

Der/Die Datenschutzbeauftragte für dieses Unternehmen ist *Name, Kontaktdaten.* Er/Sie steht mir für Fragen/Beratung mit datenschutzrechtlichem Bezug zur Verfügung.

Ort, Datum	Ort, Datum
_____	_____
Vorname Name Arbeitgeber/in	Vorname Name Arbeitnehmer/in

Als Anlage für den/die Arbeitnehmer/in entsprechende Gesetzestexte beifügen!

Zusammenfassung?

- Ersetzen Sie bestehende Auftragsdatenverarbeitungsverträge gemäß §11 BDSG durch neue Auftragsverarbeitungsverträge gemäß Artikel 28 DGSVO
- Bewerten Sie die technischen und organisatorischen Maßnahmen Ihrer Lieferanten und dokumentieren auch die Garantie bei Drittstaaten und internationalen Organisationen (Vorsicht in Sachen PrivacyShield – unklar ob das dauerhaft Bestand hat)
- Nehmen Sie die Auftragsverarbeitung auf in Ihre Risikoanalyse, auch hier gilt die Datenschutzfolgeabschätzung

- Erstellen Sie Ihre Datenschutzfolgeabschätzungen inkl. der Risikoanalyse, bei nicht ausreichenden Abhilfemaßnahmen Aufsichtsbehörde einschalten

- Erstellen Sie Ihre organisatorischen Maßnahmen – Policies und setzen diese aktiv durch und kontrollieren diese

- Erstellen Sie zu einen Prozess zum Review und erneuter Bewertung → i.d.R. 1 x jährlich → gilt für alle drei Bereiche

- Verpflichten Sie Ihre Mitarbeiter auf Vertraulichkeit

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