Datenschutz neu – Ihr Unternehmenskonzept

Gesundheitsberufe – Friseure – Fußpfleger – Kosmetiker – Masseure – Mode- und Bekleidungstechnik – Personenberatung – persönliche Dienstleistung

Teil 2

HANDWERK STATT MUNDWERK.
Wo Handwerk draufsteht, ist Kopfarbeit drin.

Zeit für Ihre Fragen!

- Bestellscheine für Endkunden: werden tw. noch handschriftlich vom Kunden ausgefüllt. Muss am Bestellschein ein Datenschutz-Hinweis draufstehen oder reicht der Verweis auf die AGB?
- GPS-Ortungssysteme in Firmenfahrzeugen: Daten des Fahrers inkl. GPS-Daten werden gesammelt. Wie lange dürfen die Daten aufbewahrt werden? Ist Zustimmung des Fahrers nötig, bei jedem Fahrzeugwechsel oder einmalig? Daten werden tw. gesammelt aber dienen nur der Dokumentation bei Unfällen, sonst keine Auswertung – ist das DSGVO-konform?
- Dokumentation der Löschung
  - Wie muss Löschung der Daten im Unternehmen dokumentiert werden?
  - Ist ein Löschungsprotokoll im Hintergrund einer Software ausreichend?
  - Muss der Name des Löschenden inkl. Löschungsdatum und Grund aufbewahrt werden? Wenn ja, wie lange?
  - Welchen Nachweis muss Unternehmer an den Betroffenen schicken?
  - Müssen Steuerberater, Bank (z.B. für Lohnverrechnungsdaten von ehemaligen Mitarbeitern nach der gesetzlichen Aufbewahrungsfrist) über ein Auskunftsbegehren und/oder eine Löschen informiert werden?

Zeit für Ihre Fragen!

- Was gilt es zu beachten, wenn man Google Analytics verwendet? (ohne Conversion Tracking)
- Was gilt es zu beachten, wenn man Google Adwords verwendet? (ohne Conversion Tracking
- Thematik Einbindung der Facebookseite oder Google Maps in die Homepage: Theoretisch würde beim Anklicken des Facebookbuttons Daten des Nutzers an Facebook übertragen, da Facebook tracked woher die Nutzer kommen. Ich als Webseitenbetreiber kann nicht sicherstellen, das Facebook die Daten nicht speichert, bin ich dafür haftbar?

Zeit für Ihre Fragen!

- Lieferscheine: Mitarbeiter/Kundendienstberater notieren auf Lieferscheinen gerne personenbezogene Daten. Reicht die Unterschrift des Kunden am Lieferschein für die Verarbeitung der Daten, auch Daten die nicht Bestand des Auftrages sind (z.B. welchen Wein der Kunde gerne trinkt)
- Was gilt es beim Betreiben einer Facebookseite als Unternehmen zu beachten? (zB. Posts mit weiterführende Links zu meiner Homepage etc.). Müssen bereits auf Facebook veröffentlichte Fotos gelöscht werden?
- WhatsApp am Handy: Firmenhandys, die auch privat genutzt werden, haben WhatsApp/Facebook installiert. Auch wenn die Geschäfte nicht über diese beiden Plattformen abgewickelt werden sind die Kundentelefonnummern trotzdem auch im Adressbuch gespeichert und damit für WhatsApp/Facebook sichtbar – Muss WhatsApp komplett von den Handys entfernt werden oder gibt es da andere Lösungen?

Zeit für Ihre Fragen!

- Bankomat- und Kreditkartenzahlung: Zahlungsdaten der Kunden werden vom Unternehmen gespeichert, auch Informationen über Kreditkartennummer usw. – ist das zulässig?
- Zusendung von aktuellen Preislisten am Jahresanfang an alle Kunden: Fällt das unter Werbung oder ist das eine bloße Kundeninformation? Darf die Preisliste, wenn es eine reine Information ist, an alle Kunden ohne deren explizites Einverständnis geschickt werden?
- Müssen die Schulungen von Mitarbeitern zum Datenschutz dokumentiert werden?

Zeit für Ihre Fragen!

Sind die nachstehenden Empfänger Auftragsverarbeiter oder eigene Verantwortlich?

- Externer IT-Dienstleister
- Konzernbuchhaltung
- Externe Lohnverrechnung
- Steuerberater
- Wirtschaftsprüfer
- Versicherungsmakler
- Entwickler einer Webapplikation zur Einsatzplanung
- Reisebüro
- Hotels/Gasthöfe/Pensionen
- Telekommunikationsunternehmen (Mobiltelefon, Festnetztelefonanlage)
- Entwickler u. Betreiber Zeiterfassungsprogramm

Zeit für Ihre Fragen!

- Entwickler u. Betreiber ERP-Programm
- Gewerkschaft
- Weiterbildungsinstitute
- Berufsschule
- Externe Arbeitsmediziner, Sicherheitsfachkraft
- Urlaubskassen (BUAK)
- Krankenkasse, Finanzamt
- Reinigungsunternehmen (Arbeitskleidung)
- Arbeitsmarktservice
- Wirtschaftskammer

Zeit für Ihre Fragen!

- Muss dokumentiert werden, dass die TOMs überprüft wurden?
- Wie erfolgt der ‚Nachweis' einer Person, die Einsicht in die Daten verlangt (oder eine Löschung der Daten anstrebt..) …. persönlich, mit Ausweiskopie …. ?
- Könnte ich für die Einsicht in die Daten (oder für die Löschung der Daten))einen Arbeitsaufwand in Rechnung stellen ☺?
- Wie vermerken wir hier die Datenschutzbestimmungen?
- FAQ zum Verzeichnis:
  - Müssen alle Daten einzelner Mitarbeiter/Kunden/… erfasst werden?
  - Wo muss der Steuerberater angegeben werden?

HANDWERK STATT MUNDWERK.
Wo Handwerk draufsteht, ist Kopfarbeit drin.

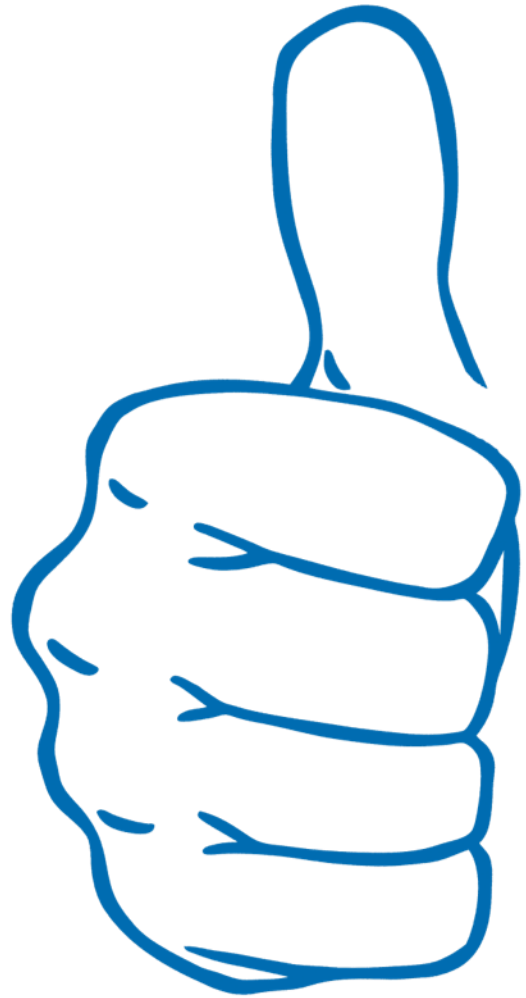
summereder & aigner
rechtsanwälte

Zeit für Ihre Fragen!

- Zählen Größe und Gewicht des Kunden zu sensiblen Daten bzw. ev. eine Kombination daraus?
- Gesundheitsberufe: Optiker, Orthopädietechniker, Zahntechniker,… bekommen die Kundendaten über Ärzte, übermitteln Daten an GKK/andere Versicherungen für Kostenersatz – was ist hier zu beachten?
- Augenoptiker: zählen Dioptrien und Daten über Sehstörungen zu den sensiblen Daten? Brauchen sie einen Datenschutzbeauftragten?
- Friseure: dürfen verwendete Produkte (Farbe, Schminkprodukte,…) ohne Einwilligung gespeichert werden? Wie sieht es mit Informationen über z.B. Farballergien aus?

Zeit für Ihre Fragen!

- Lebens- und Sozialberater: Supervision von Angestellten im Auftrag von Firmen – welche Daten dürfen an die Firma rückgemeldet werden? Ist Auftraggeber dafür verantwortlich dass Mitarbeiter zustimmt?
- Friseure: Modelle für z.B. Wimpernverlängerungen, Frisuren usw. werden über Facebook gesucht, Vereinbarung dann über Facebook-Messenger. Zulässig?
- Personenbetreuung: selbstständige Personenbetreuer sind tw. über Verein organisiert – dürfen sie an den Verein Daten der Pflegepersonen weitergeben? Auch gesundheitsrelevante Daten?
- Lebens- und Sozialberater: Ich betreibe auf Facebook eine Fan-Page und dazu eine eigene Gruppe. Bisher habe ich auf Facebook einen Link zum Impressum meiner HP gehabt. In der Gruppe werden von Mitgliedern immer wieder sehr persönliche sensible Erzählungen eingestellt. Ich habe keinen Zugriff darauf, wie andere mit diesen Infos umgehen. Es liegt in der Verantwortung der Mitglieder selbst, was gepostet wird. Selbstverständlich gebe ICH nichts weiter. Hier einen eigenen fixierten Beitrag mit entsprechender Datenschutzerklärung posten?



Die Auftragsverarbeitervereinbarung

- Zur Wiederholung – Begriffsbestimmungen nach Art. 4 EU-DSGVO:
- „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden
- „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
- https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

Die Auftragsverarbeitervereinbarung

Art. 28 EU-DSGVO normiert das Verhältnis zwischen Auftragsverarbeiter und Verantwortlichem

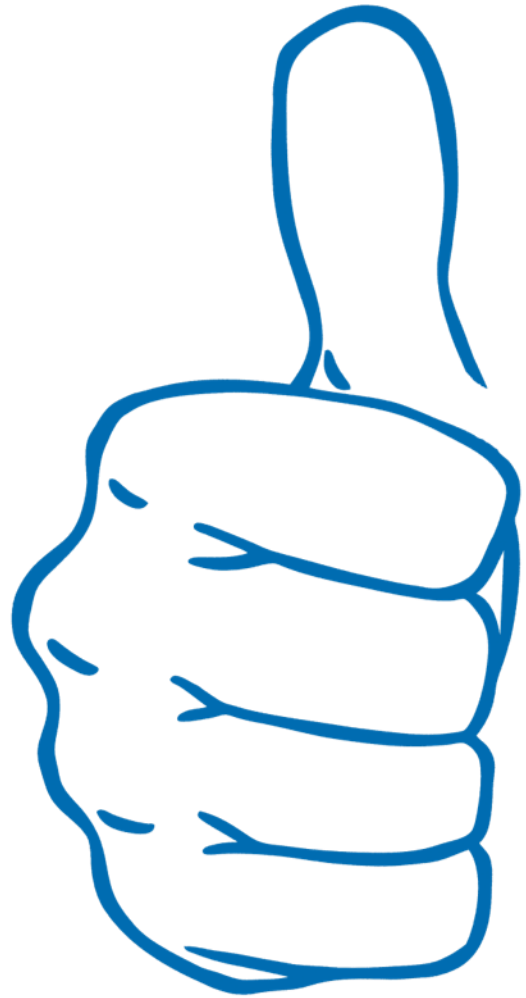
- (1)Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
- (3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind

Die Auftragsverarbeitervereinbarung

- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-vereinbarung-auftragsverarbeitung.pdf

Tipp:

Achten Sie darauf, mit Ihren Auftragsverarbeitern standardisierte Verträge abzuschließen, sonst laufen Sie Gefahr, durch Ihre Vertragspartner mit unrichtigen, unvollständigen oder sogar für Sie nachteiligen Vertragsentwürfen überrascht zu werden!



Datenschutz im Arbeitnehmerkontext

Art. 88 EU-DSGVO bestimmt den Umgang mit Arbeitnehmerdaten

- Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich **der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext**, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.
- Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.
- Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

Datenschutz im Arbeitnehmerkontext

§ 96 (1) ArbVG: Folgende Maßnahmen des Betriebsinhabers bedürfen zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates:

3. die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren;

Datenschutz im Arbeitnehmerkontext

§ 96a (1) ArbVG: Folgende Maßnahmen des Betriebsinhabers bedürfen zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates:

1. Die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen. Eine Zustimmung ist nicht erforderlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben;

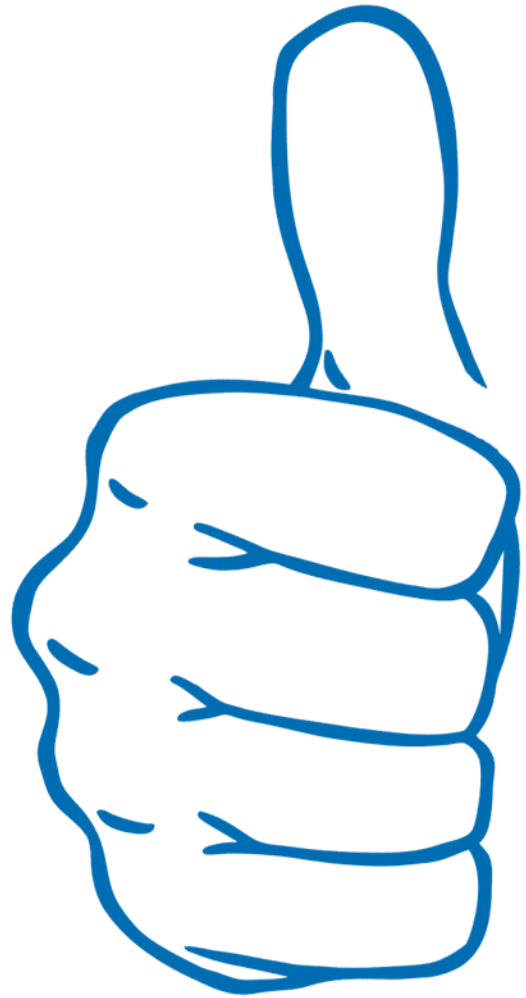
2. die Einführung von Systemen zur Beurteilung von Arbeitnehmern des Betriebes, sofern mit diesen Daten erhoben werden, die nicht durch die betriebliche Verwendung gerechtfertigt sind.

Datenschutz im Arbeitnehmerkontext

- **§ 10 AVRAG:**
- (1) Die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, ist unzulässig, es sei denn, diese Maßnahmen werden durch eine Betriebsvereinbarung im Sinne des § 96 Abs. 1 Z 3 ArbVG geregelt oder erfolgen in Betrieben, in denen kein Betriebsrat eingerichtet ist, mit Zustimmung des Arbeitnehmers.
- (2) Die Zustimmung des Arbeitnehmers kann, sofern keine schriftliche Vereinbarung mit dem Arbeitgeber über deren Dauer vorliegt, jederzeit ohne Einhaltung einer Frist schriftlich gekündigt werden.

Wichtige To-Dos:

- **Privatnutzung von E-Mail und Internet regeln**
- Betriebsvereinbarungen zu Kontrollmaßnahmen und Personaldatensystemen abschließen *oder* Einzelvereinbarungen zu Kontrollmaßnahmen abschließen
- Verpflichtung der Mitarbeiter zum Datenschutz und zur Wahrung von Geschäfts- und Betriebsgeheimnissen https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtung-datengeheimnis.pdf
- Schulung & Sensibilisierung der Mitarbeiter
- Übermittlung eines Informationsschreibens an die Mitarbeiter (Art. 13 EU-DSGVO) https://www.wko.at/service/wirtschaftsrecht-gewerberecht/dsgvo-muster-datenschutzerklaerung-mitarbeiter.html
- Holen Sie allenfalls Einwilligungen ein, sofern Sie bei der Verwendung von Mitarbeiterfotos auf Nummer Sicher gehen wollen!



TOM‘s

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; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, 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.

TOM‘s

- 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.
- Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
- 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, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

TOM‘s

- **VERTRAULICHKEIT**

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

TOM‘s

INTEGRITÄT

- **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;
- Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche **Wiederherstellbarkeit**;
- **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

TOM‘s

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.

Noch Fragen?

Mein Tipp:

Nutzen Sie die EU-DSGVO als Chance, bereits seit Langem offene Baustellen in Ihrem Unternehmen aktiv anzugehen (Vertragsmuster, Infrastruktur), Prozesse einzuführen oder zu optimieren und Licht in den Datendschungel zu bringen!

Datenschutz ist kein lästiges Gesetz – er ist Grundlage Ihres Geschäfts!

HANDWERK STATT MUNDWERK.
Wo Handwerk draufsteht, ist Kopfarbeit drin.

summereder & aigner
rechtsanwälte

Kontaktdaten des Vortragenden

Rechtsanwalt Mag. Philipp Summereder

Summereder Aigner Rechtsanwaltsgesellschaft m.b.H.

Kramlehnerweg 1a, 4061 Pasching

07229/23848 office@rechtsanwalt-pasching.at

http://www.rechtsanwalt-pasching.at

summereder & aigner

rechtsanwälte