CyberWehr

RISK MANAGEMENT SOLUTIONS GMBH

Monika Wehr ▪ Alte Landstrasse 109 ▪ 8803 Rüschlikon ▪ Telefon +41 (0) 79 348 55 63

Verzeichnis von Verarbeitungstätigkeiten (VVT)

Nach Art. 12 DSG und 30 DSGVO ist für die meisten Unternehmen die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten Pflicht zum Nachweis ("Accountability"), dass man die datenschutzrechtlichen Anforderungen laufend, auch für einen in der Vergangenheit liegenden Fall, in der Unternehmenspraxis erfüllt.

Das VVT ist ein zentraler Bestandteil der Dokumentationspflicht gegenüber den Aufsichtsbehörden und kann beispielsweise zur Grundlage für Risikobewertungen durch den DSB für dessen und den eigenen risikoorientierten Überwachungsauftrag werden (Art. 39 Abs. 2 DS-GVO). Ohne eine solche strukturierte Dokumentation sind die Beratungs- und Kontrollpflichten des Datenschutzbeauftragten kaum umsetzbar. Denkbar sind interne Erweiterungen des VVT durch Risikoabschätzungen bzw. eine zusätzliche Strukturierung, die festhält, welche Verarbeitungen ggf. eine Datenschutz-Folgenabschätzung erfordern und welche nicht. Daneben können die durchgeführten Prüfungen aufgenommen werden. Aber: Das VVT darf nicht nicht überfrachtet werden!

Die im Zusammenhang mit der Weitergabe von personenbezogenen Daten an Stellen in Drittländern geforderte Dokumentation der „Garantien“ ist in regulären Prozessen entbehrlich. Entsprechende Garantien sind ausschließlich in den Fällen des Art. 49 Abs. 1 und 2 DS-GVO zu dokumentieren. Eine Dokumentation weiterer Garantien, wie zum Beispiel eines Angemessenheitsbeschlusses der Kommission oder durch Standardvertragsklauseln kann sinnvoll sein, um den Accountability-Pflichten und Transparenzpflichten Gnü. Betroffenen nach- kommen zu können.

In der Regel müssen alle Verantwortlichen in Unternehmen, Behörden etc. ein VVT führen. Gemäss DSG und Art. 30 Abs. 5 DSGVO/Art. 7 DSG ist diese Pflicht beschränkt auf Unternehmen

- mit einer Größe ab 250 Mitarbeitern; oder
- mit einem besonderem Risiko bei der Verarbeitung; oder
- mit Verarbeitung von sensiblen Daten (Art. 9 und 10 DS-GVO); oder
- einer nicht nur gelegentlichen Verarbeitung.

Allerdings geht diese Ausnahmeregelung ins Leere. Spätestens bei Zugrundelegung einer regelmässigen Verarbeitung sind sämtliche Verantwortlichen unabhängig von ihrer Mitarbeiterstärke betroffen.

Das VVT darf in einem elektronischen Format geführt werden. Wegen der Vorlagepflicht gegenüber der Aufsichtsbehörde in Art. 30 Abs. 4 DS-GVO muss es in elektronischer oder gedruckter Form exportierbar sein.

Es bietet sich hier Bündelung von Verarbeitungen nach einem Zweck an. In diesem Verarbeitungsverzeichnis finden sich eine Reihe von Verarbeitungen, die in nahezu jedem Unternehmen vorkommen. Diese können als Hilfe zum Einstieg in die Erstellung des Verzeichnisses frei verwendet werden. Die Angaben sind jeweils individuell zu dem Unternehmen anzupassen.

Die **Inhalte des VVT** für Verantwortliche ergeben sich aus Art. 30 Abs. 1 DS-GVO und umfassen:

- den Namen und die Kontaktdaten

    - des Verantwortlichen (i.d.R. also Nennung des Unternehmens);
    - Vertretungsberechtigte Personen (bei der GmbH z.B. die Geschäftsführer)
    - ggf. des gemeinsam mit ihm Verantwortlichen;
    - ggf. des Vertreters in der EU;
    - ggf. des Datenschutzbeauftragten beim Verantwortlichen;
- die Zwecke der Verarbeitung;
- die Kategorien betroffener Personen;
- die Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
- gegebenenfalls Übermittlungen von personen- bezogenen Daten an ein Drittland oder an eine internationale Organisation
    - einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation;
    - bei den in Art. 49 Abs. 1 UAbs. 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- [wenn möglich,] die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- Es wird erwartet, dass eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen gem. DSG Art. 7 und Art. 32 Abs. 1 DSGVO vorliegt.

Zusätzlich müssen aber auch noch jeweils die Rechtsgrundlagen der Verarbeitung aufgelistet werden.

Beispielhafte *typischer* Verarbeitungen sind:

- Inkasso
- Internetseite
- Controlling
- Bewerbermanagement
- CRM
- E-Mail
- Einkauf
- Facility Management
- Finanzbuchhaltung
- Freelancer-Datenbank
- Fuhrparkmanagement
- IT
- Kontaktverwaltung
- Lohnbuchhaltung
- Marketing
- Personal – HR
- Produktion
- Projektverwaltung
- Revision – Compliance
- Terminverwaltung
- Verkauf – Vertrieb
- Verwaltung
- Videoüberwachung
- Zeiterfassung

Beschreibung der Zwecke der Verarbeitung

- **Inkasso:** Geltendmachung und Durchsetzung von Zahlungsansprüchen

- **Internetseite:** Betrieb einer Internetseite zur Außendarstellung des Unternehmens und zur Kontaktaufnahme inkl. Kontaktformular
- **Controlling**: Planung, Steuerung und Kontrolle aller Unternehmensbereiche
- **Bewerbermanagement**: Zweck des Bewerbermanagements ist die Personalbeschaffung. Dazu gehört das Finden von passenden Bewerbern und die Auswahl der Bewerber mit den besten Fähigkeiten für die jeweilige Stelle.
- **Customer-Relationship-Management (CRM)**: Pflege von Kundenbeziehungen und Beziehungen zu Interessenten
- **E-Mail:** Elektronische Kommunikation
- **Einkauf:** Einkauf von Waren oder Dienstleistungen
- **Facility Management:** Pflege und Wartung von Immobilien und Gebäuden, die vom Unternehmen genutzt werden.
- **Finanzbuchhaltung:** Ermittlung und Verwaltung aller Einnahmen und Ausgaben, insbesondere für Zwecke der Ermittlung und Abfuhr von Steuern und Abgaben.
- **Freelancer-Datenbank:** Verwaltung von Kontakten und Fähigkeiten von freien Mitarbeiter ("Freelancer")
- **Fuhrparkmanagement:** Verwaltung der vom Unternehmen genutzten Fahrzeuge
- **IT**: Bereitstellung, Wartung und Pflege von IT-Systemen
- **Kontaktverwaltung**: Verwaltung und Bereitstellung von Kontaktmöglichkeiten von Personen, Unternehmen oder öffentlichen Stellen
- **Lohnbuchhaltung**: Ermittlung von Lohn & Gehalt, Abrechnung und Auszahlung von Lohn & Gehalt
- **Marketing**: Marketing/Werbung für Waren oder Dienstleistungen und für das Unternehmen insgesamt.
- **Personal – HR**: Personendatenverarbeitung, Personalentwicklung
- **Produktion**: Produktion von Waren oder Dienstleistungen
- **Projektverwaltung**: Verwaltung von Projekten im Unternehmen
- **Revision – Compliance**: Überprüfung der Rechtskonformität von Geschäftsprozessen im Unternehmen
- **Terminverwaltung**: Planung und Verwaltung von Terminen
- **Verkauf – Vertrieb**: Verkauf und Vertrieb von Waren oder Dienstleistungen
- **Verwaltung**: Allgemeine Verwaltung des Unternehmens (Organisation, Büroorganisation, Empfang etc.)
- **Videoüberwachung**: Wahrnehmung des Hausrechts, Geltendmachung von Ansprüchen, Verfolgung von Straftaten
- **Zeiterfassung**: Erfassung von Arbeits-, Anwesenheits-, Abwesenheits- und Urlaubszeiten

Beschreibung der Kategorien personenbezogener Daten

- **Inkasso**: Vorname, Nachname, Name des Unternehmens, Anschrift (geschäftlich), Anschrift (privat), Rechnungsanschrift, Internetadresse, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Branche, Kundennummer, Kundenart, Kontaktdaten, Kontakthistorie, Bankverbindung, Angaben zu Lohnpfändungen, Daten zur Zahlungsfähigkeit, Daten zum Zahlungsausfallrisiko, Scoringdaten

- **Internetseite:** Name, Name des Unternehmens, Bestandsdaten, Nutzungsdaten, Inhaltsdaten

- **Controlling:** Vorname, Nachname, Name des Unternehmens, Anschrift (geschäftlich), Rechnungsanschrift, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Branche, Kundennummer, Kundenart, Kontaktdaten, Kontakthistorie, Vertragsdaten, Bestandsdaten, Nutzungsdaten, Umsatzdaten

- **Bewerbermanagement:** Vorname, Nachname, Titel, Lebenslauf, Schulabschluss, Berufsabschluss, Studium

- **Customer Relationship Management (CRM)**: Vorname, Nachname, Titel, Name des Unternehmens, Anschrift (geschäftlich), Internetadresse, E-Mail-Adresse, Telefonnummer, Faxnummer, Familienstand, Kundennummer, Kundenart, Kontaktdaten, Kontakthistorie, Termindaten, Daten zu Interessen, gekauften Waren, Kommunikationsdaten, Fotos, Angaben zum Beruf

- **E-Mail**: Name, E-Mail-Adresse, Nutzungsdaten, Verkehrsdaten

- **Einkauf**: Vorname, Nachname, Name des Unternehmens, Anschrift (geschäftlich), Rechnungsanschrift, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Kontakthistorie, Bankverbindung, Umsatzsteuer ID Nummer, Daten zu gekauften Waren oder Dienstleistungen, Vertragsdaten, Umsatzdaten

- **Facility Management**: Vorname, Nachname, Name des Unternehmens, Anschrift (geschäftlich), E-Mail-Adresse, Telefonnummer, Faxnummer, Kontaktdaten, Kontakthistorie, Termindaten, Vertragsdaten, Fotos

- **Finanzbuchhaltung**: Vorname, Nachname, Name des Unternehmens, Rechnungsanschrift, E-Mail-Adresse, Telefonnummer, Kundennummer, Kundenart, Bankverbindung, Umsatzsteuer ID Nummer, Daten gekauften Waren oder Dienstleistungen, Vertragsdaten, Umsatzdaten

- **Freelancer-Datenbank:** Vorname, Nachname, Titel, Name des Unternehmens, Anschrift (geschäftlich), Rechnungsanschrift, Internetadresse, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Kontaktdaten, Kontakthistorie, Termindaten, Vertragsdaten, Kommunikationsdaten, Fotos, Angaben zum Beruf und zur beruflichen Laufbahn, Schulabschluss, Berufsabschluss, Studium, Daten zu Fortbildungen

- **Fuhrparkmanagement:** Vorname, Nachname, Anschrift (geschäftlich), Anschrift (privat), E-Mail-Adresse, Telefonnummer, Geburtsdatum, Position, Führerscheindaten

- **IT**: Vorname, Nachname, Titel, E-Mail Adresse, Telefonnummer, Position, Kontakthistorie, Nutzungsdaten, Verkehrsdaten, Telekommunikationsdaten, Kommunikationsdaten

- **Kontaktverwaltung**: Vorname, Nachname, Anschrift (geschäftlich), Anschrift (privat), Rechnungsanschrift, Internetadresse, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Branche, Kundennummer, Kundenart, Kontaktdaten, Kontakthistorie, Termindaten

- **Lohnbuchhaltung**: Vorname, Nachname, Titel, Anschrift (privat), Telefonnummer, Geburtsdatum, Familienstand, Angaben zu Angehörigen (Kindern), Bankverbindung, Vertragsdaten, Sozialversicherungsdaten, Arbeitszeiten, Lohn- und Gehaltsdaten, Angaben zu Steuerklassen, Religionszugehörigkeit, Angaben zu Lohnpfändungen

- **Marketing**: Vorname, Nachname, Titel, Name des Unternehmens, Anschrift (geschäftlich), Internetadresse, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Branche, Kundennummer, Kundenart, Kontakthistorie, Termindaten, Daten zu Interessen

- **Personal – HR**: Vorname, Nachname, Titel, Anschrift (privat), Telefonnummer, E-Mail-Adresse, Geburtsdatum, Familienstand, Angaben zu Angehörigen (Kindern), Gesundheitsdaten, Daten zu Interessen, Bankverbindung, Vertragsdaten, Fotos, Sozialversicherungsdaten, Arbeitszeiten, Lohn- und Gehaltsdaten, Angaben zu Steuerklassen, Religionszugehörigkeit; Angaben zum Beruf, zur beruflichen Laufbahn und zu Lohnpfändungen, Urlaubszeiten, Daten zum beruflichen Eingliederungs-management, Schul- und Berufsabschluss, Studium, Krankheitstage, Daten zu Vorstrafen bzw. Eintragungen ins Bundeszentralregister, Daten zu beruflichen Fortbildungen

- **Produktion**: Name, Name des Unternehmens, Anschrift (geschäftlich), Anschrift (privat), Rechnungsanschrift, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Branche, Kundennummer, Kundenart, Arbeitszeiten, Umsatzdaten

- **Projektverwaltung**: Vorname, Nachname, Name des Unternehmens, Anschrift (geschäftlich), E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Branche, Termindaten, Vertragsdaten, Kommunikationsdaten, Umsatzdaten

- **Revision – Compliance**: Vorname, Nachname, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Familienstand, Position, Kontaktdaten, Kontakthistorie, Termindaten, Bankverbindung, Umsatzsteuer ID Nummer, Daten zu gekauften Waren oder Dienstleistungen, Vertragsdaten, Umsatzdaten, Nutzungsdaten, Inhaltsdaten, Kommunikationsdaten, Sozialversicherungsdaten, Arbeitszeiten, Lohn- und Gehaltsklassen, Angaben zu Steuerklassen, Religionszugehörigkeit; Angaben zum Beruf, zur beruflichen Laufbahn, Daten zu Vorstrafen bzw. Eintragungen ins Bundeszentralregister, Daten zu beruflichen Fortbildungen

- **Terminverwaltung**: Vorname, Nachname, Name des Unternehmens, Anschrift (geschäftlich), Anschrift (privat), E-Mail-Adresse, Telefonnummer, Position, Kontaktdaten, Termindaten

- **Verkauf – Vertrieb**: : Vorname, Nachname, Titel, Name des Unternehmens, Anschrift (geschäftlich), Anschrift (privat), E-Mail-Adresse, Telefonnummer, Kundennummer, Kundenart, Kontaktdaten, Kontakthistorie, Termindaten, Bankverbindung, Umsatzsteuer ID Nummer, Daten zu gekauften Waren oder Dienstleistungen, Vertragsdaten, Umsatzdaten

- **Verwaltung**: Vorname, Nachname, Titel, Name des Unternehmens, Anschrift (geschäftlich), E-Mail-Adresse, Telefonnummer, Position, Kontaktdaten, Kontakthistorie, Vertragsdaten

- **Videoüberwachung**: Name, Videos, Beschreibung der Kategorien betroffener Personen, Beschäftigte, Kunden, Interessenten, Dienstleister, Besucher

- **Zeiterfassung**: Vorname, Nachname, E-Mail-Adresse, Arbeitszeiten, Urlaubszeiten, Krankheitstage, Beschreibung der Kategorien betroffener Personen, Beschäftigte, Leiharbeiter

Beschreibung der Kategorien betroffener Personen

- **Inkasso:** Kunden, Dritte
- **Internetseite:** Interessenten, Besucher
- **Controlling:** Beschäftigte, Kunden, Dienstleister, Dritte
- **Bewerbermanagement:** Bewerber
- **Customer Relationship Management** (**CRM):** Beschäftigte, Kunden, Interessenten
- **E-Mail: Beschäftigte, Kunden, Interessenten, Dienstleister, Dritte, Bewerber**
- **Einkauf: Beschäftigte, Dienstleister, Dritte, Kreditoren**
- **Facility Management: Beschäftigte, Dienstleister, Dritte**
- **Finanzbuchhaltung: Beschäftigte, Kunden, Debitoren, Kreditoren**
- **Freelancer-Datenbank: Dienstleister, Dritte**
- **Fuhrparkmanagement: Beschäftigte**
- **IT: Beschäftigte, Kunden, Dienstleister, Dritte**
- **Kontaktverwaltung: Beschäftigte, Kunden, Interessenten, Dritte**
- **Lohnbuchhaltung: Beschäftigte**
- **Marketing: Beschäftigte, Kunden, Interessenten, Dritte - Daten zu gekauften Waren: Vertragsdaten, Fotos, Videos**
- **Personal – HR: Beschäftigte**
- **Produktion: Beschäftigte, Kunden, Interessenten, Dienstleister, Dritte**
- **Projektverwaltung: Beschäftigte, Kunden, Dienstleister, Dritte**
- **Revision – Compliance: Beschäftigte, Kunden, Dienstleister, Dritte**
- **Terminverwaltung: Beschäftigte, Kunden, Interessenten, Dienstleister, Dritte**
- **Verkauf – Vertrieb: Kunden**
- **Verwaltung: Beschäftigte, Kunden, Interessenten, Dienstleister, Dritte, Besucher**
- **Videoüberwachung: Beschäftigte, Kunden, Interessenten, Dienstleister, Dritte, Besucher**

- **Zeiterfassung: Vorname, Nachname, E-Mail-Adresse, Arbeitszeiten, Urlaubszeit, Krankheitstage, Beschreibung der Kategorien der betroffenen Personen, Mitarbeiter, Zeitarbeiter**

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden

- **Inkasso:** Rechtsanwälte, Auskunfteien, Strafverfolgungsbehörden
- **Internetseite**: zuzgl. Hosting-Provider, ggf. weitere interne Abteilungen zur Bearbeitung von Anfragen
- **Controlling:** Interessenten
- **Bewerbermanagement:** Betriebsrat, interne Stellen, die für die Einstellung des Bewerbers verantwortlich sind
- **Customer Relationship Management (CRM)**: CRM Dienstleister, Beschäftigte im Unternehmen, Auftragsverarbeiter
- **E-Mail:** Dienstleister, weitere Personen innerhalb des Unternehmens, ggf. Dritte
- **Einkauf:** Interne Abteilungen, die Waren oder Dienstleistungen in Anspruch nehmen, Betriebsrat, ggf. Dritte
- **Controlling**: Wirtschaftsprüfer, Steuerberater, Betriebsrat, Unternehmensleitung
- **Facility Management**: Dienstleister, die Leistungen im Bereich des Facility Managements übernehmen, ggf. sonstige Dritte.
- **Finanzbuchhaltung**: Finanzamt, Wirtschaftsprüfer, Steuerberater
- **Freelancer-Datenbank:** interne Abteilungen, die Freelancer-Bedarf haben, Betriebsrat
- **Fuhrparkmanagement:** Eigentümer des Fahrzeugs (Leasinggeber), Unfallbeteiligte, KFZ-Haftpflichtversicherer, ggf. Dritte

- **IT:** Beschäftigte mit Personalverantwortung, Betriebsrat

- **Kontaktverwaltung**: interne Abteilungen bzw. Personen in Abteilungen
- **Lohnbuchhaltung**: Betriebsrat, Wirtschaftsprüfer, Steuerberater, Sozialversicherungsstellen, Krankenkassen, Finanzverwaltung, Versicherer für betriebliche Altersversorgung, Abteilungsleiter bzw. Personen mit Personalverantwortung, Unternehmensleitung
- **Marketing**: Dienstleister, die für Marketing/Werbung eingesetzt werden
- **Personal – HR**: Betriebsrat, Sozialversicherungsstellen, Krankenkassen, Finanzverwaltung, Versicherer für betriebliche Altersversorgung, Abteilungsleiter bzw. Personen mit Personalverantwortung, Unternehmensleitung
- **Produktion**: Kooperationspartner, Zulieferer, Kunden, Vertriebs- und Handelspartner
- **Projektverwaltung**: Betriebsrat
- **Revision – Compliance**: Wirtschaftsprüfer, Steuerberater, Betriebsrat, Unternehmensleitung
- **Terminverwaltung**: weitere Teilnehmer an Terminen
- **Verkauf – Vertrieb**: Kooperationspartner, Logistikunternehmen
- **Verwaltung**: interne Abteilungen, Dienstleister, ggf. Dritte.
- **Videoüberwachung**: Rechtsanwälte, Strafverfolgungsbehörden
- **Zeiterfassung**: Betriebsrat, Wirtschaftsprüfer, Steuerberater

Ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

- **Inkasso:** keine
- **Internetseite**: Einbindung von Google Webfonts. In dem Zusammenhang kommt es zu Aufrufen von Servern von Google in den USA. Für die Verarbeitung ist Google "Verantwortlicher". Das angemessene Datenschutzniveau ergibt sich aus der Teilnahme von Google am Privacy Shield.
- **Controlling:** keine
- **Bewerbermanagement:** nicht geplant

- **Customer-Relationship-Management (CRM): Für das CRM-System wird bei ein Softwaresystem** eines Dienstleisters in einem Drittstaat (hier: USA) verwendet. Es besteht ein Auftragsverarbeitungsvertrag mit dem Dienstleister. Das angemessene Datenschutzniveau ist durch die Mitgliedschaft des Dienstleisters im "Privacy Shield" gewährleistet.
- **E-Mail:** Nicht geplant. Gleichwohl ist beim Versand von E-Mails über das Internet nie ausgeschlossen, dass eine Weiterleitung über einen Drittstaat erfolgt.
- **Einkauf:** keine
- **Facility Management:** keine
- **Finanzbuchhaltung**: keine
- **Freelancer-Datenbank:** keine
- **Fuhrparkmanagement:** keine
- **IT:** keine
- **Kontaktverwaltung**: keine
- **Lohnbuchhaltung**: keine
- **Marketing**: keine
- **Personal – HR**: keine
- **Produktion**: keine
- **Projektverwaltung**: keine
- **Revision – Compliance**: keine
- **Terminverwaltung**: keine
- **Verkauf – Vertrieb**: keine
- **Verwaltung**: keine
- **Videoüberwachung**: keine
- **Zeiterfassung**: keine

Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Inkasso: Daten zur Geltendmachung von offenen Forderungen werden für die Dauer von mindestens 10 Jahren gespeichert.
Nach Ablauf von 10 Jahren wird zum Ende des Kalenderjahres geprüft, ob die Forderung noch durchsetzbar ist (Vollstreckungstitel). Sollte ein Vollstreckungstitel bestehen, werden die Daten bis zur Verjährung des Vollstreckungstitels gespeichert, sofern die Forderung nicht zuvor vom Schuldner oder einem Dritten beglichen worden ist.

Internetseite: Nutzungsdaten werden nach spätestens 7 Tagen gelöscht bzw. anonymisiert.
Inhaltsdaten (z.B. Daten, die über ein Kontaktformular übermittelt wurden) werden für einen Zeitraum von 1 Jahr gespeichert. Nach Ablauf des Jahres wird ein weiteres Erfordernis der Speicherung geprüft und eine erneute Prüfung zum Ende jedes Kalenderjahres vorgesehen.
Sollten Inhaltsdaten als Geschäftsbrief einzuordnen sein, gelten die handelsrechtlichen Aufbewahrungspflichten.

Controlling: Daten, die für Zwecke des Controllings verarbeitet werden, werden grundsätzlich für einen Zeitraum von 10 Jahren gespeichert.
Nach Ablauf dieser Zeit wird zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.

Bewerbermanagement: Bewerberdaten werden grundsätzlich nach Ablauf von 6 Monaten nach Vergabe der der jeweiligen Stelle gelöscht. Ausgenommen hiervon sind die Daten der Bewerber, die eine Einwilligung zur weiteren Speicherung der Daten im Bewerberdatenpool erteilt haben. Bei diesen Daten wird nach Ablauf von zwei Jahren geprüft, ob ein Erfordernis für eine weitere Speicherung besteht. Ansonsten werden die Daten gelöscht.

Customer Relationship Management (CRM): Bei personenbezogenen Daten im CRM-System wird nach Ablauf von zwei Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung er-

forderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht. Ausgenommen hiervon sind Daten, die als Geschäftsbriefe i.S.d. HGB bzw. als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweiligen gesetzlichen Aufbewahrungspflichten.

E-Mails werden für mindestens 6 Jahre aufbewahrt, um den handelsrechtlichen Aufbewahrungspflichten für Geschäftsbriefe nachzukommen. Nach Ablauf von 6 Jahren wird zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht. Ausgenommen hiervon sind Daten, die als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweiligen steuerrechtlichen Aufbewahrungspflichten.

Einkauf: Für Daten aus dem Einkauf werden die handelsrechtlichen Aufbewahrungspflichten von 6 Jahren beachtet. Nach Ablauf von 6 Jahren werden die Daten geprüft. Sofern keine Erforderlichkeit für die weitere Speicherung besteht, werden die Daten gelöscht.

Facility Management: Daten über vorgenommen Wartungs- und Pflegearbeiten werden für einen Zeitraum von 4 Jahren gespeichert. Nach Ablauf von vier Jahren wird zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.

Finanzbuchhaltung: Finanzbuchhaltungsdaten werden nach den Vorgaben der Abgabenordnung (AO) mindestens 10 Jahre gespeichert. Für den Beginn der Frist gilt § 147 Abs. 4 AO.

Freelancer Daten werden für einen Zeitraum von 4 Jahren gespeichert. Nach Ablauf von vier Jahren wird zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.

Fuhrparkmanagement: Daten von Beschäftigten, die Fahrzeuge aus dem Fuhrpark nutzen oder nutzen können, werden für die Dauer des Beschäftigungsverhältnisses gespeichert. Die Daten von Betroffenen werden grundsätzlich 4 Jahre nach Beendigung eines Beschäftigungsverhältnisses zum Ende eines Kalenderjahres gelöscht.

IT: Bei personenbezogenen Daten, die im Bereich IT verarbeitet werden, gibt es viele unterschiedliche Speicherfristen. Diese hängen von der jeweiligen Applikation bzw. vom IT-System ab und differieren.
Bei IT-Systemen, mit denen personenbezogene Daten verarbeitet werden, gibt es in der Regel eine Protokollierungsfunktion, mit der nachvollzogen werden kann, "wer" zu "welchem Zeitpunkt" "welche Daten" "eingegeben, verändert oder gelöscht hat. Dieses Protokoll wird in der Regel ab der Löschung des jeweiligen Datensatzes für weitere 4 Jahre gespeichert. Zum Ende eines Kalenderjahres wird jeweils geprüft, ob eine Löschung von Daten erfolgen kann.
Darüber hinaus gilt für allgemein anfallende Daten im Bereich IT (Abwicklung von Aufträgen, Anforderungen etc.), dass bei diesen Daten nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft wird, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.
Ausgenommen hiervon sind Daten, die als Geschäftsbriefe i.S.d. HGB bzw. als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweiligen gesetzlichen Aufbewahrungspflichten.

Kontaktverwaltung: Bei personenbezogenen Daten wird nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.

Lohnbuchhaltung: Zwei Jahre für die Aufzeichnung von Überstunden.
Steuerrelevante Daten werden nach den Vorgaben der Abgabenordnung mindestens 10 Jahre gespeichert. Für den Beginn der Frist gilt § 147 Abs. 4 AO.
Alle anderen Daten werden für einen Zeitraum von zwei Jahren gespeichert; zum Ablauf des Kalenderjahres wird geprüft, ob eine weitere Speicherung erforderlich ist. Sollte ein Erfordernis bestehen, wird jeweils jährlich zum Ende eines Kalenderjahres wieder die Erforderlichkeit überprüft.

Marketing: Bei personenbezogenen Daten, die für Zwecke der Werbung verarbeitet werden, werden grundsätzlich zum Ablauf eines Kalenderjahres Prüfungen im Hinblick auf ein weiteres Erfordernis für die weitere Verarbeitung der Daten vorgenommen.
Abhängig vom Ergebnis werden Daten weiter gespeichert oder gelöscht.

Personal – HR: Abmahnungen: 36 Monate.
Ansonsten wird nach Ablauf von 10 Jahren nach Beendigung des Beschäftigungsverhältnisses geprüft, ob Löschung erfolgen kann. Eine Löschung wird nicht erfolgen, wenn der Beschäftigte eine betriebliche Altersversorgung in Anspruch nehmen möchte oder nimmt.

Produktion: Daten, die im Zusammenhang mit der Produktion anfallen werden für einen Zeitraum von 6 Jahren gespeichert. Grundlage für die Speicherfrist ist, dass Daten aus der Produktion in Verbindung mit Gewährleistungs- und Garantieansprüchen stehen können und für die Abwehr von Forderungen oder für die Prüfung von Ansprüchen erforderlich sein können.
Zudem können Daten aus der Produktion als Geschäftsbrief den Aufbewahrungspflichten aus dem HGB unterliegen.
Die Speicherung der Daten wird im Hinblick auf Datenklassifikationen mindestens jährlich überprüft und angepasst.

Projektverwaltung: Bei personenbezogenen Daten der Projektverwaltung wird nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.
Ausgenommen hiervon sind Daten, die als Geschäftsbriefe i.S.d. HGB bzw. als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweiligen gesetzlichen Aufbewahrungspflichten.

Revision – Compliance: Daten, die für Zwecke der Revision bzw. Compliance verarbeitet werden, werden grundsätzlich für einen Zeitraum von 10 Jahren gespeichert.
Nach Ablauf dieser Zeit wird zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.

Terminverwaltung: Bei personenbezogenen Daten der Terminverwaltung wird nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.
Ausgenommen hiervon sind Daten, die als Geschäftsbriefe i.S.d. HGB bzw. als buchhaltungsrelevante Daten einzuordnen sind. Hier werden die gesetzlichen Aufbewahrungspflichten berücksichtigt.

Verkauf – Vertrieb: Bei personenbezogenen Daten des Verkaufs / Vertriebs ist davon auszugehen, dass diese buchhaltungsrelevant sind. Eine Speicherung erfolgt daher grundsätzlich für 10 Jahre, wobei der Fristbeginn sich nach § 147 Abs. 4 AO richtet.

Verwaltung: Bei personenbezogenen Daten der allgemeinen Verwaltung wird nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.
Ausgenommen hiervon sind Daten, die als Geschäftsbriefe i.S.d. HGB bzw. als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweiligen gesetzlichen Aufbewahrungspflichten.

Videoüberwachung: Videoaufzeichnungen werden nach spätestens 10 Tagen gelöscht.

Zeiterfassung - Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien: Überstunden: 2 Jahre. Steuerrelevante Daten der Arbeitszeiterfassung werden nach den Vorgaben der Abgabenordnung mindestens 10 Jahre gespeichert.
Alle anderen Daten werden für einen Zeitraum von zwei Jahren gespeichert. Zum Ablauf des Kalenderjahres wird geprüft, ob eine weitere Speicherung erforderlich ist. Sollte dies nicht der Fall sein, werden die Daten gelöscht.

Die jeweils einschlägigen Rechtsgrundlagen - Hinweise zur Priorisierung der Compliance Checks der Datenbearbeitungen:

B2B-Unternehmen: die heikelsten Datenbearbeitungen sind meist die eigenen Mitarbeiter, in B2C-Unternehmen die Daten der Konsumenten (Kunden) und die Kernaktivitäten des Unternehmens. Als weniger heikel gelten Daten von Lieferanten und Firmenkunden (auch wenn diese Mitarbeiterdaten enthalten), Daten aus öffentlichen Quellen und Daten, deren Bearbeitung sowieso gesetzlich oder von Dritter Seite genau geregelt ist.

Folgende Kriterien können helfen, besonders heikle Datenbearbeitungen zu identifizieren. Sind zwei davon gegeben, ist dies unter der DSGVO sogar ein Indiz für ein hohes Risiko, was wiederum eine Datenschutz-Folgenabschätzung verlangt:

1. Daten werden vertieft analysiert, es findet ein Scoring oder andere Formen des Profiling statt.
2. Es finden gestützt auf die Daten automatisierte Einzelentscheide statt, die für die betroffene Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
3. Es findet eine systematische Überwachung statt, oder es ist den betroffenen Personen nicht möglich, sich der Datenerhebung zu entziehen.
4. Es werden besondere Kategorien von Personendaten (→ Glossar) der Daten über strafrechtliche Verurteilungen und Straftaten bearbeitet.
5. Daten werden in umfangreicher Weise bearbeitet, sei es im Hinblick auf die Zahl der betroffenen Personen, die Datenmenge und Datenvielfalt, die Zeitdauer bzw. Dauerhaftigkeit der Datenbearbeitung, oder örtliche Ausbreitung der Datenbearbeitung.
6. Es werden verschiedene Datensammlungen und Quellen kombiniert o- der aufeinander abgeglichen.
7. Es werden Daten von besonders schutzbedürftigen Personen wie z.B. Kinder, Arbeitnehmer, Personen mit geistigen Leiden, Asylanten, Patienten, Betagte oder sonst in einem Abhängigkeitsverhältnis stehende Personen bearbeitet.
8. Es wird im Rahmen der Datenbearbeitung auf innovative Technik oder andere neue Organisationsformen gesetzt, deren negative Folgen bzw. Risiken noch nicht vollends bekannt sind.
9. Die Datenbearbeitung dient dazu zu bestimmen, wem eine Leistung oder ein Vertrag angeboten werden soll, oder erschwert sonst die Ausübung von Rechten durch die betroffenen Personen.
10. Könnte eine Datenbearbeitung in der öffentlichen Wahrnehmung als heikel betrachtet werden oder kann sie für eine betroffene Person nachhaltig gewichtige negative Folgen zeitigen, ob bei korrekter oder missbräuchlicher Durchführung, so sollte diese Datenbearbeitung prioritär beurteilt werden.

Beispiele für die Datenbearbeitungen eines mittelgrossen Unternehmens (B2C):

Personalwesen – Personaladministration
Personalwesen – Lohnbuchhaltung
Personalwesen – Rekrutierung
Personalwesen – Sicherheit und Gesundheit
Personalwesen – Schulungsmanagement
Personalwesen – Karriereentwicklung
Marketing & Verkauf – Kundendatenverwaltung
Marketing & Verkauf – Kundenbuchhaltung, Rechnungs- & Zahlungswesen Marketing & Verkauf – Kundenbindungsprogramm

Marketing & Verkauf – Marketing, Kundenanlässe Marketing & Verkauf – Kundendienst
Marketing & Verkauf – Online-Shop
Marketing & Verkauf – App

Marketing & Verkauf – Newsletter
Marketing & Verkauf – Marktforschung

Marketing & Verkauf – Produktentwicklung und -tests Lieferanten & Partner – Lieferantenverwaltung Lieferanten & Partner – Online-Beschaffungsplattform Lieferanten & Partner – Händlerverwaltung, Lieferanten & Partner – Promotoren
Lieferanten & Partner – Vertragsmanagement

Finanzverwaltung – Finanz- und Rechnungswesen,
Finanzverwaltung – Spesenverwaltung
Finanzverwaltung – Immobilien, Finanzanlagen Kommunikation – Interne Kommunikation
Kommunikation – Medienstelle

Kommunikation – Website
Logistik & Betrieb – Videoüberwachung
Logistik & Betrieb – Gebäudezugangskontrollen
Logistik & Betrieb – Besucherdatenverwaltung
Logistik & Betrieb – Flottenmanagement
Logistik & Betrieb – Gebäudemanagement
Informatik – Verzeichnisdienste
Informatik – E-Mail-System
Informatik – Dokumentenablage
Informatik – Netzwerküberwachung
Informatik – Geräteverwaltung
Unternehmen – Rechtswesen
Unternehmen – Administration Aktionariat
Unternehmen – Administration Verwaltungsrat und Geschäftsleitung Unternehmen – Interne Revision
Unternehmen – Interne Untersuchungen