Datenschutz-Spickzettel

|  |  |
| --- | --- |
| Wenn Informationen über natürliche Personen, egal ob sensibel oder nicht, in irgendeiner Weise erfasst gespeichert oder genutzt werden: Datenschutz beachten! [🡪 2] | Kontaktdaten von Ansprechpartnern bei Kunden (B2B) in CRM (Kundendatenbank) speichern, Newsletter an Kunden versenden, Bestellung von Kunden aufnehmen, E-Mail Server betreiben, Ergebnisse aus Mitarbeitergesprächen in Personalakte ablegen, Informationen von Stellenbewerbern aufnehmen |

# Für alle Mitarbeiter

|  |  |  |
| --- | --- | --- |
| 1 | Daten nur in den **gesetzlich erlaubten Fällen** erfassen und nutzen [🡪 5.1.1, 6.1], d.h. soweit es erforderlich ist |  |
|  | a) zur Vertragsabwicklung, oder  | Kontoverbindung der Mitarbeiter zur Gehaltsauszahlung nutzen |
|  | b) zur Erfüllung von Gesetzen, oder | Identifikationsdaten von Vertragspartnern gemäß Geldwäschegesetz abfragen und speichern  |
|  | c) das Unternehmen gute Gründe hat und aus Sicht der Betroffen nichts dagegen spricht, insbesondere diese damit rechnen mussten | geschäftliche Unterlagen eines erkrankten Mitarbeiters Einsehen, um dringende Kundenanfrage zu bearbeiten |
|  | d) die Betroffenen eindeutig und informiert zugestimmt haben [🡪 6.3] | Mitarbeiter erlaubt Nutzung seines Portraits im Intranet, Kunde bestellt Newsletter |
| 2 | Daten zu Gesundheit und Religion und andere **sensible Daten** überhaupt nicht erfassen und verwenden, außer dies ist ausnahmsweise zulässig. [🡪 6.2] | Krankheitsfehlzeiten, Religionszugehörigkeit, Angaben über sexuelle Orientierung |
| 3 | Daten nur für die **Zwecke** verwenden, für die sie ursprünglich gesammelt wurden. [🡪 5.1.3] | Zur Datensicherheit gespeicherte Login- und Logout-Zeiten von Mitarbeitern nicht zur Arbeitszeitkontrolle nutzen. |
| 4 | **Nicht mehr Daten** erfassen und nutzen als für den konkreten Zweck nötig (keine Speicherung auf Vorrat). [🡪 5.1.4] | Die Abfrage von Namen und Arbeitgeber ist für die Zusendung von Newslettern nicht nötig.  |
| 5 | Daten **löschen**, wenn sie nicht mehr benötigt werden. [🡪 5.1.6] | Bewerbungen abgelehnter Kandidaten spätestens 6 Monate nach der Auswahlentscheidung löschen. |
| 6 | Unrichtige oder unvollständige Daten **korrigieren** [🡪 5.1.5] | In Dokumentation zum Mitarbeitergespräch nicht protokollierte Bedenken des Betroffenen ergänzen.  |
| 7 | Bei **Unklarheiten** den **Datenschutzbeauftragten fragen**. [🡪 3.5, 4] | Gilt für IP-Adressen der Datenschutz?  |
| 8 | Wenn Unbefugte Zugang zu Daten erhalten haben, Daten verloren gegangen bzw. nicht mehr verfügbar sind oder unzulässig verändert wurden: **Datenpanne** sofort dem Datensicherheits-Manager melden. [🡪 14] | Verlust oder Diebstahl eines Notebooks, Smartphones oder USB-Sticks, Hackerangriff auf Datenbank, Versand von Personaldaten an falschen E-Mail Empfängerkreis |
| 9 | Daten ausreichend **schützen** vor Zugriff durch Unbefugte, vor Verlust und Verfälschung [🡪 17] | Sichere und unterschiedliche Passwörter wählen, Laptops unterwegs sicher verwahren, Sicherheitskopien erstellen, Daten verschlüsselt speichern, Schreibtisch aufräumen, keine Apps mit unnötigen Berechtigungen installieren |
| 10 | Wenn Kunden oder Mitarbeiter **Ansprüche** in Bezug auf ihre **Daten** erheben, Datenschutz-Manager informieren. [🡪 9] | Kunde verlangt Auskunft, Löschung oder Herausgabe seiner Daten |

# Zusätzlich: Für Mitarbeiter, die für einen Prozess, eine Funktion oder ein Projekt mit Datenschutzrelevanz fachlich konzeptionell verantwortlich sind [🡪 3.2]

|  |  |  |
| --- | --- | --- |
| 1 | Bereits bei der Planung und später der Einführung das **Formular** für den **„Eintrag ins Verzeichnis der Verarbeitungstätigkeiten“** und die **„Checkliste DSGVO“** ausfüllen und dem Datenschutz-Manager übergeben. [🡪 10] | Zeiterfassungssysteme, digitale Personalakten, Videoüberwachung, elektronische Zugangskarten, Bewerberauswahlprozess, Gehaltsabrechnung, Newsletter-Versand, Besucher-Tracking auf Webseiten, Abwicklung von Kundenbestellungen |
| 2 | Den Betroffenen alle gesetzlich geforderten **Informationen** zum Umgang mit ihren Daten geben. [🡪 8] | Datenschutzhinweise auf Webseite platzieren, Datenschutzinformationsblatt für Mitarbeiter erstellen, Datenschutzinfos auf Formularen ergänzen |
| 3 | Sicherstellen, dass die **Datenschutzrechte** der Betroffenen, insbesondere auf Auskunft, Löschung, Sperrung und elektronische Datenherausgabe erfüllt werden können. [🡪 9] | Bei der Anschaffung von Software darauf achten, dass Löschroutinen bestehen und Datensätze gesperrt werden können.  |
| 4 | Wenn **Dienstleister** im Auftrag Daten nach den Vorgaben des Unternehmens verarbeiten, Datenschutz-Manger ansprechen, um mit dem Dienstleister die gesetzlich geforderten **Datenschutzverträge** zu schließen und die Dienstleister zu **überwachen**. [🡪 12] | Verwalten von Daten in Web-basierten Anwendungen (Salesforce, Workforce, SuccessFactors), Speichern von Daten in der Cloud, Nutzung von Webseite-Analyse-Systemen (Google Analytics), Scannen oder Vernichten von Papierdokumenten durch Dienstleister  |
| 5 | Vor einer **Weitergabe** von Daten in **nicht-EU Länder** den Datenschutz-Manager informieren, um die besonderen Anforderungen zum Datenexport zu erfüllen. [🡪 13] | Nutzung des Angebots eines US Cloud-Dienstleisters, Weitergabe von Daten an Konzernunternehmen in den USA |
| 6 | Vorsicht bei diesen Themen: Daten zu **Straftaten** [🡪 5.2], **computergestützte Entscheidungen** [🡪 5.3], **Bonitätsbewertungen** [🡪 5.4] | Abfrage von Vorstrafen, automatisierte Beurteilung von Bewerbern, Einholen von Bonitätsauskünften |
| 7 | Alles so **dokumentieren**, dass die Einhaltung der Datenschutzvorschriften nachweisbar ist. [🡪 16] | Löschprozesse, Berechtigungskonzepte, Einwilligungserklärungen dokumentieren |