Datenschutzkonzept

der

XXX GmbH

Das Datenschutzkonzept dient zur umfassenden Dokumentation der im Unternehmen geltenden Regelungen und ergriffenen Maßnahmen zur Datensicherung. Es hat die datenschutzrechtlichen Aspekte abzubilden und wird als Grundlage für datenschutzrechtliche Prüfungen genutzt. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung vom 25.5.2018 nicht nur gewährleistet werden, sondern auch der Nachweis der Einhaltung geschaffen werden.

Geltungsbereich

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten bei der XXX GmbH. Alle Mitarbeiter sind zur Einhaltung dieser Richtlinie verpflichtet.

Sie richtet sich insbesondere an:

- Die Mitarbeiter, welche personenbezogene Daten verarbeiten (Verantwortlichen)
- Den Datenschutzbeauftragten
- Die Geschäftsführung

Folgende Grundsätze werden befolgt:

- Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs. 1a DS-GVO)
- Datensparsamkeit (Art. 5 Abs. 1 lit. c DS-GVO)
- Zweckbindung (Art. 5 Abs. 1.b DS-GVO) / (Art. 6 Abs. 4 DS-GVO)
- Rechenschaftspflicht (Art 5 Abs. 2 DS-GVO)
- Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)
- Richtigkeit (Art. 5 Abs. 1d DS-GVO)
- Speicherbegrenzung (Art. 5 Abs. 1e DS-GVO)

1 Begriffsdefinitionen

personenbezogene Daten

Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener). Beispiele: Name, Geburtstag, Adressdaten, E-Mail-Inhalte etc..

besondere personenbezogene Daten (sensible Daten)

Angaben über ethnische Herkunft, politische Einstellung, religiöse oder philosophische Überzeugung, Gesundheit etc..

Verantwortlichen

ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

2 Datenschutzbeauftragte/r

Die XXX GmbH hat nach Maßgabe des Art. 37 Abs. 1 DS-GVO einen betrieblichen Datenschutzbeauftragten bestellt (Formblatt 7).

Es handelt sich um: Herrn Gernhuber, Thomas

Dieser nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr.

Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden ist allein der Datenschutzbeauftragte zuständig. Die Dachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen.

Jeder Mitarbeiter der XXX GmbH kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den Datenschutzbeauftragten wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

3 Verzeichnis von Verarbeitungstätigkeiten

Interne Verfahrensverzeichnisse von Verarbeitungstätigkeiten (Formblatt 5) nach Art. 30 DS-GVO stellen eine wichtige Dokumentationsform zur Schaffung von Transparenz innerhalb des Unternehmens aber auch gegenüber Betroffenen dar.

Ohne eine entsprechende aussagekräftige und aktuelle Dokumentation ist sowohl die Gewährleistung der Betroffenenrechte, als auch der Nachweis datenschutzrechtlicher Pflichterfüllung gegenüber den Aufsichtsbehörden aufwändig und vor allem unsicher.

Das Verarbeitungsverzeichnis ist somit gleichermaßen Grundlage zur Erfüllung unternehmerischer Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters und Hilfsmittel der Tätigkeit von deren Datenschutzbeauftragten.

4 Technische und Organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten selbst oder im Auftrag erheben, verarbeiten oder nutzen, haben technische und organisatorische Maßnahmen (Formblatt 8) nach § 9 BDSG zum Schutzzweck zu treffen. Es gilt den besonderen Anforderungen des Datenschutzes gerecht zu werden (Art.24,32 DS-GVO), unter Berücksichtigung der ISO/IEC 27002 sowie ISO/IEC 29151.

Um ein angemessenes Schutzniveau zu bieten werden nachfolgend Maßnahmen aufgelistet, welche die Sicherheit der Verarbeitung gewährleisten:

- Pseudonymisierung und Verschlüsselung der personenbezogenen Daten
- Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten
- Fehlertoleranz und Widerstandsfähigkeit gegenüber Störungen
- Wiederherstellung der Daten und Systeme in der notwendigen Zeit
- regelmäßige Überprüfung in Bezug auf die ergriffenen Maßnahmen

Darüber hinaus werden weitere Sicherheitsmaßnahmen beachtet und befolgt:

- Zutritts-, Zugangs-, und Zugriffskontrollen
- Weitergabe-, Auftrags-, und Verfügbarkeitskontrollen
- Eingabe-, und Zwecksbindungskontrollen

5 Verschwiegenheitserklärung

Für das Unternehmen ist die Wahrung von Betriebsgeheimnissen von existenzieller Bedeutung.

Alle Mitarbeiter der B&S Elektronische Geräte GmbH verpflichten sich zur Wahrung betriebsinterner vertraulicher Information.

Dies gilt sowohl für die Dauer des zwischen den Parteien bestehenden Arbeitsverhältnisses, als auch nach Beendigung des Arbeitsverhältnisses.

Die Mitarbeiter werden gebeten eine schriftliche Verschwiegenheitserklärung (Formblatt 6) zu unterzeichnen sowie zur Kenntnisnahme.

6 Einverständniserklärung

Innerhalb des Unternehmens werden personenbezogene Daten von Mitarbeitern erfasst und verarbeitet.

Die Mitarbeiter wurden über ein Informationsblatt (Formblatt 1) diesbezüglich informiert, wobei eine schriftliche Einverständniserklärung (Formblatt 0) an die Betroffenen zur Kenntnisnahme und Unterzeichnung übergeben worden ist (Art.6 1a,1b).

7 Auftragsverarbeitung

Bei XXX wird die Buchhaltung sowie die Lohnabrechnung extern durch ein Steuerbüro verarbeitet.

Darüber hinaus wird die Website von XXX (www.XXX.com) über YYY GmbH gehostet.

Sobald Verantwortliche Dienstleistungen in Anspruch genommen werden, um personenbezogene Daten in unserem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich gem Art.28 DS-GVO. (Formblatt 9)

Da es sich hierbei nicht um die Verarbeitung von sensiblen Mitarbeiter-Daten handelt, reicht die Auskunft bzw. Information (aus dem Formblatt 1) aus. Die Verantwortlichen müssen den Betroffenen Auskunft über die Erhebung und Verarbeitung (Formblatt 2) ihrer Daten geben.

8 Das Löschen von Daten

Grundsätzlich sind alle Daten zu löschen, wenn sie zur ordnungsgemäßen Erfüllung der jeweiligen Aufgabe nicht mehr benötigt werden. Die Daten und ihre Aufbewahrungsdauer sowie die jeweilige Löschfrist sind aus (Formblatt 3) zu entnehmen.

- Dabei werden Mitarbeiter-Daten, für den Zeitraum des Beschäftigungsverhältnisses aufbewahrt. Die Löschfrist sind 5 Jahre nach Ausscheiden aus dem Arbeitsverhältnis.
- Bewerber-Daten werden für die Dauer des Bewerbungsverfahrens aufbewahrt. Nach Abschluss der Bewerbungsphase werden die Daten vernichtet oder zurückgesendet.
- Sozialversicherungs- und Rentenversicherungsdaten werden dauerhaft aufbewahrt und nicht vernichtet.

- Buchungsbelege, Rechnungen, Lieferscheine, Bilanzen, Jahresabschlüsse, Inventare, Datenblätter usw. werden 10 Jahre aufbewahrt und grundsätzlich aufbewahrt.

9 Sicherheit

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind „Standardmaßnahmen" grundsätzlich ausreichend. Zu diesen Sicherheitsmaßnahmen gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Back-Ups sowie das Scannen von Viren.
Bei der Nutzung von privaten Laptops, ist sicherzustellen, dass nur Zugangsberechtigte auf diverse Daten zugreifen können. Bei der Nutzung des gemeinsamen Internet-Rechners, ist darauf zu achten, dass ebenfalls nur berechtigte Personen der Zugriff gestattet wird. (Formblatt 8)

Darüber hinaus wurde ein IT-Konzept erstellt, bei dem die Schutz-und Sicherheitsmaßnahmen skizziert werden, ebenso wie die Einhaltung derer gem. Art. 32 DS-GVO und § 64 BDSG. (Formblatt 11)

10 Datenschutzverletzungen

Wenn bei der Verarbeitung von personenbezogenen Daten Sicherheitsvorfälle, wie z.B. Diebstahl, Hacking oder Verlust von technischen Daten eintreten, bestehen gesetzliche Meldepflichten.

Im Regelfall erfolgt eine Meldung gem. Art 33 DS-GVO an die Aufsichtsbehörde. (Formblatt 4)

Betroffene Personen sind nur bei hohem Risiko in Kenntnis zu setzten.

Ein solches Risiko kann z. B. durch eine geeignete Verschlüsselung personenbezogener Daten ausgeschlossen werden, die etwa beim Verlust eines Datenträgers die Kenntnisnahme der Daten durch Dritte verhindert.

11 Datenschutz-Folgeabschätzung

Birgt die Art der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko

für die persönlichen Rechte und Freiheiten der betroffenen Person, muss der Verantwortliche bereits vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchführen.

(Formblatt 10)

Ein solches Risiko ist jedoch der Ausnahmefall, weil bei XXX z.B. kein Profiling, keine Verarbeitung besonders sensibler Daten oder umfangreiche Videoüberwachung stattfinden.