Einleitung

Ein Datenschutzprojekt berührt viele Bereiche des Unternehmens, da fast überall personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten oder anderen Personen – den Betroffenen – verarbeitet werden. Aus diesem Grund benötigt ein Datenschutzprojekt zum einen Akzeptanz bei allen Mitarbeitern und zum anderen ein Projektmanagement, damit die Maßnahmen geplant ablaufen.

Ein 10 Punkte-Plan

1. Brauche ich einen Datenschutzbeauftragten?

Ein Datenschutzbeauftragter wird benötigt wenn in der Regel mindestens **10 Personen** mit der automatisierten Verarbeitung beschäftigt sind oder Daten **besonderer Kategorien** (DSFA nötig) verarbeitet werden[1]. Der Datenschutzbeauftragte muss an die zuständige **Landesdatenschutzbehörde gemeldet** und eine **Kontaktmöglichkeit** in der Datenschutzerklärung in **Verträgen** und auf der **Webseite** angegeben werden. Eine E-Mailadresse in der Form datenschutz@meinFirma.de ist ausreichend.

2. Schulen der Mitarbeiter und Verpflichtung auf den Datenschutz

Um die Belegschaft für den Datenschutz zu sensibilisieren, sollen **Schulungen bei der Einstellung und dann regelmäßig** (z:B. jährlich oder anlassbezogen) durchgeführt werden.[2]

Mitarbeiter müssen schriftlich auf den Schutz personenbezogener Daten **verpflichtet** werden.

3. Dokumentation der Verarbeitungstätigkeiten

In der Übersicht der Verarbeitungstätigkeiten werden gemäß einem Kriterienkatalog alle **Prozesse beschrieben, die personenbezogene Daten betreffen**[3]. Hier wird vor allem beschrieben, welche Arten von personenbezogenen Daten verarbeitet werden, von welchen Personengruppen sie stammen, welche Rechtsgrundlage es dafür gibt und wer verantwortlich ist.

4. Technikgestaltung und datenschutzfreundliche Voreinstellungen

Die Verfahren zur Verarbeitung personenbezogener Daten müssen so gestaltet sein, dass nur erforderliche Daten verarbeitet werden. Dies setzt voraus, dass eine klare **Zweckbestimmung** den Umfang bestimmt und **Löschfristen** die Dauer der Speicherung begrenzen. Verfahren wie **Pseudonymisierung** oder **Anonymisierung** tragen dem Grundsatz der **Datenminimierung**[4] Rechnung.

[1] https://dsgvo-gesetz.de/bdsg-neu/38-bdsg-neu/, Selbst-Check LDI: https://bit.ly/2GvgtpO
[2] https://dsgvo-gesetz.de/art-29-dsgvo/
[3] https://dsgvo-gesetz.de/art-30-dsgvo/
[4] https://dsgvo-gesetz.de/art-25-dsgvo/

5. Auftragsverarbeitung

Werden personenbezogene Daten an andere Verantwortliche zur weiteren Bearbeitung gegeben, muss oft[5] ein **Vertrag zur Auftragsverarbeitung** geschlossen werden. Dieser Vertrag regelt nicht nur die Pflichten hinsichtlich des **Ziels der Verarbeitung** sondern auch die **technischen und organisatorische Maßnahmen** zum Schutz der Daten und mögliche **Unterauftragsverhältnisse** oder **Verarbeitungen in Drittstaaten**[6].

6. Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen **regeln die sichere Verarbeitung** der personenbezogenen Daten und müssen **dokumentiert** werden[7]. Diese Dokumentation gehört zu den einzelnen Verarbeitungstätigkeiten und beinhaltet vor allem Informationen zu: Pseudonymisierung und Verschlüsselung personenbezogener Daten, der Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Es muss vor allem ein funktionierendes System zur Datenwiederherstellung eingerichtet sein. Alle diese Maßnahmen müssen einem regelmäßigen Review unterworfen sein.

7. Information und Sicherstellen der Rechte der Betroffenen

Die Betroffenen Personen haben gegenüber dem Verantwortlichen eine Reihe von Rechten über die sie vor Beginn der Verarbeitung informiert werden müssen. Der Verantwortliche muss die Rechtsgrundlagen seiner Verarbeitungen kennen. Wenn die Verarbeitung auf einer **Einwilligung** beruht, **muss** diese **umfassend** über den Verantwortlichen, die Art der Verarbeitung, die Art der Daten, den Zweck, die Speicherdauer, mögliche Empfänger und Drittstaatentransfers **informieren**. Zusätzlich sind die Betroffenen über ihre Rechte bezgl. Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und das Recht auf Datenübertragbarkeit aufzuklären[8].

8. Auskunftsersuchen

Das Recht auf Auskunft[9] zu den über eine Person gespeicherten Daten sowie die Geltendmachung des Rechts auf Datenübertragbarkeit, kann ein Unternehmen vor große Herausforderungen stellen. Hier sollten die verantwortlichen Mitarbeiter oder Abteilungen einen Arbeitsablauf definieren, mit dessen Hilfe den o.g. Gesuchen vollständig und zeitnah entsprochen werden kann.

9. Meldung von Datenschutzvorfällen

Datenschutzvorfälle müssen innerhalb von 72 Stunden an die jeweilige Landesdatenschutzbehörde[10] gemeldet werden. Hierzu sollte ein **Ablaufplan in Form einer**

[5] Ausnahmen: z.B. Behörden, Berufsgeheimnisträger wie: Steuerberater, Ärzte, etc.
[6] https://dsgvo-gesetz.de/art-28-dsgvo/
[7] https://dsgvo-gesetz.de/art-32-dsgvo/
[8] https://dsgvo-gesetz.de/kapitel-3/
[9] https://www.heise.de/newsticker/meldung/DSGVO-Folterfragebogen-im-Selbsttest-3974512.html
[10] https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

Benachrichtigungskette erstellt werden und allen Mitarbeitern der Datenverarbeitung bekannt sein[11].

10. Prozess zur kontinuierlichen Verbesserung

Das Datenschutzprojekt ist eine Sammlung von Dokumentationen und internen Richtlinien. Da diese sich zum einen an der Entwicklung des Unternehmens und zum anderen am jeweiligen Stand der Technik orientieren, ist eine kontinuierliche Anpassung notwendig. Das Projekt wird deshalb gemäß einem PDCA-Zyklus[12] regelmäßig durchlaufen.

[11] https://dsgvo-gesetz.de/art-33-dsgvo/
[12] https://de.wikipedia.org/wiki/Demingkreis