**CHECKLISTE: Bewertung des Datenschutzes im Unternehmen**

**Thema**

**Das ist besonders relevant**

**Erledigt?**

Besteht eine solide Datenschutzorga- nisation?

* Hinterfragen Sie, wie der Datenschutz in Ihrem Unternehmen organisiert ist. Klären Sie insbeson- dere, inwieweit die vorhandene Organisation zu Struktur, Geschäftstätigkeit, Umfang der Verarbei- tung personenbezogener Daten sowie Zahl und Qualifikation der Beschäftigten passt.
* Seien Sie auch selbstkritisch im Hinblick auf Ihre Rolle und Ausstattung als Datenschutzbeauf- tragter. Sind Sie eher „Feigenblatt“ und können Sie Ihre Aufgaben nicht richtig wahrnehmen, ist das ein Problem, das das Unternehmen angehen muss.

q Ja q Nein

Inwieweit ist ein Datenschutzma- nagementsystem (DSMS) umge- setzt?

* Mit einem solchen System werden Strukturen und Prozesse etabliert, um den Datenschutzanfor- derungen gerecht zu werden.
* Typisch sind das systematische Vorgehen und das Ziel, kontinuierlich die Datenschutzsituation zu verbessern. Dazu wird meist auf den PDCA-Kreislauf gesetzt, der für die Phasen Plan, Do, Check, Act steht, also Planen, Umsetzen, Überprüfen und Verbessern.
* Im Fokus sind in erster Linie Regelungen zum Datenschutz, eine Organisation, relevante Prozesse sowie deren Umsetzung und fortlaufende Optimierung.
* Ein solches Managementsystem ist an sich als „strukturiertes und systematisches Vorgehen“ zu verstehen. Gerade bei größeren Unternehmen kann der Einsatz einer entsprechenden Software zur Umsetzung des DSMS vieles erleichtern.

q Ja q Nein

Wie werden Risiken mit Daten- schutzbezug ge- managt?

* Risikomanagement ist in jedem Unternehmen eine unerlässliche Aufgabe, auch im Datenschutz.
* Prüfen Sie, inwieweit Gefahren identifiziert, Risiken bewertet und passende Gegenmaßnahmen festgelegt werden. Dabei sollten Risikoanalysen systematisch ablaufen und klaren Regeln folgen.
* Denken Sie nicht nur an Risiken mit Bezug zum Datenschutz bei der Verarbeitung personenbezo- gener Daten. Blicken Sie auch über den Tellerrand. So sind Mitarbeiter, die nicht über das nötige Know-how verfügen, genauso eine relevante Gefahr wie eine Tür zum Serverraum, die immer sperrangelweit offen steht.

q Ja q Nein

**CHECKLISTE: Bewertung des Datenschutzes im Unternehmen**

Ist ein vollständi- ges und aktuelles Verzeichnis von Verarbeitungstä- tigkeiten vorhan- den?

* Das jeweilige Verzeichnis nach Art. 30 Abs. 1 oder 2 DSGVO ist nötig, um beispielsweise gegen- über der Datenschutzaufsichtsbehörde auskunftsfähig zu sein. Doch es ist auch wichtig für die Arbeit des Datenschutzbeauftragten. Es hilft dabei, den Überblick zu behalten und leichter die Verarbeitungen auszumachen, die einer besonderen Aufmerksamkeit bedürfen.
* Achten Sie auf die Vollständigkeit und Aktualität der Angaben. Manchmal wird das Verzeichnis nur halbherzig geführt. Drängen Sie hier darauf, dass sich das schleunigst ändert.
* Prüfen Sie auch, inwieweit Verarbeitungstätigkeiten ohne Technik (z. B. Verarbeitungen auf Messen, Listen) enthalten sind. Die werden gerne vergessen.

q Ja q Nein

Sind für die Verarbeitungen personenbezoge- ner Daten Risiko- analysen durchge- führt, Maßnahmen abgeleitet und umgesetzt?

* Grundsätzlich ist für jede Verarbeitung personenbezogener Daten eine Risikoanalyse erforderlich. Schließlich lassen sich nur so risikoangemessene technische bzw. organisatorische Maßnahmen auswählen.
* Achten Sie darauf, dass Risikoanalysen nachvollziehbar und dokumentiert sind. Schließlich be- steht auch diesbezüglich die Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO.
* „Einmal Durchführen und dann vergessen“ ist nicht drin. Die Risiken müssen fortlaufend beobach- tet und die Bewertung sowie Maßnahmen müssen ggf. angepasst werden.

q Ja q Nein

Ist die Einhaltung der Grundsätze der Verarbeitung per- sonenbezogener Daten Standard?

* Jede Verarbeitung personenbezogener Daten muss die Grundsätze aus Art. 5 Abs. 1 DSGVO ein- halten.
* Schauen Sie, inwieweit die Prüfung der Grundsätze bzw. der daraus abgeleiteten Anforderungen aus der DSGVO in Regelungen und Prozessen verpflichtend ist.

q Ja q Nein

Inwieweit wird

„Data protection by design and de- fault” umgesetzt?

* Damit Datenschutz von Anfang an mitgedacht und schon bei der Gestaltung berücksichtigt wird, müssen die Vorgaben aus Art. 25 DSGVO beachtet werden.
* Schauen Sie sich an, inwieweit Leitfäden oder Vorgaben für Projekte und IT-Vorhaben entspre- chende Vorgaben machen.
* Meist ist es unerlässlich, dass Sie als Datenschutzbeauftragter schon in der Ideenphase eingebun- den werden. Nur so werden Anforderungen frühzeitig bedacht.

q Ja q Nein

Sind die nötigen Datenschutz-Fol- genabschätzungen durchgeführt?

* Prüfen Sie, welche Regelungen es zu diesem Aspekt gibt und wie das Vorgehen aussieht.
* Entscheidend ist nicht nur, dass Folgenabschätzungen durchgeführt werden. Mindestens genauso wichtig ist, dass man Sie zur Beratung hinzuzieht (Art. 35 Abs. 2 DSGVO). Das sollte als klare An- weisung geregelt sein.
* Halten Sie im Verzeichnis von Verarbeitungstätigkeiten Ausschau nach relevanten Verarbeitungen und prüfen Sie, ob die Folgenabschätzungen dokumentiert und mit dem nötigen Inhalt (Art. 35 Abs. 7 DSGVO) durchgeführt wurden.

q Ja q Nein

Sind Prozesse zur richtigen Reaktion auf Zwischen-, Not- und Katastrophen- fälle eingerichtet?

* Um für den Fall der Fälle vorbereitet zu sein, braucht es entsprechende Pläne und Prozesse sowie die erforderlichen qualifizierten Mitarbeiter.
* Haben Sie insbesondere ein Auge auf Regelungen und Prozesse mit Bezug zum Datenschutz, bei- spielsweise zum Vorgehen bei Datenpannen oder bei einem Hackerangriff.

q Ja q Nein

Wie werden Be- troffenenrechte gemanagt?

* Hier sind klare Vorgaben zum Vorgehen unerlässlich. So sollte es Prozesse zur Bearbeitung an sich sowie speziell z. B. zum Vorgehen bei Auskunft oder Löschung geben.
* Schauen Sie, wie es um das Wissen bei besonders relevanten Stellen steht. Das sind vor allem Kol- legen, bei denen Betroffenenanfragen eingehen, etwa der Kundenservice oder die Poststelle.
* Auch diejenigen, die Betroffenenrechte umsetzen, müssen über alles Relevante Bescheid wissen.

q Ja q Nein

Werden Beschäf- tigte im angemes- senen Umfang ge- schult, qualifiziert und sensibilisiert?

* Generell gilt: Wer Bescheid weiß, macht weniger falsch und erkennt Gefahren, bevor sie zum Pro- blem werden. Also sollte jeder Mitarbeiter über das für seine Aufgabe nötige Datenschutz-Know- how verfügen.
* Schauen Sie, inwieweit es ein Schulungs- und Sensibilisierungskonzept gibt. Auch hier sollte sich die Risikoorientierung widerspiegeln. Außerdem ist das Dokumentieren wichtig.
* Klären Sie, inwieweit sichergestellt ist, dass es keine „Durchrutscher“ bei den zu sensibilisierenden Mitarbeitern gibt. Auch im Datenschutz gilt: Eine Kette ist nur so stark wie ihr schwächstes Glied.

q Ja q Nein

Sind Dienstleister sorgfältig ausge- wählt und passen die vereinbarten Schutzmaßnah- men?

* Meist gibt es Festlegungen zur Auswahl von Dienstleistern. Klären Sie, inwieweit hier auch der Datenschutz eine Rolle spielt. Ist das nicht der Fall, muss das Thema Datenschutz integriert oder ein spezifischer Prozess aufgesetzt werden.
* Achten Sie darauf, dass etwa im Verzeichnis von Verarbeitungstätigkeiten auch die beauftragten Dienstleister aufgeführt sind. Idealerweise sind die vereinbarten spezifischen Schutzmaßnahmen vermerkt oder verlinkt.

q Ja q Nein

Bestehen Aufbe- wahrungs- und Löschkonzepte?

* Kennzeichnend für den Datenschutz ist, dass personenbezogene Daten nicht für immer und ewig verarbeitet werden dürfen.
* Damit der Löschpflicht aus Art. 17 DSGVO nachgekommen wird, müssen Fristen festgelegt und eine Löschung auch tatsächlich umgesetzt werden.

q Ja q Nein