**CHECKLISTE: Wichtige Aspekte bei der Verarbeitung sensibler Daten**

**Aspekt**

**Hintergrund**

**Geprüft und in Ordnung?**

Welche personenbezoge- nen Daten sollen verarbei- tet werden?

* Am besten lassen Sie sich alle Daten möglichst konkret nennen. Zu allgemeine Beschrei- bungen wie z. B. „Kundendaten“ helfen hier meist nicht weiter.
* Fordern Sie im Bedarfsfall eine Auflistung mit Beispielen.

q Ja q Nein

Inwieweit handelt es sich um Daten im Sinne von Art. 9 Abs. 1 DSGVO?

* Bewerten Sie gemeinsam mit den Kollegen, inwieweit einzelne Daten als besondere Kate- gorien personenbezogener Daten einzustufen sind.
* Prüfen Sie auch, ob in Zusammenhang stehende Daten dazu führen, dass zunächst unprob- lematische Daten(sätze) zu sensiblen Informationen werden.

q Ja q Nein

In welcher Beziehung ste- hen die Betroffenen zum Verantwortlichen?

* Lassen Sie sich erläutern, in welcher Beziehung Ihr Unternehmen zum Betroffenen steht.
* Hinterfragen Sie, inwieweit es sich bei den Betroffenen um Beschäftigte handelt. Dabei ist wichtig: Der Begriff des Beschäftigten ist weiter, als es zunächst erscheint. Prüfen Sie gemeinsam § 26 Abs. 8 BDSG.

q Ja q Nein

Auf welche Rechtsgrund- lage soll die Verarbeitung der personenbezogenen Daten an sich bzw. der sensiblen personenbezo- genen Daten im Speziel- len gestützt werden?

* Geht es um die Verarbeitung „normaler“ persönlicher Informationen, sollte Ihr Blick in Richtung Art. 6 Abs. 1 Satz 1 DSGVO gehen. Bei sensiblen Daten muss eine Ausnahme vom Verarbeitungsverbot (Art. 9 Abs. 1 DSGVO) greifen, etwa nach Art. 9 Abs. 2 DSGVO bzw. § 22 Abs. 2 BDSG.
* Bei sensiblen Beschäftigtendaten sollten Sie insbesondere ein Auge auf die Voraussetzun- gen des § 26 Abs. 3 und 4 BDSG haben.

q Ja q Nein

Wie werden die Grund- sätze der Verarbeitung personenbezogener Daten umgesetzt?

* Alle Grundsätze sind auch bei der Verarbeitung sensibler Daten von großer Bedeutung. Schauen Sie jedoch insbesondere auf die Aspekte Rechtmäßigkeit, Zweckbindung, Daten- minimierung und Vertraulichkeit.
* Klären Sie auch, wie man nachweist, dass die Grundsätze eingehalten und umgesetzt sind. Diese Rechenschaftspflicht ergibt sich aus Art. 5 Abs. 2 DSGVO.

q Ja q Nein

Welche risikoangemesse- nen Schutzmaßnahmen sind vorgesehen und um- gesetzt?

* Um die passenden technischen bzw. organisatorischen Maßnahmen auszuwählen, müssen zunächst die Risiken ausgemacht und bewertet sein. Lassen Sie sich die Risikoanalyse erklären.
* Die Maßnahmen nach Art. 32 DSGVO müssen risikoangemessen sein. Bei sensiblen Daten kommen weitere Anforderungen hinzu. Denken Sie hier an die Vorgaben die etwa § 22 Abs. 2 BDSG für bestimmte Fälle macht. Diese Vorgaben gelten auch bei sensiblen Daten im Beschäftigungskontext (§ 26 Abs. 3 Satz 3 DSGVO).

q Ja q Nein

Inwieweit ist eine Daten- schutz-Folgenabschätzung (DSFA) erforderlich?

* Klären Sie die Erforderlichkeit aufgrund Art. 35 DSGVO bzw. auf Basis der Vorgaben der deutschen Aufsichtsbehörden im Rahmen der sogenannten DSFA-Muss-Liste.
* Wurde eine Folgenabschätzung durchgeführt, prüfen Sie, inwieweit Sie eingebunden waren. Das ist Pflicht (Art. 35 Abs. 2 DSGVO).
* Prüfen Sie, ob die DSFA den Mindestanforderungen nach Art. 35 Abs. 7 entspricht.

q Ja q Nein

Wie werden die Betroffe- nenrechte umgesetzt?

* Schauen Sie sich mit den Kollegen die Art. 12 ff. DSGVO an. Sprechen Sie durch, wie bei- spielsweise die Transparenz oder das Recht auf Auskunft oder Löschung umgesetzt werden.
* Hinterfragen Sie die Prozesse. Aufgrund der Sensibilität der Daten muss etwa bei der Klärung der Identität eines Betroffenen im Rahmen einer Auskunft sorgfältiger vorgegangen werden.

q Ja q Nein

Welche Regelungen und Arbeitsanweisungen sind festgelegt, kommuniziert und in Kraft?

* Sehen Sie sich die Festlegungen an. Prüfen Sie diese auf Vollständigkeit und Aktualität.
* Nur wenn Regelungen bekannt sind, können Sie auch beachtet werden. Klären Sie, wo die Regelungen zu finden sind.

q Ja q Nein

Wie werden die zuständi- gen Beschäftigten sensibi- lisiert und trainiert?

* Das ist unerlässlich, damit keine Fehler passieren. Die wären gerade bei sensiblen Daten besonders kritisch.
* Lassen Sie sich z. B. Schulungsmaterial vorlegen. Prüfen Sie, inwieweit das der Sache und der Schutzwürdigkeit der Daten gerecht wird.

q Ja q Nein

Welche Eintragungen wur- den im Verzeichnis von Verarbeitungstätigkeiten vorgenommen?

* Das Verzeichnis nach Art. 30 Abs. 1 DSGVO muss vollständig und aktuell sein. Werfen Sie einen Blick in die Eintragungen.
* Passt etwas nicht, adressieren Sie die entsprechende Aufgabe an die zuständigen Kollegen.

q Ja q Nein

Wie wird die Verarbeitung fortlaufend auf Vereinbar- keit mit dem Datenschutz kontrolliert?

* Gerade Risiken können sich im Laufe der Zeit ändern, sodass die Schutzmaßnahmen an- gepasst werden müssen. Lassen Sie sich erläutern, was man in diesem Zusammenhang unternimmt.
* Legen Sie großen Wert auf die Dokumentation der Prüfung. Auch das ist Teil der Rechen- schaftspflicht.

q Ja q Nein