PRIVACYXPERTS

CHECKLISTE: Bewertung des Datenschutzes im Unternehmen

Thema	Das ist besonders relevant	Erledigt?
Besteht eine solide Datenschutzorganisation?	› Hinterfragen Sie, wie der Datenschutz in Ihrem Unternehmen organisiert ist. Klären Sie insbesondere, inwieweit die vorhandene Organisation zu Struktur, Geschäftstätigkeit, Umfang der Bearbeitung von Personendaten sowie Zahl und Qualifikation der Beschäftigten passt. › Seien Sie auch selbstkritisch im Hinblick auf Ihre Rolle und Ausstattung als Datenschutzberater. Sind Sie eher „Feigenblatt" und können Sie Ihre Aufgaben nicht richtig wahrnehmen, ist das ein Problem, das das Unternehmen angehen muss.	○ Ja ○ Nein
Inwieweit ist ein Datenschutzmanagementsystem (DSMS) umgesetzt?	› Mit einem solchen System werden Strukturen und Prozesse etabliert, um den Datenschutzanforderungen gerecht zu werden.Tabelle-Muster-Auflistung › 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.	○ Ja ○ Nein
Wie werden Risiken mit Datenschutzbezug gemanagt?	› 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 Bearbeitung von Personendaten. 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.	○ Ja ○ Nein
Ist ein vollständiges und aktuelles Verzeichnis von Bearbeitungstätigkeiten vorhanden?	› Das betreffende Verzeichnis nach Art. 12 DSG ist nötig, um beispielsweise gegen über der Datenschutzaufsichtsbehörde auskunftsfähig zu sein. Doch es ist auch wichtig für die Arbeit des Datenschutzberaters. Es hilft dabei, den Überblick zu behalten und leichter die Bearbeitungen 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 Bearbeitungstätigkeiten ohne Technik (z. B. Bearbeitungen auf Messen, Listen) enthalten sind. Die werden gerne vergessen.	○ Ja ○ Nein
Sind für die Bearbeitungen von Personendaten Risikoanalysen durchgeführt, Massnahmen abgeleitet und umgesetzt?	› Grundsätzlich ist für jede Bearbeitung von Personendaten Daten eine Risikoanalyse erforderlich. Schliesslich lassen sich nur so risikoangemessene technische bzw. organisatorische Massnahmen auswählen. › Achten Sie darauf, dass Risikoanalysen nachvollziehbar und dokumentiert sind. Dann sind Sie auf der sicheren Seite. › „Einmal Durchführen und dann vergessen" ist nicht drin. Die Risiken müssen fortlaufend beobachtet und die Bewertung sowie Massnahmen müssen ggf. angepasst werden.	○ Ja ○ Nein
Ist die Einhaltung der Grundsätze der Bearbeitung von Personendaten Standard?	› Jede Bearbeitung von Personendaten muss die Grundsätze aus Art. 6 DSG einhalten. › Schauen Sie, inwieweit die Prüfung der Grundsätze bzw. der daraus abgeleiteten Anforderungen aus dem DSG in Regelungen und Prozessen verpflichtend ist.	○ Ja ○ Nein
Inwieweit wird „Data protection by design and default" umgesetzt?	› Damit Datenschutz von Anfang an mitgedacht und schon bei der Gestaltung berücksichtigt wird, müssen die Vorgaben aus Art. 7 DSG beachtet werden. › Schauen Sie sich an, inwieweit Leitfäden oder Vorgaben für Projekte und IT-Vorhaben entsprechende Vorgaben machen. › Meist ist es unerlässlich, dass Sie als Datenschutzberater schon in der Ideenphase eingebunden werden. Nur so werden Anforderungen frühzeitig bedacht.	○ Ja ○ Nein
Sind die nötigen Datenschutz-Folgenabschätzungen 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. Das sollte am besten als klare Anweisung geregelt sein. › Halten Sie im Verzeichnis von Bearbeitungstätigkeiten Ausschau nach relevanten Bearbeitungen und prüfen Sie, ob die Folgenabschätzungen dokumentiert und mit dem nötigen Inhalt (Art. 22 Abs. 3 DSG) durchgeführt wurden.	○ Ja ○ Nein

Sind Prozesse zur richtigen Reaktion auf Zwischen-, Not- und Katastrophenfälle 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, beispielsweise zum Vorgehen bei Datenpannen oder bei einem Hackerangriff.	○ Ja ○ Nein
Wie werden Betroffenenrechte 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 Kollegen, bei denen Betroffenenanfragen eingehen, etwa der Kundenservice oder die Poststelle. › Auch diejenigen, die Betroffenenrechte umsetzen, müssen über alles Relevante Bescheid wissen.	○ Ja ○ Nein
Werden Beschäftigte im angemessenen Umfang geschult, qualifiziert und sensibilisiert?	› Generell gilt: Wer Bescheid weiss, macht weniger falsch und erkennt Gefahren, bevor sie zum Problem 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.	○ Ja ○ Nein
Sind Dienstleister sorgfältig ausgewählt und passen die vereinbarten Schutzmassahmen?	› 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 Bearbeitungstätigkeiten auch die beauftragten Dienstleister aufgeführt sind. Idealerweise sind die vereinbarten spezifischen Schutzmassahmen vermerkt oder verlinkt.	○ Ja ○ Nein
Bestehen Aufbewahrungs- und Löschkonzepte?	› Kennzeichnend für den Datenschutz ist, dass Personendaten nicht für immer und ewig bearbeitet werden dürfen. › Damit der Löschpflicht aus Art. 32 Abs. 2 Buchst. c DSG nachgekommen wird, müssen Fristen festgelegt und eine Löschung auch tatsächlich umgesetzt werden.	○ Ja ○ Nein