

Checkliste Datenschutzaudit

Die Aufgaben der/des Datenschutzbeauftragten umfassen:

1. Mitarbeiter

1.1 Werden die Mitarbeiter regelmäßig, d.h. mindestens alle 2 Jahre, im Datenschutz geschult?

- Ja
- Nein

1.2 Sind die Mitarbeiter bereits über das neue Datenschutzrecht (Europäische Datenschutzgrundverordnung, in Kraft seit 25.Mai 2018) in seinen Grundzügen informiert worden?

- Ja
- Nein

1.3 Sind die Schulungen für jeden Mitarbeiter dokumentiert worden?

- Ja
- Nein

1.4 Wird eine Geburtstagsliste der Mitarbeiter geführt und wurde in diese eingewilligt?

- Ja
- Nein

1.5 Werden oder sind personenbezogene Daten von Mitarbeitern auf Webseiten oder in Prospekten veröffentlicht und liegen hierfür entsprechend dokumentierte Einwilligungen vor?

- Ja
- Nein

1.6 Findet eine Videoüberwachung statt?

- Ja
- Nein

Folgende vier Fragen von Ziffer 1.7 bis Ziffer 1.10 bitte nur beantworten, wenn die Antwort auf die Frage 1.6 „Ja“ lautete.

1.7 Wird auf die Videoüberwachung deutlich hingewiesen?

- Ja
- Nein

1.8 Werden die Aufzeichnungsbereiche auf das Erforderliche beschränkt und die übrigen Bereiche verpixelt bzw. auf andere Weise von der Aufnahme ausgeschlossen?

- Ja
- Nein

1.9 Werden die von der Videoüberwachung betroffenen Personen benachrichtigt?

- Ja
- Nein

1.10 Existieren Löschroutinen für die Aufnahmen? Wenn ja, in welchen Intervallen?

- Ja, Intervall: _____
- Nein

1.11 Gibt es eine schriftliche Regelung/Vorgabe zur privaten Nutzung des Internets im Unternehmen?

- Ja
- Nein

1.12 Gibt es eine schriftliche Regelung zur privaten Nutzung der beruflichen E-Mailadresse im Unternehmen?

- Ja
- Nein

1.13 Werden die Mitarbeiterdaten nach Ausscheiden des Mitarbeiters bis auf die Nutzung für die Ausstellung eines Arbeitszeugnisses, Wahrung gesetzlicher Aufbewahrungsfristen und Erfüllung betrieblicher Versorgungsansprüche für alle sonstigen Verarbeitungen gesperrt?

- Ja
- Nein

2. Datenschutzbeauftragter („DSB“)

2.1 Sind mindestens 20 Personen bei Ihnen beschäftigt, die Zugriff auf personenbezogene Daten haben?

- Ja
- Nein

Folgende Fragen bis zum Ende dieser Ziffer 2 bitte nur beantworten, wenn die Antwort auf die Frage 2.1 „Ja“ lautete.

2.2 Wenn mindestens 20 Personen bei Ihnen beschäftigt sind, ist ein Datenschutzbeauftragter bestellt?

- Ja
- Nein

2.3 Ist die erforderliche Fachkunde des DSB z.B. durch Ausbildung oder Teilnahme an Datenschutzseminaren nachweisbar?

- Ja
- Nein

2.4 Wird der DSB personell hinreichend unterstützt?

- Ja
- Nein

2.5 Ist die fachliche Unabhängigkeit des DSB aufgrund seiner Stellung und sonstig gewährleistet (Freistellen von potenziellen Interessenskonflikten)?

- Ja
- Nein

2.6 Ist der DSB direkt der Geschäftsleitung unterstellt bzw. existiert zu ihr eine direkte Berichtslinie?

- Ja
- Nein

2.7 Bildet sich der DSB regelmäßig fort (Schulung, Literatur, etc.)?

- Ja
- Nein

2.8 Behandelt der DSB die Anliegen Ihrer Mitarbeiter vertraulich oder kam es hier zu Vorfällen?

- Ja
- Nein

2.9 Wird der DSB in alle Prozesse mit Datenschutzbezug involviert?

- Ja
- Nein

3. Datenverarbeitungsprozesse

3.1 Sind alle Prozesse der Datenerhebung und -verarbeitung bei der Organisation dokumentarisch erfasst und geprüft?

- Ja
- Nein

3.2 Besteht zu diesen Prozessen ein Verarbeitungsverzeichnis? (früher: Verfahrensverzeichnis)

- Ja
- Nein

3.3 Ist gewährleistet, dass bei Änderung bisheriger Prozesse (z.B. neue Technologie) oder der Einführung neuer Prozesse das Verarbeitungsverzeichnis angepasst wird?

- Ja
- Nein

3.4 Ist ein fortlaufender Prüf- und Dokumentationsprozess für die Einhaltung datenschutzrechtlicher Vorgaben (Planung, Umsetzung, Kontrolle, Optimierung) vorhanden?

- Ja
- Nein

3.5 Ist ein fortlaufender Prüf- und Dokumentationsprozess für Datensicherheitsvorgaben (IT-Compliance) vorhanden?

- Ja
- Nein

3.6 Finden in Ihren Unternehmen vollautomatisierte Entscheidungen (d.h. Entscheidungen, die ohne menschliches Zutun aufgrund eingegebener Parameter getroffen werden) statt, die nicht im Zusammenhang mit der Anbahnung oder Durchführung eines Vertrags stehen oder die nicht aufgrund von Einwilligungen gerechtfertigt sind?

- Ja
- Nein

3.7 Finden bei Ihnen vollautomatisierte Entscheidungen im Hinblick auf sensible Daten (z.B. Gewerkschaftszugehörigkeit, sexuelle Orientierung, rassische oder ethnische Herkunft, Gesundheitsdaten, politische Meinung, biometrische und genetische Daten, Weltanschauung und Religionszugehörigkeit) statt?

- Ja
- Nein

3.8 Finden bei Ihnen vollautomatisierte Auswertungen von Daten anhand von Algorithmen statt, deren Ziel es ist, Verhaltenstypen oder bestimmte Verhaltensweisen von Menschen zu analysieren bzw. vorherzusagen?

- Ja
- Nein

4. Datenbanken

4.1 Welche Datenbanken gibt es?

- Teilnehmerdatenbank
 - Mitarbeiterdatenbank
 - Bewerberdatenbank
 - Dozentendatenbank
 - Interessentendatenbank
 - Robinsonliste (Liste mit Teilnehmern, die keine Werbung erhalten wollen)
 - Weitere Datenbanken bitte hier aufzählen:
-

4.2 Sind alle Datenbanken im Verarbeitungsverzeichnis erfasst?

- Ja
 - Nein
-

- 4.3 Bestehen Löschkonzepte zu den hierin enthaltenen Daten und sind diese dokumentiert?
- Ja
 - Nein
- 4.4 Ist die Erhebung, Speicherung und Verwendung der einzelnen Daten datenschutzrechtlich gerechtfertigt?
- Ja
 - Nein
- 4.5 Haben Dritte (hierzu zählen auch verbundene Unternehmen oder Provider) Zugriff auf diese Datenbanken?
- Ja
 - Nein
- 4.6 Bestehen hierfür entsprechende Berechtigungen oder Auftragsverarbeitungsverträge?
- Ja
 - Nein

5. IT-Systeme und Zertifizierung

- 5.1 Sind die vorgenannten Datenbanken ausreichend technisch geschützt?
- Ja
 - Nein
- 5.2 Gibt es eine kontinuierliche Risiko- und Schwachstellenanalyse im Hinblick auf Räume, IT-Systeme, IT-Applikationen und Netzwerkkomponenten?
- Ja
 - Nein
- 5.3 Existieren Zertifizierungen (z.B. nach ISO 27001)? Wenn ja, welche?
- Ja, und zwar: _____
 - Nein
- 5.4 Existieren Re-Zertifizierungsprozesse? Wenn ja, in welchem zeitlichen Abstand?
- Ja
 - Nein

6. Aufbewahrungs-, Sperrungs- und Löschpflichten

6.1 Werden Daten Minderjähriger gespeichert?

- Ja
- Nein

6.2 Werden Betroffenenrechte (Auskunft, Berichtigung, Löschung, Widerspruch gegen Datenverarbeitungen, Widerruf von Einwilligungen, Sperrung, Datenübertragung) wirksam umgesetzt und dokumentiert?

- Ja
- Nein

6.3 Wird über das Widerspruchsrecht deutlich getrennt von den übrigen Informationen (z.B. durch Absatz und/oder Fettdruck) informiert?

- Ja
- Nein

6.4 Wird über das Beschwerderecht bei einer Datenschutzbehörde informiert?

- Ja
- Nein

6.5 Erfolgt vor der Entscheidung, Daten zu anderen Zwecken weiter zu verarbeiten, eine Prüfung der Zulässigkeit dieser Weiterverarbeitung?

- Ja
- Nein

6.6 Wenn die Weiterverarbeitung der Daten zu anderen Zwecken als zulässig erachtet wurde, werden die Betroffenen hierüber informiert?

- Ja
- Nein

6.7 Werden die Daten gesperrt, soweit sie für vertragliche Zwecke nicht mehr benötigt werden?

- Ja
- Nein

6.8 Werden Bewerber auf die Zwecke der Verarbeitung und Löschung ihrer Daten hingewiesen?

- Ja
- Nein

6.9 Wird die Speicherung und Nutzung von Bewerberdaten auf das zur Durchführung des Bewerbungsverfahrens Erforderliche beschränkt?

- Ja
- Nein

6.10 Werden Bewerberdaten nach Absage gelöscht?

- Ja
- Nein

7. Datenverarbeitung unter Einbezug Dritter, insbesondere auch von Unternehmen aus dem Ausland

7.1 Existiert ein interner Prozess, wonach im Falle des Outsourcings bestimmter Dienstleistungen die Teilnehmer/Mitarbeiter hierüber informiert werden? Ist dieser dokumentiert?

- Ja
- Nein

7.2 Existiert ein interner Prozess, wonach vor Auswahl und Beauftragung eines bestimmten Dienstleisters dessen Datenschutzkonzept, insbesondere im Hinblick auf die Geeignetheit und Angemessenheit der Datenschutz- und Datensicherheitsmaßnahmen, geprüft und das Prüfungsergebnis dokumentiert wird?

- Ja
- Nein

7.3 Werden Dienstleister nach Beauftragung regelmäßig im Rahmen einer Stichprobenkontrolle (mind. 1x/Jahr) im Hinblick auf Datenschutz und Datensicherheit überprüft? Wird das Prüfungsergebnis dokumentiert?

- Ja
- Nein

7.4 Werden Dienstleister außerhalb der EU und des EWR aus Ländern mit Bescheinigung eines angemessenen Datenschutzniveaus beauftragt, z.B. im Rahmen von Cloud-Diensten?

- Ja
- Nein

7.5 Findet im Falle beabsichtigter Kooperationen mit Unternehmen außerhalb der EU und des EWR eine Vorabprüfung im Hinblick auf das Vorhandensein eines angemessenen Datenschutzniveaus (Kommissionsentscheidungen, wie z.B. das EU-US-Privacy Shield) in dem Land, in dem das Unternehmen sitzt, statt?

- Ja
- Nein

7.6 Werden gegenüber dritten Dienstleistern erteilte Weisungen dokumentiert?

- Ja
- Nein

8. Prüfung vorhandener Dokumente und Vereinbarungen zum Datenschutz

8.1 Existieren bei Ihnen Verhaltensregeln zum Datenschutz (z.B. in Form eines Code of Conduct oder einer internen Richtlinie) und sind diese für 2019 aktualisiert?

- Ja
- Nein

8.2 Existieren Betriebsvereinbarungen, die auch die Verarbeitung und Verwendung personenbezogener Daten regulieren und sind diese aktualisiert?

- Ja
- Nein

8.3 Ist die Datenschutzerklärung auf der Webseite jederzeit abrufbar und auf das neue Recht angepasst?

- Ja
- Nein

8.4 Ist das Impressum auf das neue Recht angepasst, insbesondere ein Kontakt zum DSB angegeben?

- Ja
- Nein

8.5 Werden auf der Webseite Cookies oder Social Plugins verwendet und sind diese ausreichend dokumentiert in der Datenschutzerklärung und auf der Webseite?

- Ja
- Nein

8.6 Bestehen mit Drittanbietern von Cookies aktualisierte Auftragsverarbeitungsverträge?

- Ja
- Nein

8.7 Bestehen datenschutzrechtliche Vereinbarungen mit Dozenten hinsichtlich der Verwendung der Teilnehmerdaten?

- Ja
- Nein

8.8 Bestehen mit sonstigen Dienstleistern erforderliche Auftragsverarbeitungsverträge bzw. Vereinbarungen zur gemeinsamen Verantwortlichkeit hinsichtlich der Datenverarbeitung?

- Ja
- Nein

9. Vorgehen bei Datenschutzverstößen und Datenpannen

9.1 Gibt es einen Krisenplan zum Vorgehen bei Datenschutzverstößen, der fortlaufend auf Effektivität und Angemessenheit überprüft wird?

- Ja
- Nein

9.2 Gibt es einen Ablaufplan für den Fall eines Datenschutzverstoßes bzw. einer Datenpanne zur Eingrenzung/Vermeidung der unbefugten Kenntnismittel Dritter?

- Ja
- Nein

9.3 Ist für die notwendigen Fälle eine Meldung an die Datenschutzaufsichtsbehörde bzw. den Betroffenen vorgesehen?

- Ja
- Nein

9.4 Ist bei Datenschutzverletzungen sichergestellt, dass Fakten, Auswirkungen und Maßnahmen dokumentiert werden?

- Ja
- Nein

10. Nachweis- und Dokumentationspflichten

10.1 Gibt es eine schriftliche Dokumentation der technischen und organisatorischen Maßnahmen? (z.B. Zutrittskontrolle, Zugriffskontrolle, Eingabekontrolle, Weitergabekontrolle etc.)

- Ja
- Nein

10.2 Gibt es einen Prozess, wonach die Effektivität und Angemessenheit dieser Maßnahmen (z.B. gestuft nach Risikoklassen) fortlaufend überprüft, dokumentiert und ggf. angepasst wird (regelmäßiges Datenschutzaudit)?

- Ja
- Nein

10.3 Wird von Werbemaßnahmen mit Einwilligung des Betroffenen hinreichend Gebrauch gemacht (d.h. keine Pausen von mehr als 18 Monaten)?

- Ja
- Nein

10.4 Gibt es eine Dokumentation der von jeder der Organisation getroffenen Werbemaßnahmen?

- Ja
- Nein

10.5 Besteht ein Berechtigungskonzept für die Zugriffsmöglichkeiten auf Teilnehmerdaten?

- Ja
- Nein

11. Neue Datenverarbeitungsprozessen und -produkte

11.1 Wird vor der Einführung bzw. Änderung von Datenverarbeitungsprozessen, in denen massenhaft Daten (z.B. CRM Anwendungen) bzw. sensible Daten (z.B. Gehaltsdaten, Krankengeschichte, Kontendaten, Nichtbestehen von Prüfungen, Anzahl von Prüfungsversuchen etc.) verarbeitet werden, eine Prüfung vorgenommen, welche Risiken für die Betroffenen entstehen können, wie wahrscheinlich deren Realisierung ist, welche risikominimierenden Maßnahmen insoweit zu ergreifen sind und ob die Datenverarbeitungsprozesse erforderlich und angemessen sind (sog. Datenschutzfolgenabschätzung)?

- Ja
- Nein

11.2 Wird der DSB vor der Einführung neuer bzw. Änderung bestehender Prozesse (z.B. Erweiterung eines Softwarepaktes, Erwerb neuer Software, Erweiterung des Dienstleistungsangebots) konsultiert?

- Ja
- Nein

11.3 Wird bei der Planung oder Änderung eines bestehenden Datenverarbeitungsprozesses das Prinzip der Datensparsamkeit und der Möglichkeit von Voreinstellungen ausreichend berücksichtigt?

- Ja
- Nein

11.4 Gibt es einen Prozess, wonach die Effektivität und Angemessenheit dieser Maßnahmen fortlaufend überprüft, dokumentiert und ggf. angepasst wird (regelmäßiges Datenschutzaudit)?

- Ja
- Nein

12. Besondere Datenschutzpflichten gegenüber Kursteilnehmern der Organisation

12.1 Erhalten alle Teilnehmer unabhängig von der Art ihrer Anmeldung (Post, Fax, telefonisch, online) vor der Erhebung ihrer Daten eine ausreichende Information über die Verwendung ihrer Daten?

- Ja
- Nein

12.2 Sind Einwilligungen für Werbemaßnahmen (E-Mailnewsletter, Anrufe) eingeholt und ausreichend dokumentiert worden?

- Ja
- Nein

12.3 Wird die Einwilligung im Wege des Double Opt-In eingeholt?

- Ja
- Nein