Die Umsetzung der DSGVO führt in Unternehmen immer wieder zu Fragen und Hindernissen.
Zur Sicherheit ist eine regelmäßige Überprüfung der Umsetzung erforderlich.
Für Unternehmen kann deshalb ein Selbstaudit zur Umsetzung der DSGVO hilfreich sein.
Der IHK-Fragebogen schafft die Möglichkeit einer Bestandsaufnahme in Ihrem Unternehmen.

Fragebogen Selbstaudit zur DSGVO

Verantwortlicher: Klicken oder tippen Sie hier, um Text einzugeben.

Datum: Klicken oder tippen Sie hier, um Text einzugeben.

☐ Erstaudit
☐ Wiederholungsaudit
☐ Nachaudit

A. Einführung

Der Fragebogen soll dem Verantwortlichen und – falls vorhanden - betrieblichen Datenschutzbeauftragten ermöglichen, die Einhaltung des Datenschutzes im Betrieb zu überwachen. Für eine datenschutzrechtliche Compliance sind auch eine gesetzeskonforme Planung und das Beachten der gesetzlichen Regelungen grundlegend. Die Einhaltung der verschiedenen Anforderungen muss in jedem Prozess sichergestellt werden. Dazu sollte der Verantwortliche, ggf. delegiert an seinen Datenschutzbeauftragten, in wiederkehrenden Zeitintervallen die erforderlichen Analysen durchführen. Nur so kann ein gleichbleibendes Datenschutzniveau aufrechterhalten werden.

B. Organisation des Datenschutzes

1. Verantwortlichkeiten

Zur Durchsetzung von Datenschutzmaßnahmen im Unternehmen ist es wichtig, dass derv Inhaber/die Geschäftsführung die Verantwortung hierfür übernimmt. Zusätzlich sollten für die Abgrenzung der Aufgabengebiete, aber auch zur Vermeidung von Zuständigkeitslücken die Verantwortlichkeiten für alle wesentlichen Aufgaben nachvollziehbar geregelt sein. Hierfür sollte ein Datenschutz- und Informationssicherheitsmanagement eingerichtet sein.

1.1 Ist für die Umsetzung eine Leitlinie innerhalb des Unternehmens vorhanden?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

1.2 Das Unternehmen hat klare Verantwortlichkeiten für den Datenschutz definiert.

☐ Ja
☐ Nein

☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

1.3 Ausschließlich mündlich gegebene Anweisungen sind in der Regel nicht nachhaltig und geraten schnell in Vergessenheit. Daher sollten Richtlinien und Anweisung in schriftlicher Form dokumentiert werden. Das Unternehmen hat Richtlinien, in denen definiert ist, wie mit personenbezogenen Daten umgegangen werden muss.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

1.4 Ist ein Datenschutzbeauftragter bestellt und der Aufsichtsbehörde gemeldet?

☐ Ja

☐ intern
☐ extern

Meldedatum: Klicken oder tippen Sie hier, um Text einzugeben.
Art der Meldung: ☐ Online ☐ Brief ☐E-Mail

☐ Die Daten des behördlichen Datenschutzbeauftragten wurden veröffentlicht

☐ Nein
Grund: Klicken oder tippen Sie hier, um Text einzugeben.

1.5 Welche Aufgaben hat der Datenschutzbeauftragte?

☐ Beratung der Geschäftsführung
☐ Beratung der Fachabteilungen
☐ Sensibilisierung der Mitarbeiter
☐ Durchführung interner Audits/Kontrollen
☐ Beantwortung/Klärung von Datenschutzbeschwerden
☐ Durchführung von Anfragen zu Betroffenenrechten
☐ Aufgabenplanung der Fachabteilungen
☐ Durchführung der Meldung von Datenschutzverletzungen (Art. 33/34 DS-GVO)
☐ Sonstige: Klicken oder tippen Sie hier, um Text einzugeben.

1.6 Gibt es bei Ihnen einen Betriebsrat?

☐ Ja
☐ Wird er vom Datenschutzbeauftragten, wenn es den bei Ihnen gibt, kontrolliert?
☐ Nein (Regelung im Personalvertretungsgesetz des Landes?)

1.7 Sind, sofern mehrere Standorte vorhanden sind, die anderen Niederlassungen in ein einheitliches Datenschutzkonzept eingebunden?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

2. Mitarbeiter

Informiertes und geschultes Personal ist die Grundlage einer sicheren Durchführung von Geschäftsprozessen. Neben der Information des Personals über die etablierten Prozesse, unternehmensspezifische Regelungen und Handlungsanweisungen sind insbesondere regelmäßige Schulungen zu Datenschutzmaßnahmen erforderlich, um eine Verbesserung des Datenschutzniveaus zu erreichen.

2.1 Alle internen und externen Mitarbeiter kennen die betreffenden Regelungen zum Datenschutz.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

2.2 Alle internen und externen Mitarbeiter haben eine schriftliche Vertraulichkeitserklärung abgegeben.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

2.3 Alle internen und externen Mitarbeiter werden regelmäßig über unsere Maßnahmen zum Datenschutz informiert.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

3. Analyse

3.1 Das Unternehmen identifiziert rechtzeitig, d. h. zu Planungsbeginn, die Geschäftsprozesse, in denen eine Verarbeitung personenbezogener Daten stattfindet.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

3.2 Das Unternehmen hat für jede Verarbeitung ermittelt, welche Kategorien personenbezogener Daten sie verarbeitet.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

3.3 Das Unternehmen hat für jede Verarbeitung eine Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO (Anbahnung oder Durchführung von Vertragsverhältnissen, Einwilligung, berechtigte Interessen etc.) zugeordnet.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

4. Verarbeitungen

Die Verarbeitung personenbezogener Daten ist einer der Hauptaspekte eines Datenschutzmanagementsystems. Dieser umfasst Festlegungen zum sogenannten Verarbeitungsverzeichnis, in dem alle Verarbeitungen aufgeführt werden. Für jede Verarbeitung müssen deren Grundlagen, die zugehörigen technischen Aspekte, eine Risikobewertung und die Notwendigkeit einer Datenschutz-Folgeabschätzung festgelegt werden.

4.1 Das Unternehmen führt ein Verzeichnis ihrer internen und ausgelagerten Verarbeitungen.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

4.2 Das Unternehmen definiert und pflegt die gesetzlich geforderten Inhalte der im Verzeichnis geführten Verarbeitungen in einem für jede Verarbeitung festgelegten Revisionszyklus.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

4.3 Das Unternehmen ermittelt das technische und organisatorische Umfeld für die Verarbeitung von personenbezogenen Daten.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

4.4 Das Unternehmen ermittelt die damit in Zusammenhang stehenden Risiken.

☐ Ja
☐ Nein
☐ Sachstand

Klicken oder tippen Sie hier, um Text einzugeben.

4.5 Das Unternehmen hat geprüft, ob eine Datenschutz-Folgeabschätzung erforderlich ist.

☐ Ja
☐ Nein
☐ Sachstand

Klicken oder tippen Sie hier, um Text einzugeben.

5. Informationspflichten

Die Informationspflichten nach Art. 13 und 14 DSGVO müssen erfüllt und dokumentiert werden. Zudem müssen sie den betroffenen Personen zur Kenntnis gegeben werden.

5.1 Die Informationspflichten werden umgesetzt,

☐ durch Anlage an die betroffenen Personen (Antwortschreiben, Bestätigung, E-Mail)
☐ durch Verweis auf die Informationen auf der eigenen Webseite mit entsprechendem Link
☐ Auslage/Aushang in Geschäftsräumen
☐ Flyer

5.2 Wurden die Webseite(n) seit dem 25.05.2018 derart überarbeitet, dass über die Datenverarbeitung (der Webseite) ausreichend gem. Art. 13 DSVO informiert wird?

☐ Ja
☐ Nein
☐ Sachstand

Klicken oder tippen Sie hier, um Text einzugeben.

6. Informationssicherheit

Zwar ist grundsätzlich zwischen den Anforderungen an ein Datenschutzmanagementsystem (DSMS) und an ein Informationssicherheitsmanagementsystem (ISMS) zu unterscheiden. Eine Anforderung des DSMS ist es jedoch, die Grundzüge eines ISMS abzubilden. Das Unternehmen hat ein DSISMS etabliert, in dem geeignete Security-Maßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DSGVO getroffen sind?

☐ Ja
☐ Nein
☐ Sachstand

Klicken oder tippen Sie hier, um Text einzugeben.

7. Auftragsverarbeitung

7.1 Im Falle der Auslagerung von Verarbeitungen schließt das Unternehmen mit ihren Auftragsverarbeitern einen entsprechenden Vertrag.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

7.2 Als Anbieter von Auftragsverarbeitungen schließt der Auftragsverarbeiter mit dem jeweiligen Auftraggeber einen entsprechenden Vertrag.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

7.3 Das Unternehmen überprüft ihre Auftragsverarbeiter.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

Dabei wird die Überprüfung durchgeführt per

☐Kontrollen vor Ort
☐schriftlichem Fragebogen
☐ Vorlage von Zertifikaten

Klicken oder tippen Sie hier, um Text einzugeben.

7.4 Das Unternehmen weiß, ob seine Auftragsverarbeiter Unterauftragnehmer einsetzen und wo diese ihren Sitz haben.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

8. gemeinsame Verantwortlichkeiten

Gibt es bei Ihnen Verarbeitungstätigkeiten, für die eine gemeinsame Verantwortlichkeit gegeben ist?

☐ Ja
☐ Nein

9. Datenschutzvorfälle

9.1 Es gibt eine Regelung, die den Umgang mit Datenschutzvorfällen einschließlich der Meldung an die Aufsichtsbehörde und die betroffenen Personen festlegt.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

9.2 Es ist Verfahren implementiert, dass die Reaktion auf Datenschutzvorfälle strukturiert vorgibt.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

10. Datenmanagement

Existiert ein Löschkonzept (z. B. nach DIN 66398), das auch den Umgang mit Archiven und Backups regelt?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

11. Betroffenenrechte

11.1 Es gibt ein Verfahren für die Wahrung der Betroffenenrechte.

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

11.2 Ist ein dokumentierter Prozess vorhanden, wie mit Auskunftsansprüchen umgegangen wird?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

11.3 Ist ein Verfahren vorhanden, mit dem die Fristeinhaltung für die Antwort auf Betroffenenrechte (Auskunftsersuchen, Löschbegehren, Widerspruch, Berichtigungsantrag, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit) sichergestellt wird?

☐ Ja

☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

11.4 Ist ein Verfahren vorhanden, mit dem auf Anfragen der Datenschutzaufsichtsbehörden bezüglich dort eingegangener Datenschutzbeschwerden reagiert wird?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

12. Datenübermittlungen in Drittländer

12.1 Das Unternehmen weiß, ob und in welche Drittländer (Länder außerhalb der Europäischen Union) Daten übermittelt werden, oder ob Drittländer Zugriff auf den eigenen Datenbestand haben?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

12.2 Es liegen geeignete Garantien (Angemessenheitsbeschluss der EU-Kommission, EU-Standardvertragsklauseln, bilaterale Abkommen oder eine explizite Einwilligung) für die Datenübermittlung in Drittländer oder den Zugriff auf Daten durch Drittländer vor?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

12.3 Das Unternehmen weiß, ob seine Auftragsverarbeiter Unterauftragnehmer in Drittländern einsetzen und um welche Drittländer sich handelt?

☐ Ja
☐ Nein
☐ Sachstand
Klicken oder tippen Sie hier, um Text einzugeben.

13. Vorschläge zu Maßnahmen, die ergriffen werden sollten:

Klicken oder tippen Sie hier, um Text einzugeben.

14. Verantwortlichkeiten für die Umsetzung der Maßnahmen

Klicken oder tippen Sie hier, um Text einzugeben.

Erstellt:

Datum	Unterschrift behördliche/r Datenschutzbeauftragte

Zur Kenntnis genommen

Datum	Unterschrift Geschäftsführung

Hinweis:
Dieser Fragebogen soll – als Service Ihrer IHK– nur erste Hinweise geben und erhebt daher keinen Anspruch auf Vollständigkeit. Obwohl dieses Muster mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.
Bitte beachten Sie, dass die Inhalte dieses Fragebogens unverbindlich erfolgen und eine anwaltliche Beratung nicht ersetzen können.