

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Checkliste zur Überprüfung der Informationssicherheit

Die Fragen im Fragenkatalog sind so gestellt, dass „ja“ Antworten erwartet werden. Werden Fragen mit „Teilweise“ oder „Nein“ beantwortet, ist dies zu erklären. Es ist dann zu entscheiden, ob Maßnahmen eingeleitet werden müssen, um einen systemkonformen Zustand zu erreichen, oder ob zu einem späteren Zeitpunkt die Überprüfung zu wiederholen ist.

Bestellung eines Datenschutzbeauftragten

Gesetzlich erforderlich?

Ja Nein Kommentar

Ist ein Datenschutzbeauftragter bestellt?

Ja Nein Kommentar

Ist die erforderliche Fachkunde des Datenschutzbeauftragten nachgewiesen?

Ja Teilweise Nein Kommentar

Ist die „Zuverlässigkeit“ des Datenschutzbeauftragten gewährleistet („keine Interessenskonflikte“)?

Ja Teilweise Nein Kommentar

Ist der Datenschutzbeauftragte direkt der Geschäftsleitung unterstellt und in die Informationsprozesse im Unternehmen, insbesondere bei der Planung und Anschaffung von Informationstechnologie eingebunden?

Ja Teilweise Nein Kommentar

Hat der Datenschutzbeauftragte die Möglichkeit, sich regelmäßig fortzubilden (Schulung, Literatur etc.)?

Ja Nein Kommentar

Verpflichtung auf das Datengeheimnis

Sind alle Beschäftigten auf das Datengeheimnis i.S.d. Art. 5 DSGVO, Art. 24 DSGVO verpflichtet worden?

Ja Nein Kommentar

Werden auch externe Mitarbeiter (z.B. Reinigungskräfte, Werkstudenten u.ä.) auf das Datengeheimnis verpflichtet?

Ja Teilweise Nein Kommentar

Gibt es ein **Verzeichnis von Verarbeitungstätigkeiten** nach Art. 30 DSGVO, mit denen personenbezogene Daten verarbeitet werden (ehemals „internes Verzeichnisse“ / Verarbeitungsübersicht)?

Ja Nein Kommentar

Ist gewährleistet, dass bei der Anschaffung/Änderung neuer IT, bei der Gestaltung neuer IT-Abläufe oder der Änderung im IT-Bereich eine Anpassung der Verarbeitungsübersicht erfolgt?

Ja Teilweise Nein Kommentar

^

Checkliste zur Überprüfung der Informations-Sicherheitskomponenten (IT+DS-Sicherheitscheck, klein)

Version 2.1, Februar 2018

Seite 1 von 15

Dr. Thomas Pudelko, Datenschutzbeauftragter

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Meldepflicht

Erfolgt die Meldung bei der geschäftsmäßigen Übermittlung von Daten oder für Zwecke der Markt- und Meinungsforschung)?

Ja Nein Anforderung nicht anwendbar/relevant

Falls ja, wurde die Meldepflicht eingehalten?

Ja Teilweise Nein

Datenschutz-Folgenabschätzung (ehemals Vorabkontrolle)

Werden Datenschutz-Folgenabschätzungen (Art. 33 DSGVO) vor der Einführung von automatisierten Datenverarbeitungsvorgängen durchgeführt, wenn diese Vorgänge besondere Risiken für die Rechte der Betroffenen beinhalten?

Ja Teilweise Nein Kommentar

IT-Sicherheit

Technische und organisatorische Maßnahmen gemäß Art. 32 EU-DSGVO und § 58 Abs. 3 des deutschen Ausführungsgesetz zur Datenschutz-Grundverordnung

Gibt es schriftliche Dokumentation der technischen und organisatorischen Maßnahmen i.S.d. Art. 32 EU-DSGVO

Ja Nein Anmerkung

Gibt es eine Leitlinie zur Informationssicherheit?

Ja Nein Anmerkung

Gibt es eine IT-Richtlinie (o.ä.) für Beschäftigte, aus der sich ergibt, ob und wie diese IT-Systeme im Unternehmen verwenden dürfen?

Ja Nein Anmerkung

Gibt es eine Risiko- und Schwachstellenanalyse im Hinblick auf Räume, IT-Systeme, IT-Applikationen und Netzwerkkomponenten?

Ja Nein Anmerkung

Gibt es einen Notfallplan?

Ja Nein Anmerkung

Compliance bei der Verarbeitung von Daten

Direkterhebung

Werden personenbezogene Daten grundsätzlich selbst beim Betroffenen erhoben?

Ja Teilweise Nein Kommentar

Festlegung von Verantwortlichkeiten und Regelungen für den Computer- und Interneteinsatz

Sind Verantwortliche für die IT-Sicherheit und den Datenschutz in allen Untergliederungen (Abteilungen/Bereichen/Standorten etc.) benannt?

Ja Teilweise Nein Kommentar

Sind deren Befugnisse festgelegt worden?

Ja Teilweise Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Gibt es Regeln über:

- | | | | | | | |
|--|----|--------------------------|-----------|--------------------------|------|-----------|
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Dokumentation von IT-Verfahren, Software, IT-Konfiguration? | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Zutrittsberechtigungen (Räume) | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Zugangsberechtigungen (Computer) | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Zugriffsberechtigungen (Dateien) | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Gebrauch von Passwörtern | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Datenübertragung | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Schutz gegen Schadsoftware | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Datenträgertransport | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Datensicherung | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Datenarchivierung | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Datenschutz | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Notfallvorsorge | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Wartungs- und Reparaturarbeiten | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |
| Vorgehensweise bei Verletzung der Sicherheitspolitik (s. auch Informationspflicht bei „Datenpannen“) | | | | | | |
| <input type="checkbox"/> | Ja | <input type="checkbox"/> | Teilweise | <input type="checkbox"/> | Nein | Kommentar |

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Information der Mitarbeiter/-innen

- Sind diese Regelungen den betroffenen Mitarbeiter/-innen in geeigneter Weise bekannt gegeben worden?
- Ja Teilweise Nein Kommentar
- Ist die Bekanntgabe dokumentiert worden?
- Ja Teilweise Nein Kommentar
- Werden alle Regelungen in der aktuellen Fassung an einer Stelle vorgehalten, so dass sie bei einem berechtigten Interesse zugänglich sind?
- Ja Teilweise Nein Kommentar
- Werden die Regelungen regelmäßig aktualisiert?
- Ja Teilweise Nein Kommentar

Dokumentation von IT-Verfahren, Software, IT-Konfiguration

Einspielung neuer und freigegebener Software

- Gibt es ein Software-Freigabe-Verfahren, welche Software wann von wem verwendet werden darf?
- Ja Nein Kommentar
- Gibt es ein Verzeichnis der freigegebenen und eingesetzten Software (Software-Bestandsverzeichnis)?
- Ja Teilweise Nein Kommentar
- Ist ein Nutzungsverbot nicht freigegebener Software schriftlich fixiert?
- Ja Teilweise Nein Kommentar
- Sind alle Mitarbeiter/-innen über das Nutzungsverbot unterrichtet?
- Ja Teilweise Nein Kommentar
- Wurde in regelmäßigen Abständen an das Nutzungsverbot erinnert?
- Ja Nein Kommentar

Überprüfung des Software-Bestandes

- Werden regelmäßig Überprüfungen des Software-Bestandes durchgeführt (mind. Jährlich)?
- Ja Teilweise Nein Kommentar
- Wird der Software-Bestand komplett überprüft?
- Ja Nein Kommentar
- Wird der Software-Bestand stichprobenartig überprüft?
- Ja Teilweise Nein Kommentar
- Werden Verstöße angemessen geahndet?
- Ja Teilweise Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Ja Teilweise Nein Kommentar
Werden die Ergebnisse der Überprüfung nachvollziehbar dokumentiert?

Ja Nein Kommentar
Werden Veränderungen in den grundsätzlichen Konfigurationen des IT-Systems dokumentiert?

Vergabe von Zutrittsberechtigungen

Ja Teilweise Nein Kommentar
Sind die schutzbedürftigen Räume eines Gebäudes bestimmt worden?

Ja Teilweise Nein Kommentar
Wird die Dokumentation schutzbedürftiger Räume und zutrittsberechtigter Personen regelmäßig aktualisiert?

Ja Teilweise Nein Kommentar
Ist für jeden dieser Räume festgelegt worden, welche Person welche Zugriffsrechte hat?

Ja Teilweise Nein Kommentar
Wird die Vergabe und Zurücknahme von Zutrittsrechten dokumentiert?

Ja Teilweise Nein Kommentar
Werden alle Zutrittsberechtigungen kontrolliert (durch Personen und technisch)?

Ja Teilweise Nein Kommentar
Existiert eine Regelung zur Schlüsselverwaltung?

Ja Nein Kommentar
Existiert ein Schließplan für alle Schlüssel der Gebäudeteile der Organisation?

Ja Teilweise Nein Kommentar
Wird die Ausgabe der Schlüssel dokumentiert?

Ja Nein Kommentar
Wird regelmäßig (mindestens jährlich) kontrolliert, ob die Dokumentation über ausgegebene Schlüssel noch aktuell ist?

Vergabe von Zugangsberechtigungen

Ja Teilweise Nein Kommentar
Werden die Vergabe sowie der Einzug von Zugangsberechtigungen und Zugangsmitteln dokumentiert?

Ja Teilweise Nein Kommentar
Wird die Dokumentation über Vergabe sowie Einzug von Zugangsberechtigungen und Zugangsmitteln regelmäßig (mindestens einmal im Jahr) aktualisiert?

Ja Teilweise Nein Kommentar
Werden personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt?

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Werden die Benutzer/-innen bei der Vergabe von Zugangsberechtigungen über die Handhabung von Zugangs- und Authentifikationsmitteln (z.B. Umgang mit Chipkarten, Passworhandhabung) informiert?

Ja Teilweise Nein Kommentar

Werden Zugangsberechtigungen bei längerer Abwesenheit von Benutzern gespeist?

Ja Teilweise Nein Kommentar

Wird die Nutzung von Zugangsberechtigungen protokolliert?

Ja Teilweise Nein Kommentar

Wird dies regelmäßig ausgewertet?

Ja Teilweise Nein Kommentar

Der Arbeitsplatz

Sind die Mitarbeiter/-innen dazu angehalten worden, bei längerer Abwesenheit die Arbeitsplätze „aufgeräumt“ zu hinterlassen?

Ja Teilweise Nein Kommentar

Sind die Mitarbeiter/-innen dazu angehalten worden, bei kürzerer Abwesenheit die Arbeitsräume zu schließen?

Ja Teilweise Nein Kommentar

Sind die Mitarbeiter/-innen dazu angehalten worden, bei kürzerer Abwesenheit die Monitore „dunkel“ zu schalten?

Ja Teilweise Nein Kommentar

Vergabe von Zugriffsrechten

Ist für jedes IT-System bzw. jede IT-Anwendung festgelegt worden, welche Personen welches Zugriffsrecht (Schreiben, Lesen, Gesperrt, Löschen etc.) haben?

Ja Nein Kommentar

Liegen aktuell Dokumentationen der vergebenen Zugriffsrechte vor?

Ja Teilweise Nein Kommentar

Sind Zugriffsrechte für Benutzergruppen definiert worden?

Ja Teilweise Nein Kommentar

Regelung des Passwortgebrauchs

Existiert eine Regelung zum Passwortgebrauch?

Ja Teilweise Nein Kommentar

Werden darin konkrete Anforderungen an Passwörter gestellt?

Ja Teilweise Nein Kommentar

- an Erratbarkeit, Passwortgüte?

Ja Teilweise Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Ja Teilweise Nein Kommentar
- an die Passwortlänge (mind. 8 Zeichen?)

Ja Teilweise Nein Kommentar
- an die Geheimhaltung?

Ja Teilweise Nein Kommentar
- an die Hinterlegung?

Ja Teilweise Nein Kommentar
- an die Häufigkeit des Passwortwechsel (mindestens alle drei Monate)?

Ja Teilweise Nein Kommentar
Sind die Benutzer/-innen über diese Regelung bzw. den korrekten Umgang mit Passwörtern unterrichtet worden?

Ja Teilweise Nein Kommentar
Ist sichergestellt, dass für den Zugriff auf alle IT-Systeme bzw. IT-Anwendungen ein Passwort erforderlich ist?

Ja Teilweise Nein Kommentar
Werden sofort nach Inbetriebnahme von IT-Systemen oder Benutzerwechsel individuelle Passwörter vergeben?

Datenübertragung / Datenaustausch mit externen Partnern

Ja Teilweise Nein Kommentar
Wurden Regelungen zum Austausch von Daten definiert? (Wege über das Internet, mit CD, USB-Stick, in Papierform, welche Verantwortlichkeiten sind damit verbunden?)

Ja Teilweise Nein Kommentar
Wurden dabei entsprechende Sicherheitsstufen der Informationssicherung vereinbart?

Ja Teilweise Nein Kommentar
Wurden Datenaustauschformate (DOC, RTF, TXT, PDF, HTML) mit den Partnern vereinbart?

Ja Teilweise Nein Kommentar
Wurden die anzuwendenden Verschlüsselungen der Daten jeweils eingerichtet, getestet und angewandt?

Ja Teilweise Nein Kommentar
Wird sichergestellt, dass in Abwesenheit von Mitarbeitenden dieser Datenaustausch bei Bedarf weiter stattfinden kann?

Ja Teilweise Nein Kommentar
Wird eine Sicherungskopie für auszutauschende Datenträger erstellt?

Schutz gegen Schadsoftware

Ja Teilweise Nein Kommentar
Werden Schadsoftwareschutzprogramme auf allen Servern eingesetzt?

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Ja Nein Teilweise Keine Angabe Kommentar
 Werden Schadsoftwareschutzprogramme auf allen PC eingesetzt?

Ja Teilweise Nein Keine Angabe Kommentar
 Werden die Schadsoftwareschutzprogramme in regelmäßigen Abständen durch neue Versionen ersetzt?

Ja Teilweise Nein Keine Angabe Kommentar
 Sind die Verantwortlichkeiten zur Aktualisierung geregelt und werden die Aktualisierungen auf den jeweiligen Systemen dokumentiert?

Ja Teilweise Nein Keine Angabe Kommentar
 Wurden Verhaltensregeln des Schadsoftwareschutzes und der Reaktion im Schadensfall allen betroffenen Mitarbeiter/-innen bekannt gemacht?

Ja Teilweise Nein Keine Angabe Kommentar
 Sind die zuständigen Personen in der Lage im Bedarfsfall angemessene Schritte durchzuführen?

Datenträgerverwaltung

Ja Teilweise Nein Keine Angabe Kommentar
 Gibt es eine Datenträgerverwaltung?

Ja Teilweise Nein Keine Angabe Kommentar
 Existieren Bestandsverzeichnisse für Datenträger?

Ja Teilweise Nein Keine Angabe Kommentar
 Liegt ein aktuelles Ordnerverzeichnis vor?

Ja Teilweise Nein Keine Angabe Kommentar
 Gibt es klare Regelungen für die Kennzeichnung der Datenträger?

Ja Teilweise Nein Keine Angabe Kommentar
 Werden regelmäßig (mind. halbjährlich) Vollständigkeitskontrollen des Datenträgerbestandes vorgenommen?

Ja Teilweise Nein Keine Angabe Kommentar
 Werden alle Datenträger sachgerecht aufbewahrt?

Ja Teilweise Nein Keine Angabe Kommentar
 Sind alle Datenträger vor unbefugtem Zugriff geschützt?

Ja Teilweise Nein Keine Angabe Kommentar
 Ist der Umgang mit alten oder unbrauchbaren Datenträgern so geregelt, dass sie auf sicherem Wege vernichtet werden?

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Datensicherung

Ja Teilweise Nein Kommentar
Wird eine regelmäßige Datensicherung der Daten auf allen Systemen durchgeführt?

Ja Teilweise Nein Kommentar
Sind die entsprechenden Verantwortlichkeiten für die Durchführung der Datensicherung geregelt?

Ja Teilweise Nein Kommentar
Wird die Datensicherung protokolliert?

Ja Teilweise Nein Kommentar
Werden die Sicherungsmedien an einem sicheren Ort (z.B. Fernsicherung) aufbewahrt?

Ja Nein Kommentar
Werden Tests für die Rücksicherung regelmäßig durchgeführt?

Datenarchivierung

Ja Teilweise Nein Kommentar
Wird in regelmäßigen Abständen eine Datenarchivierung der jeweiligen Arbeitsbereiche durchgeführt?

Ja Teilweise Nein Kommentar
Sind die Befugnisse und Verantwortlichkeiten für die Archivierung verbindlich geregelt?

Ja Teilweise Nein Kommentar
Werden die archivierten Daten an einem sicheren Ort aufbewahrt?

Ja Teilweise Nein Kommentar
Ist verbindlich geregelt, wer auf die ausgelagerten Daten Zugriff bekommt?

Entsorgung von schützenswerten Betriebsmitteln

Ja Nein Kommentar
Existiert eine verbindliche Regelung zur Entsorgung von schützenswerten Betriebsmitteln?

Ja Nein Kommentar
Werden in dieser Regelung alle schützenswerten Betriebsmittel genannt?

Ja Teilweise Nein Kommentar
Werden mit der Entsorgung beauftragte Unternehmen auf die Einhaltung erforderlicher Sicherheitsmaßnahmen verpflichtet?

Ja Teilweise Nein Kommentar
Wird der Entsorgungsvorgang regelmäßig (mindestens jährlich) kontrolliert?

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung**Datenschutz**

Liegen Regelungen zur Umsetzung und zur Beachtung des Datenschutzes vor?
 Ja Teilweise Nein Kommentar

Wurden die Arbeitsbereiche mit besonderen Datenschutzbestimmungen definiert?
 Ja Teilweise Nein Kommentar

Wird eine Vorabkontrolle bei besonders schutzwürdigen Daten nach Art. 9 – EU-DSGVO durchgeführt?

Ja Teilweise Nein Kommentar

Wird das Verzeichnis der Verfahren geführt?
 Ja Teilweise Nein Kommentar

Gibt es ein Risikomanagement bezüglich des Datenschutzes?
 Ja Nein Kommentar

Gibt es ein IT- Sicherheitskonzept?
 Ja Nein Kommentar

Werden Änderungen an der Dateioorganisation vollständig protokolliert?
 Ja Teilweise Nein Kommentar

Wird die Durchführung von Datensicherungsmaßnahmen protokolliert?
 Ja Teilweise Nein Kommentar

Werde alle Versuch des unbefugten Einloggens und Überschreitens von Befugnissen protokolliert?
 Ja Teilweise Nein Kommentar

Kennen die Mitarbeiter/-innen die Möglichkeiten der eingesetzten Protokollierung und dessen Verwendung?
 Ja Teilweise Nein Kommentar

Notfallvorsorge

Ist eine Übersicht der Verfügbarkeitsanforderungen vorhanden?
 Ja Teilweise Nein Kommentar

Existiert eine Untersuchung interner und externer Auseichmöglichkeiten?
 Ja Teilweise Nein Kommentar

Gibt es Regelungen für den Notfall für ausgewählte Schadensereignisse?
 Ja Teilweise Nein Kommentar

Existiert ein Alarmierungsplan?
 Ja Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Wurden entsprechende Notfallübungen bereits durchgeführt?
 Ja Teilweise Nein Kommentar

Werden die Partner/Landesverbände/Mitgliedsorganisationen über entsprechende Notfallpläne informiert?
 Ja Teilweise Nein Kommentar

Regelungen für Wartungs- und Reparaturarbeiten

Sind Verantwortliche für die Beauftragung von Wartungs- und Reparaturarbeiten der IT-Architektur und Komponenten benannt?
 Ja Teilweise Nein Kommentar

Werden dabei durch Externe im Haus durchgeführte Wartungs- und Reparaturarbeiten durch fachkundige Mitarbeiter/-innen beaufsichtigt?
 Ja Teilweise Nein Kommentar

Wird nach Abschluss der Wartungs- und Reparaturarbeiten überprüft, ob der Wartungsauftrag vollständig und erfolgreich ausgeführt wurde?
 Ja Teilweise Nein Kommentar

Gibt es besondere Regelungen, wenn auf von Wartungs- und Reparaturarbeiten betroffenen Speichermedien besonders sensible Daten gespeichert sind?
 Ja Teilweise Nein Kommentar

Werden nach Abschluss von Wartungs- und Reparaturarbeiten in den betroffenen Bereichen die Passwörter geändert?
 Ja Teilweise Nein Kommentar

Werden die durchgeführten Wartungs- und Reparaturarbeiten dokumentiert (Umfang, Ergebnis, Zeitpunkt, etc.)?
 Ja Teilweise Nein Kommentar

Werden die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen IT- Sicherheitsmaßnahmen verpflichtete?
 Ja Teilweise Nein Kommentar

Reaktion auf Verletzung der Sicherheitspolitik

Ist die Vorgehensweise bei Verdacht auf Verletzung der IT- Sicherheitspolitik klar definiert?
 Ja Teilweise Nein Kommentar

Ist festgelegt worden, welche Reaktion auf Verletzung der IT- Sicherheitspolitik erfolgen soll?
 Ja Teilweise Nein Kommentar

Ist jemand in der Organisation benannt worden, der für Kontakte mit anderen Organisationen (Mitgliedsorganisationen, Partnerorganisationen) verantwortlich ist, um diese Informationen über aufgetretene Sicherheitslücken weiterzugeben?
 Ja Teilweise Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Rechtsgrundlage

Wird Sorge dafür getragen, dass personenbezogene Daten grundsätzlich nur dann verarbeitet werden, wenn dies zur Erbringung vertraglicher Leistungen erforderlich ist, im Rahmen einer Interessenabwägung zulässig ist oder eine Einwilligung des Betroffenen vorliegt?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Einwilligung

Wird bei der Verwendung von Einwilligungen darauf geachtet, dass der Betroffene über Zweck, Art und Umfang der Verwendung der von ihm freiwillig angegebenen Daten informiert wird?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Kann der Betroffene die Einwilligungserklärung auch ohne Fachkenntnisse verstehen und erkennen, dass die Einwilligung freiwillig ist und ggf. welche Konsequenzen eine Nichterteilung einer Einwilligung hat?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Ist im Falle eines Widerrufs der Einwilligung gewährleistet, dass die betroffenen personenbezogenen Daten nicht weiter verwendet werden?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Ist bei der Einholung der Einwilligung die Trennung von ggf. verschiedenen Zwecken der Datenverarbeitung gewährleistet (keine konkludierende Einwilligung)?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Auftragsdatenverarbeitung

Gibt es eine Übersicht aller Dienstleister/Lieferanten, die entweder Daten im Auftrag der Gesamtorganisation verarbeiten oder IT- Systeme warten und pflegen?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass bei den Auftragnehmern/Dienstleistern ein Auftragsdatenverarbeitungsvertrag geschlossen wurde (und wird)?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Gibt es ein Muster für einen Auftragsdatenverarbeitungsvertrag im Unternehmen?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass der Auftragnehmer bei einer Auftragsdatenverarbeitung vor Vertragsschluss im Hinblick auf die getroffenen IT- Sicherheitsmaßnahmen kontrolliert wird?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Ist gewährleistet, dass Auftragnehmer regelmäßig (grundsätzlich 1x jährlich) im Hinblick auf Änderungen im Bereich der IT- Sicherheit kontrolliert werden?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Informationspflicht bei „Datenpannen“ (Art. 4 Nr.12 DSGVO)

Werden Verfahren, mit denen besondere Arten personenbezogener Daten, personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten gesondert intern gekennzeichnet bzw. überwacht?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

Wird Sorge dafür getragen, dass im Falle einer unbefugten Kenntnisnahme durch Dritte von Daten, die nach Art. 4 Nr.12 DSGVO geschützt sind, sofort der Datenschutzbeauftragte informiert wird?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

Gibt es einen Ablaufplan für den Fall einer Datenpanne?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

Betroffenenrechte

Gibt es ein „Betroffenenmanagement“ dahingehend, dass Betroffene, die ihre Betroffenenrechte i.S.d. Art. 15 EU-DSGVO geltend machen, direkten Kontakt zum Datenschutzbeauftragten erhalten?

Ja Nein Anmerkung

Werden Auskunftersuchen von Betroffenen kurzfristig und vollständig beantwortet?

Ja Nein Anmerkung

Gibt es ein Löschkonzept im Unternehmen, das Regelfristen für die Löschung von Daten vorsieht?

Ja Nein Anmerkung

Internet / E-Mail

Internetseite

Gibt es für die Internetseite des Unternehmens gesonderte Datenschutzhinweise, die von jeder Seite der Internetseite aus erreichbar sind (nicht nur im „Impressum“)

Ja Nein Anmerkung

Wird über Webanalyse-Software informiert?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

Wird über die Verwendung und das „Blocken“ von Cookies informiert?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

Wird über Tracking-Pixel oder sonstige verwendete Methoden für Zwecke der Werbung oder des Marketings informiert und werden Möglichkeiten für ein „Opt-Out“ angezeigt?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

E-Mail-Marketing

Wird ein E-Mail-Newsletter angeboten?

Ja Nein

Werden Newsletter-Abonnenten hinreichend über Zweck, Art und Umfang der Datenverarbeitung beim E-Mail-Newsletter informiert (insbes. Tracking von „Open Rates“, „Click Rates“ u.Ä.)?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Gibt es ausreichende vertragliche Regelungen zur Verwendung der Daten durch einen externen Newsletter-Dienstleister (z.B. Auftragsdatenverarbeitungsvertrag, Einwilligung etc.)

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Private Internet-/E-Mail-Nutzung im Unternehmen

Gibt es eine unternehmensinterne Regelung zur privaten Nutzung des Internets im Unternehmen

Ja Nein Anmerkung

Gibt es eine unternehmensinterne Regelung zur privaten Nutzung von E-Mail im Unternehmen

Ja Nein Anmerkung

Betriebsrat

Gibt es einen Betriebsrat im Unternehmen

Ja Nein

Gibt eine Übersicht der Betriebsvereinbarungen, die Regelungen zum Umgang mit personenbezogenen Daten enthalten?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Datenflüsse in der Gesamtorganisation

Gehören mehrere Organisationen zur Gesamtorganisation („Konzerngesetz der EU“)?

Ja Nein

Falls ja, gibt es Regelungen zur gemeinsamen Nutzung von Daten oder IT-Infrastrukturen im Unternehmen?

Ja Nein Anforderung nicht anwendbar/relevant

Grenzüberschreitender Datenverkehr

Werden Daten des Unternehmens im Ausland verarbeitet bzw. in das Ausland übermittelt?

Ja Nein Anmerkung

Europäische Union / EWR

Ist im Falle einer Verarbeitung von Daten in anderen EU-Mitgliedsstaaten oder EWR-Staaten gewährleistet, dass eine Rechtsgrundlage für die Verwendung im Ausland besteht (z. B. Art. 9 Abs. 3 EU-DSGVO) und ggf. Auftragsdatenverarbeitung)?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

„Drittstaaten“

Werden Daten in „Drittstaaten“ verwendet bzw. dorthin übermittelt?

Ja Nein

Ist von der Organisation geprüft worden, ob es für die Übermittlung in den Drittstaat bzw. die Verarbeitung dort eine Rechtsgrundlage in der EU-DSGVO (Art. 44ff.) gibt („erste Stufe“)?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Handelt es sich bei dem Drittstaat um einen Staat mit „angemessenen Datenschutzniveau“?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Gibt es eine Einwilligung des Betroffenen zur Übermittlung von personenbezogenen Daten an das Unternehmen in dem Drittstaat?

Ja Nein Anmerkung | Anforderung nicht anwendbar/relevant

Checkliste zur Überprüfung der Informations-Sicherheitskomponenten (IT+DS-Sicherheitscheck, klein

Version 2.1, Februar 2018

Seite 14 von 15

Dr. Thomas Pudelko, Datenschutzbeauftragter

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Ist mit dem Unternehmen in dem Drittstaat ein Vertrag auf Basis der EU-Standardvertragsklauseln geschlossen worden?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

Ist bei einer Übertragung in die USA im Rahmen des EU-US Privacy Shield die Angemessenheit des Datenschutzniveaus festgestellt worden?

Ja Nein Anmerkung

Anforderung nicht
anwendbar/relevant

Stand: 08.02.2018