Frage- und Antwortbogen

Datenschutz Querschnittsprüfung PF-A

Verantwortliche Stelle (Anschrift/Stempel)

1. Allgemeine Rahmenbedingungen

Haben Sie einen betrieblichen Datenschutzbeauftragten (DSB) bestellt?

◯ Ja Name des betrieblichen DSB:

◯ Nein

2. Pflichten des Verantwortlichen

Gibt es eine allgemeine Datenschutzdokumentation?

◯ Ja ◯ Nein

Gibt es einen Prozess, der den Umgang mit Datenschutzvorfällen oder Beschwerden regelt?

◯ Ja ◯ Nein

Ist ein Verzeichnis der Verarbeitungstätigkeiten (§ 31 KDG) vorhanden?

◯ Ja ◯ Nein

Bitte übersenden Sie uns das Verzeichnis für Verarbeitungstätigkeiten (alternativ eine Übersicht mit den Verarbeitungstätigkeiten)!

3. Personal und Mitarbeiter

Wurde mit Mitarbeitern und Mitarbeitenden im Rahmen ihrer Tätigkeit eine schriftliche Verpflichtungserklärung gem. § 5 KDG abgeschlossen und wurden sie dahingehend belehrt?

◯ Ja ◯ Nein

Bitte übersenden Sie uns ein Muster der Verpflichtungserklärung!

Verteilen Sie an Mitarbeitende personenbezogen Daten (z.B. Listen, Adressdaten, E-Mail Adressen, etc.) unabhängig davon, wie eine Weitergabe erfolgt (elektronisch, Schriftform, u.a.)?

◯ Ja ◯ Nein

Falls "Ja" geben Sie bitte den Zweck der Datenverarbeitung an, um welche Daten es sich handelt und wie die Vertraulichkeit und eine Vernichtung/Löschung sichergestellt/geregelt ist. Bitte übersenden Sie uns diese Informationen als Anlage oder als Teil zum Verzeichnis für Verarbeitungstätigkeiten.

Wurden alle Beschäftigte, Mitarbeitende und sonstige Dritte (u.a. Ehrenamtliche), die mit personenbezogenen Daten betraut sind, hinsichtlich des Datenschutzes geschult?

◯ Ja ◯ Nein Wann fand die letzte Schulung statt?

4. Informationspflichten und Betroffenenrechte

Können Sie Anfragen von Personen (Betroffenen im Allgemeinen) bzgl. Auskunft, Berichtigung, Einschränkung, Löschung, Widerspruch, Übertragung und Sperrung nachkommen?

◯ Ja ◯ Nein

Gibt es dafür eine einheitliche Vorgehensweise (Richtlinie o. Prozess) und ist sie dem Personal bekannt?

◯ Ja ◯ Nein

Bitte übersenden Sie uns die Richtlinie bzw. die Anleitung oder schildern Sie uns die Vorgehensweise!

Verarbeiten Sie personenbezogene Daten auf Basis von Einwilligungen nach § 8 KDG? (z.B. zur Verwendung von Fotos, Adressdaten, etc.)

◯ Ja ◯ Nein

Falls "Ja" übersenden Sie uns bitte Ihre verwendeten Muster!

Wo werden Einwilligungen, die u.a. personenbezogene Daten enthalten, aufbewahrt?

5. Technische und Organisatorische Maßnahmen (KDG-DVO)

Werden Daten regelmäßig gelöscht bzw. vernichtet, bei denen eine Aufbewahrungspflicht oder deren Zweck zur Verarbeitung nicht mehr bestehen?

◯ Ja ◯ Nein

Ist die ordnungsgemäße Vernichtung von Daten sowie von sensiblen Informationen allen Mitarbeitenden bekannt? Das betrifft u.a. auch E-Mail-Postfächer und ggfs. Daten auf privaten Endgeräten. *Übersenden Sie uns bitte eine Übersicht der Löschfristen oder verweisen auf das entsprechende Verfahrensverzeichnis (Löschkonzept).*

☐ Anlage liegt bei / Hinweis im Verfahrensverzeichnis:

Fertigen Sie regelmäßig Datensicherungen an? Personenbezogen Daten sowie betrieblich wichtige Daten müssen u.a. nach einem Systemausfall verfügbar gemacht werden können.

◯ Ja ◯ Nein

Wo werden Datensicherungen aufbewahrt/gelagert? Datensicherungen sollten nicht auf dem selben System und auch nicht im selben Raum der Datenverarbeitungssysteme aufbewahrt werden (anderer Brandabschnitt).

Sind alle Datenverarbeitungssysteme und Programme (PC, u.ä.) vor unberechtigtem Zugriff auf betriebliche Daten geschützt (Zugriffsbeschränkung, Berechtigungen)?

◯ Ja ◯ Nein Wie?

Wird ein Computerschutz zum Schutz vor Schadsoftware (Virus, Trojaner, etc.) eingesetzt?

◯ Ja ◯ Nein Wird diese regelmäßig aktualisiert? ◯ Ja ◯ Nein

Wird der Zutritt zu Räumen beschränkt, in denen sich personenbezogene Daten (Akten, Schriftgut, Datenträger etc.) bzw. betrieblich sensible Daten befinden (Zutrittsbeschränkung)?

◯ Ja ◯ Nein

Gibt es externe Dienstleister, die nach § 29 KDG personenbezogene Daten in Ihrem Auftrag verarbeiten oder auf personenbezogene oder betrieblich sensible Daten Zugriff hätten?
Mit Auftragsverarbeitern sollten entsprechende Vereinbarungen zur Auftragsdatenverarbeitung geschlossen werden. Ggfs. hätten auch EDV Dienstleister Zugriff auf betriebliche Daten.

◯ Ja ◯ Nein

Private Geräte für betriebliche/dienstliche Zwecke

Werden private Endgeräte für betriebliche/dienstliche Zwecke verwendet? Das betrifft u.a. auch betriebliche E-Mails, Chats, etc. und könnte u.U. bei der Administration einer Website relevant werden.

◯ Ja ◯ Nein

Sollte dies der Fall sein, gibt es eine Regelung zur Nutzung privater Endgeräte? Zu beachten sind u.a. die Anforderungen zur Nutzung privater IT-Systeme gem. § 20 KDG-DVO.

◯ Ja ◯ Nein

Übersenden Sie uns bitte ein aktuelles Muster der Vereinbarung zur Nutzung privater Endgeräte für betriebliche/dienstliche Zwecke.

Wie stellen Sie sicher, dass Datenschutzverstöße bei der Datenverarbeitung auf privaten Endgeräten erkannt und fristgemäß an die Aufsichtsbehörde gemeldet werden?

__.__.____

Datum, Unterschrift

Dieses Formular und weitere Prüfaktionen im Internet unter: https://www.kdsa-ost.de/pruefaktion

Hinweis gem. § 7 Abs. 2 KDG (Art. 5 Abs. 2 DS-GVO)“ - Inwieweit ist der Verantwortliche in der Lage die Einhaltung der gesetzlichen Vorgaben aus dem KDG und der KDG-DVO nachzuweisen (Rechenschaftspflicht).