Technische und organisatorische Maßnahmen

Best Practice Checkliste auf Basis des Art. 32 DSGVO

Oktober | 2021

Wichtige Datenschutzinformationen für Ihr Unternehmen

dasax

Inhalte | Datenschutzinformationen

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

die Datenschutzgrundverordnung (DSGVO) fordert im Art. 32 von allen Verantwortlichen den Einsatz von technischen und organisatorischen Maßnahmen (TOM) mit denen ein Schutzniveau gewährleistet wird, dass dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen ist.

Diese TOM sollen zur Gewährleistung der Sicherheit insbesondere die Risiken berücksichtigen, die sich, bezogen auf beteiligte IT-Systeme, Dienste und Fachprozesse, aus einer potenziellen Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität personenbezogener Daten ergeben könnten.

Da die DSGVO aber technikneutral formuliert wurde, finden sich darin leider keine konkreten Maßnahmen, mit der ein Verantwortlicher Schritt für Schritt alle Vorgaben abarbeiten könnte. Stattdessen überlässt es die DSGVO jedem selbst die richtigen Maßnahmen auszuwählen und diese umzusetzen.

Nur was sind technische und organisatorische Maßnahmen im Detail, wie sollten diese eingesetzt werden und wie kann man prüfen, ob die Sicherheit der Verarbeitung nach Art. 32 DSGVO gewährleistet und ein angemessenes Schutzniveau erreicht ist?

Um Sie genau bei diesen Fragen zu unterstützen, habe wir mit dieser Datenschutzzeitung eine *Best Practice Checkliste* zusammengetragen, mit der auch Sie Ihr Schutzniveau prüfen und verbessern können. Zudem erhalten Sie einen ersten Einblick zum Thema technische und organisatorische Maßnahmen.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung zum Thema Datenschutz im Allgemeinen wünschen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer + 49 (0) 371 83652245 oder per E-Mail an datenschutz@dasax.de.

Mit besten Grüßen

Madlen Vogt

Was sind technische und organisatorische Maßnahmen (TOM)?

Unter *technischen und organisatorischen Maßnahmen (TOM)* versteht man ein Bündel von Handlungsanweisungen, die die Sicherheit für die Verarbeitung personenbezogener Daten sicherstellen soll. Sie können, je nach Firmengröße und potentiellen Risiken, unterschiedliche Aufwendungen nach sich ziehen, die in einer ordentlichen Datenschutz-Dokumentation vom Verantwortlichen verpflichtend nachgewiesen werden müssen.

Um einen ersten Ansatz zur Beschreibung diese technischen und organisatorischen Maßnahmen (TOM) zu finden, könnte der §64 Art. 3 im Bundesdatenschutzgesetzt (BDSG) sehr hilfreich sein. Hier werden die Anforderungen an die Sicherheit der Datenverarbeitung in folgende 14 Hauptrubriken unterteilt:

1. *Zugangskontrolle,*
2. *Datenträgerkontrolle,*
3. *Speicherkontrolle,*
4. *Benutzerkontrolle,*
5. *Zugriffskontrolle,*
6. *Übertragungskontrolle,*
7. *Eingabekontrolle,*
8. *Transportkontrolle,*
9. *Wiederherstellbarkeit,*
10. *Zuverlässigkeit,*
11. *Datenintegrität,*
12. *Auftragskontrolle,*
13. *Verfügbarkeitskontrolle und*
14. *Trennbarkeit*

Im Einzelnen sind das aber erst mal nur die Hauptthemen, die mit den Anforderungen des Unternehmens abgeglichen und in deutlich detailliertere Handlungsanweisungen untergliedert werden müssen.

In Verbindung mit dem folgend dargestellten *Art. 32 DSGVO | Sicherheit der Verarbeitung* erhält man so, einen sehr guten Überblick über die gesetzlichen Vorgaben, was für die Entwicklung und Erstellung individueller, dem Unternehmen angepasster, Checklisten sehr hilfreich ist.

Der Art. 32 DSGVO | Sicherheit der Verarbeitung

Art. 32 DSGVO | Sicherheit der Verarbeitung

1) *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:*

    1. *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
    2. *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
    3. *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
    4. *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

2) *Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.*

3) *Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*

4) *Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass Ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.*

Allgemeines zur Best Practice Checkliste

Die folgende Checkliste stellt eine Best Practice Empfehlung dar, die auch unter Berücksichtigung der Implementierungskosten, Firmengröße und potentieller Risiken individuell ergänzt oder reduziert werden sollte!

Best Practice Check: Management und Organisation

Mangelhafte Sicherheitsstrukturen in einer Organisation können den Betriebsablauf erheblich gefährden. Daher sollten immer alle bestehende Fachkompetenzen genutzt und in den Prozess zur Umsetzung von Sicherheitsanforderungen mit eingebunden werden. Unter anderem sollte nicht nur der IT-Verantwort liche, sondern immer auch der Datenschutzbeauftragte (DSB) und - wenn vorhanden - der IT-Sicherheitsbeauftragte in die Entscheidungsfindungen mit einbezogen werden.

- ❑ Eine geeignete Organisationstruktur für Informationssicherheit ist vorhanden und die Informationssicherheit ist in die organisationsweiten Prozesse und Abläufe integriert?
- ❑ Sicherheitsricht- und -leitlinien sind definiert, von der Geschäftsleitung genehmigt und dem Personal kommuniziert?
- ❑ Die Rollen der einzelnen Mitarbeiter im Sicherheitsprozess sind eindeutig festgelegt?
- ❑ Eine regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus (Plan-Do-Check-Act) ist gewährleistet?
- ❑ Konzepte und Dokumentationen im Sicherheitsumfeld werden regelmäßig überprüft und aktuell gehalten?
- ❑ Je nach Unternehmensgröße: Wird ein geeignetes Informationssicherheitsmanagementsystem (ISMS), z. B. nach ISO/IEC 27001, BSI-Standards oder ISIS12 eingesetzt?
- ❑ Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind im eigenen Betrieb bekannt und besetzt (u. a. Informationssicherheitsbeauftragter (ISB), IT-Leiter, Datenschutzbeauftragter (DSB))?
- ❑ Die konsequente Einbindung des DSB bei Sicherheitsfragen ist sichergestellt?
- ❑ Die ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen, bzw. die Möglichkeiten zur Themenspezifischen Fortbildung ist sichergestellt?
- ❑ Die regelmäßige Durchführung von Audits des DSB nach Art. 32 DSGVO zur Sicherheit der Verarbeitung ist organisiert und sichergestellt?

- ❑ Kenntnis der zuständigen Datenschutzaufsichtsbehörde sowie Wissen über die Meldeverpflichtungen nach Art. 33 und 34 DSGVO (Verletzung der Sicherheit)
- ❑ Vorhandensein von Eskalationsprozessen bei Sicherheitsverletzungen (Wer ist wann wie zu informieren?), u. a. im Notfallmanagement
- ❑ Konsequente Dokumentation bei Sicherheitsvorkommnissen (Security Reporting)
- ❑ Aktive Unterstützung der Zusammenarbeit des DSB mit dem ISB durch die Unternehmensleitung
- ❑ Erkenntnisse über (neue) digitale Bedrohungen sind zu sammeln und potentielle Auswirkungen auf den eigenen Betrieb abzuleiten

Best Practice Check: Physikalische Sicherheit der Infrastruktur

Der persönliche Zugang zu IT-Systemen und damit auch zu personenbezogenen Daten muss Unbefugten erschwert werden. Ebenso sind gravierende Schäden durch (Natur-) Ereignisse wie Feuer oder Wasser bestmöglich zu verhindern.

- ❑ Es besteht ein umfassendes Gesamtkonzept zur Gebäudeabsicherung im Allgemeinen (z. B. Brandschutz, Zutrittsbeschränkung und -kontrolle)?
- ❑ Es besteht ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz)?
- ❑ Es gibt klare Regelungen zum Umgang mit Besuchern (z. B. Begleitung, Sicherheitszonen, Besucherausweise, Protokollierung, Zuständiger Mitarbeiter für Besucher) als Bestandteil des Konzepts?
- ❑ Es gibt gelebte Regelungen zum Umgang mit externen Dienstleistern (z. B. bei Werkverträgen, Handwerkern, Wartung von Systemen) – wie Verschwiegenheitserklärung, persönliche Begleitung in Sicherheitszonen oder Protokollierung?
- ❑ Sicherheitszonen:
  - ❍ wurden eingerichtet (z. B. Besprechungsräume, Serverräume, Arbeitsplätze, Forschungsbereich)?
  - ❍ es gibt eine aktuelle Übersicht zur Berechtigungsverwaltung? Welcher Mitarbeiter darf in welche Zone?
  - ❍ der Zugang zu Sicherheitszonen ist mit geeigneter Technik begrenzt (z. B. über Schlüssel/Chipkarten/…, weitere Faktoren)?
  - ❍ bei Zonenübergängen wurden selbstschließende Türen eingesetzt?
  - ❍ Gibt es ggf. eine Beschilderung, welche Zone nicht betreten werden soll/darf?

- ❑ Es gibt sichere Schließsysteme samt dokumentierter Schlüsselverwaltung?
- ❑ Besteht ein Brandschutzkonzept?
- ❑ Sind Feuer-/Rauchmeldeanlagen (im Rahmen des Brandschutzkonzepts) im Einsatz?
- ❑ Sind automatische Löschsysteme in Serverräumen (z. B. CO2-Löschung) unter Berücksichtigung von Arbeitsschutzvorschriften im Einsatz?
- ❑ Sind feuerhemmende Schränke/Tresore zur Lagerung essentieller Komponenten (z. B. Backup-Bänder, wichtige Originaldokumente) im Einsatz?
- ❑ Das Gebäude (z. B. Wände, Fenster) und die Infrastruktur (z. B. Leitungen, Gefahrenmeldeanlagen) werden regelmäßig geprüft und gewartet?
- ❑ Gibt es eine Umzäunung des Betriebsgeländes?
- ❑ Gibt es stabile, einbruchshemmende Fenster und Türen im EG (z. B. nach DIN EN 1627)?
- ❑ Sind Alarmanlagen zur Einbruchserkennung, insbesondere außerhalb der Arbeitszeit aktiv?
- ❑ Wird Sicherheitspersonal (ggf. extern) eingesetzt?
- ❑ Sind Videoüberwachungssysteme (unter Berücksichtigung aller datenschutzrechtlicher Anforderungen (Monitoring des Zugangsschutzes)) im Einsatz?
- ❑ Ist eine ausreichende Klimatisierung der Serverräume gewährleistet?
- ❑ In Serverräumen sollte es keine zu öffnenden Fenster geben. Ist das so sichergestellt, oder sind die Fenster vor unberechtigtem Eindringen ausreichend geschützt?
- ❑ Sind Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (unterbrechungsfreie Stromversorgung (USV)), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen im Einsatz?
- ❑ Wurde vor Elementargefahren vorgebeugt (insb. vor Feuer, Rauch, Erschütterungen, chemische Reaktionen, Überschwemmungen, Stromausfälle, Explosionen und Anschläge/Vandalismus)?
- ❑ Wurden Risiken durch Überflutung/Starkregen geprüft, insbesondere bei Serverräumen im Keller oder anderen gefährdeten Bereichen?

Best Practice Check: Awareness der Mitarbeiter:innen

Beschäftige stehen mittlerweile verstärkt im Fokus von Cyberattacken. Zum Beispiel sollen sie mittels raffiniertem Social Engineering dazu verleitet werden, sicherheitskritische Aktionen auszuführen. Mitarbeiter:innen müssen daher gerade in Sicherheitsfragen stetig geschult und sensibilisiert werden, um solche Angriffe schon im Vorfeld zu vereiteln.

- ❑ Hat jede:r Mirarbeiter:in eine der Funktion angemessene Schulung für Informationssicherheit und Datenschutz erhalten?
- ❑ Werden auch neue Beschäftigte zeitnah geschult/unterwiesen?
- ❑ Werden regelmäßige Auffrischungsschulungen für bestehendes Personal durchgeführt (z. B. einmal pro Jahr)?
- ❑ Werden im Betrieb regelmäßig Informationen über Neuigkeiten zum Datenschutz und der IT-Sicherheit (z. B. per E-Mail, im Intranet, einer Kollaborationsplattform, Aushang) bereitgestellt?
- ❑ Werden relevante Richtlinien, z. B. zur E-Mail-/Internetnutzung, zum Umgang mit Schadcodemeldungen, zum Einsatz von Verschlüsselungstechniken, aktuell gehalten und sind diese für alle leicht auffindbar?
- ❑ Ist ein Datenschutzhandbuch (welches z. B. auch Schulungsinhalte bereitstellt) zugänglich und für alle betroffenen Mitarbeiter:innen verfügbar?
- ❑ Schulungsinhalte:
  - ❍ ausgewählte Mitarbeiter:innen, die bei der Erkennung von Sicherheitsverletzungen beteiligt sind (z. B. IT, DSB, Geschäftsführung, Führungskräfte, Geschäftsstelle, Telefonzentrale oder Sekretariat) kennen die internen Prozesse zum Umgang mit Vorfällen (u. a. Meldung nach Art. 33 DSGVO, Notfallplan)?
  - ❍ Beschäftigte wissen, wie Cyberangriffe mittels Social-Engineering eingeleitet werden (Hilfe zur Selbsthilfe)?
  - ❍ Beschäftigte kennen die Gefahren der E-Mail-Kommunikation, insbesondere bei verschlüsselten E-Mail-Anhängen (z. B. bei Zip-Dateien)?
  - ❍ Beschäftigte erkennen gefälschte E-Mails (z. B. an Absenderadressen, Auffälligkeiten, eingebettete Links)?
- ❑ Das Personal wurde sensibilisiert, u. a. wie man mit Externen interagiert und welche Daten in welcher Form weitergegeben werden dürfen, bzw. was sicherheitskritisch sein kann (angemessene Einsatzregeln, Richtlinien, Prozesse und Verhalten)?
- ❑ Von Heimarbeit betroffenen Mitarbeiter wurde die sichere Nutzung von Home-Office Lösungen erläutert und spezifische Gefahren aufgezeigt?

Best Practice Check: Authentifizierung

Digitale Zugangsbeschränkungen helfen im Alltag. Nutzer von IT-Systemen und Diensten müssen daher Ihre Zugangsberechtigung mit geeigneten Mitteln nachweisen.

- ❑ Alle Mitarbeiter:innen haben in den Umgang mit Authentifizierungsverfahren und –mechanismen eine Einweisung erhalten?
- ❑ Es gibt einen geregelten Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage, Änderung oder Löschung eines Mitarbeiters, bzw. einer Mitarbeiterin?
- ❑ Hat jeder Nutzer eine eindeutige Kennung?
- ❑ Wurden Gruppenkennungen vermieden?
  Kommen Gruppenkennungen zum Einsatz, sollte eine datenschutz konforme Protokollierung der jeweiligen Nutzeraktivitäten sichergestellt sein!
- ❑ Ist die Verwendung von starken Passwörtern sichergestellt?
- ❑ Gibt es eine Passwortrichtlinie, z. B. möglichst mit automatischer Umsetzung der Richtlinie.
- ❑ Wird die Auswahl schwacher Passwörtern (z. B. über die Richtlinien oder technisch erzwungen über das IMS) verhindert?
- ❑ Gibt es eine Regel, dass Passwörter nach festgelegten Zeiträumen (z. B. alle 60 Tage) geändert werden müssen?
- ❑ Ist gewährleistet, dass Passwörter nach einem Sicherheitsvorfall, auch im Verdachtsfall, gesperrt und vom Nutzer neu vergeben werden müssen?
- ❑ Ist dem Personal bekannt, dass beim erstmaligen Login eines neuen Nutzers oder nach der Zurücksetzung des Passworts durch die IT (z. B. bei Vergessen des Passworts) eine Passwortänderung erfolgen muss?
- ❑ Ist bekannt, dass Passwörter nicht (auch nicht an Kollegen, Vorgesetze oder die IT-Abteilung) weitergegeben werden dürfen, bzw. im Notfall (z. B. bei einer längeren Erkrankung) durch die IT zurückgesetzt werden und die Rücksetzung dokumentiert werden muss?
- ❑ Sind alle Beschäftigten eingewiesen, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen?
- ❑ Ist sichergestellt, dass keine Speicherung von Passwörtern im Browser stattfindet, ohne mind. durch ein Masterpasswort abgesichert zu sein?
- ❑ Ist sichergestellt, dass es keine Mehrfachverwendung eines Passworts für verschiedene Dienste gibt, sofern kein zentrales Identitätsmanagement (z. B. Active Directory) verwendet wird?

- ❑ Ist sichergestellt, dass keine Passwörter per E-Mail übermittelt werden (z. B. für einen Firmenaccount zu einem Cloud-Dienst)?
- ❑ Gibt es für lokale Admin-Konten besonders starke Passwörter (z. B. mind. 16-stellig, komplex und ohne übliche Wortbestandteile sowie unterschiedlich für jeden PC)?
- ❑ Kommen Verfahren zur Zwei- oder Mehr-Faktor-Authentifizierung bei Verarbeitungstätigkeiten mit hohem Risiko (z. B. Chipkarten, USB-Sticks, Token) zum Einsatz?
- ❑ Soweit möglich sollte ein konsequenter Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung für Administratorkonten bei Anwendungen realisiert werden. Ist das der Fall?
- ❑ Bei Zwei-Faktor-Authentifizierung ist der Einsatz von biometrischen Merkmalen (z. B. Fingerprint) bei zentralen Systemen (z. B. Zugangssteuerung zu Sicherheitszone) nur in Ausnahmefällen anzuwenden – lokale Speicherung (z. B. iPhone) ist dagegen häufiger zu realisieren.
  Wurde dies berücksichtigt?
- ❑ Ist die automatische Sperrung von Zugängen bei zu vielen Fehlversuchen durch ein falsches Passwort realisiert?
- ❑ Gibt es eine Zeitverzögerung zwischen einzelnen Login-Versuchen (insbesondere bei über das Internet erreichbaren Anwendungen) zur Erschwerung von automatischen Online-Angriffen?
- ❑ Gibt es eine Darstellung der Anzahl der fehlgeschlagenen Logins für einen Nutzer, der sich erfolgreich anmeldet hat? Ziel: Transparenz für stattgefundene Angriffe bzw. Angriffsversuche schaffen.
- ❑ Werden Passwörter mit geeignete kryptographischen Verfahren verschlüsselt?
- ❑ Sind Regelungen zum automatischen Sperren von Passwörtern nach einem Sicherheitsvorfall getroffen (z. B. Passwort-Hash so abändern, dass kein Klartextpasswort dazu besteht)?
- ❑ Falls Chipkarten als Mitarbeiterausweise eingesetzt werden, prüfen, ob diese für Standardauthentifizierungen (z. B. für einen Betriebssystem-Login) verwendet werden können. Wurde die Prüfung abgeschlossen?
- ❑ Ist bekannt, dass Standard-Authentifizierungsinformationen durch Hersteller bei Software nach der Installation geändert werden müssen?

Best Practice Check: Rollen-/Rechtekonzept

Nutzer sollen nur auf die personenbezogenen Daten zugreifen können, die für ihre Tätigkeit erforderlich sind. Durch Einführung von Benutzerrechten zu bestimmten Rollen (z. B. Buchhaltung, IT-Administration) werden unterschiedliche Rechte an konkrete Personen zugewiesen.

- ❑ Wurden Rollenprofile für die Beschäftigten unter Einbeziehung der Einträge des Verzeichnisses der Verarbeitungstätigkeiten erstellt?
- ❑ Wird über das Rollen-/Rechtekonzept der Zugang zu Informationen und Gebäuden/Bereichen gezielt gesteuert und reglementiert?
- ❑ Gibt es Regelungen zur Verwaltung der Rollen (Zuweisung, Entzug) und wurden diese bei allen Mitarbeiter:innen etabliert?
- ❑ Wird eine regelmäßige Überprüfung realisiert (z. B. einmal pro Jahr), ob die Zuweisung der Rollen noch den Vorgaben entsprechen, bzw. ob diese noch den Anforderungen der Geschäftstätigkeit entsprechen?
- ❑ Wird berücksichtigt, dass Administratorkennungen für Nutzer gelten, die auch administrative Tätigkeiten ausführen?
- ❑ Gibt es administrative Rollen, z. B. zur Anlage neuer Benutzer, zur regelmäßigen Durchführung von Backups, der Konfiguration der Firewall?
- ❑ Ist gewährleistet, dass Superuser (z. B. root unter Linux) soweit möglich nicht zum Einsatz kommen?
- ❑ Wurden für Beschäftigte mit IT-Administrationsaufgaben zwei Benutzerkennungen eingerichtet (eine Administrationskennung und eine normale Nutzerkennung (z. B. für nicht-administrative Zwecke)?
- ❑ Wurden Regelungen etabliert, dass unter Nutzung von Administratorenrechten nicht im Internet gesurft oder E-Mails gelesen/ versendet werden dürfen?

Best Practice Check: Endgeräte (Clients)

Die für die tägliche Arbeit genutzten Endgeräte der Nutzer müssen dauerhaft abgesichert werden. Keine oder unzureichende Regelungen führen meist zu offenen Schwachstellen auf Clientsystemen, von denen dann eine erhebliche Gefährdung für die gesamte Organisation ausgehen kann.

- ❑ Eine Geräteverwaltung (wer setzt welche Geräte in welchem Bereich ein?) ist vorhanden?
- ❑ Ist ein automatisches Sperren nach einer gewissen Zeitspanne der Inaktivität eingestellt, falls manuelles Sperren bei Verlassen des Einflussbereichs nicht gewährleistet werden kann?

- ❑ Wurden bei potentiell unbefugter Einsichtnahme (z. B. im Kundenempfangsbereich) Blickschutzfolien angebracht?
- ❑ Wurde eine Firewall aktiviert, die unerwünschte Servicedienste auf dem Endgerät blockiert?
- ❑ Wird eine Anti-Viren-Lösung mit tagesaktuellen Signatur-Updates genutzt und gibt es Regeln, wie im Falle einer Warnmeldung zu verfahren ist?
- ❑ Gibt es eine zentrale Erfassung von Schadcode-Alarmmeldungen durch die IT-Administration?
- ❑ Gibt es einen Ablaufplan für die IT-Administration bei Schadcode-Befall?
- ❑ Ist ein Konzept zum Patch Management vorhanden?
- ❑ Gibt es regelmäßige Auswertungen von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software und Fachanwendungen (z. B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen)?
- ❑ Ist - sofern möglich - das automatische Einspielen von Sicherheitsupdates des Betriebssystems, der installierten Software oder von Softwarebibliotheken (z. B. Java) eingestellt?
- ❑ Ist gewährleistet, dass alle personenbezogene Daten von einem Backup erfasst und mitgesichert werden (z. B. über ein Netzlaufwerk)?
- ❑ Ist die Einbindung von externen Geräten durch technische Maßnahmen auf das erforderliche Mindestmaß begrenzt (z. B. bei USB-Sticks, Smartphones, externe Festplatten)?
- ❑ Ist der Auto-Start von externen Medien (z. B. USB-Sticks) deaktiviert?
- ❑ Ist sichergestellt, dass Fernwartungen ausschließlich über verschlüsselte Verbindungen und nach Authentifizierung durch den Administrator und Freigabe durch den Nutzer erfolgen?
- ❑ Werden nur Betriebssysteme und Software eingesetzt, für die noch Sicherheitsupdates zur Verfügung gestellt werden?
- ❑ Wird die Ausführung von (aus dem Internet) heruntergeladener Software, deren Quellen als unsicher gekennzeichnet werden, verhindert?
- ❑ Der Zugang zu Internet sollte restriktiv verwaltet werden, so dass das Risiko einer Kompromittierung z. B. durch Malware verringert und der Zugriff auf nicht autorisierte Websites verhindert wird (z. B. über Web-Proxy mit aktuellen Sperrlisten). Ist das so umgesetzt?
- ❑ Wird die automatische Ausführung von Programmen aus dem temporären Download-Verzeichnis des Internetbrowsers unterbunden?

- ❑ Werden Anwendungen an den Endgeräten möglichst ohne Administratorrechte ausgeführt?
- ❑ Wurde ein Prozess aufgesetzt, mit dem eine wirksame Datenlöschung vor der Weitergabe eines Endgeräts sichergestellt ist?
- ❑ Ist ein Sicherheitskonzept für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten vorhanden (z. B. um die unerlaubte Einsicht in ausgedruckte Dokumente zu unterbinden, einen ausreichenden Schutz gespeicherter Informationen oder die ordnungsgemäße Entsorgung zu gewährleisten)?

Best Practice Check: Mobile Datenspeicher

Der weit verbreitete Einsatz von USB-Datenträgern, Notebooks und Smartphones macht Regelungen zur Nutzung und auch für den Verlustfall erforderlich. Ungeschützte Speichermedien ermöglichen ansonsten Unbefugten ohne großen Aufwand Zugriff auf sensible Daten.

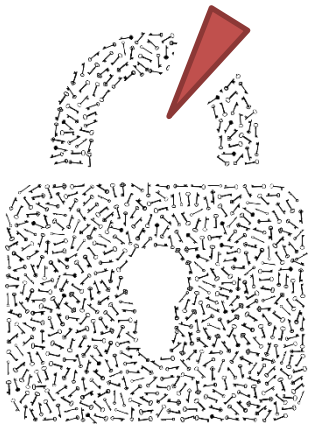
- ❑ Ist eine starke Verschlüsselung der mobilen Endgeräte (z. B. Festplattenverschlüsselung, Container-Lösungen) sichergestellt?
- ❑ Werden Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust und Diebstahl eingesetzt?
- ❑ Bei Smartphones – werden folgende Vorgaben beachtet:
  - ❍ Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort) – Länge der Kennung in Abhängigkeit von automatischen Sperr- und Löschfunktionen.
  - ❍ Einsatz von biometrischen Zugangsverfahren nur bei ausschließlich lokaler Speicherung der biometrischen Templates innerhalb eines Secure-Chips auf dem Smartphone und bei personenbezogenen Daten mit keinem hohen Risiko.
  - ❍ Cloud-Speicher für Datenbackup erst nach sorgfältiger Prüfung der datenschutzrechtlichen Anforderungen einsetzen (auch Beschäftigtendatenschutz bei „Find my Phone“-Funktionen).
  - ❍ Mobile Device Management Lösungen zur Konfiguration und Verwaltung der Geräte, der installierten Apps sowie dem Auffinden/Löschen im Verlustfall.
  - ❍ Nur sichere Quellen werden für die Installation von Apps verwendet.
  - ❍ Apps werden vorher getestet und zur Anwendung freigegeben.

- ❑ Wurden Regelungen geprüft, ob es ausreichend ist, bei Nutzung mobiler Arbeitsplätze (z. B. Notebook auf Dienstreise) auf weniger Daten als innerhalb des internen Unternehmensnetzes zugreifen zu können?
- ❑ Gibt es eine Diebstahlsicherung?
- ❑ Gibt es eine Regelung zur Privatnutzung bei Notebooks und Smartphones? Empfehlung: Keine Privatnutzung!
- ❑ Die Mitarbeiter kennen die Regelungen bei Verlust eines mobilen Endgerätes, z. B. Verlustmeldung beim Unternehmen und/oder Polizei?
- ❑ Bei mobilen Datenträgern:
  - ❍ es gibt eine Richtlinie zum sicheren Umgang mit mobilen Datenträgern. Die Mitarbeiter kennen diese Richtlinie und sind im Umgang mit mobilen Datenträgern geschult?
  - ❍ das sichere Löschen der Datenträger vor und nach der Verwendung ist sichergestellt?

Best Practice Check: Serversysteme

Serversysteme müssen mit besonderer Sorgfalt abgesichert werden, da Sicherheitsverletzungen dort i. d. R. aufgrund der großen Menge personenbezogener Daten enorme Auswirkungen haben können.

- ❑ Sind alle Administratoren entsprechend qualifiziert?
- ❑ Es werden verschiedene Administrationsrollen mit reduzierten Rechten nach dem Least-Privileg-Prinzip für unterschiedliche Administrationsaufgaben (z. B. Softwareupdates, Konfiguration, Backup) eingesetzt?
- ❑ Es gibt einen Prozess zum zeitnahen Einspielen von Sicherheitsupdates? Kritische Updates müssen unverzüglich eingespielt werden!
- ❑ Werden eigene Administrations-Endgeräten über eine dezidierte Netzwerkverbindung verwendet?
- ❑ Werden - soweit möglich - Verfahren zur Zwei-Faktor-Authentifizierung eingesetzt?
- ❑ Wurden nicht benötigte Standard Server-Dienste (z. B. Webserver, Printserver) deaktiviert/deinstalliert?
- ❑ Wurden lokale Dienste über eine Firewall vor Außenzugriffen blockiert?
- ❑ Wurden weitere Härtungsmaßnahmen für das eingesetzte System geprüft?
- ❑ Wurde die Versendung von Telemetriedaten an den Hersteller deaktiviert, sofern diese nicht als erforderlich eingeschätzt werden?



Best Practice Check: Websites und Webanwendungen

Webseiten und Webanwendungen stellen meist leicht zugängliche Plattformen für Angriffe dar, die mit bekannten Best-Practice-Ansätzen meist gut abgesichert werden können.

- ❑ Wird ein HTTPS-Protokoll nach Stand der Technik (TLS1.2 oder TLS1.3) eingesetzt?
- ❑ Werden alle Datenbanken auf dem Webserver mittels Firewalls geschützt?
- ❑ Werden die Fernzugänge zu Webservern verschlüsselt und mit einer Zwei-Faktor-Authentifizierung (z. B. SSH mit Client-Zertifikaten) geschützt?
- ❑ Werden Administrationsbereiche der Webanwendungen auf bestimmte IP-Adressen (z. B. Unternehmens- Gateway) limitiert?
- ❑ Sind die Administratoren entsprechend der Aufgabe ausreichend qualifiziert?
- ❑ Gibt es einen geregelten Prozess zum zeitnahen Einspielen von Sicherheitsupdates (Server, Webserver, Datenbanken, CMS, …)?
- ❑ Werden regelmäßig Sicherheitstests nach Best Practice-Vorgehen (z. B. OWASP Testing Guide) durchgeführt?
- ❑ HTTP-GET-Requests werden in den Webserver-Log-Dateien gespeichert und könnten durch eingesetzte Website-Tracker ausgeleitet werden. Werden HTTP-GET-Requests bei personenbezogener Daten (z. B. Mail-Adresse) vermieden?
- ❑ Ist die Trennung von Webserver, Anwendungslogik und Datenhaltung einer Webanwendung durch eigene Server, die in eine geeignete Firewall-Architektur (z. B. DMZ – Demilitarisierte Zone) eingebunden sind, gewährleistet?
- ❑ Ist eine Sperrung der Auffindung von Inhalten durch Suchmaschinen (über robots.txt) eingestellt, sofern diese Inhalte nicht durch eine Suchmaschine gefunden werden sollen?

Best Practice Check: Netzwerk

Angriffe über das Internet auf das eigene Netzwerk sind in vielen Organisationen möglich. Damit sich dadurch z. B. kein Schadcode ausbreiten kann, ist die eigene Netzwerkstruktur vor solchen negativen Fremdeinflüssen aktiv zu schützen.

- ❑ Werden geeignete Netzwerksegmentierungen durchgeführt?
  Restriktive (physikalische) Trennung sensitiver Netze (z. B. medizinische Netze in Krankenhäusern oder Personalverwaltung) von Verwaltungsnetzen (mittels Firewall-Systemen)

- ❑ Wird ein Proxy Server eingesetzt, über den alle HTTP(S)-Verbindungen gehen müssen?
- ❑ Werden HTTP(S)-Verbindungen abseits des Proxys blockiert? Ausnahmeregeln vermeiden!
- ❑ Werden IOCs (Indicators of Compromise, meist URL und IP-Hashes) protokolliert und blockiert?
- ❑ Werden IOCs aus geeigneten Quellen regelmäßig aktualisiert?
- ❑ Wurde eine DMZ eingerichtet?
  Einsatz geeigneter Firewall-Architekturen zur Absicherung rein interner Systeme (z. B. Arbeitsplatz, Drucker) zu den über das Internet erreichbaren Servern (z. B. Mail-Server, Web-Server, VPN-Endpunkt) - Gängig: Konzept einer DMZ (Demilitarisierten Zone)
- ❑ Sind alle WLAN-Zugänge auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen (z. B. WPA-2 mit mind. 24-stelligem Passwort, WP3-Enterprise oder Einsatz eines Radius-Servers)?
- ❑ Sind WLAN-Gastzugänge vom internen Netzwerk getrennt?
- ❑ Gibt es einen geregelten Prozess zur ordnungsmäßigen Konfiguration der Firewalls und der regelmäßigen Überprüfung der selbigen (z. B. zu der Notwendigkeit von Freigaben)?
- ❑ Gibt es Protokollierungen auf Firewall-Ebene, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren?
- ❑ Sind automatische Benachrichtigungen an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen eingerichtet?
- ❑ Gibt es eine regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans auf die eigenen IP-Adressen von extern und periodischer Pentests)?
- ❑ Sind die Administratoren der Firewall ausreichend qualifiziert?
- ❑ Wird eine Prüfung eingehender E-Mails mittels Anti-Malwareschutz durchgeführt?
- ❑ Werden gefährliche E-Mail-Anhänge (z. B. .exe, .doc, .cmd) blockiert?
- ❑ Werden unverschlüsselte Protokolle (z. B. FTP, Telnet) vermieden?
- ❑ Kommen Intrusion-Detection-Systeme (IDS) oder Intrusion-Prevention-Systeme (IPS) zum Einsatz?
- ❑ Wird die Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen mit Client-Zertifikatsauthentifizierung realisiert?

Best Practice Check: Archivierung

Archivdaten werden zwar für die tägliche Arbeit nicht mehr benötigt, müssen aber mitunter aufgrund gesetzlicher Aufbewahrungsfristen eine bestimmte Zeit lang weiterhin aufbewahrt werden. Eine Absicherung der enthaltenen personenbezogenen Daten ist daher auch dann zu gewährleisten.

- ❑ Sind Regelungen etabliert, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist?
- ❑ Wurden Zugänge zu den Archivdateien festgelegt?
  Dokumentieren, Umsetzen und Prüfen
- ❑ Archivdaten müssen nach Ablauf der Aufbewahrungsfrist wirksam gelöscht werden. Ist die Löschung geregelt?
- ❑ Archivierungen müssen auf Datenträgern gespeichert werden, die für eine lange Speicherdauer geeignet sind (z. B. keine wiederbeschreibbare DVDs). Ist das gewährleistet?
- ❑ Archivdaten sollten nicht in Produktivdatenbanken gespeichert, sondern in Archivsysteme überspielt werden. Ist das so eingestellt?
- ❑ Werden Archivdateien verschlüsselt aufbewahrt (an mind. zwei örtlich getrennten Stellen)?
- ❑ Wurden geeignete Datenformate für die Archivierung von Dokumenten ausgewählt, damit eine langfristige Lesbarkeit der Daten gewährleistet ist?

Best Practice Check: Wartung durch Dienstleister

Die Tätigkeiten von externen IT-Dienstleistern, insbesondere bei Wartung, müssen überwacht und dokumentiert werden. Um eine ungewollte Datenweitergabe zu verhindern, müssen personenbezogene Daten auf ausgemusterter Hardware sorgfältig gelöscht werden.

- ❑ Gibt es eine Dokumentation aller Tätigkeiten externer Dienstleister?
- ❑ Wurde eine Verschwiegenheitsverpflichtung in den Dienstleistungsvertrag aufgenommen oder vom externen Mitarbeiter unterzeichnet?
- ❑ Wurde Personal festgelegt, welches die Tätigkeiten von externen Dienstleistern überwacht (bzw. ggf. begleitet) und dokumentiert?
- ❑ Wurden Regelungen zur wirksamen Datenlöschung auf Hardware (z. B. PCs, Drucker, Smartphones) festgelegt, die vom Dienstleister oder Hersteller zurückgenommen werden (z. B. bei Defekten, Abschreibung)?
- ❑ Werden bei Einsatz von Fernwartungssoftware regelmäßig Sicherheitsupdates eingespielt und auf Informationen über bekannte Schwachstellen oder Fehlkonfigurationen hingewiesen?

Best Practice Check: Protokollierung

Mittels geeigneter Protokollierungen können Sicherheitsverletzungen nach Art. 33 DSGVO auch im Nachhinein erkannt und aufgearbeitet werden. Ohne Auflistung von Benutzeraktivitäten kann dagegen meist keine valide Bewertung stattfinden, ob und in welchem Umfang ein unbefugter Datenzugriff erfolgte.

- ❑ Wurde ein Konzept zur Protokollierung von Benutzeraktivitäten, technischen Systemereignissen, Fehlerzuständen und Internetaktivitäten unter Berücksichtigung datenschutzrechtlicher Anforderungen (u. a. auch Beschäftigtendatenschutz) erstellt?
- ❑ Speicherung der Log-Dateien auf einem eigenen Log-Server?
- ❑ Die Uhren der verwendeten Informationsverarbeitungssysteme (PCs, Notebooks, etc.) sollten mit geeigneten Zeitquellen synchronisiert werden, um eine gezielte Analyse bei Sicherheitsereignissen zu ermöglichen. Ist das so eingestellt?
- ❑ Wird die Einhaltung der Zweckbindung der Log-Dateien sichergestellt? Die Personalvertretung ist ggf. einzubinden.
- ❑ Regelmäßige anlasslose Auswertung der Log-Dateien zur Erkennung von ungewöhnlichen Einträgen – bevorzugt: Automatische Heuristiken

Best Practice Check: Business Continuity

Die Verfügbarkeit der Geschäftsprozesse und der damit verbundenen IT-Systeme und Daten ist zu gewährleisten. Im Rahmen des Backup-Konzepts ist daher ein geordnetes Zusammenspiel beim Wiedereinspielen gespeicherter Datenbestände wichtig, um im Notfall weiter betriebsfähig zu bleiben.

- ❑ Wurde ein Notfallplan zur Business Continuity erstellt?
  Regelungen, welche Systeme in welcher Reihenfolge wiederinstandgesetzt werden, welche (externen) Personen/Dienstleister im Notfall zu Rate gezogen werden können sowie welche Meldeverpflichtungen es gibt.
- ❑ Der Notfallplan wird regelmäßig überprüft, z. B. durch Notfallübungen?
- ❑ Vorhandensein eines schriftlich fixierten Backup-Konzepts?
- ❑ Werden Backups nach der 3-2-1 Regel durchgeführt?
  3 Datenspeicherungen, 2 verschiedene Backupmedien (auch „Off-line“ wie Bandsicherungen) und 1 davon an einem externen Standort.
- ❑ Gibt es eine geeignete physische Aufbewahrung von Backupmedien (z. B. Tresor, unterschiedliche Brandabschnitte, Gefahr von Wasserschäden, …)?
- ❑ Gibt es regelmäßige Überprüfungen, ob mindestens ein Backup täglich durchgeführt wird und die Wiederherstellung funktioniert?

- ❑ Mindestens ein Backup-System ist durch Schadcode nicht verschlüsselbar, z. B. spezielles Datensicherungsverfahren wie Pull-Verfahren des Backup-Systems oder getrennt (offline) nach Abschluss des Backup-Prozesses?
- ❑ Weitestgehend wird auf Makros in Office-Dokumenten im Betriebsalltag zum Schutz vor Ransomware verzichtet?
- ❑ Zulassen ausschließlich signierter Microsoft Office-Makros oder (regelmäßige) Information, bspw. einmal pro Jahr, der Beschäftigten über Risiken einer Makro-Aktivierung (z. B. in Microsoft Word)?
- ❑ Wird das automatische Ausführen von heruntergeladenen Programmen (z. B. Software Restriction Policy und Sandboxing) verhindert?
- ❑ Deaktivierung von Windows Script Hosts (WSH) auf Clients (sofern nicht zwingend benötigt) der Prüfung, ob die Einschränkung von Powershell-Skripten mit dem „Constrained-Language Mode“ auf Windows-Clients sinnvoll durchführbar ist der Nutzen eines Web-Proxys mit (tages-) aktuellen Sperrlisten von Schadcode-Download-Seiten (IOCs)
- ❑ Der Notfallplan beinhaltet den Umgang mit Verschlüsselungstrojanern und dieser liegt auch in Papierform vor?
- ❑ Findet eine regelmäßige Überprüfung der Backup- und Recovery-Strategie statt, die sicherstellt, dass Backups durch die Ransomware nicht verschlüsselt werden können?

Best Practice Check: Kryptographie

Mittels kryptographischen Verfahren nach Stand der Technik kann die Vertraulichkeit, Integrität und Authentizität von Daten, Systemen und Entitäten sichergestellt werden.

- ❑ Wurden Regeln für die effektive Nutzung der Kryptographie, einschließlich der Schlüsselverwaltung, definiert?
- ❑ Mit Hash-Verfahren kann die Integrität von Daten, Software und IT-Systemen erreicht werden – Stand der Technik sind u. a SHA-256, SHA-512, SHA-3, bcrypt, Blowfish. Werden solche Hash-Verfahren eingesetzt?
- ❑ Passwortspeicherung nur dann mit „normalen“ Hashfunktionen (z. B. SHA-Klasse), wenn Passwort mind. 12 stellig ist – Einsatz von Salt-Werten als Schutz vor Eintrag in verfügbaren Datenbanken (Rainbow Tables).
- ❑ Passwortspeicherung mit Salt nach Stand der Technik mit z. B. HMAC/SHA256, bcrypt, scrypt, PBKDF2.
- ❑ Symmetrische Verschlüsselung nach Stand der Technik mit z. B. AES-256 mit CBC/GCM Modus.

- ❑ Gibt es eine asymmetrische Verschlüsselung nach Stand der Technik mit z. B. RSA-2048 Bit (oder höher), EC-256 Bit (oder höher)?
- ❑ Eine wirksame Schlüsselverwaltung (Generierung, Ausgabe, Sperrung) ist bei Einsatz kryptographischer Verfahren essentiell. Wurde das umgesetzt?
- ❑ Ist der Schutz von geheimen Schlüsseln durch starke Passwörter mit mindestens 16 Stellen gewährleistet? Bei hohem Risiko Einsatz von HSM (Hardware Security Modulen) prüfen!
- ❑ Wurden alle SSL-Zertifikate bei vertrauenswürdigen Zertifizierungsstellen beschafft?
- ❑ HTTPS nach Stand der Technik (z. B. mind. 2048-Bit RSA, Perfect Forward Secrecy, HSTS, ggf. Client Zertifikate) einsetzen.
- ❑ Keine kryptographischen Verfahren mit bekannten Schwachstellen oder zu kurzer Schlüssellänge mehr verwenden, z. B. DES, 3-DES, MD5, SHA-1 – falls Altsystem diese noch erfordern, ist eine individuelle Risikoanalyse durchzuführen.

Best Practice Check: Datentransfer

Sowohl der Datenaustausch mit anderen Stellen über elektronische Kommunikationsnetze als auch der physikalische Transport von mobilen Datenträgern und Dokumenten müssen derart abgesichert werden, dass die Vertraulichkeit und Integrität der personenbezogenen Daten nicht beeinträchtigt wird.

- ❑ Wurden Regeln für alle Arten von Datentransfers sowohl innerhalb der Organisation als auch zwischen der Organisation und anderen Parteien getroffen?
- ❑ Wurden für Cloud-Diensten Verfahren zur Nutzung etabliert? (inklusive einer möglichen Ausstiegsstrategie, um Abhängigkeiten zu einzelnen Cloud-Diensten zu reduzieren).
- ❑ Wurden Verschlüsselungen von mobilen Datenträgern (wie DVD, USB-Sticks, Festplatte) nach Stand der Technik eingerichtet?
- ❑ Bei E-Mail, Cloud-Plattformen:
  - ❍ Transportverschlüsselung von personenbezogenen Daten nach Stand der Technik bei normalem Risiko.
  - ❍ Transportverschlüsselung und Inhaltsverschlüsselung von personenbezogenen Daten nach Stand der Technik bei hohem Risiko.

- ❑ Bei Messenger:
  - ❍ Transport- und Inhaltsverschlüsselung der Nachrichten und Dateien
- ❑ Ist die Integrität von personenbezogenen Daten durch digitale Signaturen zumindest bei hohem Risiko gewährleistet?
- ❑ Bei HTTPS:
  - ❍ Einsatz von Client-Zertifikaten zum Nachweis der Authentizität bei geschlossenem Nutzerkreis.
- ❑ Wird die verschlüsselte Nutzung von DNS-Diensten (DNSSec, DNS-over-TLS) regelmäßig geprüft?

Best Practice Check: Entwicklung und Auswahl von Software

Datenschutz und Sicherheit müssen frühzeitig bei der Entwicklung von eigenen Softwaresystemen bzw. bei der Auswahl von Softwareprodukten im eigenen Betrieb berücksichtigt werden.

- ❑ Relevante Mitarbeiter sind darüber geschult, dass Security-by-Design (Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität) als Teilmenge von Data-Protection-By-Design eine gesetzliche Datenschutzanforderung ist und Einfluss auf zentrale Designentscheidungen (Produktauswahl, zentral vs. dezentral, Pseudonymisierung, Verschlüsselung, Land eines Dienstleisters) hat?
- ❑ Es findet eine Trennung von Produktivsystem zu Entwicklungs-/Testsystem statt?
- ❑ Der Zugang zum Source-Code wurde bei der Entwicklung von Software beschränkt?
- ❑ Es werden keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung abgelegt?
- ❑ System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests, werden regelmäßig durchgeführt?
- ❑ Ausreichende Testzyklen werden berücksichtigt?
- ❑ Das fortlaufende Inventarisieren der Versionen von Software oder Komponenten (z. B. Frameworks, Bibliotheken) sowie deren Abhängigkeiten ist realisiert?
- ❑ Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen?
- ❑ Wurde sichergestellt, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen für die gesamte Lebenszeit einer Softwareanwendung besteht?

Best Practice Check: Auftragsverarbeiter

Dienstleister, die personenbezogene Daten im Rahmen einer Auftragsverarbeitung behandeln, benötigen geeignete Garantien, damit auch die Sicherheit der Verarbeitung gewährleistet werden kann.

Folgende Anforderungen sollten erfüllt sein:

- ❑ Nur Dienstleister verwenden, die die Garantien (in Form von Dokumenten) zur Verfügung stellen können.
- ❑ Sicherheitsmaßnahmen nach Art. 32 DSGVO als Bestandteil eines AV-Vertrags müssen zur Dienstleistung passen – das Abstraktionsniveau der Maßnahmen ist mitunter leicht höher als bei internen TOM-Listen eines Verantwortlichen.
- ❑ Die Wirksamkeit der Garantien kann durch geeignete Zertifizierungen (ansatzweise) nachgewiesen werden – Bsp.: ISO 27001 bei Rechenzentrum mit Scope Physikalische Sicherheit ist meist aussagekräftig.
- ❑ Eine Vor-Ort-Kontrolle durch den Verantwortlichen darf nicht ausgeschlossen werden.
- ❑ Der Auftragsverarbeiter darf keine weiteren Subdienstleister ohne Information des Auftraggebers aufnehmen – dieser hat dann ein Widerspruchsrecht.
- ❑ Der Auftragsverarbeiter muss Prozesse bei der Erkennung von Datenschutzverletzungen haben und diese unverzüglich dem Verantwortlichen im Sinne der DSGVO melden.
- ❑ Transfers in unsichere Drittländer sind ggf. nur mit weiteren technischen Schutzmaßnahmen, primär dem Einsatz von kryptographischen Verfahren, möglich.
- ❑ Daten werden bei Auftragsverarbeitung (spätestens) nach Vertragsende wirksam gelöscht.
- ❑ Angaben zur Löschmethodik können zur Verfügung gestellt werden?
- ❑ Eine regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung ist sichergestellt.

Quellenangabe und allgemeine Informationen zur *TOM Best Practice Checkliste*

Die Vorangegangene *Checkliste* wurde auf Basis des Art. 32 DSGVO und einer Veröffentlichung des Bayerisches Landesamt für Datenschutzaufsicht „Generischer Ansatz nach Art. 32 DSGVO zur Sicherheit“ erstellt. Sie hat keinen Anspruch auf Vollständigkeit und sollte, auch unter Berücksichtigung der Implementierungskosten, Firmengröße und den potentiellen Risiken, für jedes Unternehmen individuell ergänzt oder reduziert werden!

Oktober | 2021

Impressum

Dasax GmbH
Hainstraße 105
09130 Chemnitz
Tel.: +49 (0) 371 83652245
Web: www.dasax.de
E-Mail: datenschutz@dasax.de

Amtsgericht Chemnitz, HRB 31934
Ust-IdNr.: DE319948987

Redaktion
Madlen Vogt

Bildnachweise
Diese Unterlage wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Einige der dargestellten Bilder wurden von der ITKservice bei https://www.ccvision.de gekauft und lizensiert. Weitere stammen von https://pixabay.com/de/ einer Plattform für lizenzfreie Bilder.