Good Practice bei technischen und organisatorischen Maßnahmen (Version 2020)

Generischer Ansatz nach Art. 32 DSGVO zur Sicherheit

Ziel und Inhalt dieses Papiers

Die DSGVO fordert von Verantwortlichen und Auftragsverarbeitern in Art. 32 DSGVO ein Schutzniveau, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen ist. Dabei sollen zur Gewährleistung der Sicherheit der insbesondere die Risiken berücksichtigt werden, die aus einer Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten, der an deren Verarbeitung beteiligten IT-Systeme, Dienste und Fachprozesse hervorgehen können. Ziel ist es, diese Risiken einzudämmen, indem wirksame technische und organisatorische Maßnahmen (TOM) umgesetzt werden.

Da die DSGVO technikneutral formuliert wurde, finden sich darin keine konkreten Maßnahmen, die Schritt für Schritt abgearbeitet werden können. Stattdessen steht es grundsätzlich jedem Verantwortlichen frei, selbst diejenigen TOM auszuwählen, die passend zu der eigenen Art der Verarbeitung und Unternehmensgröße sind, sofern damit ein wirksames angemessenes Schutzniveau erreicht werden kann.

Die in diesem Papier dargestellten TOM stellen keinesfalls einen Anspruch auf Vollständigkeit dar, sondern sollen als Empfehlung eines gelebten Good-Practice verstanden werden. Dies bedeutet, dass nicht alle genannten Maßnahmen – auch unter Berücksichtigung der Implementierungskosten – zwangsläufig umgesetzt werden müssen, sondern vielmehr jeder Verantwortlicher im eigenen Betrieb festzustellen hat, welche der Kriterien für die eigene Anwendung relevant und welche dagegen über dieses Papier hinaus weiter zu ergänzen sind, um den gesetzlichen Vorgaben zu genügen.

Diese Checkliste dient deshalb insbesondere dazu, kleinen und mittleren Unternehmen eine Auswahl an TOM anzubieten, die bei geläufigen Verarbeitungstätigkeiten innerhalb eines Betriebs verwendet werden können. Entsprechend werden häufig in der Praxis adressierte Punkte behandelt wie bauliche Schutzmaßnahmen, Einsatz von mobilen Endgeräten, internetfähige Arbeitsplatzumgebung und Sensibilisierung von Mitarbeitern – dies entspricht einem generischen Ansatz bei IT-gestützten Datenverarbeitungen. Spezialisierte Anwendungen wie vernetzte Fahrzeuge, künstliche Intelligenz oder Cloud-Computing-Services würden dagegen deutlich spezifischere und teils abweichende Maßnahmen benötigen.

Das Abstraktionsniveau der Maßnahmen dieser Liste unterscheidet sich insgesamt sehr stark – teilweise sind z. B. sehr wirksame technische Einstellungen bei Systemen im Detail aufgeführt, teilweise auch grundsätzliches Vorgehen auf Konzeptebene. Zur Auswahl von Auftragsverarbeitern nach Art. 28 DSGVO sind diese Kriterien nur bedingt geeignet.

Manche Punkte könnten von IT-Dienstleistern bspw. aus Sicherheitsgründen nicht im Detail veröffentlicht werden. Zukünftige Zertifizierungen nach Art. 42 DSGVO werden daher die daraus resultierenden praktischen Herausforderungen der Wirksamkeitsprüfung bei Auftragsverarbeitungen schließen.

Von der Struktur der Gliederung dieses Papier findet eine starke Orientierung an der Veröffentlichung zur Sicherheit personenbezogener Daten der französischen Datenschutzaufsichtsbehörde statt. Diesen Ansatz, der sich vom Prinzip auch in internationalen Normen zur Informationssicherheit wiederfindet, betrachten wir gerade für klassische Verarbeitungen bei kleinen und mittleren Unternehmen als einen möglichen und interessanten Weg. Hinweisen möchten wir an dieser Stelle auf weitere Maßnahmen des technischen Datenschutzes zur Umsetzung einer Risikoeindämmung des Art. 25 Abs.1 DSGVO (Datenschutz durch Technikgestaltung), bei denen die TOM zur Sicherheit der Verarbeitung nach Art. 32 DSGVO nur eine Teilmenge darstellen. Eine weitere Checkliste mit „Privacy-by-Design"-Maßnahmen ist geplant.

Das Dokument ist trotz seines Umfangs nicht abschließend und wird laufend weiterentwickelt.

Als geeignete Basis hierfür dienen auch Veröffentlichungen anderer Behörden und Institutionen, die wir gerne an dieser Stelle referenzieren.

Verweise

- Security of Personal Data, CNIL (Frankreich): www.cnil.fr/en/new-guide-regarding-security-personal-data
- Handbook on Security of Personal Data Processing, ENISA (EU): www.enisa.europa.eu/publications/handbookon-security-of-personal-data-processing
- IT-Grundschutz-Kompendium, BSI: www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
- ISO/IEC 27002:2019

Selbst-Check: Sicherheit der Verarbeitung nach Art. 32 DSGVO.

1 Management und Organisation.

Mangelhafte Sicherheitsstrukturen in einer Organisation können den Betriebsablauf erheblich gefährden. Bestehende Fachkompetenzen sind daher zu nutzen. Dabei ist nicht nur der IT-Verantwortliche, sondern auch der Datenschutzbeauftragte (DSB) im Prozess der Umsetzung von Sicherheitsanforderungen einzubinden.

	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.
	Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus (Plan-Do-Check-Act).
	Konzepte und Dokumentationen im Sicherheitsumfeld werden regelmäßig überprüft und aktuell gehalten.
	Je nach Unternehmensgröße: Einsatz eines geeigneten Informationssicherheitsmanagementsystem (ISMS), z. B. nach ISO/IEC 27001, BSI-Standards oder ISIS12.
	Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind im eigenen Betrieb bekannt und besetzt (u. a. Informationssicherheitsbeauftragter (ISB), IT-Leiter, Datenschutzbeauftragter (DSB)).
	Konsequente Einbindung des DSB bei Sicherheitsfragen.
	Ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema.
	Durchführung von regelmäßigen Audits des DSB nach Art. 32 DSGVO zur Sicherheit der Verarbeitung.
	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.

2 Physikalische Sicherheit der Infrastruktur.

Der persönliche Zugang zu IT-Systemen und 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).
	Klare Regelungen zum Umgang mit Besuchern (z. B. Begleitung, Sicherheitszonen, Besucherausweise, Protokollierung, Zuständiger Mitarbeiter für Besucher) als Bestandteil des Konzepts.
	Gelebte Regelungen zum Umgang auch mit externen Dienstleistern (z. B. bei Werkverträgen, Handwerker, Wartung von Systemen) – wie Verschwiegenheitserklärung, persönliche Begleitung in Sicherheitszonen oder Protokollierung.
	Schaffung von verschiedenen Sicherheitszonen (z. B. Besucherbesprechungen, Serverräume, Arbeitsplätze, Forschungsbereich).
	Bei Sicherheitszonen: Aktuelle Übersicht zur Berechtigungsverwaltung (Welcher Mitarbeiter darf in welche Zone?).
	Bei Sicherheitszonen: Zugang zu Sicherheitszonen mit geeigneter Technik begrenzen (über Schlüsseln/Chipkarten, ggf. auch weiteren Faktoren).
	Bei Sicherheitszonen: Bei Zonenübergang selbstschließende Türen einsetzen.
	Bei Sicherheitszonen: Ggf. Beschilderung, welche Zone nicht betreten werden soll/darf.
	Sichere Schließsysteme samt dokumentierter Schlüsselverwaltung.
	Es besteht ein Konzept zum Brandschutzkonzept.
	Verwendung von Feuer-/Rauchmeldeanlagen (im Rahmen des Brandschutzkonzepts).
	Einsatz von automatischen Löschsystemen in Serverräumen (z. B. CO_2-Löschung) unter Berücksichtigung von Arbeitsschutzvorschriften.
	Feuerhemmende Schränke/Tresore zur Lagerung essentieller Komponenten (z. B. Backup-Bänder, wichtige Originaldokumente).
	Das Gebäude (z. B. Wände, Fenster) und die Infrastruktur (z. B. Leitungen, Gefahrenmeldeanlagen) werden regelmäßig geprüft und gewartet.
	Umzäunung des Betriebsgeländes.
	Stabile, einbruchshemmende Fenster und Türen im EG (z. B. nach DIN EN 1627).
	Einsatz von Alarmanlagen zur Einbruchserkennung, insbesondere außerhalb der Arbeitszeit.
	Einsatz von Sicherheitspersonal (ggf. extern).
	Einsatz von Videoüberwachungssystemen unter Berücksichtigung datenschutzrechtlicher Anforderungen (Monitoring des Zugangsschutzes).
	Ausreichende Klimatisierung von Serverräumen.
	Keine (zu öffnenden) Fenster in Serverräumen.
	Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (unterbrechungsfreie Stromversorgung (USV)), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen.
	Elementargefahren vorbeugen (insb. Feuer, Rauch, Erschütterungen, chemische Reaktionen, Überschwemmungen, Stromausfälle, Explosionen und Anschläge/Vandalismus).
	Risiken durch Überflutung/Starkregen prüfen, insbesondere bei Serverräumen im Keller oder anderen gefährdeten Bereichen.

3 Awareness der Mitarbeiter.

Beschäftige stehen mittlerweile verstärkt im Fokus von Cyberattacken. Mittels raffinierten Social Engineering Techniken sollen sie dazu verleitet werden, sicherheitskritische Aktionen auszuführen. Mitarbeiter müssen daher gerade in Sicherheitsfragen geschult sein, um solche Angriffe zu vereiteln.

	Das gesamte Personal der Organisation sollte eine angemessene Schulung für Informationssicherheit und Datenschutz erhalten, soweit dies für die jeweilige Funktion relevant ist.
	Datenschutzschulungen für neue Beschäftigte zeitnah nach Aufnahme des Beschäftigungsverhältnisses.
	Regelmäßige Auffrischungsschulungen für bestehendes Personal (z. B. einmal pro Jahr).
	Regelmäßige Informationen im Betrieb an alle über Neuigkeiten zum Datenschutz und der IT-Sicherheit (z. B. per Mail, Intranet, Kollaborationsplattform, Aushang).
	Relevante Richtlinien, z. B. zur E-Mail-/Internetnutzung, Umgang mit Schadcodemeldungen, Einsatz von Verschlüsselungstechniken, werden aktuell gehalten und sind leicht auffindbar (z. B. im Intranet).
	Datenschutzhandbuch (welches z. B. auch Schulungsinhalte bereitstellt) ist zugänglich für alle betroffenen Mitarbeiter.
	Schulungsinhalte: Ausgewählte Mitarbeiter, die bei der Erkennung von Sicherheitsverletzungen beteiligt sind (wie z. B. IT, DSB, Geschäftsführung, Führungskräfte, Geschäftsstelle, ggf. Telefonzentrale oder Sekretariat) kennen die internen Prozesse zum Umgang mit Vorfällen (u. a. Meldung nach Art. 33 DSGVO, Notfallplan).
	Schulungsinhalte: Beschäftigten lernen kennen, wie Cyberangriffe mittels Social-Engineering eingeleitet werden (Hilfe zur Selbsthilfe).
	Schulungsinhalte: Beschäftigten erfahren von den Gefahren der E-Mail-Kommunikation, insbesondere bei verschlüsselten E-Mail-Anhängen (z. B. Zip-Datei mit Passwort).
	Schulungsinhalte: Beschäftigten erkennen gefälschte E-Mails (z. B. Absenderadressen, Auffälligkeiten, eingebettete Links).
	Sensibilisierung des Personals, das mit Externen wie z. B. Lieferanten interagiert, in Bezug auf angemessene Einsatzregeln, Richtlinien, Prozesse und Verhalten (u. a. welche Daten dürfen in welcher Form weitergegeben werden, was kann sicherheitskritisch sein).
	Von Heimarbeit betroffenen Mitarbeiter werden die sichere Nutzung von Home Office Lösungen erläutert und spezifische Gefahren aufgezeigt.

4 Authentifizierung.

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

	Einweisung aller Mitarbeiter in den Umgang mit Authentifizierungsverfahren und -mechanismen.
	Geregelter Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage (z. B. neuer Mitarbeiter), Änderung (z. B. Namenswechsel nach Heirat) und Löschung (z. B. Weggang Mitarbeiter).
	Vergabe von eindeutigen Kennungen für jeden Nutzer.
	Vermeidung von Gruppenkennungen.
	Bei zwingender Nutzung von Gruppenkennungen: Einsatz von datenschutzkonformer Protokollierung der dazugehörigen Nutzeraktivitäten.
	Verwendung von starken Passwörtern und Veröffentlichung einer Richtlinie dafür – z. B. mind. 10-tellig bei zufälligen komplexen Zeichen oder mind. 16-stellig bei einfacheren Zeichenfolgen ohne direkte Verwendung von üblichen Wörtern.
	Möglichst automatische Umsetzung der Passwortrichtlinie für starke Passwörter in den Systemen mit Nutzerkennungen.
	Verhinderung der Auswahl schwacher Passwörtern bei Anwendungen (z. B. über Richtlinien oder technisch erzwungen über das Identity Management System).
	Ggf. Überprüfung der Regel, dass Passwörter nach festgelegten Zeiträumen (z. B. 60 Tage) geändert werden müssen – falls diese Passwörter „stark" sind, kann ein anlassloses Passwortwechselintervall deutlich länger ausfallen (z. B. einmal pro Jahr).
	Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden.
	Bei erstmaligem Login eines neuen Nutzers oder Zurücksetzung des Passworts durch IT (z. B. bei Vergessen des Passworts) muss eine Passwortänderung durch den Nutzer erfolgen.
	Passwörter dürfen nicht weitergegeben werden (auch nicht an Kollegen, Vorgesetze oder die IT-Abteilung) – im Ausnahmefall (z. B. längere Erkrankung) wird das Passwort durch die IT zurückgesetzt und dieser Vorgang dokumentiert.
	Unterrichtung der Beschäftigten, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen.
	Keine Speicherung von Passwörtern im Browser ohne Sicherung durch ein Masterpasswort.
	Keine Mehrfachverwendung eines Passworts für verschiedene Dienste, sofern kein zentrales Identitätsmanagement (z. B. Active Directory) verwendet wird.
	Keine Passwörter per E-Mail übermitteln (z. B. für einen Firmenaccount zu einem Cloud-Dienst).
	Für lokale Admin-Konten besonders starke Passwörter (z. B. mind. 16-stellig, komplex und ohne übliche Wortbestandteile sowie unterschiedlich für jeden PC).
	Einsatz von Verfahren zur Zwei- oder Mehr-Faktor-Authentifizierung bei Verarbeitungstätigkeiten mit hohem Risiko (z. B. Chipkarten, USB-Sticks, Token).
	Soweit möglich konsequenter Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung für Administratorkonten bei Anwendungen.
	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.
	Automatische Sperrung von Zugängen bei zu vielen Fehlversuchen durch falsches Passwort: Entweder zeitbasiert (eine Stunde, sechs Stunden, 24 Stunden) oder komplett (Kontaktaufnahme mit IT notwendig).
	Zeitverzögerung zwischen einzelnen Login-Versuchen (insbesondere bei über das Internet erreichbaren Anwendungen) zur Erschwerung von automatischen Online-Angriffen.
	Darstellung der Anzahl der fehlgeschlagenen Logins für einen Nutzer, der sich erfolgreich anmeldet. Ziel: Transparenz für stattgefundene Angriffe bzw. Angriffsversuche schaffen.
	Passwörter nicht im Klartext speichern sondern geeignete kryptographische Verfahren einsetzen (z. B. bcrypt mit Salt).
	Regelungen zum automatischen Sperren von Passwörtern nach einem Sicherheitsvorfall treffen (z. B. Passwort-Hash so abändern, dass kein Klartextpasswort dazu besteht).
	Falls Chipkarten als Mitarbeiterausweise eingesetzt werden, prüfen, ob diese für Standardauthentifizierungen (z. B. Betriebssystem-Login) verwendet werden können.
	Standard-Authentifizierungsinformationen durch Hersteller bei Software sollten nach der Installation geändert werden.

5 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.

	Erstellen von Rollenprofilen für die Beschäftigten unter Einbeziehung der Einträge des Verzeichnisses der Verarbeitungstätigkeiten.
	Über das Rollen-/Rechtekonzept den Zugang zu Informationen und Gebäuden/Bereichen gezielt steuern und reglementieren.
	Regelungen zur Verwaltung der Rollen (Zuweisung, Entzug) an die Mitarbeiter etablieren.
	Regelmäßige Überprüfung (z. B. einmal pro Jahr), ob die Zuweisung der Rollen den Vorgaben entspricht sowie, ob die Rollen noch den Anforderungen der Geschäftstätigkeit entspricht.
	Keine Administratorkennungen für Nutzer, die keine administrativen Tätigkeiten ausführen.
	Verschiedene administrative Rollen (z. B. Anlage neuer Benutzer, Durchführung von Backups, Konfiguration der Firewall) für die IT-Administration erstellen.
	Die Nutzung von Superuser (z. B. root unter Linux) soweit möglich nicht verwenden.
	Für Beschäftigte mit IT-Administrationsaufgaben zwei Benutzerkennungen einrichten: eine Administrationskennung und eine normale Nutzerkennung (für nicht-administrative Zwecke wie z. B. das Surfen im Internet).
	Regelung etablieren, dass nicht unter Nutzung von Administratorenrechten im Internet gesurft oder E-Mails gelesen/versendet werden.

6 Endgeräte (Clients).

Die für die tägliche Arbeit genutzten Endgeräte der Nutzer müssen dauerhaft abgesichert werden. Keine oder nur 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.
	Automatisches Sperren nach einer gewissen Zeitspanne der Inaktivität, falls manuelles Sperren bei Verlassen des Einflussbereichs nicht gewährleistet werden kann.
	Blickschutzfolien bei potentieller unbefugter Einsichtnahme (z. B. im Kundenempfangsbereich) bei Monitoren und Notebookbildschirmen anbringen.
	Aktivierung einer Firewall, die unerwünschte Servicedienste auf dem Endgerät blockiert (z. B. versehentlich installierter Webserver).
	Verwendung einer Anti-Viren-Lösung bzw. eines EndpointProtection-System mit regelmäßigen, mindestens tagesaktuellen Signatur-Updates und Regelungen, wie im Falle einer Warnmeldung zu verfahren ist.
	Zentrale Erfassung von Schadcode-Alarmmeldungen durch die IT-Administration.
	Ablaufplan der IT-Administration bei Schadcode-Befall.
	Konzept zum Patch Management vorhanden (u. a. UpdatePlan mit Übersicht der eingesetzten Software).
	Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software und Fachanwendungen (z. B. durch E-MailNewsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen).
	Automatisches Einspielen von Sicherheitsupdates des Betriebssystems, der installierten Software (z. B. PDF-Reader) oder von Softwarebibliotheken (z. B. Java), sofern möglich.
	Personenbezogene Daten sollten auf einem Speichermedium gespeichert werden, das von dem Backup erfasst wird (z. B. Netzlaufwerk).
	Einbindung von externen Geräten durch technische Maß- nahmen auf das erforderliche Mindestmaß begrenzen (z. B. bei USB-Sticks, Smartphones, externe Festplatten).
	Auto-Start von externen Medien (z. B. USB-Sticks) deaktivieren.
	Fernwartung für Clients zu IT-Administrationszwecken ausschließlich über verschlüsselte Verbindungen nach Authentifizierung durch den Administrator und Freigabe durch den Nutzer.
	Nur Betriebssysteme und Software einsetzen, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden.
	Verhinderung der Ausführung von (aus dem Internet) heruntergeladener Software, deren Quellen als unsicher gekennzeichnet werden.
	Der Zugang zu Websites sollte restriktiv verwaltet werden, sodass 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).
	Verhinderung der automatischen Ausführung von Programmen aus dem temporären Download-Verzeichnis des Internetbrowsers.
	Anwendungen sind an den Endgeräten möglichst ohne Administratorrechte auszuführen.
	Prozess zur wirksamen Datenlöschung vor Vergabe eines Endgeräts an einen anderen Mitarbeiter aufsetzen.
	Ein Sicherheitskonzept für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten ist vorhanden (z. B. keine unerlaubte Einsicht in ausgedruckte Dokumente, ausreichender Schutz gespeicherter Informationen, ordnungsgemäße Entsorgung).

7 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.

Einsatz starker Verschlüsselung der mobilen Endgeräte (z. B. Festplattenverschlüsselung, Container-Lösungen).
Einsatz von Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust und Diebstahl.
Bei Smartphones: Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort) – Länge der Kennung in Abhängigkeit von automatischen Sperr- und Löschfunktionen.
Bei Smartphones: 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.
Bei Smartphones: Cloud-Speicher für Datenbackup erst nach sorgfältiger Prüfung der datenschutzrechtlichen Anforderungen einsetzen (auch Beschäftigtendatenschutz bei „Find my Phone"-Funktionen).
Bei Smartphones: Mobile Device Management Lösungen zur Konfiguration und Verwaltung der Geräte, der installierten Apps sowie dem Auffinden/Löschen im Verlustfall.
Bei Smartphones: Nur sichere Quellen werden für die Installation von Apps verwendet. Apps werden vorher getestet und freigegeben.
Regelungen prüfen, ob es ausreichend ist, bei Nutzung mobiler Arbeitsplätze (z. B. Notebook auf Dienstreise) auf weniger Daten als innerhalb des internen Unternehmensnetzes zugreifen zu können.
Diebstahlsicherungen (z. B. Anbringung von verschließbaren Stahlkabeln) für Notebooks bei Bedarf zur Verfügung stellen.
Regelungen zur Privatnutzung bei Notebooks und Smartphones schaffen - 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.
Bei mobilen Datenträgern: Sicheres Löschen der Datenträger vor und nach der Verwendung ist sichergestellt.

8 Serversysteme.

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

Nur kompetent geschulte Personen dürfen Administrationstätigkeiten auf den Servern durchführen.
Verschiedene Administrationsrollen mit Rechten nach dem Least-Privileg-Prinzip für unterschiedliche Administrationsaufgaben (z. B. Softwareupdates, Konfiguration, Backup) einsetzen.
Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server – kritische Updates müssen unverzüglich eingespielt werden.
Verwendung von eigenen Administrations-Endgeräten (über dezidierte Netzwerkverbindung).
Soweit möglich konsequenter Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung bei Anwendungen, die dies insbesondere für Administratoren unterstützen.
Deaktivierung/Deinstallation von Standard Server-Diensten, die nicht benötigt werden (z. B. Webserver, Printserver).
Serverlokale Dienste über Firewall auf Servern vor Außenzugriff blockieren.
Weitere Härtungsmaßnahmen für das eingesetzte Serverbetriebssystem prüfen.
Versendung von Telemetriedaten an Hersteller deaktivieren, sofern diese nicht als erforderlich eingeschätzt werden.

9 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.

Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 oder TLS1.3).
Absicherung von Datenbanken auf dem Webserver mittels Firewalls.
Fernzugang zu Webservern nur mit verschlüsselter Verbindung und Zwei-Faktor-Authentifizierung (z. B. SSH mit Client-Zertifikaten).
Limitierung von Administrationsbereichen der Webanwendungen auf bestimmte IP-Adressen (z. B. UnternehmensGateway).
Nur geschulte bzw. kompetente Personen dürfen Administrationstätigkeiten auf den Servern durchführen.
Geregelter Prozess zur Information über Sicherheitsupdates und zeitnahes Einspielen derselben, insbesondere bei gängigen Content-Management-Systemen (CMS).
Durchführung von Sicherheitstests auf Webanwendungen nach Good-Practice-Vorgehen (z. B. OWASP Testing Guide).
Keine Übertragung personenbezogener Daten (z. B. MailAdresse) per HTTP-GET-Request, da diese in den WebserverLog-Dateien gespeichert werden und durch eingesetzte Website-Tracker ausgeleitet werden können.
Trennung von Webserver, Anwendungslogik und Datenhaltung einer Webanwendung durch eigene Server, die in eine geeignete Firewall-Architektur (z. B. DMZ – Demilitarisierte Zone) eingebunden sind.
Sperrung der Auffindung von Inhalten durch Suchmaschinen (über robots.txt), sofern diese Inhalte nicht durch eine Suchmaschine gefunden werden sollen.

10 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.

	Geeignete Netzwerksegmentierung durchführen: Restriktive (physikalische) Trennung sensitiver Netze (z. B. medizinische Netze in Krankenhäusern oder Personalverwaltung) von Verwaltungsnetzen (mittels Firewall-Systemen).
	Einsatz einer Firewall am zentralen Internetübergang.
	Blockierung aller nicht benötigten Dienste (z. B. VoIP, Peerto-Peer, Telnet).
	Einsatz eines Web-Proxies über den alle HTTP(S)-Verbindungen gehen müssen.
	Blockierung von HTTP(S)-Verbindungen abseits des WebProxies – Ausnahmeregeln vermeiden.
	Protokollierung und Blockierung von IOCs (Indicators of Compromise, meist URL und IP-Hashes).
	Regelmäßige Aktualisierung der IOCs aus geeigneten Quellen.
	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).
	Einsatz von Funkzugängen per WLAN nur auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen (z. B. WPA-2 mit mind. 24-stelligem Passwort, WP3-Enterprise oder Einsatz eines Radius-Servers).
	Nutzung eines WLAN-Gastzugang ohne Zugangsmöglichkeit zum internen Netzwerk.
	Geregelter Prozess zur ordnungsmäßigen Konfiguration der Firewalls und regelmäßige Überprüfung der selbigen (z. B. zu der Notwendigkeit von Freigaben).
	Protokollierungen auf Firewall-Ebene, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren.
	Automatische Benachrichtigungen an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen.
	Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans auf die eigenen IPAdressen von extern und periodischer Pentests).
	Einsatz von ausreichend qualifiziertem Personal/Dienstleister zur Konfiguration der Firewall.
	Prüfung eingehender E-Mails mittels Anti-Malwareschutz.
	Blockieren von gefährlichen Email-Anhängen (z. B. .exe, .doc, .cmd).
	Keine unverschlüsselten Protokolle (z. B. FTP, Telnet) verwenden.
	Einsatz von Intrusion-Detection-Systemen (IDS) oder Intrusion-Prevention-Systemen (IPS).
	Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen mit Client-Zertifikatsauthentifizierung.

11 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.

	Regelungen etablieren, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist.
	Zugänge zu den Archivdateien festlegen: Dokumentieren, Umsetzen und Prüfen.
	Archivdaten müssen nach Ablauf der Aufbewahrungsfrist wirksam gelöscht werden.
	Keine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind (z. B. wiederbeschreibbare DVDs).
	Keine Aufbewahrung von Archivdaten in Produktivdatenbanken, sondern Überspielen von Archivdaten aus Produktivsystemen in die Archivsysteme.
	Verschlüsselung von Archivdateien mit geeignetem Schlüsselmanagement: Entschlüsselungsschlüssel an mind. zwei (örtlich) getrennten Stellen aufbewahren.
	Geeignete Datenformate für die Archivierung von Dokumenten wurden ausgewählt, damit eine langfristige Lesbarkeit der Daten gewährleistet ist.

12 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.

	Aufzeichnung aller Tätigkeiten von externen Dienstleistern.
	Verschwiegenheitsverpflichtung in den Dienstleistungsvertrag aufnehmen oder von dem externen Mitarbeiter unterzeichnen lassen.
	Internen Mitarbeiter festlegen, der die Tätigkeiten des externen Dienstleistern überwacht (bzw. ggf. begleitet) und dokumentiert.
	Regelungen zur wirksamen Datenlöschung auf Hardware (z. B. PCs, Drucker, Smartphones) schaffen, die vom Dienstleister oder Hersteller zurückgenommen werden (z. B. bei Defekten, Abschreibung).
	Bei Einsatz von Fernwartungssoftware regelmäßig Sicherheitsupdates einspielen und auf Informationen über bekannte Schwachstellen oder Fehlkonfigurationen achten.
	Fernwartung externer Dienstleister protokollieren und den Zugang nur auf das zu wartende System begrenzen – sofern möglich, durch einen Mitarbeiter am Bildschirm des gewarteten Systems digital nachverfolgen.

13 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.

	Konzept zur Protokollierung von Benutzeraktivitäten, technischen Systemereignissen, Fehlerzuständen und Internetaktivitäten unter Berücksichtigung datenschutzrechtlicher Anforderungen (u. a. auch Beschäftigtendatenschutz) erstellen.
	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.
	Einhaltung der Zweckbindung der Log-Dateien muss sichergestellt werden: Die Personalvertretung ist ggf. einzubinden.
	Regelmäßige anlasslose Auswertung der Log-Dateien zur Erkennung von ungewöhnlichen Einträgen – bevorzugt: Automatische Heuristiken.

14 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 betriebsfä- hig zu bleiben.

Erstellung eines Notfallplans zur Business Continuity: Regelungen, welche Systeme in welcher Reihenfolge wieder instandgesetzt 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 Tests und Notfallübungen.
	Vorhandensein eines schriftlich fixiertes Backup-Konzepts.
	Durchführung von Backups nach der 3-2-1 Regel: 3 Datenspeicherungen, 2 verschiedene Backupmedien (auch „Offline“ wie Bandsicherungen) und 1 davon an einem externen Standort.
	Geeignete physische Aufbewahrung von Backupmedien (z. B. Tresor, unterschiedliche Brandabschnitte, Gefahr von Wasserschäden, ...).
	Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird.
	Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert.
	Mindestens ein Backup-System ist durch Schadcode nicht verschlüsselbar, z. B. spezielles Datensicherungsverfahren wie Pull-Verfahren des Backup-Systems oder Air-Gapgetrennt (offline) nach Abschluss des Backup-Prozesses.
	Weitestgehender Verzicht auf Makros in Office-Dokumenten im Betriebsalltag zum Schutz vor Ransomware.
	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).
	Verhinderung einer automatischen Ausführung von heruntergeladenen Programmen (z. B. Software Restriction Policy und Sandboxing).
	Deaktivierung von Windows Script Hosts (WSH) auf Clients (sofern nicht zwingend benötigt) oder Prüfung, ob die Einschränkung von Powershell-Skripten mit dem „ConstrainedLanguage Mode“ auf Windows-Clients sinnvoll durchführbar ist oder Nutzen eines Web-Proxys mit (tages-)aktuellen Sperrlisten von Schadcode-Download-Seiten (IOCs).
	Notfallplan beinhaltet den Umgang mit Verschlüsselungstrojanern – dieser liegt auch in Papierform vor.
	Überprüfung der Backup- und Recovery-Strategie, die sicherstellt, dass Backups durch die Ransomware nicht verschlüsselt werden können.

15 Kryptographie

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

	Regeln für die effektive Nutzung der Kryptographie, einschließlich der Schlüsselverwaltung, sollten definiert werden.
	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.
	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.
	Asymmetrische Verschlüsselung nach Stand der Technik mit z. B. RSA-2048 Bit (oder höher), EC-256 Bit (oder höher).
	Wirksame Schlüsselverwaltung (Generierung, Ausgabe, Sperrung) ist bei Einsatz kryptographischer Verfahren essentiell.
	Schutz von geheimen Schlüsseln durch starke Passwörter mit mindestens 16 Stellen. Bei hohem Risiko Einsatz von HSM (Hardware Security Modulen) prüfen.
	SSL-Zertifikate bei vertrauenswürdigen Zertifizierungsstellen beschaffen.
	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.

16 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.

	Regeln sollten für alle Arten von Datentransfers sowohl innerhalb der Organisation als auch zwischen der Organisation und anderen Parteien bestehen.
	Insbesondere für Cloud-Dienste sind Verfahren zur Nutzung zu etablieren (inklusive einer möglichen Ausstiegsstrategie, um Abhängigkeiten zu einzelnen Cloud-Diensten zu reduzieren).
	Verschlüsselung von mobilen Datenträgern (wie DVD, USBSticks, Festplatte) nach Stand der Technik.
	Bei E-Mail, Cloud-Plattformen: Transportverschlüsselung von personenbezogenen Daten nach Stand der Technik bei normalem Risiko.
	Bei E-Mail, Cloud-Plattformen: Transportverschlüsselung und Inhaltsverschlüsselung von personenbezogenen Daten nach Stand der Technik bei hohem Risiko.
	Bei Messenger: Transport- und Inhaltsverschlüsselung der Nachrichten und Dateien.
	Sicherstellung der Integrität von personenbezogenen Daten durch digitale Signaturen zumindest bei hohem Risiko.
	Bei HTTPS: Einsatz von Client-Zertifikaten zum Nachweis der Authentizität bei geschlossenem Nutzerkreis.
	Verschlüsselte Nutzung von DNS-Diensten (DNSSec, DNS-over-TLS) prüfen.

17 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.
	Den Zugang zum Source-Code bei der Entwicklung von Software beschränken.
	Keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung ablegen.
	System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests, sollten durchgeführt werden.
	Ausreichende Testzyklen werden berücksichtigt.
	Fortlaufendes Inventarisieren der Versionen von Software oder Komponenten (z. B. Frameworks, Bibliotheken) sowie deren Abhängigkeiten.
	Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen.
	Sicherstellung, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen für die gesamte Lebenszeit einer Softwareanwendung besteht.

18 Auftragsverarbeiter

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

	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 bei Bedarf zur Verfügung gestellt werden.
	Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung.