Checkliste:
Technische und organisatorische Maßnahmen

Herausgeber:
BVS-KMU
Magdeburger Straße 70
55218 Ingelheim

Telefon: (06132) 88133
0175 2904618
E-Mail: schueler@bvs-kmu.de

Webseite: www.bvs-kmu.de

Stand: Okt. 2021

Einführender Hinweis

Notwendig sind technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (Artikel 5 DSGVO und § 64 BDSG). Die nachfolgenden Prüfpunkte stellen einerseits einen Überblick der grundlegenden erforderlichen Maßnahmen und Fragestellungen und andererseits die wesentlichen Kriterien für Prüfungen durch die Datenschutzaufsichtsbehörden dar.

1. Zutrittskontrolle

Ziel:
Durch die Zutrittskontrolle soll verhindert werden, dass Unbefugte Zutritt zu relevanten Gebäuden und Räumen erhalten.

Mögliche Maßnahmen der Zutrittskontrolle sind:

- Perimeterschutz
- Sicherheitskonzept
- Einbruchmeldeanlage
- Videoüberwachung

Prüffokus:
Welche technischen bzw. organisatorischen Maßnahmen werden zur Zutrittskontrolle, insbesondere auch zur Legitimation, eingesetzt?

- Lage der Räume:
  Sind die Zugänge der Räume ausreichend abgesichert (z. B. Türen, Türschlösser, Lichtschächte, Lüftungsöffnungen, Fenster, Verglasungsart, Rollos gegen Hochschieben, Feuerleiter, Feuertreppe, elektrische Türöffner)? Erfolgt eine Bewachung der Räumlichkeiten (z. B. durch einen Sicherheitsdienst)? Handelt es sich um ein bewohntes Gebäude? Existiert ein Empfang und wann ist diese besetzt?

- Verschließbarkeit der Räume:
  Sind Sicherheitsschlösser vorhanden? Erfolgt ein Auf- und Abschließen der Räume bei Arbeitsbeginn bzw. –ende und in den Pausen? Gibt es ein geregeltes Konzept zur Schlüsselverwaltung? Findet eine Quittierung bei der Schlüsselausgabe (Schlüsselbuch) statt? Wer besitzt einen Generalschlüssel?

- Überwachungseinrichtung:
  Sind Alarmanlagen vorhanden? Wird der Zutritt in den Serverraum über Videokameras überwacht? Werden Bewegungssensoren eingesetzt?

- Schriftliche Festlegungen zur Zugangsberechtigung:
  Wird auf die Trennung von Bearbeitungs- und Publikumszonen geachtet? Sind schriftliche Besucherregelungen vorhanden? Werden Besuche in einem Besucherbuch dokumentiert? Wie findet die Kundenbetreuung statt?

- Reinigungs- und Wartungsarbeiten:

Ist sichergestellt, dass sowohl mit dem Reinigungspersonal als auch mit IT-Dienstleistern bei Wartungen entsprechende Regelungen getroffen sind?

- Anwesenheitskontrollen:
  Wie wird die Anwesenheit überprüft (z. B. Zeiterfassung)? Werden auch kurzzeitige Abwesenheiten protokolliert?
- Sicherheit bei Heimarbeiten/Telearbeiten:
  Wird auch bei fernangebundenen Arbeitsplätzen für ausreichende Sicherheit gesorgt?
- Beratung:
  Findet ggf. eine Beratung durch kriminalpolizeiliche Beratungsstellen oder spezialisierte Dienstleister statt?

2. Zugangskontrolle

Ziel:
Durch die Zugangskontrolle soll verhindert werden, dass Unbefugte zugang zu DV-Anlagen erhalten und somit Schäden anrichten könnten.

Mögliche Maßnahmen der Zugangskontrolle sind:
- Sichere Kennwörter
- Zwei-Faktor-Authenifizierung
- Zugangsberechtigungen
- Firewall

Prüffokus:
Welche Maßnahmen sind hinsichtlich der Benutzeridentifikation und Authentisierung technisch und organisatorisch vorhanden?

- Firewall und Virenschutz:
  Welche Produkte werden eingesetzt? Existiert eine zentrale Firewall? Ist eine zentrale Antivirensoftware installiert? Welche dezentralen Lösungen (Personal Firewall, Virenscanner) werden an den Arbeitsplätzen verwendet?
- Benutzeridentifikation und Passwortverfahren:
  Werden ausreichend sichere Passwörter verwendet (z. B. keine Eigennamen und Wörter aus dem Wörterbuch, auch Sonderzeichen verwenden, empfohlene Länge von zehn Stellen)? Ist ein regelmäßiger Passwortwechsel verpflichtend? Findet eine Auswertung der Protokolleinträge bei Falscheingaben des Passworts statt? Werden Verfahren zur Zwei-Faktor-Authentifizierung eingesetzt (z. B. Tokens, Smartcards)?
- Systemsperrung:
  Erfolgt eine automatische Sperrung der Bildschirme mit Passwortschutz bei Pausen? Findet ein Sperren eines Zugangs bei mehr als drei Anmelde-Fehlversuchen statt? Hat die Falscheingabe eines Passworts eine zeitliche Verzögerung für einen Neuversuch zur Folge?
  Kommt eine Mobile Device Management-Lösung zum Einsatz?
- Benutzerkennungen:
  Wird auf Gruppenkennungen verzichtet? Besteht ein eigenes Benutzerkonto für jeden Mitarbeiter (d. h. Einrichtung eines Benutzerstammsatzes)?

- Verschlüsselung:
  Werden Datenträger und Smartphones verschlüsselt? Welche Verschlüsselungsverfahren kommen zum Einsatz?
- Geräteanschlüsse:
  Sind externe Schnittstellen (z.B. USB-Anschlüsse bzw. DVD/CD-Laufwerke) gesperrt?
- Mobile Geräte
  Kommt VP-Technologie zum Einsatz?

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Mögliche Maßnahmen der Zugriffskontrolle sind:
- Berechtigungskonzepte
- Protokollierung von Zugriffen
- Revisionsfähige Dokumentation von Benutzerzugriffen
- gesicherte Schnittstellen (USB, Netzwerke etc.)
- elektronische Signaturen bzw. Verschlüsselung von Datenträger

Prüffokus:
Welche Maßnahmen sind vorhanden, um die unerlaubte Tätigkeit in DV-Systemen außerhalb eingeräumter Berechtigungen zu verhindern?

- Berechtigungskonzept und Zugriffsrechte:
  Entspricht das Konzept sowohl für Anwender als auch für Administratoren den aufgabenbedingten und datenschutzrechtlichen Erfordernissen? Existieren differenzierte Berechtigungen für Auswertungen, Kenntnisnahme, Veränderung und Löschung? Können Berechtigungen nur ausschließlich durch den Systemadministrator verändert werden?

- Schutz gegen unberechtigte Zugriffe:
  Bestehen Schutzmaßnahmen gegen unbefugte interne und externe Zugriffe (z. B. durch Verschlüsselung, Firewalls)? Werden Verfahren zur Data Leak Prevention (Erkennung unerwünschter Datenabflüsse) eingesetzt? Werden regelmäßig Penetrationstests gegen Attacken von Hackern durchgeführt?
- Überwachung und Protokollierung:
  Werden Zugriffe bzw. Zugriffsversuche auf Anwendungen protokolliert? Wann findet eine Auswertung der Protokolle statt? Wo und wie lange werden die Protokolle aufbewahrt (mindestens ein Jahr)?
- Datenträgerverwaltung:
  Sind die Datenträger inventarisiert (Art und Anzahl)? Wird die Lagerung von Datenträgern überprüft (dauernd/zeitweise, Bestandsverzeichnisse)? Werden Nachweise über Eingang, Ausgang sowie Bestand von Datenträgern festgehalten? Wo werden die Datenträger, insbesondere mobile wie USB-

Festplatten, nach Dienstschluss aufbewahrt (abschließbare Schränke, Schlüsselregelung)? Findet eine Auslagerung von Sicherungsdatenträgern statt?

- Datentrennung:
  Findet eine äußerliche Kennzeichnung der eigenen Datenträger zur Unterscheidung von fremden statt? Werden Datenträger verschiedener Auftraggeber getrennt behandelt? Gibt es einen eigenen Datenträger-Pool für jeden Kunden? Besteht eine Regelung/Verbot des Einsatzes privater Datenträger?
- Datenlöschung:
  Werden Datenträger verschlüsselt? Werden Datenträger vor neuer Verwendung vollständig von bestehenden Daten bereinigt? Werden Daten auf den Datenträger vor Weitergabe, wie z. B. Verkauf, gelöscht?
- Entsorgung/Vernichtung:
  Werden auch Fehldrucke sorgfältig entsorgt? Werden veraltete Datenträgern geregelt gem. DIN 32757 vernichtet (entsprechende Lagerung der zu vernichtenden Datenträger, Datenträgerlöschgeräte, Verbrennen/Zerstören)? Wird die Vernichtung protokolliert? Findet Kontrollen der tatsächlichen Vernichtung bei Dienstleistern statt (zuverlässiges Entsorgungsunternehmen, vertragliche Regelung, Entsorgungsbescheinigung)? Welche Aktenvernichter werden im Unternehmen eingesetzt (Sicherheitsstufe)?
- Regelung für das Kopieren von Datenträgern:
  Existieren Richtlinien für das Kopieren von Datensätzen bzw. auch für das vollständige Kopieren von Datenträgern? Besteht ein Taschenverbot bzw. erfolgen Kontrollen von Taschen?
- Regelungen für mobile Geräte:
  Gibt es Anweisungen zum Umgang mit mobilen Datenträgern und Geräte (z. B. USB-Sticks, PDAs, externe Festplatten, Tablets, Smartphones)? Werden die Datenträger verschlüsseltß Wird BYOD (Bring-Your-Own-Device) in der Organisation gelebt?
- Fernwartung:
  Bestehen Regelungen und gezielte Kontrollen bei Wartungsarbeiten durch Dienstleister (externe Wartung und Fernwartung)?

4. Weitergabe-/Transportkontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Mögliche Maßnahmen der Weitergabekontrolle sind:

- Sicherung der elektronischen Übertragung
  - Verschlüsselung
  - VPN
  - Firewall
- Sicherung beim Transport
  - Sichere versiegelte Transportbehälter
  - Verschlüsselung der Datenträger
- Sicherung bei der Übermittlung

- Protokolle
- Nachweis über Versand

Prüffokus:
Welche Regelungen existieren bezüglich der Weitergabe personenbezogener Daten (elektronische Übertragung, Datentransport, Übermittlungskontrolle)?

- Datenträgertransportart:
  Welche unterschiedlichen Datenträgertransporte finden statt (z. B. nur innerhalb des Unternehmens, zur Auslagerung, zwischen Auftraggeber/-nehmer, zu Dritten)?
- Versendungsarten:
  Wie werden die Daten versendet (z. B. Post, Bahn, Kuriere, Taxi, elektronisch). Werden Transportpersonal und –fahrzeuge sorgfältig ausgewählt? Wir geprüft ob eine Weitergabe der Daten in anonymisierter oder pseudonymisierter Form möglich ist?
- Transportregelungen:
  Sind die Bereiche festgelegt, in denen sich Datenträger befinden dürfen? Ist definiert, welche Personen die Datenträger befugt entnehmen dürfen? Gibt es schriftliche Festlegung der Transportwege und der Transportverfahren? Werden beim Transport Datenträgerbegleitpapiere ausgestellt bzw. mitgenutzt? ? Existiert eine verbindliche Regelung, wer als Datenempfänger fungieren darf und wer zur Weitergabe berechtigt ist? Werden Empfänger von Daten und die Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen dokumentiert? Findet eine Vollständigkeitsüberprüfung bei Rücklieferung vom Auftragnehmer statt?
- Elektronischer Transport
  Werden VPN-Tunnel zur Datenübermittlung benutzt? Werden bei elektronischer Übertragung die E-Mails verschlüsselt?

5. Eingabekontrolle

Die Eingabekontrolle soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme zu welcher Zeit bzw. von wem eingegeben, verändert oder entfernt worden sind.

Mögliche Maßnahmen der Eingabekontrolle sind:
- Protokollierung von Log-In / Log-Out
- Benutzeridentifikation

Prüffokus:
Welche Maßnahmen werden insbesondere zur Protokollierung bei Änderungen in den Datenverarbeitungssystemen ergriffen?

- Protokollierung:
  Welche Protokollierungs- und Protokollauswertungssysteme kommen zum Einsatz? Was wird im Rahmen der Protokollierung aufgezeichnet (z. B. wer erfasst, wer hat wann was eingegeben oder gelöscht)? Werden auch Aktivitäten der Heimarbeiter erfasst? Findet eine Kennzeichnung der erfassten Belege oder Laufzettel mit Namenszeichen/Stempel statt? Werden auch Online-

Eingaben bzw. Änderungen sorgfältig protokolliert? (Nachvollziehbarkeit von Eingabe, Änderungen und Löschungen von Daten durch individuelle Benutzernamen [nicht Benutzergruppen]). Welche Regelungen zur Aufbewahrungsdauer der Protokolle bestehen?

- Dokumentation:
  Erfolgt eine Dokumentation der Eingabeverfahren mit Festlegung der für die Erstellung von Datenträgern und der Bearbeitung von Daten Befugten (z. B. mit Stellenbeschreibung, Dienstanweisung, Geschäftsverteilungsplan)? Gibt es eine Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert oder gelöscht werden können? Werden Formulare, von denen Daten in automatisierte verarbeitungen übernommen worden sind aufbewahrt?

6. Auftragskontrolle

Die Auftragskontrolle soll gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Mögliche Maßnahmen der Auftrags sind:
- Bindende verpflichtung per vertrag nach Art. 28 DSGVO
- Erteilung von Weisungsbefugnissen
- Vor-Ort-Kontrollen (rechtzeitig angemeldete Stichprobenkontrollen der technischen und organisatorischen Maßnahmen nach Art. 28 DSGVO)
- Zertifiziertes Datenschutzmanagement
- Getroffene Maßnahmen, wie
  - genehmigte Verhaltensregeln (Art. 40 DSGVO)
  - genehmigtes Zertifizierungsverfahren (Art. 42 DSGVO)
  - Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, DSB, Auditoren etc)
  - Zertifizierung durch IT-Sicherheitsstandards oder Datenschutzaudits

Prüffokus:

Welche Regelungen bestehen im Umgang mit Auftragnehmern?

- Auswahl von Auftragnehmer:
  Findet eine Auswahl der Auftragnehmer sorgfältig (insbesondere hinsichtlich Datensicherheit) statt? Welche Kriterien zur Auswahl des Auftragnehmers bestehen?

- Unterauftragnehmer:
  Ist das geprüfte Unternehmen selbst als Auftragnehmer tätig? Welche Auftragnehmer werden dort nach welchen Kriterien ausgewählt?

- Schriftliches Auftragsverhältnis:
  Bestehen detaillierte schriftliche Regelungen der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes - auch zum Einsatz von Subunternehmen (Erfassung, Scannen, Entsorgung)? Gibt es eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim Datenträgertransport)? Erfolgt eine formalisierte Auftragserteilung (Auftragsformular)? Exisitieren schriftliche Anweisungen an den Auftragnehmer (z.B. durch einen Auftragsdatenverarbeitungsvertrag) i.S.d. Artikel 62 DSGVO)? Ist die Vernichtung von Daten nach

Beendigung des Auftrags geregelt? Sind die Mitarbeiter des Auftragnehmers auf das Datengeheimnis verpflichtet? Wurden Vertragsstrafen bei Verstößen festgelegt? Wurden beim Auftragnehmer getroffene Sicherheitsmaßnahmen überprüft und entsprechend dokumentiert? Wurden wirksame Kontrollrechte gegenüber dem Auftraggeber und dem Landesdatenschutzbeauftragten vereinbart?

- Kontrolle:
  Findet eine regelmäßige Kontrolle des Auftragnehmers statt (formal, inhaltlich)? Erfolgt auch eine Kontrolle der Unterauftragnehmer (z. B. durch den DSB)?

7. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass alle DV-Systeme und sich darauf befindende Daten zu jeder Zeit Verfügbar sind.

Mögliche Maßnahmen der Verfügbarkeitskontrolle sind:
- Backup-Routinen
- sichere Serverräume
- Notfallpläne

Prüffokus:

Welche Regelungen bestehen, um die Daten dauerhaft verfügbar bereitzustellen?

- Brandschutz:
  Welche Einrichtungen zum Brandschutz sind vorhanden (z. B. Feuerlöscher, Rauch- oder Brandmelder, Geräte zur Überwachung der Temperatur und Feuchtigkeit / Klimanlage in Serverräumen)? Besteht Rauchverbot? Existieren effektive Wasserschutzeinrichtungen?
- Stromversorgung:
  Ist eine unterbrechungsfreie Stromversorgung (USV) etabliert? Sind Schutzsteckdosenleisten in Serverräumen installiert?
- Sicherungen:
  Werden Sicherungsdatenträger getrennt an einem sicheren ausgelagerten Ort aufbewahrt? Gibt es ein Backup- & Recoverykonzept? Wo erfolgen die Backup-Verfahren? Werden Speichereinheiten redundant ausgelegt? Sind die Datensicherungen verschlüsselt? Werden Cloud-Lösungen zur Datensicherung eingesetzt?
- Virenschutz/Firewall:
  Bestehen ausreichende Schutzmaßnahmen durch Security-Werkzeuge?
- Notfallplan:
  Gibt es auch für einen Katastrophenfall entsprechende Vorkehrungen (z. B. durch Angriffe von in-tern/extern, Schäden durch Feuer)? Wurde die Datenwiederherstellung getestet?
- Lage:
  Befinden sich Serverräume nicht unter sanitären Anlagen? In Hochwassergebieten: Sind die Serverräume über der Wassergrenze?

8. Trennungskontrolle

Die Trennungskontrolle besagt, dass Daten, die zu unterschiedlichen Zwecken erhobene wurden auch getrennt verarbeitet werden müssen.

Mögliche Maßnahmen der Trennungskontrolle sind:
- Logische und / oder physikalische Trennung der Datenbestände
- Benutzerrechteverwaltung
- Unterweisung der Mitarbeiter zur Trennungskontrolle
- Funktionstrennung

Prüffokus:

Wie wird gewährleistet, dass Daten getrennt voneinander verarbeitet werden können?

- Getrennte Speicherung:
  Welche Regelungen/Maßnahmen zur Sicherstellung der getrennten Speicherung existieren? Wie erfolgt die Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Vertragszwecken (z. B. getrennte DV-Systeme für unterschiedliche Verarbeitungszwecke)? Wie werden Daten mit hohem Schutzbedarf verarbeitet?
- Mandantenfähigkeit:
  Werden Systeme verwendet, die eine interne Mandantenaufteilung ermöglichen (Zweckbindung)? Besteht ein Konzept zur Mandantentrennung?
- Funktionstrennung:
  Werden Produktion- und Testumgebungen stets voneinander getrennt? Werden personenbezogene Daten zu Entwicklungszwecken pseudonymisiert/anonymisiert?

9. Organisationskontrolle

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird.

Prüffokus:

Welche innerbetrieblichen Reglungen bestehen, um ein entsprechendes Datensicherheitsniveau zu gewährleisten?

- IT-Sicherheitskonzept:
  Bestehen schriftliche Regelungen über den Betrieb und die Abläufe der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen (z. B. Richtlinien, Arbeitsanweisungen, Stellenbeschreibungen)? Erfolgen Sicherungen des Datenbestandes nach festgelegtem Schema?
- Standards:
  Wird auf etablierte Standards für die IT-Sicherheit bzw. zur Abwicklung von IT-Projekten zurückgegriffen (IT-Grundschutzprofil für Handwerksbetriebe, etc.)?
- Revision:
  Werden Protokollierungen und Log-Dateien ausgewertet (z. B. stichprobenartig)? Finden auch

gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Da-tensicherungsmaßnahmen statt?

- Mitarbeiter:
  Ist im Urlaub- und Krankheitsfall für eine Vertretung gesorgt (z. B. Vertreterregelungen, Freigaben, Berechtigungen)? Werden die Mitarbeiter über den sicheren Umgang mit den Daten entsprechend geschult? Gibt es regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern? Werden mobile Datenträger der Mitarbeiter standardmäßig verschlüsselt? Besteht eine ausreichende Funktionstrennung? Findet bei wichtigen Datenverarbeitungen das „4-Augen-Prizip" Anwendung?

Organisationskontrolle

xxx

Prüffokus:
Xxx

Werden Änderungen im Datenschutzrecht und von anderen Rahmenbedingungen verfolgt und in den Datenschutzprozess integriert?

- Regelung der Verantwortlichkeiten:
  Wurde ein Datenschutzbeauftragter bestell?
  Ist der Datenschutzbeauftragte ausreichend qualifiziert?
  Stehen dem Datenschutzbeauftragten ausreichend Ressourcen zur Verfügung?
  Sind die Aufgaben und Kompetenzen des Datenschutzbeauftragten klar definiert?

- Aspekte eines Datenschutzkonzeptes
  Liegt ein Datenschutzkonzept vor, das alle Bereiche des Betriebes abdeckt?
  Wird das Datenschutzkonzept regelmäßig aktualisiert?
  Werden sämtliche Mitarbeiter, auch neu eingestellte, auf das Datenschutzkonzept verpflichtet bzw. unterrichtet?
  Sind ausreichende Betriebsmittel für die Umsetzung des Datenschutzkonzepts vorhanden?

- Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung von pbD
  Wird vor der Erhebung, verarbeitung oder Nutzung pbD geprüft, ob dies erforderlich und rechtlich zulässig ist?
  Wird bei allen Geschäftsprozessen darauf geachtet, dass pbD angemessen geschützt sind?

- Festlegung von TOMen entsprechend dem Stand der Technik
  Sind alle tom getroffen, die erforderlich sind, um ausreichend Datenschutz zu gewährleisten?
  Existieren geeignete Vorgaben zum Umgang mit pbD im gesamten Betrieb?

- Verpflichtung/Unterrichtung der Mitarbeiter bei der verarbeitung pbD
  Werden alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet bzw. darüber unterrichtet?
  Werden Mitarbeiter regelmäßig für die Belange des Datenschutzes sensibilisiert?

- Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung von pbD
  Existieren technisch-organisatorische Verfahren, umd die Rechte der Betroffenen bei der Verarbeitung pbD zu wahren?

- Führen von Verzeichnissen der Verarbeitungstätigkeiten und zur Erfüllung der Meldepflicht bei der Verarbeitung von pbD
  Existiert ein Verzeichnis der eingesetzen Hardware, Software und Verfahren sowie der erfassten pbD?

- Datenschutzrechtliche Freigabe
  Wir der Datenschutzbeauftragte vor den Softwaretests mit Daten, die Personenbezug haben könnten informiert?
  Wird vor der Freigabe von IT-Verfahren, die pbD verarbeiten, eine datenschutzrechtliche Prüfung durchgeführt?

- Regelungen der Auftragsdatenverarbeitung bei der Verarbeitung von pbD
  Wurden bei der Vertragsgestaltung zur Auftragsdatenverarbeitung, bei der pbD verarbeitet werden, alle relevanten Datenschutz-Aspekte berücksichtigt?

Ist sichergestellt, dass externe Dienstleister die Daten, die im Auftrag verarbeitet werden nur entsprechend den Weisungen des Auftraggebers verarbeitet werden?
Wurden auch beim Auftragnehmer alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet?

- Dokumentation der datenschutzrechtlichen Zulässigkeit
  Wird Hard- und Software, die für die Verarbeitung pbD eingesetzt wird, auf die datenschutzrechtliche Zulässigkeit geprüft?
  Werden die Prüfergebnisse dokumentiert?

- Aufrechterhaltung des Datenschutzes im laufenden Betrieb
  Wird die Einhaltung der datenschutzrechtlichen Anforderungen regelmäßig überprüft?
  Sind die Zulassigkeiten und Kompetenzen der Datenschutzkontrolle abgestimmt?

- Datenschutzgerechte Löschung/Vernichtung
  Werden Datenträger, die pbD enthalten, sicher gelöscht bzw. vernichtet?
  Kontrolliert der Datenschutzbeauftragte regelmäßig, dass Datenträger mit pbD datenschutzgerecht gelöscht bzw. vernichtet werden?

Überprüfung, Bewertung und Evaluierung

Ziel:
Die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen ist regelmäßig zu bewerten und zu evaluieren..

Mögliche Maßnahmen der Überprüfung, Bewertung und Evaluierung sind:

- Datenschutz-Management-Systeme (ISIS 12, ISA+)
- Datenschutz-Folgeabschätzung (DSFA)
- Penetrations-Testing (Schwachstellenidentifikation)
- Incident-Response-Management

Prüffokus:
Nach Artl 32 DSGVO Abs.1 Satz 1d gilt es Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen.

- Datenschutz-Folgeabschätzung
  Wurde eine Datenschutz-Folgeabschätzung nach Art. 35 DSGVO durchgeführt?

- Incident-Response-Management
  Gibt es schriftlicher Anweisungen, die im Falle eines Sicherheitsvorfalles entsprechend umgesetzt werden müssen?

Informationspflichten

Ziel:
Werden personenbezogene Daten betroffener Personen erhoben, so muss der verantwortliche nach Art. 13 DSGVO den Betroffenen alle relevanten Informationen übermitteln. Der Auftragnehmer ist dazu verpflichtet, den Auftraggeber bei der Einhaltung der Informationspflichten zu unterstützen. Nach Ablauf der vom Auftraggeber gesetzten Frist müssen zudem alle personenbezogenen Daten gelöscht oder zurückgegeben werden, Artl. 28 DSGVO.

Mögliche Maßnahmen zur Einhaltung der Informationspflichten sind:

- Aufsteller im Unternehmen
- Informationsblätter
- Hinweise auf Angeboten und Rechnungen ggf. mit Link auf die Internetseite

- **Prüffokus**
  xxxxx

Wahrung der Vertraulichkeit durch Beschäftigte

Ziel:
Aus der DSGVO läßt sich eine Pflicht zur „Wahrung der Vertraulichkeit“ für Beschäftigte ableiten (Art. 28 Abs. 3, Artl 29 sowie Art. 32 Abs. 4 DSGVO). Demnach soll ein Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte einstellen, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten bestimmungen zum Datenschutz vertraut gemacht wurden.

Mögliche Maßnahmen zur Wahrung der Vertraulichkeit durch Beschäftigte sind:

- Verpflichtungserklärung
- Schulung oder andere geeignete Sensibilisierungsmaßnahmen
- Einbeziehung in Jour Fixe / regelmäßige Treffen zum Datenschutz/IT-Sicherheit

- **Prüffokus**
  xxxxx

Benennung eines Datenschutzbeauftragten

Ziel:
Gemäß Art 37 DSGVO ist ein/eine Beauftragte/r für den Datenschutz (bDSB) zu benennen, die/der die Aufgaben (Art. 39 DSGVO) wahrnimmt. In welchen Fällen ein/e bDSB zu bennenn ist, ergibt sich aus Art. 37 DSGVO. Besonders hervorzuheben ist, dass der bDSB auf Grundlage seiner beruflichen Qualifikation und Fachwissens dem/der Landesdatenschutzbeauftragten benannt werden muss.

Mögliche Maßnahmen der Überprüfung Benennung sind:
- Bennenungspflicht
- Benennung
- Fachkunde
- Stellung im Unternehmen

Prüffokus:
Welche Maßnahmen hinsichtlich der Bestellung einer/es bDSB wurden ergriffen?

- Benennung
  Wurde ein/e bDSB benannt? Wenn nein, warum nicht?

- Fachkunde
  Liegt Fachkunde und Zuverlässigkeit sowie Unabhängigkeit vor?

- Stellung
  Wie ist der/die bDSB in die Prozesse eingebunden?

Verzeichnis der Verarbeitungstätigkeiten

Ziel:
Prüfung ob ein Verzeichnis der Verarbeitungstätigkeiten mit den in Art. 30 Abs. 2 DSGVO benannten Inhalten schriftlich oder elektronisch geführt wird.

Mögliche Maßnahmen der Überprüfung des Verzeichnisses der Verarbeitungstätigkeiten sind:
- Liste der Kategorien betroffener Personen
- List der Kategorien von Empfängern
- Liste von Drittländer in die Daten übermittelt werden
- Aufbewarungsvorschriften
- technisch-organisatorische Maßnahmen

Prüffokus:
Sind die in Art. 30 Abs. 2 DSGVO benannten Inhalten aufgeführt und ist das verzeichnis der Verarbeitungstätigkeiten vollständig?

- Kontaktdaten
  Sind die Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten genannt?

- Zweck
  Sind die Zwecke der einzelnen Verfahren benannt?

- Kategorien betroffener Personen
  Erfolgt eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten?

- Kategorien von Empfängern
  Wir die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen angegeben?

- Übermittlung in ein Drittland
  Ist ein Drittland oder eine internationale Organisation in das personenbezogenen Daten übermittelt werden sollen benannt sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien aufgeführt?

- Löschung
  Sind die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien angegeben?

- technischen und organisatorischen Maßnahmen
  Sind die ergriffenen technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 allgemein beschrieben?

Auftragsdatenverarbeitungsverträge

Ziel:
Prüfung ob Auftragsdatenverabeitungsverträge alle gemäß § 64 BDSG erforderlichen Maßnahmen erfüllen

Mögliche Maßnahmen der Überprüfung des Verzeichnisses der Verarbeitungstätigkeiten sind:

- xxx

Prüffokus:
Sind die in § 64 BDSG geforderten Maßnahmen erfüllt?

- Zugangskontrolle
  Ist der Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte verwerth?

- Datenträgerkontrolle
  wird das unbefugte Lesen, Kopieren, verändern oder löschen von Datenträgern verhindert?

- Speicherkontrolle
  Wird die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert?

- Benutzerkontrolle
  Wird die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert?

- Zugriffskontrolle
  Ist gewährleistet, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben?

- Übertragungskontrolle
  Ist gewährleistet, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können?

- Eingabekontrolle
  Ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind?

- Transportkontrolle
  Ist gewährleistet, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden?

- Wiederherstellbarkeit
  Ist gewährleistet, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können?

- Zuverlässigkeit
  Ist gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden?

- Datenintegrität
  Ist gewährleistet, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können?

- Auftragskontrolle
  Ist gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können?

- Verfügbarkeitskontrolle
  Ist gewährleistet, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind?

- Trennbarkeit
  Ist gewährleistet, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können?

- Berichtspflicht
  Ist gewährleistet, dass der Auftragsdatenverarbeiter bei einer Datenschutzverletzung unverzüglich dem Auftraggeber Bericht erstattet?

- Informationspflichten
  Das der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Informationspflichten gegenüber dem Betrpffenen unterstützt? Dazu gehört auch die unverzügliche Bereitstellung relevanter Informationen.

- DASF
  Unterstützt der Auftragsverarbeiter den Auftraggeber bei der Erstellung einer DASF sowie bei der vorherigen Konsultation mit einer Aufsichtsbehörde?

Drittstaatenübermittlung

Ziel:
Prüfung ob das Ziel-Land ein hohes bzw. gleich hohes Datenschutz-Niveau hat, wie die EU-Mitgliedsstaaten

Mögliche Maßnahmen der zulässigen Datenübermittlung in Länder außerhalb der EU:

- Angemessenheitsbeschluss
- Vorlage geeignete Garantien
- Vorlage verbindlicher interner Datenschutzvorschriften
- Ausnahmeregelung für bestimmte Fälle nach Art. 49 DSGVO

Prüffokus:
Sind die Bedingugen der Art. 45-50 DSVGO erfüllt?

- Schutzniveau
  Hat das betreffende Drittland ein angemessenes Schutzniveau (Art. 45 Abs. 1)?

- Angemessenheitsbeschluss
  Liegen geeignete Garantie für ein angemessenes Schutzniveau vor?

- interner Datenschutzvorschriften
  Hat der Auftraggeber geeignete Garantien vorgesehen und darüber hinaus den betroffenen Personen angemessene Rechte zur Verfügung gestellt?

- Ausnahmeregelung
  Liegen Ausnahmeregelung für bestimmte Fälle nach Art. 49 DSGVO vor?
-

Vertreter innerhalb der EU

Ziel:
sofern Art 3 Abs. 2 Anwendung findet („Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen"), muss der Auftragsdatenverarbeiter gem. Art. 27 DSGVO einen Vertreter innerhalb der EU wählen. Dieser vertreter muss innerhalb der Mitgliedsstaaten der EU niedergelassen sein, in denen die personen befinden, deren personenbezogenen Daten verarbeitet werden. Dieser Vertreter dienst darüber hinaus als Kontaktstelle für Aufsichtsbehörden oder betroffene Personen.

Mögliche Maßnahmen der zulässigen Datenübermittlung in Länder außerhalb der EU:
- Angemessenheitsbeschluss
- Vorlage geeignete Garantien
- Vorlage verbindlicher interner Datenschutzvorschriften
- Ausnahmeregelung für bestimmte Fälle nach Art. 49 DSGVO

Prüffokus:
Sind die Bedingugen der Art. 45-50 DSVGO erfüllt?