Checkliste zur Erstellung von Datenschutz- und Informationssicherheitskonzepten

Verantwortlichkeiten im Datenschutz festlegen

Organisatorische Festlegungen von Verantwortlichkeiten im Datenschutz, z. B.:

- Festlegung der Abteilung, des Sachgebietes etc. welches für die Verarbeitung der Daten zuständig ist
- Evtl. Festlegungen zur Auftragsdatenverarbeitung (vgl. § 7 SächsDSG)
- Frühzeitige Einbeziehung des behördlichen Datenschutzbeauftragten (falls bestellt) in die Verfahrenseinführung bzw. bereits zum Zeitpunkt der Verfahrensausschreibung

Sicherstellung der Verpflichtung gemäß § 6 SächsDSG

- Verpflichtung der Mitarbeiter auf das Datengeheimnis

Verfahrensverzeichnis gemäß § 10 SächsDSG erstellen

- Bekanntmachung des Sächsischen Datenschutzbeauftragten zum Verzeichnis automatisierter Verarbeitungsverfahren

Vorabkontrolle gemäß § 10 Abs. 4 SächsDSG durchführen

- Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Vorabkontrolle

Festlegungen in Datenschutz- und Informationssicherheitskonzepten

Ziel des Einsatzes und rechtlichen Rahmen des eingesetzten Verfahrens dokumentieren

- Nennung des Zwecks zum Einsatz des Verfahrens
- Aufführen der rechtlichen Grundlage zur Verarbeitung der personenbezogenen Daten
- Bei Verarbeitung auf der Grundlage der Einwilligung des Betroffenen: Klärung, dass die Verarbeitung der Daten zur Erfüllung gesetzlich vorgeschriebener Aufgaben erforderlich ist.

Festlegung der zu verarbeitenden personenbezogenen Daten (Bürger- und Mitarbeiterdaten)

- Der Umfang der personenbezogenen Daten, die bei einer E-Government-Anwendung verarbeitet werden sollen, ist im Datenschutzkonzept festzulegen. Die zu verarbeitenden personenbezogenen Daten sind abschließend aufzuzählen.
- Erforderlichkeit für die Aufgabenerfüllung prüfen
- Prüfung der Geeignetheit der Daten
- Grundsatz der Zweckbindung gewährleisten
- Grundsätze der Datenvermeidung und Datensparsamkeit gewährleisten

    - Der Datenverarbeitungsprozess ist so zu organisieren und die Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass die Verarbeitung personenbezogener Daten nur im erforderlichen Rahmen stattfindet, indem z. B. nur die erforderlichen Daten verarbeitet werden oder sogar auf einen Personenbezug verzichtet wird.
    - Soweit rechtlich und technisch möglich und zumutbar, ist den Betroffenen zu ermöglichen, anonym oder pseudonym zu handeln oder pseudonym zu bezahlen. Hierfür können unterschiedliche Zahlungsverfahren genutzt werden, die diese Möglichkeit bieten.

- Ist eine Anonymisierung oder eine Pseudonymisierung erforderlich, so ist für das jeweilige System / Teilsystem oder den jeweiligen Arbeitsschritt eine entsprechende Prozedur zu finden, die die personenbezogenen Daten frühestmöglich anonymisiert bzw. pseudonymisiert (siehe hierzu auch Orientierungshilfe »Datenschutzfreundliche Technologien« des Arbeitskreises »Technik« der Datenschutzbeauftragten des Bundes und der Länder).

Ermittlung des Schutzbedarfes der verarbeiteten Daten pro Schutzziel gemäß § 9 Abs. 2 SächsDSG

- Hinweise zur Schutzbedarfsfeststellung im BSI-Standard 100-2

Aufzählung und Beschreibung der eingesetzten IT-Komponenten

- Aufzählung und zumeist grafische Darstellung der eingesetzten technischen Komponenten
- Darstellung und Dokumentation in welcher Weise die Komponenten miteinander in Verbindung stehen
- Darstellung der Einbettung der technischen Komponenten in die Gesamt-IT-Infrastruktur

Prozessbezogene Verfahrensbeschreibung, in der die Verfahrensweisen bei der Verarbeitung der personenbezogener Daten vollständig und aktuell dokumentiert sind

- Konkrete Beschreibung, wie die personenbezogenen Daten verarbeitet werden

Dokumentation der Festlegung der erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzrechtlichen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionssicherheit, Transparenz)

- Konkrete Maßnahmen aufführen und beschreiben, die die Vertraulichkeit sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der **Vertraulichkeit** z. B. festzulegen:
    - Sicherstellung, dass eine Kenntnisnahme von personenbezogenen Daten nur durch gesetzlich dazu Befugte erfolgt
    - Differenzierte Zugriffsrollen und -rechte mit Vertretungsregelungen
    - Zutritts- und Zugriffsregelungen durch Passwörter, Chipkarten u. ä.
    - Bildschirmschoner mit Passwort
    - Regelungen für sicheres Löschen
- Konkrete Maßnahmen aufführen und beschreiben, die die **Integrität** sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der Integrität z. B. festzulegen:

  - Daten dürfen nicht unbefugt geändert werden
  - Differenzierte Schreibrechte bei elektronischen Daten
  - Beschränkte Vergabe von Administratorbefugnissen
  - Verschlüsselung bei besonderen Risiken:
    - Mobile Technik / Datenträger
    - Heimarbeit
    - WLAN
    - Internet / E-Mail

- Konkrete Maßnahmen aufführen und beschreiben, die die **Verfügbarkeit** sicherstellen. Zur Feststellung der Anforderungen an die Verfügbarkeit sind z. B. folgende Fragen zu klären:

  - Wie lange kann höchstens auf den Rechner bzw. die Daten verzichtet werden (Stunden, Tage oder Wochen)?
  - Welcher Termin ist der kritischste für den Ausfall des Rechners oder den Verlust der Daten?
  - Welche Folgen hat ein längerfristiger Rechnerausfall?
  - Welcher Schaden tritt ein, wenn Daten endgültig verloren sind?
  - Wie lange dauert es und wie viel kostet es, das System wiederherzustellen oder die Daten erneut zu erfassen?

- Konkrete Maßnahmen aufführen und beschreiben, die die **Authentizität** sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der Authentizität z. B. festzulegen:

  - Vergabe von Benutzernamen und Passwort, Verwendung von Chipkarten
  - Verwendung von qualifizierten elektronischen Signaturen gemäß § 1 SächsVwVfZG i. V. m. § 3a Absatz 2 VwVfG

- Konkrete Maßnahmen aufführen und beschreiben, die die **Revisionsfähigkeit** sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der Revisionsfähigkeit z. B. festzulegen:

  - Umfang des Protokolls
  - Anlass, Zweck und Zeitpunkt der Protokollauswertung
  - Ablauf der Protokollauswertung
  - Befugte, die die Protokolle auswerten
  - Löschung der Protokolle
  - In der Regel Dienstvereinbarung

- Konkrete Maßnahmen aufführen und beschreiben, die die **Transparenz** sicherstellen:

  - Das Transparenzgebot wird z. B. durch Unterrichtungspflichten über die Möglichkeit anonymen und pseudonymen Handelns, über Profilbildungen gewährleistet. Diese Informationen sollten in einer Datenschutzerklärung zusammengefasst und den Nutzern zugänglich gemacht werden.

Verfahrensweisen festlegen, die die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung sicherstellen (§§ 18-23 SächsDSG)

- Es ist festzulegen, wie die o. g. Rechte der Betroffenen vom Verfahren gewährleistet werden, z. B. wie beauskunftet wird.

- Auf die systemseitige Gewährleistung der Betroffenenrechte sollte schon bei der Ausschreibung des Verfahrens geachtet werden.
- Die Datenschutzhinweise sollten eine Erklärung enthalten zu Grundsätzen der Verfahrensweise bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Angebots im Internet anfallen. Außerdem sollte über die Auskunftsansprüche und Korrekturrechte informiert werden. Die Hinweise sollten an zentraler Stelle – etwa auf der Eingangsseite im Internet – erscheinen und leicht verständlich formuliert sein. Zur Gewährleistung der Transparenz gehört insbesondere die Information darüber, wer für die Gestaltung des Angebots verantwortlich zeichnet.
- Wenn die Nutzung eines Angebots die Erhebung personenbezogener Daten voraussetzt, sind die Nutzer über die Zweckbestimmung der Verarbeitung, für die die Daten bestimmt sind, zu unterrichten.
- Bei elektronischer Antragsstellung ist der Antragsteller darüber zu informieren, wie das Gesamtverfahren abgewickelt wird.

Rollen und Zugriffsrechte festlegen

- Wenn verschiedene Stellen bei der Erbringung einer E-Government-Dienstleistung zusammenwirken, ist darauf zu achten, dass die beteiligten Einrichtungen nur die für die jeweilige Teilaufgabe erforderlichen Daten zur Kenntnis nehmen können.
- Es muss sichergestellt sein, dass nur berechtigte Nutzer den Zugang zu den Daten haben. Die Identifizierung und Authentisierung sollte an zentraler Stelle durchgeführt werden (Authentifizierungsserver) bzw. über das jeweilige Betriebssystem erfolgen.
- Rechte sind sowohl benutzerbezogen als auch datei- oder programmbezogen zu vergeben, um die Zugriffsmöglichkeiten zweckgebunden zu begrenzen. Dabei ist der Maßstab immer das fachliche Anforderungsprofil und die Arbeitsaufgabe des einzelnen Benutzers.
- Arbeitsschritte, die im Hinblick auf die Einhaltung der Zweckbindung besonders sensibel sind, sind zu Zwecken der Beweissicherung soweit notwendig zu protokollieren. Beweissicherung bedeutet in diesem Zusammenhang, dass es im Nachhinein möglich sein muss, den Missbrauch zugestandener Rechte nachzuweisen oder die versuchte Ausübung von nicht zugestandenen Rechten aufzudecken.
- Daten sind logisch getrennt zu speichern. In diesem Fall ist eine gegenseitige Abschottung der zweckgebundenen Datenbestände am einfachsten und am datenschutzfreundlichsten zu realisieren.
- Moderne Datenverarbeitungsanlagen bieten die Möglichkeit, gleichzeitig mehrere Anwendungen abzuarbeiten. Hier ist darauf zu achten, dass die einzelnen Anwendungen und ihre jeweils zweckgebundenen Daten gegenseitig voneinander abgeschottet verarbeitet werden. Dies kann in der Praxis durch den Einsatz technischer Zusatzsysteme erreicht werden, die beispielsweise auf einem Prozessor mehrere virtuelle Maschinen simulieren, welche die jeweiligen Anwendungen einschließlich deren Daten gegeneinander abgekapselt verarbeiten.
- Sensible Daten sind verschlüsselt zu speichern und zu übertragen, damit eine inhaltliche Kenntnisnahme der Daten durch Unbefugte verwehrt wird. Die Prozeduren der Verschlüsselung sind für die Benutzer transparent zu halten.

- Für besondere Zwecke erhobene Daten sollten mit einem spezifischen Kennzeichen versehen werden, welches den Zweck ihrer Erhebung sowie einer eventuellen Verarbeitung und Übermittlung spezifiziert, sodass eine Verwendung für einen anderen Zweck kontrolliert werden kann. Die Vergabe solcher Kennzeichen und die Sicherung der Zweckbindung anhand der Auswertung dieser Kennzeichen, stellt eine elegante und zukunftsorientierte Sicherheitstechnologie dar. Für ihre technische Realisierung wären allerdings erhebliche Änderungen bzw. Erweiterungen der bestehenden Betriebs- und Datenbanksysteme sowie Anwendungsprogramme erforderlich, die derzeit noch nicht über solche Funktionalitäten verfügen.

Festlegungen zur Löschung von Daten

Es ist festzulegen,

- Welche Löschregeln für welche Datenbestände gelten,
- Wie aus den Löschregeln die Umsetzung der Löschung in Prozessen der verantwortlichen Stelle erreicht wird,
- Wie die Löschregeln, Umsetzungsvorgaben und durchgeführten Löschmaßnahmen zu dokumentieren sind,
- Wer für die aus dem Löschkonzept entstehenden Aufgaben der Umsetzung, Überprüfung und Fortschreibung verantwortlich ist.

Festlegungen zur Protokollierung

- Erhebung, Verarbeitung und Weitergabe von personenbezogenen Daten (Bestands-, Verbindungs- und Nutzungsdaten) sollten grundsätzlich anonymisiert oder mittels eines Pseudonyms erfolgen.
- Für Art, Umfang und Aufbewahrung der Protokollierung und Bestandsdaten gilt der Grundsatz der Erforderlichkeit. Die Protokollierung sollte so erfolgen, dass sensitive Aktivitäten und vorab zu definierende Systemzustände für eine nachfolgende Kontrolle festgehalten werden. Unter anderem sollte Folgendes protokolliert werden:
    - Systemgenerierung und Modifikation von Systemparametern,
    - Einrichten von Benutzern,
    - Erstellung von Rechteprofilen,
    - Einspielen und Änderung von Anwendungssoftware,
    - Änderungen an der Dateiorganisation,
    - Durchführung von Datensicherungsmaßnahmen,
    - Sonstiger Aufruf von Administrations-Tools,
    - Datenübermittlungen,
    - Zugriffe auf aktive Systemkomponenten,
    - Falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze,
    - Versuche von unberechtigten Zugriffen, insbesondere sicherheitskritische Zugriffe mit oder ohne Erfolg,
    - Verteilung der Rechner- / Systemlast über die Betriebsdauer eines Tages oder eines Monats und die allgemeine Performance,
    - Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können.

- Protokolldaten dürfen nur zu Zwecken genutzt werden, die Anlass für ihre Speicherung waren.
- Die Daten über die Inanspruchnahme verschiedener Online-Dienste werden getrennt gespeichert.
- Eine unzulässige Zusammenführung der Nutzungsdaten ist technisch zu verhindern.
- Die Protokolldaten werden bei kostenfreier Nutzung des Online-Dienstes nach Ende der jeweiligen Nutzung gelöscht. Bei kostenpflichtiger Nutzbarkeit sind die Protokolldaten spätestens nach Ablauf von sechs Monaten nach Versendung der Rechnung und des Einzelnachweises zu löschen, soweit es nicht zu Einwendungen gekommen ist oder nach bereichsspezifischen Regelungen besondere Aufbewahrungsfristen zu beachten sind.
- Die Verwendung von Protokolldaten zu Zwecken der Verhaltens- und Leistungskontrolle ist untersagt. Nur im Einzelfall ist eine Auswertung der Protokolldaten zur Aufdeckung von Missbräuchen zulässig.

Festlegungen zur Auftragsdatenverarbeitung

- Den Regeln der Auftragsdatenverarbeitung entsprechend, muss für jedes »Outsourcing-Vorhaben« ein schriftlicher Auftrag erteilt werden. Darin sind insbesondere darzustellen:
    - Detaillierte Festlegung der Rechte und Pflichten der Daten verarbeitenden Stelle und des Auftragnehmers
    - Gegenstand und Umfang der übertragenen Tätigkeiten
    - Die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Datenschutzmaßnahmen
    - Etwaige Unterauftragsverhältnisse des Auftragnehmers
- Ferner muss vereinbart werden, dass der Auftraggeber dem Auftragnehmer Weisungen hinsichtlich der Verarbeitung personenbezogener Daten erteilen darf.
- Das Personal des beauftragen Unternehmens ist auf das Datengeheimnis nach § 6 SächsDSG zu verpflichten.
- In der Vereinbarung ist ferner festzulegen, dass der Auftragnehmer sich der Kontrolle der zuständigen staatlichen Datenschutzaufsichtsbehörde und des Auftraggebers unterwirft; dabei sind die Vorgaben des jeweils einschlägigen Datenschutzgesetzes zu beachten.
- Vor allem bei größeren Projekten bietet es sich an, die technisch-organisatorischen Maßnahmen in einem Datenschutz- und Sicherheitskonzept zusammenzufassen, dessen Umsetzung und Einhaltung vertraglich vereinbart wird. Die technisch-organisatorischen Maßnahmen können dann dem Stand der Technik folgend fortgeschrieben werden, ohne dafür den »Outsourcing-Vertrag« selbst ändern zu müssen.