Datenschutzanforderungen im Kontext zur IT-Sicherheit für öffentliche Stellen

Stand: Februar 2021

Datenschutzanforderungen im Kontext zur IT-Sicherheit für öffentliche Stellen

Inhalt

I. Anforderungen der Verordnung (EU) 2016/279 – Datenschutz-Grundverordnung (DS-GVO)

Als Grundsatz und zentrales Prinzip des Datenschutzes wurde in der seit 25.05.2018 umzusetzenden Datenschutz-Grundverordnung (DS-GVO) für die Verarbeitung personenbezogener Daten insbesondere die Gewährleistung der Datensicherheit verankert (Art. 5 Abs. 1 lit. f) und Art. 32 DS-GVO). Das Papier richtet sich an die Verantwortlichen und ggf. an Auftragsverarbeiter, die geeignete technische und organisatorische Maßnahmen zu treffen haben, um einen Schutz etwa vor unbefugter oder unrechtmäßiger Verarbeitung oder dem unbeabsichtigten Verlust der personenbezogenen Daten zu gewährleisten. Zu berücksichtigen sind dabei der Stand der Technik, die Implementierungskosten sowie die Art, die Umstände und der Zweck der Datenverarbeitung, aber auch die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten natürlicher Personen. Das Sicherheitsniveau muss im Verhältnis zum Risiko angemessen sein.

Auch müssen gemäß Art. 24 Abs. 2 DS-GVO Maßnahmen geeignete Datenschutzvorkehrungen durch den Verantwortlichen umfassen, sofern diese in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten stehen.

Die Maßnahmen richten sich darauf, die Grundsätze der Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO zu gewährleisten: die Rechtmäßigkeit, die Verarbeitung nach Treu und Glauben, die Transparenz; die Zweckbindung; die Datenminimierung; die Richtigkeit; die Speicherbegrenzung; die Integrität und Vertraulichkeit sowie die Rechenschaftspflicht. Die Ergebnisse vorgenommener Risikoanalysen gemäß Art. 32 Abs. 1 DS-GVO sind darin aufzunehmen, da sie Grundlage für die zu treffenden Maßnahmen sind.

Nicht zuletzt weisen diese Grundsätze der Verarbeitung sowie die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 DS-GVO[1], eindeutig auf die Pflichten des Verantwortlichen hin. Zu den Pflichten des Verantwortlichen heißt es insbesondere in Art. 5 Abs. 2 DS-GVO:

> *„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“*

[1] vgl. hierzu auch Erwägungsgründe 38 sowie 39 DS-GVO

Ist die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich[2] oder ist sie zur Wahrnehmung einer Aufgabe[3] erforderlich, die im öffentlichen Interesse liegt oder aber in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so enthalten §§ 16, 17 sowie 18 Thüringer Datenschutzgesetz (ThürDSG) weitergehende Regelungen für den öffentlichen Bereich, die in diesem Zusammenhang zusätzlich zu berücksichtigen sind[4]. So regelt § 16 ThürDSG die Verarbeitung personenbezogener Daten, § 17 ThürDSG die Zweckbindung und Zulässigkeit der Weiterverarbeitung sowie § 18 ThürDSG die Übermittlung personenbezogener Daten.

(1) Ergänzende Anforderungen aus Bundes- sowie Landesgesetzgebung

Bei öffentlichen Stellen sind dabei zudem verschiedene fachliche Vorgaben zu berücksichtigen, die sich unmittelbar aus der spezialgesetzlichen **Bundes- sowie Landesgesetzgebung** ergeben.

So schreibt bspw. das Bundesmeldegesetz (BMG) vor, dass …

- … in den Melderegistern zu speichernde Daten nur nach Maßgabe des Bundesmeldegesetzes oder sonstiger Rechtsvorschriften verarbeitet werden dürfen (§ 2 Abs. 4 BMG),
- … es bei den Meldebehörden beschäftigten Personen auch über ihre aktive Dienstzeit hinaus untersagt ist, personenbezogene Daten unbefugt zu verarbeiten (§ 7 BMG - Meldegeheimnis),
- … die Meldebehörde Meldedaten an andere öffentliche Stellen nur übermitteln darf, soweit dies zur Erfüllung der in ihrer Zuständigkeit oder in der Zuständigkeit des Empfängers liegenden öffentlichen Aufgaben erforderlich ist (§ 34 BMG).

Aber auch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) regelt in § 8a Abs. 1 i. V. m. Abs. 3, dass Betreiber „Kritischer Infrastrukturen“ verpflichtet sind, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen „Kritischen Infrastrukturen“ maßgeblich sind.

[2] vgl. Art. 6 Abs. 1 Satz 1 lit. c) DS-GVO
[3] vgl. Art. 6 Abs. 1 Satz 1 lit. e) DS-GVO
[4] vgl. Art. 6 Abs. 2 DS-GVO: Regelungsraum für Mitgliedstaaten;
s.a. Erwägungsgründe 40 bis 50 DS-GVO

Dies ist auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

Die Verordnung zur Bestimmung „Kritischer Infrastrukturen“ nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) regelt, welche Dienstleistungen aus den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen und Transport und Verkehr als kritisch anzusehen sind.

Die Verantwortlichen haben ergänzende Anforderungen aus der Bundes-sowie Landesgesetzgebung daher zwingend zu prüfen und vollständig in ihre Verwaltungsabläufe einzubeziehen.

II. SDM als Unterstützung der geforderten technischen und organisatorischen Maßnahmen

Mit dem **Standard-Datenschutzmodell (SDM)**[5] stellt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein Werkzeug bereit, mit dem die risikoadäquate Auswahl und rechtliche Bewertung der von der DS-GVO geforderten technischen und organisatorischen Maßnahmen unterstützt wird.

Das SDM verwendet zur Systematisierung der datenschutzrechtlichen Anforderungen den Begriff „Gewährleistungsziele“, die bereits aus dem Bundesamtes für Sicherheit in der Informationstechnik (BSI) definierten IT-Grundschutz des BSI bekannt sind[6]. Datenschutzrechtliche Anforderungen zielen auf die rechtskonforme Verarbeitung, die durch technische und organisatorische Maßnahmen (TOM) gewährleistet werden muss. Durch Festlegung und Umsetzung der TOM wird das Risiko des Eintretens von Abweichungen bzgl. der rechtskonformen Verarbeitung gemindert. Gewährleistungsziele bündeln und strukturieren auch im Datenschutz die festgeschriebenen gesetzlichen Anforderungen. Mit ihrer Hilfe können Maßnahmen messbar gestaltet werden. Die beschriebene Methode lehnt sich an den IT-Grundschutz an und hat sich dort bereits seit den 90er Jahren des vergangenen Jahrhunderts bewährt.

Gewährleistungsziele des Datenschutzes gemäß SDM sind:

- Datenminimierung
- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz,
- Intervenierbarkeit.

Bei der praktischen Umsetzung des SDM wird für jede zu betrachtenden Komponente der gesamten Systemstruktur – das sind Daten, Systeme, Dienste sowie Prozesse – ein Vergleich bzgl. der Gewährleistungsziele mit den vorgegebenen Referenzmaßnahmen durchgeführt. Daraus resultierend werden dann einzelne, konkrete TOM benannt und dokumentiert. Beachtet werden sollte, dass bestimmte Einzelmaßnahmen zur Erreichung mehrerer Gewährleistungsziele beitragen können. Dies ist im Einzelfall ebenfalls zu dokumentieren mit

[5] DSK:
vgl. https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf

[6] eine Kurzzusammenfassung dazu gibt https://de.wikipedia.org/wiki/IT-Grundschutz

dem Ziel, Datenschutzanforderungen sinnvoll zu strukturieren und in der Folge systematisch in der Organisation umzusetzen.

Dies gilt bspw. auch für Websiten. So sind für Kontaktformulare einer Webseite die technischen und organisatorischen Maßnahmen zu ergreifen und zu dokumentieren, um die o.g. Gewährleistungsziele zu erreichen.

Entsprechend DS-GVO sind die TOM nicht nur einmalig zu implementieren, sondern vielmehr sollte ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM vorgesehen sein (Art. 32 Abs. 1 lit. d) DS-GVO). Die aktuelle Angemessenheit der TOM orientiert sich dabei am Stand der Technik[7].

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 (Art. 32 Abs. 2 DS-GVO).

Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte **IT-Grundschutz** ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium[8] konkrete Anforderungen. Bei der Auswahl von Maßnahmen orientiert sich der Grundschutz vorrangig an den aus der IT-Sicherheit bekannten Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit.[9]

In Abgrenzung dazu betrachtet das SDM neben den o. g. aus der IT-Sicherheit bekannten Schutzzielen vorrangig die Gewährleistungsziele mit Datenschutzbezug. Auch hieraus werden – wie im Bereich der IT-Sicherheit – in analoger Methodik TOM abgeleitet. Im Bereich des Datenschutzes werden additiv auch die Risiken betrachtet, die von den Aktivitäten der Organisation selbst innerhalb und außerhalb ihrer Geschäftsprozesse für die Rechte und Freiheiten natürlicher Personen bestehen. Insofern erfordert die Anwendung der Methodik eine erweiterte Betrachtungsperspektive hinsichtlich der Risiken, die zu bewerten sind.

Deshalb wurde Rahmen der Modernisierung der Grundschutzmethodik durch das BSI – veröffentlicht im Oktober 2017 – das Verhältnis von Datenschutz und Informationssicherheit neu justiert. Im neuen BSI-Standard 200-2 wird auf das SDM verwiesen, wenn es darum geht,

---

7 vgl. Art. 32 Abs. 1 DS-GVO

8 vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

9 Quelle: https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf/ > SDM, Version 2a vom 06.12.2019, S. 57f

das Risiko eines Grundrechtseingriffs und den daraus folgenden Schutzbedarf zu bestimmen. So werden im neuen Baustein „CON.2 Datenschutz“ Abgrenzungsmerkmale zwischen Informationssicherheit und Datenschutz beschrieben.[10]

Die Umsetzung von IT-Sicherheitsmaßnahmen ist für den Datenschutz essentiell. Sie stellt im SDM jedoch nur die auf den Bereich Datenschutz bezogene Auswahl geeigneter TOM aus der Perspektive der betroffenen Person(en) und dessen/deren Grundrechtsausübung dar.[11]

BSI-Grundschutz und SDM ergänzen sich. Sie liefern gemeinsam die Informationen, die erforderlich sind, um die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten zu treffen und diese nachweisen zu können (Art. 5 Abs. 2 DS-GVO).

Der Verantwortliche hat unabhängig davon in jedem Falle ein **Verzeichnis von Verarbeitungstätigkeiten** gemäß Art. 30 DS-GVO[12] zu führen. Dieses Verzeichnis ist nicht zwingender Bestandteil des oben beschriebenen Managementkonzepts zur Datensicherheit.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat hierzu für die öffentlichen Stellen Thüringens Hinweise sowie ein Anwendungsbeispiel, als Muster auf seiner Website veröffentlicht[13].

Bedient sich der Verantwortlichen eines **Auftragsverarbeiters**, so müssen gem. Art. 28 DS-GVO geeignete technische und organisatorische Maßnahmen durchgeführt werden, so dass die Verarbeitung im Einklang mit der DS-GVO erfolgen kann und die Rechte der betroffenen Person gewahrt werden. Alle Anforderungen müssen den aktuellen Stand der Technik abbilden.

Die Verarbeitung durch den Auftragsverarbeiter erfolgt gem. Art. 28 Abs. 3 DS-GVO **auf** der **Grundlage eines Vertrages** oder eines anderen Rechtsinstruments nach dem Unionsrecht mit festgelegten Pflichten und Rechten der Vertragspartner.

---

[10] Erläuterung aus dem SDM: Die Anforderung „CON.2.A1 Umsetzung Standard-Datenschutzmodell“ besagt konkret, dass geprüft werden sollte, ob das SDM angewendet wird. Das etwaige Nichtberücksichtigen aller Gewährleistungsziele verbunden mit der Nichtanwendung der SDM-Methodik sowie der empfohlenen Referenzmaßnahmen sollten stichhaltig und ausführlich sachlich begründet werden.; ebenda

[11] Erläuterung aus dem SDM: „IT-Grundschutz hat vorrangig die Informationssicherheit im Blickfeld und soll die datenverarbeitende Institution schützen. Für die Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die ein Betroffener durch die Datenverarbeitung der Institution hinnehmen muss. Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen durch verantwortliche Stellen und der von Maßnahmen zur Gewährleistung der Betroffenenrechte zu unterscheiden.“, ebenda

[12] vgl. Art. 30 Abs. 1 DS-GVO, s.a. Erwägungsgrund 82

[13] https://www.tlfdi.de/tlfdi/datenschutz/kommunales/

Für einige IT-Verfahren ist eine **Datenschutz-Folgenabschätzung** nach Art. 35 DS-GVO notwendig. Entsprechende Hinweise sind auf der Homepage[14] des TLfDI zu finden.

[14] vgl. https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf

III. Checkliste für Managementkonzept

Die nachfolgende **Checkliste** des TLfDI soll die Erstellung / Überarbeitung eines entsprechenden Managementkonzepts zur Datensicherheit im Kontext zur IT-Sicherheit unterstützen, indem sie Kernfragen in den Mittelpunkt rückt. **Die Checkliste erhebt indessen keinen Anspruch auf Vollständigkeit.**

Weiterführende Hinweise erhalten Sie neben den oben in Fußnoten aufgeführten Dokumenten auch in Veröffentlichungen bei den verschiedenen Landesbeauftragten für den Datenschutz (bspw. Mecklenburg-Vorpommern, die der DSK[15]) sowie beim Bundesamt für Sicherheit in der Informationstechnik (BSI)[16].

(1) Sicherstellung der Verfügbarkeit

Art. 32 Abs. 1 lit. b), c) DS-GVO

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
1. Welches Konzept existiert zur Anfertigung von Sicherheits-kopien von Daten, Prozess-zuständen, Konfigurationen, Datenstrukturen, Transaktions-historien?			
2. Welche Maßnahmen werden zum Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt) angewendet? 3. Sind Server in Räumen unter-gebracht, bei denen einbruchs- sowie brandhemmende bau-liche Vorrichtungen vorhanden sind? Welche sind das? 4. Gibt es ein Notfallvorsorge- bzw. Havariekonzept, das die			

[15] DSK:
vgl. https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf/

[16] Bundesamt für die Sicherheit in der Informationstechnik (BSI): vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards100/Standard02/ITGStandard02_node.html

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
Belange der IT-Sicherheit berücksichtigt?			
5. Wurden die Maßnahmen in den Konzepten aus Nr.1 und Nr. 4 schon einmal getestet? 6. Wenn ja, in welchem zeitlichen Abstand geschieht dies? Wenn nein, wann ist dies erstmalig geplant? 7. Wenn nein, wann ist dieses geplant?			
8. Welche Vorgaben existieren, dass IT-Systeme oder auch einzelne Komponenten (z.B. bestimmte Fachanwendungen) nach Ausfall innerhalb einer bestimmten Zeit wieder zur Verfügung stehen? 9. Wird die Dokumentation der Strukturierung der Daten regelmäßig vorgenommen? 10. Gibt es Maßnahmen bzgl. des redundanten Betriebs von Hard-und Software sowie räumlicher Infrastruktur? 11. Gibt es Reparaturstrategien und Ausweichprozessen, die dokumentiert sind? 12. Wenn ja, an welcher Stelle erfolgt die Dokumentation?			
13. Gibt es Vertretungsregelungen für abwesende Mitarbeitende? 14. Wie und wo sind diese Regelungen dokumentiert?			

(2) Sicherstellung der Integrität

Art. 5 Abs. 1 lit. f) DS-GVO, Art. 32 Abs. 1 lit. a), b) DS-GVO

Bereiche / Fragen / Probleme	***gar nicht** geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich** geregelt* *(Bezug / Dokument / Wo?)*	***anders** geregelt* *(Form / Fundort / Wie?)*
15. Gibt es Regelungen, wie der IT-Betrieb wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes durch - technisches Versagen, - versehentliches Löschen, - Manipulationen verloren gegangen oder unbrauchbar geworden sind („Datensicherungskonzept“)? Wird die Wiederherstellung aus Störungszuständen regelmäßig getestet?			
16. Wie ist geregelt, dass Datensicherungen räumlich getrennt vom Server aufbewahrt werden (anderer Brandabschnitt?) 17. Welcher in Bezug auf Zugang und Zutritt sichere Ablageort wird verwendet?			
18. Kommt ein aktueller Virenscanner auf Clients und Servern zum Einsatz, der mehrmals täglich bzgl. Viren-Erkennungsmustern geupdatet wird?			
19. Ist gewährleistet, dass die von Herstellern veranlassten kritischen sowie Sicherheitsupdates zeitnah auf die IT-Systeme ausgerollt werden?			
20. Sind Fachanwendungen / Verfahren im Einsatz, bei denen ein Authentizitätsnachweis rechtlich vorgeschrieben ist? Wenn ja, welche sind das?			

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
Welche Regeln sind dabei vorgeschrieben?			
21. Ist das Arbeiten mit sogenannten „Gruppenkennungen“ untersagt? 22. Nutzt jeder Benutzer seine eigenen, persönlichen und geheimen Passwörter?			

(3) Sicherstellung der Vertraulichkeit

Art. 5 Abs. 1 lit. f) DS-GVO, Art. 32 Abs. 1 lit. b) DS-GVO

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
Zutrittsberechtigung: 23. Sind Zutrittsbefugnisse für Gebäude und Räume festgelegt (Schlüsselordnung …)?			
Zugangsberechtigung: 24. Ist die Zugangsberechtigung zu Akten geregelt? 25. Ist die Zugangsberechtigung zu IT-Systemen geregelt? 26. Ist die Zugangsberechtigung bzgl. zu vernichtender personenbezogene Daten, Akten sowie elektronischer personenbezogene Daten geregelt? 27. Ist die Zugangsberechtigung zu Archivakten/ -daten/ -datenträgern geregelt? 28. Gibt es ein Rollen- und Berechtigungskonzept für den gesamten IT-Bereich?			
Passwortverwendung: 29. Gibt es Regelungen für zentrale IT-Systeme? 30. Gibt es Regelungen für dezentrale IT-Systeme? 31. Gibt es zusätzliche Regelungen für Einzelverfahren?			

32. Ist sichergestellt, dass Akten und elektronische Daten (einschl. Post) der Personalabteilung, des Personalrates, der/des Gleichstellungsbeauftragten, der/des Datenschutzbeauftragten sowie als „persönlich“ gekennzeichnete Sendungen nur diesen selbst zur Kenntnis gelangen?			
33. Wie ist geregelt, dass der behördliche DSB vor Einführung neuer IT-Verfahren oder bei wesentlichen Änderungen bestehender Verfahren in das Verfahren zur Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO einbezogen wird? (vgl. § 15 Abs. 2 ThürDSG)			
34. Im Falle der Auftragsverarbeitung: Ist diese gem. Art. 28 Abs. 3 DS-GVO vertraglich geregelt? Siehe Kurzpapier Nr. 13 der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf			
35. Ist die (private) Nutzung von Internet und E-Mail am Arbeitsplatz geregelt?			
36. Sind Aufgaben und Zugriffsrechte der Administratoren von IT-Systemen geregelt?			
37. Gibt es Regelungen zu besonderen Sicherheitsbereichen?			
38. Ist geregelt, dass für zuständige Organisationseinheiten, die Daten gem. Art. 4 Nr. 13, 14, 15 (genetische Daten, biometrische Daten, Gesundheitsdaten) DS-GVO sowie weitere personenbezogener Daten besondere Kategorien gem. Art. 9 Abs. 1 DS-GVO			

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
verarbeiten, zusätzliche technische und organisatorische Maßnahmen getroffen wurden?			
39. Welche Vorgaben gibt es zur Löschung von Daten?			
40. Welche Vorgaben gibt es zur Aussonderungs- / Archivierungsverfahren und -methoden von - Akten, - elektronischen Daten, - Datenträgern, - IT-Hardware, wie PC, Server, Kopierer u.ä.? siehe auch: https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/datentragervernichtung.pdf			

(4) Sicherstellung der Nichtverkettung

Art. 25 Abs. 2 DS-GVO, Art. 32 Abs. 1 lit. a), d) DS-GVO

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
41. Wie werden Verarbeitungs-, Nutzungs-und Übermittlungsrechte konkret eingeschränkt (Rechte- und Rollenkonzept)?			
42. Wie ist sichergestellt, dass Schnittstellen bei Verarbeitungsverfahren bzw. Komponenten von Programmen nicht für andere als die vorgesehenen Zwecke benutzt werden können? (z.B. durch Auftragsverarbeitung oder andere Verträge, Code-Audits) Gibt es eine technische Lösung?			
43. Wie werden regelnde Maßgaben zur Verhinderung von sog. “Backdoors“ („Hintertüren“) in			

qualitätssichernden Programm-Revisionen umgesetzt? (z.B. regelmäßige Patches)			
44. Wie werden Organisations-/Abteilungsgrenzen gemäß ihrer Aufgabenstellung aus technischer Sicht in Bezug auf mögliche Datenzugriffe getrennt?			
45. Wie erfolgt in diesem Kontext die abgestufte Zugriffsrechte-verwaltung (Rollenkonzept) im Rahmen des Identitätsmanage-ments?			
46. Werden zweckspezifische Pseudonyme, Anonymisie-rungsdienste, anonyme „Credentials“ (Anmeldeinfor-mationen) im Zusammenhang mit der Verarbeitung pseudo-nymer bzw. anonymisierter Daten eingesetzt?			

(5) Sicherstellung der Transparenz

Art. 5 Abs. 1 lit. a), Art. 32 Abs. 1 d) DS-GVO

Bereiche / Fragen / Probleme	***gar nicht** geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich** geregelt* *(Bezug / Dokument / Wo?)*	***anders** geregelt* *(Form / Fundort / Wie?)*
47. Wie ist konkret geregelt, dass das Sicherheitskonzept, alle darauf bezogenen Dienstan-weisungen, Organisationsver-fügungen, und Verfahrensbe-schreibungen einer regelmäßi-gen Prüfung auf Aktualität unterzogen werden? 48. In welchen zeitlichen Abständen geschieht dies?			
IT-Infrastruktur: 49. Gibt es eine systematische, nachvollziehbare und aktuelle Dokumentation zur eingesetz-ten IT? (dies betrifft Netzwerk-dokumentation, eingesetzte			

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
Hardware incl. angeschlossener Peripheriegeräte, eingesetzte Software)			
Sicherheit sowie Grundsätze der Verarbeitung: 50. Wie ist sichergestellt, dass bei der Verarbeitung personenbezogener Daten gem. Art. 4 Nr. 13, 14, 15 DS-GVO, insbesondere jedoch bei Verarbeitung von besonderen Kategorien gem. Art. 9 Abs. 1 DS-GVO die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO gewährleistet wird? (Dokumentation der besonderen Maßnahmen, welche das hohe Risiko minimieren)			
IT-Verfahren zur Verarbeitung: 51. Gibt es (ggfs. neue) IT-Verfahren, in denen personenbezogene Daten entsprechend Ziffer 36. verarbeitet werden und bei denen eine Datenschutz-Folgenabschätzung (DS-FA) vor deren Inbetriebsetzung oder bei wesentlichen Änderungen dieser Verfahren erfolgen muss? 52. Welche Verfahren sind das? Gibt es dafür bereits Verfahrensbeschreibungen und entsprechende Dienstanweisungen? (bitte hier mehrere Verfahren einzeln betrachten) 53. Wurden diese IT-Verfahren bereits vorab einer Risikoanalyse unterzogen, die den Schutzbedarf der zu verarbeitenden Daten betreffen? 54. Wo ist dies dokumentiert? 55. Gibt es Verfahren, die ein separates Sicherheitskonzept gemäß gesetzlichen oder anderen verbindlichen Vorgaben verlangen? 56. Welche Verfahren sind das? (bitte hier mehrere Verfahren jeweils einzeln betrachten)			

57. Enthalten die Maßnahmen-kataloge zur IT-Sicherheit dieser Verfahren alle notwendigen technischen und organisatorischen Maßnahmen gemäß aktuellem Stand der Technik? (Maßnahmen siehe Bausteine des BSI-Grundschutz-Kompendiums: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/bausteine_node.html) 58. Wo genau ist dies dokumentiert?			
Datenflüsse: 59. Ist für alle IT-Verfahren nachvollziehbar dokumentiert, welche regelmäßige Datenübermittlungen innerhalb des öffentlichen Bereichs gemäß §§ 17, 18 ThürDSG stattfinden?			
60. Ist für alle IT-Verfahren nachvollziehbar dokumentiert, welche regelmäßigen Datenübermittlungen außerhalb des öffentlichen Bereichs gemäß §§ 17, 18 ThürDSG stattfinden?			
61. Sind im Zusammenhang mit Ziffer 46 und 47 automatisierte Abrufverfahren gemäß gesetzlichen Vorgaben des Bundes und / oder der Länder eingerichtet? 62. Sind diese Verfahren nachvollziehbar dokumentiert (ggfs. i. Zus. mit Ziffer 42 bis 44 - bitte hier mehrere Verfahren einzeln betrachten)			
63. Welchen landesbezogenen Vorgaben sind zusätzlich relevant? (z.B. Anschlussbedingungen Landesdatennetz (CNNG), TESTA, DOS) 64. Wie / an welchen Stellen werden die Vorgaben in der technischen Dokumentation berücksichtigt?			

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
65. Wie / an welchen Stellen sind alle relevanten technischen und organisatorischen Regelungen namentlich dem bDSB sowie den IT-Mitarbeitern bekannt gemacht worden?			
Protokollierung: 66. Ist eine zusätzliche, anlassbezogene Protokollierung geregelt? 67. Ist dabei geregelt, dass vorab der bDSB (gemäß § 14 Abs. 1 ThürDSG) und ggfs. der Personalrat (gemäß § 73 Abs. 3 Nr. 1 ThürPersVG) einzubeziehen ist? 68. Ist die Zweckbindung der Auswertung von Protokolldateien gem. § 17 Abs. 3 ThürDSG geregelt? 69. Ist geregelt, bei welchen Fachanwendungen/Verfahren der lesende und/oder schreibende Zugriff auf Daten (-änderungen) protokolliert wird? 70. Nach welchen Verfahren / Vereinbarungen / Vorgaben werden durch wen Protokolldateien ausgewertet? 71. Wie ist die Löschung von protokollierten Daten / Protokolldateien formal geregelt?			

(6) Sicherstellung der Intervenierbarkeit

Art. 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 DS-GVO

Bereiche / Fragen / Probleme	***gar nicht** geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich** geregelt* *(Bezug / Dokument / Wo?)*	***anders** geregelt* *(Form / Fundort / Wie?)*
72. Wie werden bzgl. der einzelnen Informationspflichten des Verantwortlichen sowie der Auskunftsrechte der betroffenen Person differenzierte Einwilligungs-, Rücknahme-sowie Widerspruchsmöglichkeiten umgesetzt? 73. Wie und an welchen Stellen in den Programmen werden aus technischer Sicht notwendige Datenfelder, z.B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen vorgesehen?			
74. Gibt es standardisierte Abfrage-und Dialogschnittstellen für die betroffene Person?			
75. An welcher Stelle in Programmen / Systemen können Aktivitäten der verantwortlichen Stelle zur Gewährung der Rechte der betroffenen Person nachvollzogen werden? 76. Trifft die Verarbeitung automatisierte Entscheidungen mit rechtlicher Wirkung oder in ähnlicher Weise erheblicher Beeinträchtigung (siehe Art. 22 Abs. 1 DS-GVO)? (wenn ja, Nr. 78. beachten) 77. Wurde Art. 22 Abs. 3 DS-GVO berücksichtigt und kann der Betroffene bei einer automatisierten Entscheidung ein manuelles Eingreifen erwirken? Wenn ja, wie? Wurde die Möglichkeit des Eingriffs dem Betroffenen geeignet mitgeteilt?			
78. Wie und wo werden die Bearbeitung von Störungen,			

Bereiche / Fragen / Probleme	***gar nicht*** *geregelt* *(nicht bekannt = n.b.) (nicht notwendig = n.n.) (nachzuholen = nzh.)*	***schriftlich*** *geregelt* *(Bezug / Dokument / Wo?)*	***anders*** *geregelt* *(Form / Fundort / Wie?)*
Problemen und Änderungen an Verarbeitungstätigkeiten selbst sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes dokumentiert?			
79. Wie werden einzelne Funktionalitäten – z.B. im Falle von Aufgabenwegfall – in Programmen / technischen Systemen deaktiviert, ohne das Gesamtsystem in Mitleidenschaft zu ziehen? 80. Wo wird letzteres revisionssicher dokumentiert?			
81. Gibt es einen sog. „Single Point of Contact“ (d.h. benannten Ansprechpartner) für die betroffene Person? 82. Ist dazu die Schaffung eines solchen „Single Point of Contacts“ vorgesehen?			
83. Gibt es seitens des Verantwortlichen die operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten?			

IV. Weitere Quellen mit Informationen

Verzeichnis von Verarbeitungstätigkeiten

https://www.tlfdi.de/mam/tlfdi/themen/muster_verarbeitungsverzeichnis_auftragsverarbeiter.pdf

Auftragsverarbeitung

Kurzpapier DSK:
https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSK_KPNr_13_Auftragsverarbeitung.pdf
Formulierungshilfe, Fragebogen:
https://tlfdi.de/mam/tlfdi/start/fragebogen.pdf

Orientierungshilfen

Kommunales:
https://www.tlfdi.de/tlfdi/datenschutz/kommunales/

Informationen nach Artikel 13 und 14 DS-GVO zur Verarbeitung von personenbezogenen Daten durch den TLfDI (Stand Juli 2018)

Hinweise zum Verzeichnis über Verarbeitungstätigkeiten nach Art. 30 DS-GVO

Anwendungsbeispiel für ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO

Vorschlag für eine Adaptionsverfügung für Verarbeitungsverzeichnisse

Verpflichtungserklärung der Beschäftigten auf die Vertraulichkeit

Muster für einen Vertrag zur Auftragsverarbeitung

Europa:
https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/

Pflichten der Verantwortlichen und Auftragsverarbeiter gegenüber der Aufsichtsbehörde (TLfDI)

Meldepflichten der Verantwortlichen
Dateigröße: 78.7 kB | Dokument ist nicht Barrierefrei

Formular zur Meldung einer Datenpanne nach Art. 33 DS-GVO

Formular zur Meldung einer Datenpanne nach Artikel 33 DS-GVO

Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO

Vorläufige Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung (DSFA) von Verantwortlichen durchzuführen ist.

Dateigröße: 235.0 kB | Dokument ist nicht Barrierefrei

Handreichung zur Datenschutz-Folgenabschätzung (DS-FA) nicht-öffentlicher Bereich - Art. 35 DS-GVO

Handreichung zur Datenschutz-Folgenabschätzung (DS-FA) nicht-öffentlicher Bereich - Art. 35 DS-GVO

In der Handreichung des TLfDI finden Sie Angaben dazu, wann eine Datenschutz-Folgenabschätzung (DS-FA) durchzuführen ist. Die verschiedenen Phasen der Durchführung dieses Verfahrenswerden hier beschieben.

Stand: September 2019

Info-Broschüre zur Datenschutz-Grundverordnung (DS-GVO)

Info 1 des BfDI DSGVO - BDSG Stand: Juni 2018