Hinweise zur Dokumentation einer ordnungsgemäßen Verarbeitung personenbezogener Daten

Stand Januar 2020

Mit Datum des 31.12.2018 ist die „Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten“ (Datenschutzverordnung, DSVO) vom 05.12.2013, GVOBl. 2013 S. 554, außer Kraft getreten. Von der Ermächtigung in § 7 Abs. 2 LDSG zum Erlass einer Nachfolgeverordnung hat die Landesregierung bisher keinen Gebrauch gemacht.

Zur Erleichterung der Erstellung der erforderlichen Dokumentationsunterlagen zur Umsetzung der Datenschutzgrundverordnung (DSGVO) und des Landesdatenschutzgesetzes gibt das Unabhängig Landeszentrum für Datenschutz die nachfolgenden Hinweise. Sie sind in ihrer Struktur an die bisherigen Regelungen der DSVO angepasst.

Ziel ist es, dass Verantwortliche ihre Verpflichtungen nach Artikel 5 Absatz 1 DSGVO und § 22 LDSG (Grundsätze für die Verarbeitung personenbezogener Daten) erfüllen und gemäß Artikel 5 Absatz 2 DSGVO (Nachweispflicht) einen Nachweis darüber führen. Im Hinblick auf die Konzeption und Durchführung der Verarbeitung und der Wahl technisch-organisatorischer Maßnahmen gemäß Artikel 24, 25 und 32 DSGVO bzw. §§ 40, 47 LDSG haben die Verantwortlichen einen Gestaltungsspielraum, wie sie die Grundsätze für die Verarbeitung personenbezogener Daten erfüllen und dabei Risiken für die Rechte und Freiheiten natürlicher Personen eindämmen. Von der Umsetzung der nachfolgenden Anforderungen kann in begründeten Fällen abgewichen werden, sofern die Risiken für die Rechte und Freiheiten natürlicher Personen in gleichem Maße eingedämmt werden.

§ 1 Prüfbarkeit einer Verarbeitung sicherstellen

(1) Die Verarbeitung ist

- zu konzipieren, um die Prüfbarkeit einer geplanten Verarbeitung oder Verarbeitungstätigkeit sicherzustellen,
- zu dokumentieren, um die Prüfbarkeit des laufenden Betriebs einer Verarbeitung oder einer Verarbeitungstätigkeit sicherzustellen, und
- zu protokollieren, um die Prüfbarkeit des vergangenen Betriebs einer Verarbeitung oder Verarbeitungstätigkeit sicherzustellen.

Von der Dokumentation kann ausnahmsweise abgesehen werden, wenn durch die Verarbeitung die Rechte und Freiheiten von Personen nur geringfügig berührt werden. In diesem Fall ist eine entsprechende Begründung schriftlich niederzulegen.

(2) Die Konzeption ist eine schriftliche Darstellung des Planungsstandes einer Verarbeitung. Sie umfasst

1. den Verarbeitungszweck,
2. die funktionalen Abläufe,
3. die Akteure und betroffenen Personen,
4. die Rechtsgrundlagen,
5. eine Beschreibung des Risikos für die Rechte und Freiheiten natürlicher Personen,
6. eine Beurteilung, ob eine Datenschutz-Folgenabschätzung gem. Artikel 35 DSGVO bzw. § 43 LDSG notwendig ist,
7. ggf. eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO bzw. § 43 LDSG,
8. die Maßnahmen zur Umsetzung der Anforderungen von Artikel 25 DSGVO bzw. § 47 LDSG
9. die risikoangemessene Festlegung von technisch-organisatorischen Maßnahmen zur Umsetzung der Anforderungen von Artikel 5 DSGVO bzw. § 22 LDSG sowie Artikel 32 DSGVO, §§ 12 und 40 LDSG.
10. ggf. die Einbeziehen von Auftragsverarbeitung oder Verarbeitung als gemeinsame Verarbeitung
11. ggf. ein Migrationskonzept,
12. die Pilotierungsphase,
13. die Test- und Freigabeprozesse und
14. die Einbindung der Verarbeitung in das organisationsweite Datenschutz-Management.

(3) Die Dokumentation ist eine schriftliche Darstellung der Verarbeitung im laufenden Betrieb. Es sind, unter Rückgriff auf die tatsächliche Umsetzung der Konzeption nach Absatz 2 sowie auf das Verarbeitungsverzeichnis nach Artikel 30 DSGVO bzw. § 46 LDSG, zu dokumentieren:

1. die Angaben im Sinne von Absatz 2 Nummern 1-4, 8, 9, 10,
2. die für die Verarbeitung verwendeten informationstechnischen Geräte einschließlich der Gebäude, der Räume und des Standorts,
3. die für die Verarbeitung verwendeten Programme einschließlich ihrer Konfiguration und einer Datenfeldbeschreibung,
4. bei vernetzten informationstechnischen Geräten die physikalischen und logischen Verbindungen zu anderen informationstechnischen Geräten (Netzplan) sowie eine Darstellung, an welche Systeme welche personenbezogenen Daten übertragen werden (Schnittstellen und Datenflussdiagramm),
5. die technischen und organisatorischen Vorgaben für die Datenverarbeitung einschließlich der Darstellung, welche Personen für welche Aspekte der Datenverarbeitung verantwortlich und berechtigt sind,
6. die vorgesehenen Datenübermittlungen (Kategorien von Daten sowie von Empfängerinnen und Empfängern),

7. die Maßnahmen zum Erfüllen von Rechtsansprüchen betroffener Personen (Artikel 12 bis 22 DSGVO bzw. §§ 31-35 LDSG),
8. die Maßnahmen, mithilfe derer die Verarbeitung im Rahmen des Datenschutzmanagements kontinuierlich überprüft wird.

(4) Die Dokumentation muss für sachkundige Personen in angemessener Zeit nachvollziehbar sein. Sie ist nach jeder Änderung der Verarbeitung fortzuschreiben und muss erlauben, die Einzelheiten der Verarbeitung (im Sinne von Absatz 3) der letzten drei Jahre nachvollziehen zu können.

(5) Änderungen an informationstechnischen Geräten, Programmen oder Verarbeitungstätigkeiten des Verantwortlichen, die sich auf die Verarbeitung personenbezogener Daten auswirken oder auswirken können, sind einschließlich der Personen, die die Veränderungen vorgenommen haben, zu dokumentieren. Soweit möglich, sind diese Änderungen durch eine automatisierte Protokollierung (Absatz 7) zu dokumentieren.

(6) Die Dokumentation mehrerer automatisierter Verarbeitungen oder die Dokumentation von einzelnen Verarbeitungstätigkeiten kann zusammengefasst werden.

(7) Die Protokollierung dient zum Nachweis der Datenverarbeitung gemäß Artikel 5 Absatz 2 i.V.m. Artikel 24 DSGVO, §§ 12, 40 LDSG, zur Umsetzung der Anforderungen des § 52 LDSG sowie zur Umsetzung von Absatz 5 dieses Paragraphen.

Soweit in Art und Umfang nicht gesetzlich vorgeschrieben (z.B. § 52 LDSG), legen Verantwortliche geeignete Protokollierungsmaßnahmen fest. Bei der Festlegung der Protokollierungsmaßnahmen (z. B. im Hinblick auf Detaillierungsgrad, Speicherfristen, automatisierte Auswertungen, Zugriffsbefugnisse) sind neben zwingenden rechtlichen Vorgaben (z.B. Artikel 15 Absatz 1 lit. c DSGVO, § 52 LDSG) die Umstände der Verarbeitung und der Risiken für die Rechte und Freiheiten natürlicher Personen, die sich aus der Verarbeitung ergeben, zu berücksichtigen. Dies kann besondere Maßnahmen des Zugriffs-, Integritäts- und Verfügbarkeitsschutzes der Protokolle erfordern. Ebenso zu berücksichtigen sind Risiken für die Rechte und Freiheiten natürlicher Personen, die sich aus der Protokollierung selbst ergeben können (z.B. im Hinblick auf Verhaltens- und Leistungskontrollen von Beschäftigten, die Speicherung zu löschender Daten in Protokollen).

Zur Darstellung des prüfbaren Einsatzes von Informationstechnik im vergangenen Betrieb ist im Regelfall zu protokollieren:

- die Verarbeitungsvorgänge der Sachbearbeitung,
- die automatisierten Verarbeitungsvorgänge (insbesondere Aktivitäten an Schnittstellen wie Datenübertragungen und -abrufe)
- Datenübermittlungen und –abrufe einschließlich Empfängerinnen und Empfänger sowie der übermittelten bzw. abgerufenen Daten

- die Tätigkeiten der Administration insbesondere Konfigurationstätigkeiten einschließlich der Administration von Berechtigungen.

Es sind Protokolle der Verarbeitungsvorgänge zu erzeugen, die

- eine Zeitkomponente (Zeitstempel, „Wann?“),
- eine Bezeichnung für die auslösende Instanz sowohl für manuelle Tätigkeiten als auch automatische Abläufe („Wer?“) und
- eine Bezeichnung für diese Vorgänge („Was“?)

umfassen.

Für die bei der Datenverarbeitung zu erzeugenden Protokolle ist zu dokumentieren, welche technischen und organisatorischen Maßnahmen hinsichtlich des Zugriffs, der Auswertung und der Löschung der Protokolle getroffen wurden.

§ 2 Dokumentation des Tests und der Freigabe

(1) Die in automatisierten Verarbeitungen eingesetzten informationstechnischen Geräte und Programme sowie die technisch-organisatorischen Datenschutzmaßnahmen (§ 1 Absatz 2 Nr. 8 und 9) sind vor der Aufnahme der Verarbeitung personenbezogener Daten zu testen. Dies gilt insbesondere – soweit implementiert – für die Maßnahmen

1. zur Datensicherung (Backup),
2. zur Nutzung kryptographischer Verfahren ,
3. zur Zugriffskontrolle (Umsetzung eines Berechtigungskonzepts),
4. zur Pseudonymisierung oder Anonymisierung,
5. zur Umsetzung der Zwecktrennung,
6. zur Löschung nicht mehr erforderlicher Daten,
7. zur Protokollierung (§ 1 Absatz 7).

Die Testmaßnahmen und die dabei erzielten Ergebnisse sind zu dokumentieren. Die Dokumentation soll durch eine Darstellung der einzelnen Prüfschritte erfolgen und die verwendeten Ein- und erhaltenen Ausgabedaten beinhalten, soweit dies technisch möglich ist. Festgestellte Mängel sind durch den Verantwortlichen nach ihrer Bedeutung zu gewichten.

(2) Die nach § 7 Absatz 1 LDSG bzw. § 40 Absatz 4 LDSG vorzunehmende Freigabe automatisierter Verarbeitungen und Verarbeitungstätigkeiten hat schriftlich zu erfolgen. Sie ist nur zulässig, soweit bei den Tests keine wesentlichen Mängel festgestellt wurden. Die Beseitigung geringfügiger Mängel muss in angemessener Zeit vorgenommen werden.

(3) Test und Freigabe können gestuft erfolgen. In jeder Stufe können der Test und die Freigabe auf die geplante Verarbeitung personenbezogener Daten begrenzt werden.

(4) Soweit informationstechnischen Geräte, Programme und technisch-organisatorischen Datenschutzmaßnahmen im Sinne des Absatz 1 von mehreren Verantwortlichen eingesetzt

werden sollen, können eigene Tests des Verantwortlichen mit Testergebnissen von anderen Verantwortlichen oder Auftragsverarbeitern kombiniert oder ergänzt werden. Die kombinierten oder ergänzten Tests sind gemäß Absatz 1 zu dokumentieren.

§ 3 Auftragsverarbeitung

(1) Liegt eine Verarbeitung personenbezogener Daten im Auftrag vor, sind die technischen und organisatorischen Sicherheitsmaßnahmen des Auftragsverarbeiters vom Verantwortlichen gemäß § 1 Absatz 2 zu konzipieren. Dabei kann auf Dokumente des Auftragsverarbeiters zurückgegriffen werden. Soweit die Verarbeitung durch den Auftragsverarbeiter erfolgt, dokumentiert dieser die relevanten Aspekte gemäß § 1 Absatz 3 und protokolliert gemäß § 1 Absatz 7.

(2) Der Verantwortliche hat die Verpflichtung, die Tätigkeiten des Auftragsverarbeiters zu überwachen (Artikel 28 Absatz 3 Buchstabe h DSGVO, § 40 Absatz 2 Nr. 12 LDSG). Dazu stellt ihm der Auftragsverarbeiter Zugriffsmöglichkeiten auf die relevanten Teile der Dokumentation und der Protokollierung zur Verfügung.

(3) Der Verantwortliche und der Auftragsverarbeiter treffen Vereinbarungen darüber, bei welchen Störungen, Problemen und Änderungen von Betriebsabläufen der Verantwortliche seitens des Auftragsverarbeiters zu unterrichten ist, und legen dazu Kommunikationswege und Ansprechpartner fest. Gleiches gilt für Kommunikationswege und Ansprechpartner zur Umsetzung der Pflichten von Artikel 33, 34 DSGVO bzw. §§ 41, 42 LDSG.

§ 4 Gemeinsam Verantwortliche

(1) Bei gemeinsamer Verantwortlichkeit nach Artikel 26 DSGVO bzw. § 39 LDSG ist das Verzeichnis nach Artikel 30 DSGVO bzw. 46 LDSG um die Feststellung zu ergänzen, für welche jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten jede der beteiligten Stellen zuständig ist.

(2) Sofern nicht durch Rechtsvorschrift festgelegt, regeln gemeinsam Verantwortliche in ihrer Vereinbarung nach Artikel 26 DSGVO bzw. § 39 LDSG insbesondere,

- welcher Verantwortliche für welche Teile Verarbeitung einschließlich der Festlegung der Mittel und Wege verantwortlich ist,
- welcher Verantwortliche für welche Teile der Konzeption, Dokumentation und Protokollierung verantwortlich ist,
- wie Verantwortliche einander mit geeigneten Mitteln unterstützen, die Einhaltung der Bestimmungen über die Rechte und Freiheiten natürlicher Personen zu gewährleisten,
- wie Verantwortliche einander mit geeigneten Mitteln unterstützen, alle erforderlichen Informationen, insbesondere die gemäß § 52 LDSG erstellten Protokolle, zum Nachweis der Einhaltung ihrer Pflichten zur Verfügung zu stellen,

- wie Verantwortliche einander mit geeigneten Mitteln bei Kontrollen, die von einem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, unterstützen,
- wie Verantwortliche einander mit geeigneten Mitteln bei der Einhaltung der in den Artikeln 25, 32 bis 36 DSGVO bzw. der in den §§ 40 bis 43, §§ 45 und 47 LDSG genannten Pflichten unterstützen, und bei welchen Störungen, Problemen und Änderungen von Betriebsabläufen gegenseitige Unterrichtungen erfolgen. Dazu legen sie dazu Kommunikationswege und Ansprechpartner fest.

§ 5 Datenschutz-Management

Es ist ein organisationsweites Datenschutz-Managementsystem zu betreiben (Artikel 24 Absatz 1 und Artikel 32 Absatz 1 Buchstabe d DSGVO, § 12 Absatz 3 Nr. 7 LDSG), das sowohl der kontinuierlichen Gewährleistung der Wirksamkeit der Datenschutzmaßnahmen und deren Prüfbarkeit dient als auch auf Änderungen solcher Umstände reagiert, die sich auf Verarbeitungen personenbezogener Daten auswirken können.

Das Datenschutz-Managementsystem ist zu dokumentieren. Dazu gehören mindestens Aussagen

- über die Bereitstellung von Ressourcen,
- zur Einbindung der oder des behördlichen Datenschutzbeauftragten in die Organisation des Verantwortlichen, in die Planung von Verarbeitungstätigkeiten und in Datenschutz-Folgenabschätzungen (Artikel 35 DSGVO),
- zur Vorgehensweise in Bezug auf Prüfungen laufender Verarbeitungstätigkeiten, insbesondere der Wirksamkeit der technisch-organisatorischen Datenschutzmaßnahmen,
- zur Vorgehensweise in Bezug auf die Ergebnisse solcher Prüfungen (Festlegung und Umsetzung von Korrekturmaßnahmen) sowie
- zur Vorgehensweise in Bezug auf die Maßnahmen zum Erfüllen von Rechten betroffener Personen einschließlich der Beschäftigten (Artikel 12 bis 22 DSGVO bzw. §§ 31-35 LDSG).

Kontakt:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200, Fax: -1223
E-Mail: mail@datenschutzzentrum.de