Datenschutzrechtliche Anforderungen

Worum geht es?

Gemäß Artikel 5 der EU-Datenschutz-Grundverordnung (DS-GVO) gelten bei der Verarbeitung personenbezogener Daten die Grundsätze der Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit.
Die verantwortliche Stelle muss nachweisen, dass diese Grundsätze eingehalten werden; hierzu ist u.a. ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Sofern ein externer Dienstleister mit der Datenverarbeitung oder -speicherung beauftragt ist, sind darüber hinaus Vereinbarungen zur Auftragsverarbeitung zu schließen.

Rechtsgrundlagen

- **EU Datenschutz-Grundverordnung (DS-GVO) vom 27. April 2016**[1]
- **Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) vom 17.05.2018**

Erläuterung/Grundinformation

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet[2]. Mit der EU-Datenschutzgrundverordnung (DS-GVO) wird das Datenschutzrecht europaweit einheitlich geregelt. Die Verordnung ist am 25.05.2016 in Kraft getreten und gilt gem. Artikel 99 Abs. 2 DS-GVO ab dem 25.05.2018 unmittelbar in allen EU-Mitgliedsstaaten, d.h. es besteht ein Anwendungsvorrang vor nationalem Recht.

Voraussetzung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist erstens das Vorhandensein einer ausreichenden und tragfähigen Rechtsgrundlage (Zulässigkeit der Verarbeitung) und zweitens die Gewährleistung der Sicherheit der Datenverarbeitung.[3]

Verzeichnis von Verarbeitungstätigkeiten (Verarbeitungsübersicht)

Lt. Artikel 30 DS-GVO hat der Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen.

Datenschutzfolgeabschätzung (DSFA)

Sofern aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung personenbezogener Daten eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person

[1] Link auf eine Seite, auf der die DSGVO sehr übersichtlich dargestellt ist: https://dsgvo-gesetz.de/
[2] Quelle: Glossar BSI IT-Grundschutz-Kompendium: Stand Februar 2019
[3] Quelle: Das Standard-Datenschutzmodell, AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

anzunehmen ist, so ist gem. Artikel 35 DS-GVO eine Abschätzung der Folgen der Verarbeitungsvorgänge vorzunehmen und mit bestimmten Pflichtinhalten (z.B. Bewertung der Notwendigkeit und Verhältnismäßigkeit) zu dokumentieren.

Auftragsverarbeitung

Auftragsverarbeitung im Sinne des Datenschutzrechts bedeutet die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter (i.d.R. ein Dienstleister) im Auftrag des Verantwortlichen. Die Auftragsverarbeitung erleichtert arbeitsteiliges Handeln. Dabei wird dem Auftragsverarbeiter nicht die eigentliche (Verwaltungs-)Aufgabe übertragen, sondern nur eine Hilfstätigkeit.

Artikel 28 DS-GVO enthält keine Beschränkung der Auftragsverarbeitung im Zusammenhang mit besonderen Rechtsgebieten. Grundsätzlich ist die Auftragsverarbeitung für alle Formen der Datenverarbeitung in allen Rechtsgebieten zulässig. Die Öffnungsklausel des Artikels 6 DS-GVO ermöglicht jedoch den Mitgliedstaaten der EU den Erlass spezifischer Bestimmungen zur Auftragsverarbeitung im öffentlichen Bereich (z.B. für Meldedaten).

Die Auftragsverarbeitung kann sowohl innerhalb der Räume des Verantwortlichen als auch außerhalb stattfinden. Typische Beispiele sind:

- Erledigung von Massenarbeiten auf der Basis eines vom Verantwortlichen zur Verfügung gestellten Adressenbestandes
- Datenerfassung, Datenumsetzung und Scannen von Dokumenten
- Outsourcing im klassischen Sinn (z.B. Nutzung eines Backup-Rechenzentrums)
- Cloud Computing
- Programmerstellung (z.B. die Entwicklung von Apps)
- Archivierung / Löschung bzw. Vernichtung von Daten

Die Auftragsverarbeitung beruht regelmäßig auf einem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter. Der Vertrag ist schriftlich abzufassen. Art. 28 Abs. 3 DS-GVO bestimmt den Mindestinhalt, den der Vertrag über die Auftragsverarbeitung regeln muss. Erforderlich ist eine genaue Beschreibung der geschuldeten Tätigkeit des Dienstleisters.[4]

Technische und organisatorische Maßnahmen (TOM)

Art. 32 Abs. 1 DS-GVO verlangt vom Verantwortlichen und vom Auftragsverarbeiter konkret, dass zum Schutz personenbezogener Daten angemessene Sicherheitsmaßnahmen ergriffen werden müssen: *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;“*. Abhängig vom Risiko müssen also geeignete TOMs ausgewählt und eingesetzt werden, die darauf abzielen müssen, das ermittelte Risiko soweit wie möglich zu minimieren.

[4] Quelle: Orientierungshilfe Auftragsverarbeitung Version 2.0, Stand April 2019, Der Bayrische Landesbeauftragte für den Datenschutz

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
1	Artikel 4 DS-GVO (Begriffsbestimmungen)	Werden mit der zu prüfenden IT-Anwendung personenbezogene Daten verarbeitet?	Personenbezogene Daten sind: • Allgemeine Personendaten (z.B. Name, Geburtsdatum, Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer, Foto, Ausbildung, Beruf, Familienstand, Staatsangehörigkeit, Gesundheitsdaten, Vorstrafen) • Kennnummern (z.B. Sozialversicherungsnummer, Steueridentifikationsnummer, Krankenversicherungsnummer, Personalausweisnummer) • Bankdaten (Kontonummer, Kreditinformationen, Kontostände) • Onlinedaten (IP-Nummer, Standortdaten usw.) • Physische Merkmale (Geschlecht, Haut-, Haar-, Augenfarbe, Kleidergröße) • Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten, usw.) • Kundendaten (Bestellungen, Adressdaten, Kontodaten, usw.) • Werturteile (z.B. Schul- und Arbeitszeugnisse) • Sachliche Verhältnisse (z.B. Einkommen, Kapitalvermögen, Schulden) • Bestimmbare Daten (= Daten, die in Kombination mit weiteren Informationen Rückschlüsse auf eine Person ermöglichen, z.B. Personalnummer, Kfz-Kennzeichen) Im Sinne der DS-GVO bezeichnet der Ausdruck “Verarbeitung” jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
			personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
2	Artikel 6 DS-GVO (Rechtmäßigkeit der Verarbeitung) § 3 DSG NRW	Ist die Verarbeitung der personenbezogenen Daten durch eine Rechtsgrundlage gedeckt?	Die Verarbeitung ist nur rechtmäßig, wenn eine der nachfolgenden Bedingungen erfüllt ist: • Die Verarbeitung erfolgt mit Einwilligung der betroffenen Person. • Die Verarbeitung ist für die Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung erforderlich. • Die Verarbeitung ist erforderlich, um lebenswichtige Interessen von Personen zu schützen • Die Verarbeitung ist zur Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt. • Die Verarbeitung ist zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritter erforderlich.
3	Artikel 30 DS-GVO (Verarbeitungsübersicht) IDW PH 9.860.1 Anlage 1, Ziff. 40	Wurde ein Verzeichnis von Verarbeitungstätigkeiten erstellt?	Informationen der Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI) sowie ein Muster für ein Verzeichnis von Verarbeitungstätigkeiten unter https://www.ldi.nrw.de

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
4	Artikel 30 DS-GVO / (Verarbeitungsübersicht)	Ist die zu prüfende IT-Anwendung im Verzeichnis der Verarbeitungstätigkeiten aufgeführt?	
5	Artikel 30 DS-GVO (Verarbeitungsübersicht) IDW PH 9.860.1 Anlage 1, Ziff. 40	Enthält das Verzeichnis der Verarbeitungstätigkeiten die Pflichtangaben?	Artikel 30 DS-GVO Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben: a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten; b) die Zwecke der Verarbeitung; c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten; d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen; e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
			f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien; g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
6	Artikel 38 DS-GVO (Stellung DSB) Artikel 39 DS-GVO (Aufgaben DSB)	Wurden dem betrieblichen Datenschutzbeauftragten software- und verfahrensspezifische Informationen (u.a. Verarbeitungsübersicht) zur Verfügung gestellt, damit dieser seine Kontroll- und Beratungstätigkeiten durchführen kann?	
7	Artikel 17 DS-GVO (Recht auf Löschung) IDW PH 9.860.1 Anlage 1 Ziff. 58-61	Liegt ein Löschkonzept für dieses Verfahren vor? Sind Löschroutinen definiert / installiert?	Siehe auch BSI-Grundschutz-Kompendium Baustein CON.6.A1 Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen
8	Artikel 25 DS-GVO (Technik / TOM) Artikel 32 DS-GVO (Datensicherheit / TOM) IDW PH 9.860.1 Anlage 1 Ziff. 49-57	Ist die Sicherheit der Verarbeitung personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen gewährleistet?	Diese Maßnahmen schließen gem. Art. 32 Abs. 1 S.2 lit. a) – c) unter anderem Folgendes ein: • die Pseudonymisierung und Verschlüsselung personenbezogener Daten; • die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
			• die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; • ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
9	Artikel 5 DS-GVO (Grundsätze) Artikel 25 DS-GVO (Technik / TOM) Artikel 32 DS-GVO (Datensicherheit / TOM)	Wie wird das Gewährleistungsziel Datenminimierung erreicht?	Das Gewährleistungsziel Datenminimierung kann erreicht werden durch: • Reduzierung von erfassten Attributen der betroffenen Person • Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessen • Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten • Bevorzugung automatisierter Verarbeitungsprozesse • Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren[5]
10	Artikel 5 DS-GVO (Grundsätze) Artikel 25 DS-GVO (Technik / TOM) Artikel 32 DS-GVO (Datensicherheit / TOM)	Wie wird das Gewährleistungsziel Verfügbarkeit erreicht?	Das Gewährleistungsziel Verfügbarkeit kann erreicht werden durch: • Anfertigung von Sicherheitskopien von Daten • Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, …) • Dokumentation der Syntax der Daten • Redundanz von Hard- und Software • Ausweichprozesse / Vertretungsregelungen[6]

[5] Quelle: Das Standard-Datenschutzmodell Version 2.0, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)
[6] Quelle: Das Standard-Datenschutzmodell Version 2.0, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
11	Artikel 5 DS-GVO (Grundsätze) Artikel 25 DS-GVO (Technik / TOM) Artikel 32 DS-GVO (Datensicherheit / TOM)	Wie wird das Gewährleistungsziel Integrität erreicht?	Das Gewährleistungsziel Integrität kann erreicht werden durch: • Einschränkung von Schreib- und Änderungsrechten • Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen gemäß eines Kryptokonzeptes • Dokumentierte Zuweisung von Berechtigungen und Rollen • Prozesse zur Aufrechterhaltung der Aktualität von Daten • Definition von SOLL-Prozessen und regelmäßige Überprüfungen der IST-Prozesse hinsichtlich Funktionalität, Risiken und Sicherheitslücken[7]
12	Artikel 5 DS-GVO (Grundsätze) Artikel 25 DS-GVO (Technik / TOM) Artikel 32 DS-GVO (Datensicherheit / TOM)	Wie wird das Gewährleistungsziel Vertraulichkeit erreicht?	Das Gewährleistungsziel Vertraulichkeit kann erreicht werden durch: • Festlegung eines Rechte- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements • Implementierung eines sicheren Authentisierungsverfahrens • Eingrenzung des Datenzugriffs im Hinblick auf Zuständigkeit, Befähigung und Zuverlässigkeit des Personals • Festlegung und Kontrolle der Nutzung zugelassener Ressourcen und Kommunikationskanäle • Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (z.B. Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen)[8]

[7] Quelle: Das Standard-Datenschutzmodell Version 2.0, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)
[8] Quelle: Das Standard-Datenschutzmodell Version 2.0, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
13	Artikel 5 DS-GVO (Grundsätze) Artikel 22 DS-GVO (Profiling) Artikel 25 DS-GVO (Technik / TOM) Artikel 32 DS-GVO (Datensicherheit / TOM)	Wie wird das Gewährleistungsziel Nichtverkettung erreicht?	Das Gewährleistungsziel Nichtverkettung kann erreicht werden durch: • Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten • Programmtechnische Unterlassung von Schnittstellen • Trennung von Organisations-/Abteilungsgrenzen • Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements und Authentisierungsverfahrens • Einsatz von zweckspezifischen Pseudonymisierungs- oder Anonymisierungsverfahren[9]
14	Artikel 5 DS-GVO (Grundsätze) Artikel 13f. DS-GVO (Informationspflichten) Artikel 15 DS-GVO (Auskunftsrecht) Artikel 25 DS-GVO (Technik / TOM) Artikel 30 DS-GVO (Verarbeitungsübersicht) Artikel 32 DS-GVO (Datensicherheit / TOM)	Wie wird das Gewährleistungsziel Transparenz erreicht?	Das Gewährleistungsziel Transparenz kann z.B. erreicht werden durch: • Dokumentation von Verarbeitungsprozessen (Datenbestände, Datenflüsse, IT-Systeme, Zusammenspiel mit anderen Verarbeitungstätigkeiten) • Protokollierung von Zugriffen und Änderungen • Nachweis der Quellen von Daten • Versionierung[10]

[9] Quelle: Das Standard-Datenschutzmodell Version 2.0, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)
[10] Quelle: Das Standard-Datenschutzmodell Version 2.0, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
15	Artikel 5 DS-GVO (Grundsätze) Artikel 15 DS-GVO (Auskunftsrecht) Artikel 16 ff. DS-GVO (Berichtigung / Löschung) Artikel 25 DS-GVO (Technik / TOM) Artikel 32 DS-GVO (Datensicherheit / TOM)	Wie wird das Gewährleistungsziel Intervenierbarkeit erreicht?	Das Gewährleistungsziel Intervenierbarkeit kann erreicht werden durch: • Differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten • Einrichtung von Datenfeldern für Sperrkennzeichen, Einwilligungen, Widersprüche, … • Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an den Verarbeitungstätigkeiten sowie Schutzmaßnahmen.[11]
16	Artikel 25 DS-GVO / (Technik / TOM)	Sind die ergriffenen TOMS geeignet, um die Einhaltung der Datenschutzgrundsätze wirksam umzusetzen?	
17	Artikel 28 DS-GVO / Artikel 29 DS-GVO (Auftragsverarbeitung)	Liegt in dem zu prüfenden IT-Verfahren eine Auftragsverarbeitung vor?	Eine Auftragsverarbeitung liegt vor, wenn personenbezogene Daten im Auftrag durch andere Personen oder Stellen verarbeitet werden. Hinweise dazu, wann eine Auftragsverarbeitung vorliegt, können dem Kurzpapier Nr. 13 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK entnommen werden. Hiernach liegt Auftragsverarbeitung z. B. auch vor bei Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren o-der von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf)

[11] Quelle: Das Standard-Datenschutzmodell Version 2.0, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
18	Artikel 28 DS-GVO (Auftragsverarbeitung) IDW PH 9.860.1 Anlage 1 Ziff. 82-85	Enthält die mit dem Auftragsverarbeiter / externen Dienstleister geschlossene Vereinbarung die Mindestinhalte gem. Artikel 28 DS-GVO?	<u>Mindestanforderungen an den Vertrag zur Auftragsverarbeitung:</u> • Gegenstand und Dauer der Verarbeitung • Art und Zweck der Verarbeitung • Art der personenbezogenen Daten • Kategorien betroffener Personen • Pflichten und Rechte des Verantwortlichen • Umfang der Weisungsbefugnisse • Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit • Sicherstellung von technischen & organisatorischen Maßnahmen • Hinzuziehung von Subunternehmern • Unterstützung des Verantwortlichen bei Anfragen und Ansprüchen Betroffener • Unterstützung des Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung • Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung • Regelung, wie der Nachweis der Einhaltung der in Art. 28 niedergelegten Pflichten erfolgt. Dies kann auch durch Überprüfungen und Inspektionen durch einen beauftragten Prüfer vereinbart werden.

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
			• Pflicht des Auftragsverarbeiters, den Verantwortlichen unverzüglich zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt Darüber hinaus zu regelnde Inhalte: • Haftung Weitere Informationen im Kurzpapier Nr. 13 / Auftragsverarbeitung: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf
19	Artikel 28 DS-GVO (Auftragsverarbeitung) Artikel 32 DS-GVO (Datensicherheit / TOM)	Sind die vom Auftragsverarbeiter ergriffenen Maßnahmen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?	Mögliche TOMs können sein (vgl. § 58 DSG NRW analog): • Zugangskontrolle • Datenträgerkontrolle • Speicherkontrolle • Benutzerkontrolle • Zugriffskontrolle • Übertragungskontrolle • Eingabekontrolle • Transportkontrolle • Wiederherstellbarkeit • Zuverlässigkeit • Datenintegrität • Auftragskontrolle • Verfügbarkeitskontrolle • Trennbarkeit
20	Artikel 35 DS-GVO (DSFA) IDW PH 9.860.1 Anlage 1, Nr. 32	Ist aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung von einer erheblichen	Ein Rechtsgut ist ein durch die Rechtsordnung geschütztes Gut oder Interesse, u.a. das Recht auf informationelle Selbstbestimmung. Weitere Rechtsgüter sind z.B. Leib und Leben, Gesundheit, Freiheit, Eigentum, Besitz und Ehre.

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
		Gefahr für die Rechtsgüter betroffener Personen auszugehen? Wenn ja: Wurde eine Datenschutz-Folgenabschätzung durchgeführt und dokumentiert? Enthält die Folgenabschätzung die Mindestinhalte gemäß Artikel 35 DS-GVO?	Die Landesbeauftragte für Datenschutz und Informationsfreiheit veröffentlicht eine Liste von Verarbeitungsvorgängen, für die eine DSFA durchzuführen ist. Diese Liste ist verbindlich, aber nicht abschließend. *https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Datenschutz-Folgenabschaetzung.html* <u>Artikel 35 DS-GVO</u> Die Folgenabschätzung enthält zumindest Folgendes: a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen; b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
			§ 24 DSG NRW beachten: Sofern ein IT-Verfahren im Wesentlichen unverändert von einer öffentlichen Stelle übernommen wird, kann die DSFA von dort übernommen werden.
21	Art. 33 DS-GVO (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde)	Wurde ein Prozess für die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde definiert?	Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen (Art. 33 DSGVO) Weitere Informationen sowie das Meldeformular zur Meldung von Datenpannen finden Sie auf der Seite der LDI NRW unter folgendem Link: https://www.ldi.nrw.de/mainmenu_Aktuelles/Formulare-und-Meldungen/index.html

Weiterführende Literatur:

- Das Standard-Datenschutzmodell –Version 2.0-, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz); AK Technik / UAG „Standard-Datenschutzmodell“
- Leitfaden „Das Verarbeitungsverzeichnis“, Bitkom 2017
- Mustervertragsanlage Auftragsdatenverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO), Bitkom 2017
- Leitfaden „Begleitende Hinweise zu der Anlage Auftragsdatenverarbeitung“ Bitkom 2017
- Orientierungshilfe Auftragsverarbeitung, Der Bayrische Landesbeauftragte für Datenschutz

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen

- Checkliste zur Prüfung der Datenschutzorganisation, Deutsches Institut für Interne Revison e.V. (DIIR), DIIR-Arbeitskreis Interne Revision & Datenschutz, 2017
- IDW-Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)
  => beachten: Dieser Prüfungshinweis *bezieht* sich auf die Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen!