Big Data und Recht

Eine Einführung

Bearbeitet von
Von Dr. Maria Cristina Caldarola, LL.M., MBA, Rechtsanwältin, und Prof. Dr. Joachim Schrey, Rechtsanwalt

1. Auflage 2019. Buch. XX, 184 S. Hardcover (In Leinen)
ISBN 978 3 406 73284 3
Format (B x L): 16,0 x 24,0 cm

Datenschutzerklärung gemäß § 4 Abs. 3 BDSG a. F. / § 13 Abs. 1 TMG	Informationspflichten gemäß Art. 13 (Erhebung beim Betroffenen) und 14 (Erhebung aus anderen Quellen) DS-GVO
Unterrichtung über • Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie • über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG in allgemein verständlicher Form (§ 13 Abs. 1 TMG)	Unterrichtung über • Kategorien personenbezogener Daten, die verarbeitet werden, nur wenn personenbezogene Daten nicht bei dem Betroffenen erhoben wurden (Art. 14 Abs. 1 lit. (d) DS-GVO • Übermittlung an eine Stelle in einem Drittland sowie Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses oder Verweis auf Garantien und deren Verfügbarkeit (Art. 13 Abs. 1 lit. (f), 14 Abs. 1 lit. (f) DS-GVO)
	Zusätzlich, wenn personenbezogene Daten nicht bei dem Betroffenen erhoben werden (Art. 14 Abs. 1 und 2 DS-GVO): • die Kategorien personenbezogener Daten, die verarbeitet werden (Art. 14 Abs. 1 lit. (d) DS-GVO) • Angaben, aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen (Art. 14 Abs. 2 lit. (f) DS-GVO).

Abbildung 61: Informationspflichten

Eine Nichterfüllung der Informationspflichten gemäß Art. 13 oder 14 DS-GVO kann die Sanktionen gemäß Rn. 497 ff. dieses Leitfadens zur Folge haben. **422**

Leitsatz:

Für eine Big Data-Anwendung, in der personenbezogene Daten gespeichert und verarbeitet werden, ist eine Datenschutzerklärung zu erstellen, in der die Betroffenen über die in Art. 13 und 14 DS-GVO aufgeführten Inhalte informiert werden.

II. Betroffenenrechte gemäß Art. 15 ff. DS-GVO

Nach Art. 12 und 15 bis 21 DS-GVO hat der Betroffene, dessen personenbezogene Daten als solche in einer Big Data-Anwendung verarbeitet werden („**Big Data-Betroffene**“) diverse Rechte, die er gegenüber die für die Big Data-Anwendung verantwortliche Stelle als jeweils Verantwortliche geltend machen kann. Für die Geltendmachung solcher Betroffenenrechte gegen die für die Big Data-Anwendung verantwortliche Stelle kann sich der Big Data-Betroffene an den (Konzern-)Datenschutzbeauftragten der für die Big Data-Anwendung verantwortlichen Stelle wenden. Bei diesem sind also entsprechende Prozesse zur unverzüglichen und fristgerechten Behandlung innerhalb von einem Monat (Art. 12 Abs. 3 Satz 1 DS-GVO) einzurichten; erfolgt die Erfüllung der Betroffenenrechte nicht innerhalb dieser Frist, hat die für die Big Data-Anwendung verantwortliche Stelle den Big Data-Betroffenen über die Gründe hierfür **423**

zu informieren. In diesem Fall könnte sich der jeweilige Big Data-Betroffene gemäß Art. 12 Abs. 4 DS-GVO, Art. 77 Abs. 1 DS-GVO bei der zuständigen Aufsichtsbehörde beschweren; über dieses Beschwerderecht ist der Big Data-Betroffene jeweils im Zusammenhang mit einer Mitteilung über Verzögerungsgründe zu belehren.

424 Dabei kann die für die Big Data-Anwendung verantwortliche Stelle verlangen, dass sich der Big Data-Betroffene identifiziert. Die Nichterfüllung von Betroffenenrechten kann wiederum die in Rn. 497 ff. dieses Leitfadens erläuterten Rechtsfolgen nach sich ziehen.

1. Auskunftsrechte

425 Gemäß Art. 15 DS-GVO hat der Big Data-Betroffene das Recht auf Auskunft über die ihn betreffenden personenbezogenen Daten und

a) die Verarbeitungszwecke;
b) die Kategorien personenbezogener Daten, die verarbeitet werden; sowie
c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d) die geplante Dauer, für die die personenbezogenen Daten als solche in der Big Data-Anwendung gespeichert werden (falls möglich), oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
e) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten; sowie
f) die weiteren im Folgenden erläuterten Betroffenenrechte.

2. Berichtigungsrecht

426 Gemäß Art. 16 DS-GVO sind von der für die Big Data-Anwendung verantwortliche Stelle unrichtige oder unvollständige personenbezogene Daten auf Verlangen der betroffenen Person zu berichtigen.

3. Recht auf Löschung und „Vergessenwerden“

427 Gemäß Art. 17 Abs. 1 DS-GVO hat der Big Data-Betroffene einen Anspruch auf Löschung seiner personenbezogenen Daten, wenn die in Art. 17 Abs. 1 DS-GVO normierten Voraussetzungen gegeben sind und keiner der in Art. 17 Abs. 3 DS-GVO genannten Ausschlussgründe vorliegt.

428 Der Big Data-Betroffene hat in den in Art. 17 Abs. 2 DS-GVO normierten Fällen ein Recht auf Vergessenwerden (siehe hierzu Rn. 401 f.), wenn die für die Big Data-Anwendung verantwortliche Stelle zuvor die personenbezogenen Daten eines Big Data-Betroffenen öffentlich gemacht hatten, jedoch gemäß Art. 17 Abs. 1 DS-GVO zur Löschung verpflichtet ist. Ob ein Fall des „Öffentlich-Machens“ im Sinne der DS-GVO, d. h. ein Zugänglichmachen an einen unbestimmten Personenkreis, jeweils gegeben ist, muss insbesondere bei jeder Big Data-Anwendung in einem Konzern anhand der jeweils gegebenen Umstände des Einzelfalls geprüft werden; liegt ein solcher Fall vor, sind verfahrensseitig sowie technisch Prozesse zu etablieren, mit denen der Erfüllung des Rechts auf Vergessenwerden Rechnung getragen werden kann.

4. Recht auf Einschränkung der Verarbeitung

Der Big Data-Betroffene kann die einer Sperrung entsprechende Einschränkung der Verarbeitung von der für die Big Data-Anwendung verantwortlichen Stelle verlangen, wenn **429**

- die Richtigkeit der personenbezogenen Daten von dem Big Data-Betroffenen bestritten wird, und zwar für eine Dauer, die es der für die Big Data-Anwendung verantwortlichen Stelle ermöglicht, die Richtigkeit der bei ihr gespeicherten Rohdaten zu überprüfen
- die Verarbeitung der personenbezogenen Daten unrechtmäßig ist und der Big Data-Betroffene die Löschung der ihn betreffenden personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt
- die für die Big Data-Anwendung verantwortliche Stelle die personenbezogenen Daten für die Zwecke der Verarbeitung in der Big Data-Anwendung nicht länger gerade als personenbezogene Daten im Sinne der DS-GVO benötigt (etwa weil der Big Data-Betroffene nicht mehr aktiv ist), der Big Data-Betroffene sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- der Big Data-Betroffene Widerspruch gegen die Verarbeitung der ihn betreffenden personenbezogenen Daten in der Big Data-Anwendung durch die hierfür verantwortliche Stelle gemäß Art. 21 Abs. 1 DS-GVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe der für die Big Data-Anwendung verantwortlichen Stelle gegenüber denen des Big Data-Betroffenen überwiegen.

5. Recht auf Datenübertragbarkeit

Der Big Data-Betroffene hat gemäß Art. 20 Abs. 1 DS-GVO das Recht, die ihn betreffenden personenbezogenen Daten aus der Big Data-Anwendung in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Der Big Data-Betroffene hat zudem das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch die für die Big Data-Anwendung verantwortliche Stelle, zu übermitteln, sofern **430**

- die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 Satz 1 lit. (a) DS-GVO oder Art. 9 Abs. 2 lit. (a) DS-GVO oder auf einem Vertrag mit dem Big Data-Betroffenen gemäß Art. 6 Abs. 1 Satz 1 lit. (b) DS-GVO beruht und
- die Verarbeitung in der Big Data-Anwendung mithilfe automatisierter Verfahren erfolgt.

Bei der Ausübung seines Rechts auf Datenübertragbarkeit gemäß Art. 20 Abs. 1 DS-GVO hat der Big Data-Betroffene gemäß Art. 20 Abs. 2 DS-GVO das Recht, zu erwirken, dass die personenbezogenen Daten direkt von der für die Big Data-Anwendung verantwortlichen Stelle einem anderen, vom Big Data-Betroffenen zu benennenden Verantwortlichen übermittelt werden, soweit dies technisch machbar ist. Die für die Big Data-Anwendung verantwortliche Stelle hat also auch hierfür nicht nur einen entsprechenden Prozess zu etablieren, sondern auch die technischen Voraussetzungen für einen solchen Export der noch als personenbezogene Daten geführten Daten der Big Data-Anwendung zu schaffen, bzw. das Vorhandensein solcher Möglichkeiten beim Aufbau einer Big Data-Anwendung zu berücksichtigen (privacy by design, Art. 25 DS-GVO). **431**

6. Beschwerderecht

Auch Big Data-Betroffene haben gemäß Art. 77 DS-GVO ein Beschwerderecht bei der für die für die Big Data-Anwendung verantwortlichen Stelle zuständigen Datenschutzaufsichtsbehörde, wenn der Big Data-Betroffene der Ansicht ist, dass die Verarbeitung seiner perso- **432**

nenbezogenen Daten in der Big Data-Anwendung rechtswidrig erfolgt. Hierüber ist der Big Data-Betroffene gemäß Art. 13 Abs. 2 lit. (d) DS-GVO von der für die Big Data-Anwendung verantwortlichen Stelle im Rahmen der Datenschutzerklärung zu belehren.

Leitsatz:

Wenn in einer Big Data-Anwendung personenbezogene Daten gespeichert und verarbeitet werden, haben die Betroffenen die Betroffenenrechte gemäß Art. 15 – 21 DS-GVO. Es sind also die zur Erfüllung dieser Betroffenenrechte notwendigen Prozesse und technischen Voraussetzungen zu schaffen.

III. Verarbeitungsverzeichnis gemäß Art. 30 DS-GVO

433 In der nachfolgenden Tabelle sind die inhaltlichen Anforderungen an das Verfahrens-/Verarbeitungsverzeichnis für eine Big Data-Anwendung aufgeführt, die bis zum 25.5.2018 gemäß § 4e Satz 1 BDSG a. F. und ab dem 25.5.2018 gemäß Art. 30 Abs. 1 DS-GVO zu erfüllen sind, und – zur Verdeutlichung, inwieweit sie sich gleichen – einander gegenüber gestellt.

Verfahrensverzeichnis (§ 4e Satz 1 BDSG a. F.)	**Verzeichnis für Verarbeitungstätigkeiten (Art. 30 Abs. 1 DS-GVO)**
Name oder Firma der für die Big Data-Anwendung verantwortlichen Stelle als verantwortlichen Stelle (Nr. 1) Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen (Nr. 2) Anschrift der verantwortlichen Stelle (Nr. 3)	Name und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten (lit. (a))
Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung (Nr. 4)	Zwecke der Verarbeitung (lit. (b))
Beschreibung der betroffenen Personengruppen (Big Data-Betroffene) und der diesbezüglichen Daten oder Datenkategorien (Nr. 5)	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (lit. (c))
Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können (Nr. 6).	Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten in oder aus der Big Data-Anwendung offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen (lit. (d).

Verfahrensverzeichnis (§ 4e Satz 1 BDSG a. F.)	Verzeichnis für Verarbeitungstätigkeiten (Art. 30 Abs. 1 DS-GVO)
Geplante Datenübermittlung in Drittstaaten, (Nr. 8)	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 Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien (lit. (e).
Regelfristen für die Löschung der Daten sowie der von der für die Big Data-Anwendung verantwortlichen Stelle auf spezifische Big Data-Betroffene bezogenen Analyseergebnisse (Nr. 7)	Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien (lit. (f)).
Allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG a. F. zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind (Nr. 9); gemäß § 4g Abs. 2 Satz 2 BDSG a. F. nur für das interne Verzeichnis.	Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 lit. (g) DS-GVO)

Abbildung 62: Verfahrensverzeichnis

Verstöße gegen die Pflicht zur Aufstellung und Führung eines Verarbeitungsverzeichnisses gemäß Art. 30 DS-GVO können die in Rn. 497 ff. dieses Leitfadens beschriebenen Rechtsfolgen nach sich ziehen. **434**

Werden zum Betrieb der Big Data-Anwendung Leistungen Dritter als Auftragsdatenverarbeiter genutzt, so hat auch der Auftragsdatenverarbeiter ab dem 25.5.2018 ein solches Verarbeitungsverzeichnis zu führen. **435**

Leitsatz:

Für jede Big Data-Anwendung, in der personenbezogene Daten gespeichert und verarbeitet werden, ist sowohl von dem für die Big Data-Anwendung Verantwortlichen als auch dem gegebenenfalls zu deren Betrieb eingesetzten Auftragsverarbeiter ein Verarbeitungsverzeichnis im Sinne von Art. 30 DS-GVO zu führen.

Im Übrigen können sich auch bei nicht-personenbezogenen Daten vergleichbare Dokumentationspflichten ergeben, etwa wenn Anzahl und Art der Verwendung solcher Daten gegenüber dem Datenlieferanten vergütungsrelevant sind.

IV. Umsetzung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten vor unbefugtem Zugriff

Gemäß § 9 BDSG a. F. musste die für die Big Data-Anwendung verantwortliche Stelle die noch in der Anlage zum BDSG a. F. lediglich nach ihren Schutzzielen aufgeführten technischen und organisatorischen Maßnahmen ergreifen und diese regelmäßig daraufhin prüfen, ob sie **436**

noch dem Gefährdungspotential genügen, dem die Rohdaten, die in der Big Data-Anwendung erzeugten Datensätze sowie und die auf spezifische Big Data-Betroffene bezogenen Analyseergebnisse ausgesetzt sind.

437 In dem ab dem 25.5.2018 anzuwendenden Art. 32 Abs. 1 DS-GVO ist diese Verpflichtung wesentlich allgemeiner formuliert. Danach hat die für die Big Data-Anwendung verantwortliche Stelle 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 geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Als Regelbeispiele für solche Maßnahmen werden sodann einige Maßnahmen aufgeführt, nämlich

- die Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

438 Die Wortwahl des Verordnungstextes ist in vielen Formulierungen zwar anders als noch im BDSG a. F., gleichwohl werden die zu § 9 BDSG a. F. und zur Anlage zum BDSG a. F. entwickelten Grundsätze und Überlegungen heranzuziehen sein, stellt man auf den Sinn und Zweck der Vorschrift in Art. 32 DS-GVO ab.[115] Daraus ergeben sich folgende Schutzziele und die jeweils hierzu beispielhaft aufgeführten Maßnahmen. Ob und welche dieser Maßnahmen zu ergreifen sind, ist dann noch einmal im Einzelfall zu prüfen, vor allem unter Berücksichtigung der konkreten technischen und architekturellen Gegebenheiten bei der für die Big Data-Anwendung verantwortlichen Stelle.

1. Zutrittskontrolle

439 Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Benennung der autorisierten Personen (intern und extern)
- Zutrittsüberwachungssystem
- Zutrittskontrollsystem wie Ausweisleser, Magnetkarte oder Chipkarte
- Register von Schlüsselinhabern
- Vorgaben für externe Personen (Besucher; Reinigungskräfte oder sonstige Fremdfirmen)
- Anwesenheitslisten
- Besucherausweise
- Alarmsystem, Werkschutz oder anderweitige Schutzmaßnahmen außerhalb der Geschäftszeiten
- Einrichtung von Sicherheitszonen mit Zugangsbeschränkungen
- Gesicherter Lieferantenein- und -ausgang
- Türsicherung (z. B. elektrische Türöffner, Kartenleser, TV-Monitore, Wachpersonal)
- Installation von Luftschleusen
- Geschlossener Rechenzentrumsbetrieb
- Gegenseitige Überwachung

[115] Vgl. *Paulus,* in: Wolff/Brink, BeckOK DatenSR, 25. Ed., Stand: 1.8.2018, Art. 32 DS-GVO Rn. 6.

- Geeignete Maßnahmen Gebäudesicherung (z. B. Spezialverglasung, Eindringlingsalarm, Stockwerkskontrollen, Abschottung von Steigleitungen)

2. Zugangskontrolle

Das Eindringen Unbefugter in die Big Data-Anwendung ist zu verhindern. Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung sind zu ergreifen: **440**

- Sperrfunktion an Arbeitsplätzen
- Identifikation eines Terminals oder Nutzers gegenüber der Big Data-Anwendung
- Passwortverfahren (u. a. Sonderzeichen, Mindestlänge, regelmäßiger Kennwortwechsel)
- Funktionsgebundene Zuweisung von individuellen Terminals und Kennungen
- Funktionale und/oder zeitliche Beschränkung der Nutzung von Terminals und Kennungen
- Kontrolle von Zugangsrechten der Nutzer
- Verpflichtung auf das Datengeheimnis nach § 5 BDSG a. F. / Art. 5 Abs. 1 lit. (f) DS-GVO
- Verwendung von Nutzercodes für Dateien und Programme
- Verwendung von Verschlüsselungsprogrammen für Dateien und Datenträger
- Differenzierte Zugangsvoraussetzungen
- Richtlinien für die Dateiorganisation
- Erfassung und Analyse der Datennutzung
- Besondere Kontrolle der Nutzung von Hilfsprogrammen, soweit diese geeignet sind, Sicherheitsmaßnahmen zu umgehen
- Kontrollierte Vernichtung von Datenträgern
- Arbeitsanweisungen und Verfahren für Datenerfassung
- Kontroll-, Genehmigungs- und Monitoringsysteme
- Programmüberprüfungen und Releaseprozesse

3. Zugriffskontrolle

Unerlaubte Tätigkeiten mit oder in der Big Data-Anwendung außerhalb eingeräumter Berechtigungen sind zu verhindern. Maßnahmen zur bedarfsorientierten Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung umfassen insbesondere: **441**

- Arbeitsplätze mit funktionsgebundenen Zugriffsschlüsseln
- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte) einschließlich dokumentiertes Berechtigungskonzept
- Automatische Kontrolle von Zugriffsrechten z. B. durch Identifikationsschlüssel
- Führen von Zugriffsprotokollen
- Analyse der Zugriffsprotokolle
- Kartenleser am Terminal
- Zeitliche Begrenzung des Zugriffs
- Zuweisung von abgegrenzten Zugriffsrechten nur auf bestimmte Daten oder Funktionen
- Regelmäßige Prüfung, ob erteilte Berechtigungen noch benötigt werden, Stornierung von Berechtigungen für ausgeschiedene Mitarbeiter

4. Datenträgerkontrolle

442 Das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern ist zu verhindern. Mögliche Maßnahmen hierfür können sein:

- Verschlüsselung von Datenträgern
- Verschlossenes Aufbewahren von Datenträgern
- Protokollierung der Aushändigung von Datenträgern an Mitarbeiter sowie deren Rückgabe in eine verschlossene Aufbewahrung
- etc.

5. Zugriffs- und Benutzerkontrolle

443 Es ist zu gewährleisten, dass die zur Benutzung der Big Data-Anwendung berechtigten Nutzer ausschließlich auf solche Inhalte einschließlich ihrer Auswertungen und Analyseergebnisse zugreifen können, für welche sie berechtigt sind und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern in der Big Data-Anwendung und eventuellen Vorsystemen zur Aufbereitung dieser Daten nicht unbefugt kopiert, verändert oder gelöscht werden können. Maßnahmen der Zugriffs- und Benutzerkontrolle können beispielsweise sein

- Berechtigungskonzept
- Benutzerkennung mit Passwort
- gesicherte Schnittstellen
- Datenträgerverwaltung
- zertifikatsbasierte Zugriffsberechtigung
- System interne Berechtigungsverwaltung
- Berechtigungsverwaltung durch den zuständigen Systemadministrator

6. Weitergabe-, Übertragungs- und Transportkontrolle

444 Folgende Aspekte der Weitergabe personenbezogener Daten mit Bezug auf Daten der Big Data-Betroffenen sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle, Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie nachträgliche Überprüfung. Solche Maßnahmen können insbesondere sein:

- Benennung der autorisierten Personen und Kontrolle der Autorisation bei Datenübergabe durch Vorlage geeigneter Berechtigungsnachweise
- Gegenseitige Überwachung
- Gesicherter Lieferantenein- und -ausgang
- Verwendung von Verschlüsselung bei der Übertragung oder von Tunnelverbindungen (z. B. VPN)
- Elektronische Signatur
- Inventarkontrollen
- Separate, gesicherte Aufbewahrung von Datenträgern mit vertraulichem Inhalt
- Zugriffsberechtigungen auf archivierte Datenträger
- Verbot des Beisichführens von Taschen oder anderen Gepäckstücken in Sicherheitsbereichen
- Überwachung der Vernichtung von Datenträgern und Ausschussmaterialien (z. B. Fehldrucken)
- Kontrolle der Anfertigung von Datenkopien