Grundsätze für die Datenverarbeitung

DIENSTVEREINBARUNGEN *Die Grundsätze zur Verarbeitung personenbezogener Daten sind verbindlich. Auch bei Dienstvereinbarungen zu IT-Systemen sind sie unbedingt zu beachten.*

VON **BRUNO SCHIERBAUM**

DARUM GEHT ES

1. Die DS-GVO legt die Grundsätze für die Verarbeitung personenbezogener Daten fest.

2. Diese Grundsätze sind auch beim Verarbeiten von Beschäftigtendaten zu beachten.

3. Bei Dienstvereinbarungen zu IT-Systemen sind die Grundsätze praxisnah umsetzbar.

Art. 5 Datenschutz-Grundverordnung (DS-GVO) listet einen Katalog von Grundsätzen zum Datenschutz auf (siehe Tabelle 1 auf Seite 29). Die konkreten Inhalte waren bisher im deutschen Datenschutzrecht nicht so klar formuliert.[1] Diese Grundsätze werden an verschiedensten Stellen in der DS-GVO wiederholt bzw. es wird auf sie Bezug genommen.[2]

Die Grundsätze haben den Charakter verbindlicher Regelungen und sind – trotz ihrer offenen und unbestimmten Formulierungen – unmittelbar geltendes Recht.[3] Zum Teil sind die Grundsätze bereits durch Art. 8 Grundrechtecharta der Europäischen Union (GRC) abgesichert.[4] In Art. 16 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) sind ebenfalls Regelungen zum Datenschutz und zur Gesetzgebungskompetenz des Europäischen Parlaments und des Rates enthalten. Die Erforderlichkeit der Umsetzung und die Verbindlichkeit der Grundsätze werden unter anderem dadurch deutlich, dass der Verantwortliche nach Art. 5 Abs. 2 DS-GVO nicht nur für deren Einhaltung verantwortlich ist, sondern auch die Einhaltung nachweisen muss. Zudem wird eine Verletzung von Art. 5 DS-GVO gemäß Art. 83 Abs. 5a DS-GVO mit einer Geldbuße geahndet, wobei Behörden nach § 43 Abs. 3 BDSG[5] von Geldbußen ausgenommen sind.

Dienstvereinbarungen und Mitbestimmung

Art. 88 DS-GVO enthält eine allgemeine Regelung zum Beschäftigten-Datenschutz. Dem nationalen Gesetzgeber wird über eine sogenannte Öffnungsklausel die Möglichkeit eingeräumt, »spezifischere Vorschriften« zu erlassen. Es besteht nach Vorgabe der DS-GVO die Möglichkeit, durch Rechtsvorschriften oder Kollektivvereinbarungen die Gewährleistung des Schutzes der Rechte und Freiheiten der Betroffenen vorzusehen. Im Erwägungsgrund 155 der DS-GVO wird zudem klargestellt, dass Betriebsvereinbarungen Kollektivvereinbarungen in diesem Sinne sind. Der deutsche Gesetzgeber hat von der Öffnungsklausel Gebrauch gemacht. Durch die Novellierung des BDSG gibt es in § 26 eine spezifischere Regelung zum Beschäftigten-Datenschutz. Entsprechende Regelungen sind in den Landesdatenschutzgesetzen erhalten (siehe Tabelle 2 auf Seite 30). § 26 BDSG gilt hinsichtlich der Zulässigkeit/Rechtmäßigkeit neben Art. 6 DS-GVO. Denn der Verantwortliche/Arbeitgeber kann unter anderem auch auf der Basis einer Einwilligung, zur Erfüllung rechtlicher Pflichten, wenn es zum Schutz lebenswichtiger Interessen einer Person oder in Ausübung öffentlicher Interessen erforderlich ist, rechtmäßig Beschäftigten-Daten verarbeiten.

§ 26 BDSG enthält weitere Zulässigkeitsvoraussetzungen für die Verarbeitung von Beschäftigten-Daten. So kann nach § 26 Abs. 4 BDSG auf der Grundlage von Kollektivvereinbarungen die Verarbeitung personenbezogener Daten, einschließlich der besonderen Kategorien personenbezogener Daten[6], rechtlich zulässig geregelt werden. Zu den Kollektivvereinbarungen gehören nicht nur Betriebsvereinbarungen, sondern auch

1 Vgl. Roßnagel, ZD 8/18, 239.
2 Vgl. Paal/Pauly, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl., Art. 5 Rn. 1; Schantz/Wolff, Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, Rn. 382.
3 Roßnagel, ZD 8/18, 243.
4 Vgl. Schantz/Wolff, a.a.O., S. 127.
5 Siehe aktuelles BDSG vom 30.6.2017 (BGBl. I S. 2097).
6 Näher hierzu Kersting, PersR 4/2018, 34 ff.

TABELLE 1

Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO

Grundsatz	Inhalt
· Rechtmäßigkeit · Treu und Glauben · Transparenz (Abs. 1a)	· personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden
· Zweckbindung (Abs. 1b)	· personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden
· Datenminimierung (Abs. 1c)	· personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein
· Richtigkeit (Abs. 1d)	· personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein · es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden
· Speicherbegrenzung (Abs. 1e)	· personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist · personenbezogene Daten dürfen länger gespeichert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke
· Integrität und Vertraulichkeit (Abs. 1f)	· personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz · vor unbefugter oder unrechtmäßiger Verarbeitung und · vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder · unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen
· Rechenschaftspflicht (Abs. 2)	· der Verantwortliche ist für die Einhaltung des Art. 5 DS-GVO verantwortlich und muss dessen Einhaltung nachweisen können

Dienstvereinbarungen.[7] Weiterhin können also Dienstvereinbarungen mit Datenschutzregelungen abgeschlossen werden, die allerdings unter Beachtung der Grundsätze der Datenverarbeitung des Art. 5 DS-GVO sehr klare, eindeutige und abschließende Datenschutzregelungen enthalten müssen.

Vorsetzungen für den Abschluss von Dienstvereinbarungen zum Datenschutz sind entsprechende Mitbestimmungsrechte des Personalrats (vgl. § 73 Abs. 1 BPersVG i.V.m. §§ 75 Abs. 3, 76 Abs. 2 BPersVG). Ein Mitbestimmungsrecht ist gegeben bei der Einführung und Anwendung einer technischen Überwa-

7 Vgl. BT Drs. 18/11325, S. 98.

AUS DEM GESETZ

Art. 8 GRC
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

Art. 16 AEUV
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.

TABELLE 2

Beschäftigten-Datenschutz im BDSG und den LDSG

Vorschrift	Beschäftigten-Datenschutz/ Datenschutz in Dienst- und Arbeitsverhältnissen
§ 26 BDSG	Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
§ 15 LDSG BW	Datenverarbeitung bei Dienst- und Arbeitsverhältnissen
§ 18 BlnDSG	Verarbeitung personenbezogener Beschäftigtendaten
§ 26 BbgDSG	Datenverarbeitung bei Beschäftigungsverhältnissen
§ 12 BremDSG	Datenverarbeitung im Beschäftigtenkontext
§ 10 HmbDSG	Verarbeitung von Beschäftigtendaten
§ 23 HDSIG	Datenverarbeitung für Zwecke des Beschäftigtenverhältnisses
§ 10 DSG M-V	Datenverarbeitung bei Beschäftigungsverhältnissen
§ 12 NDSG	Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen
§ 18 DSG NRW	Datenverarbeitung im Beschäftigtenkontext
§ 20 Rh-Pfl.	Datenverarbeitung in Dienst- und Beschäftigungsverhältnissen
§ 22 SaarlDSG	Verarbeitung von Beschäftigten-Daten
§ 12 SächsDSG	Verarbeitung von Beschäftigten-Daten
§ 28 DSG LSA	Erhebung, Verarbeitung oder Nutzung von Personal- und Bewerberdaten
§ 15 Schl.-Holst.	Datenverarbeitung im Beschäftigtenzusammenhang
§ 27 ThürDSG	Datenverarbeitung im Beschäftigtenkontext

chungseinrichtungen (IT-Systeme) nach § 75 Abs. 3 Nr. 17 BPersVG. Eine entsprechende Regelung ist auch in den Landespersonalvertretungsgesetzen enthalten. In den meisten Landespersonalvertretungsgesetzen gibt es zusätzlich das Mitbestimmungsrecht bei der Festlegung des Umfangs der Verarbeitung personenbezogener Daten oder in einigen Landespersonalvertretungsgesetzen auch bei der Einführung von behördlichen Netzwerken.[8] Ein spezielles, umfassendes Mitbestimmungsrecht zum »Datenschutz« selbst gibt es allerdings nicht. Somit können die Personalräte lediglich Regelungen im Rahmen der vorhandenen Mitbestimmungsrechte treffen.[9] Beim Abschluss von Dienstvereinbarungen müssen die Grundsätze der Verarbeitung unbedingt beachtet werden. Das ergibt sich bereits aus der DS-GVO selbst. Zudem wird in § 26 Abs. 5 BDSG ausdrücklich darauf hingewiesen, dass geeignete Maßnahmen zu ergreifen sind, um sicherzustellen, dass insbesondere die in Art. 5 DS-GVO enthaltenen Grundsätze zu beachten sind. Aus den Grundsätzen lässt sich wichtiger Regelungsbedarf ableiten, der in einer Dienstvereinbarung zu IT-Systemen hinsichtlich des Datenschutzes vereinbart werden sollte. In welcher Form die Grundsätze in eine Dienstvereinbarung integriert werden, sei es im Textteil oder im Rahmen von Anlagen zur Dienstvereinbarung, bleibt dem Personalrat und der Dienststellenleitung überlassen.

Grundsätze der Verarbeitung

▸ Rechtmäßigkeit

Art. 5 Abs. 1a DS-GVO regelt die Pflicht, personenbezogene Daten auf rechtmäßige Weise zu verarbeiten. Diese Vorgabe kann vor allem durch die Vorgaben des Art. 6 DS-GVO umgesetzt werden. Dieser Artikel enthält die zentrale Vorgabe für rechtmäßige Verarbeitung personenbezogener Daten und geht von einem sogenannten Verbot mit Erlaubnisvorbehalt aus.[10] »Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden.«[11] Für besondere Kategorien personenbezogener Daten richtet sich die Rechtmäßigkeit nach Art. 9 DS-GVO. Beim Beschäftigten-Datenschutz kann die Zulässigkeit der Verarbeitung auf § 26 BDSG[12] und Art. 6 DS-GVO gestützt werden. Fehlt es an einer rechtlichen Basis, ist die Verarbeitung rechtswidrig.

DV-Tipp 1:
Grundsatz der Rechtmäßigkeit

In einer Dienstvereinbarung zu einem IT-System muss vor dem Hintergrund der Rechtmäßigkeit die Zulässigkeit der Verarbeitung für jedes personenbezogene Datum nach § 26 BDSG oder Art. 6 DS-GVO geprüft werden. Es dürfen nur die Daten verarbeitet

8 Näher zu den Mitbestimmungsrechten Thannheiser, PersR 4/18, 11.

9 Vgl. Wedde, CuA 10/17, 26.
10 Vgl. andere Auffassung: Roßnagel, ZD 8/18, 239.
11 Erwägungsgrund 40.
12 § 26 BDSG verdrängt nur Art. 6 Abs. 1 b und f DS-GVO.

werden, die zum Durchführen des Beschäftigungsverhältnisses erforderlich sind. Eine entsprechende Zulässigkeitsprüfung muss auch hinsichtlich zugriffsberechtigter Personen, Auswertungen mit personenbezogenen Daten und der Speicherdauer erfolgen.

Treu und Glauben

Als weiteren Grundsatz nennt Art. 5 Abs. 1a DS-GVO die Verarbeitung nach Treu und Glauben. Es finden sich in den Erwägungsgründen keine weiteren Erläuterungen, was der europäische Gesetzgeber unter »Treu und Glauben« verstanden wissen will.[13] Auch wenn die inhaltlichen Vorgaben des Grundsatzes der Verarbeitung nach Treu und Glauben nicht abschließend geklärt sind[14], dürfte dieser Grundsatz zwei Ausprägungen haben, nämlich

- die Vorhersehbarkeit der Verarbeitung personenbezogener Daten und
- die Transparenz der Verarbeitung personenbezogener Daten.

So meint Treu und Glauben die Verarbeitung dessen, womit der Betroffene bei der Erhebung redlicher Weise hat rechnen müssen. Dieses ergänzt den Grundsatz der Zweckbindung. Somit dürfte regelmäßig die Verwendung verborgener Techniken, wie zum Beispiel heimliche Videoüberwachung oder Spyware, treuwidrig sein.[15] Eine zentrale Folge des Gebots der Verarbeitung nach Treu und Glauben ist es, dass die Daten zu löschen sind, wenn die Rechtsgrundlage wegfällt.[16]

DV-Tipp 2:
Grundsatz von Treu und Glauben

In einer Dienstvereinbarung ist transparent und präzise der Umfang der Verarbeitung personenbezogener Daten zu vereinbaren. Es ist deutlich und für die Beschäftigten nachvollziehbar zu regeln, in welchem Rahmen möglicherweise Kontrollen der Beschäftigten stattfinden können. Diese sind in jedem Fall zu begrenzen. Eine heimliche Überwachung der Beschäftigten ist grundsätzlich auszuschließen. Diese Vorgaben müssen auch dann gelten, wenn der Arbeitgeber oder die Dienststellenleitung Auftragsverarbeitung ausführen lässt.

Transparenz

Art. 5 Abs. 1a DS-GVO gibt außerdem vor, dass die Verarbeitung in einer für die betroffene Person nachvollziehbaren Weise erfolgt. Was mit dieser Grundpflicht zur Transparenz gemeint ist, wird aus Erwägungsgrund 39 erkennbar. »Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.« Sowohl die Informationspflichten nach Art. 12 und 13 DS-GVO, als auch das Auskunftsrecht nach Art. 15 DS-GVO oder die Benachrichtigungspflicht des Betroffenen bei sogenannten Datenschutz-Pannen[17] sind Konkretisierungen des Transparenzgebots.[18]

Der europäische Verordnungsgeber hat in der Regelung zum Beschäftigten-Datenschutz in Art. 88 Abs. 2 DS-GVO das Transparenzgebot noch einmal verankert. Der Arbeitgeber muss seine Beschäftigten über alle Verarbeitungen der personenbezogenen Daten in präziser, verständlicher und leicht zugänglicher Form informieren. Denn auch Beschäftigte müssen erkennen und nachvollziehen können, in welchen Rahmen, in welchem Umfang und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden.[19]

DV-Tipp 3: Grundsatz der Transparenz

In einer Dienstvereinbarung ist in einer sehr klaren, verständlichen und einfachen Sprache der Umfang der Verarbeitung personenbezogener Daten abschließend festzulegen. Dazu gehört die eingesetzte Hardware mit

13 Vgl. Kazemi, Die EU-Datenschutz-Grundverordnung in der anwaltlichen Beratungspraxis, S. 88.
14 Vgl. Schantz/Wolff, a.a.O., Rn. 58.
15 Gola (Hrsg.), Datenschutz-Grundverordnung (EU) 2016/679, Art. 5 Rn. 9; anderer Auffassung in Bezug auf heimliche Überwachung: Auernhammer, DSGVO – BDSG, Art. 5 Rn. 13.
16 Vgl. Schantz/Wolff, a.a.O., S. 17 f.
17 Näher zu Datenschutz-Pannen Schierbaum, PersR 4/18, 29 ff.
18 Vgl. auch Moos/Schefzig/Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, S. 66.
19 Vgl. Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 88 Rn. 34.

den Standorten, was insbesondere bei Videoüberwachung, Zugangskontroll- und Zeiterfassungssystemen von besonderer Bedeutung ist. Es müssen außerdem klar und deutlich der Umfang der Auswertungen und der Zugriffsberechtigungen, der Schnittstellen mit übertragenen Daten und die Löschungsfristen vereinbart und dokumentiert werden. Zusätzlich ist zu regeln, wo und durch wen die Datenverarbeitung erfolgt – durch die Dienststellenleitung selbst oder im Rahmen von Auftragsverarbeitung. Zudem sollte auf die Informations-, Auskunfts- und Korrekturrechte der Beschäftigten (Art. 12 ff. DS-GVO) verwiesen werden.

▸ Zweckbindung

Der Grundsatz des Art. 5 Abs. 1b DS-GVO regelt, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Die Zweckbindung ist seit jeher eines der zentralen und tragenden Prinzipien des Datenschutzrechts und begrenzt die Datenverarbeitung. »Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein.«[20] Die Zweckbindung ist somit auch der Maßstab für die Erforderlichkeit und Angemessenheit, für die Richtigkeit und Vollständigkeit und für die Dauer der Verarbeitung.[21] Grundsätzlich müssen die Zwecke zum Zeitpunkt der Erhebung feststehen.[22]

Die Zwecke müssen eindeutig sein und festgelegt werden. Das ist dann der Fall, wenn sie ausdrücklich als Zwecke der Verarbeitung bezeichnet werden und ein Maß an Begrenzung festgelegt ist.[23] Somit ist zum Beispiel die anlasslose Sammlung von personenbezogenen Daten »auf Vorrat« zu unbestimmten oder noch nicht bestimmbaren Zwecken mit der DS-GVO unvereinbar.[24]

Beim Weiterverarbeiten sind die Zwecke, die bei einer Erhebung festgelegt werden, einzuhalten. Eine Zweckänderung ist grundsätzlich unzulässig. Die Zulässigkeit einer Weiterverarbeitung muss bei einer Zweckänderung erneut nach den Vorgaben des Art. 6 DS-GVO und § 26 BDSG-neu geprüft werden. Dieser Grundsatz folgt der Zweckbindung und Erforderlichkeit. Bei einer Zweckänderung sind die Betroffenen gemäß Art. 13 Abs. 4 und 14 Abs. 4 DS-GVO zu informieren.

DV-Tipp 4: Grundsatz der Zweckbindung

In einer Dienstvereinbarung sind die Zwecke, die mit dem Einsatz eines bestimmten IT-Systems verfolgt werden sollen, abschließend zu regeln und zu dokumentieren. Daten, die für die Verfolgung des festgelegten Zwecks nicht erforderlich sind, dürfen nicht gespeichert werden. Zudem ist bei einer geplanten Erweiterung oder Änderung der Verarbeitungszwecke die Dienstvereinbarung anzupassen.

▸ Datenminimierung

Nach Art. 5 Abs. 1c DS-GVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung das notwendige Maß beschränkt sein. Dem Verarbeitungszweck angemessen sind Daten nur dann, wenn ihre Zuordnung und Erforderlichkeit hinsichtlich des Zwecks der Verarbeitung nicht beanstandet werden kann. Zudem müssen die Daten für die Zweckerreichung erheblich sein. Der Umfang und die Art der Daten müssen überhaupt geeignet sein, um den Zweck zu erreichen.[25] Deshalb dürfen Daten nicht verarbeitet werden, wenn der Verarbeitungszweck auch ohne sie erreicht werden kann.[26] Die Verarbeitung personenbezogener Daten muss auf das notwendige und geringstmögliche Maß beschränkt sein[27]. Es dürfen nicht mehr Daten verarbeitet werden, als diejenigen, die für die Erreichung des Zwecks erforderlich sind. Datenverarbeitung auf Vorrat ist nicht zulässig. Es muss eine Löschungsroutine etabliert werden, so dass im Rahmen festgelegter Termine eine Kontrolle stattfindet, ob gespeicherte personenbezogene Daten noch benötigt werden. Ist dies nicht der Fall, sind die Daten zu löschen.[28]

DV-Tipp 5:
Grundsatz der Datenminimierung

Beim Abschluss einer Dienstvereinbarung muss der Grundsatz der »Datenminimie-

20 So Erwägungsgrund 39, Satz 6; vgl. auch Härting, Datenschutz-Grundverordnung, S. 27.
21 Vgl. Dammann, ZD 7/16, 311; Roßnagel, ZD 8/18, S. 340.
22 Gola (Hrsg.), a.a.O., Art. 5 Rn. 16.
23 Vgl. Schantz/Wolff, a.a.O., S. 132.
24 Vgl. Kazemi, a.a.O., S. 93; vgl. auch Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 5 Rn. 15; Moos/Schefzig/Arning, a.a.O., S. 67.
25 Vgl. Schantz/Wolff, a.a.O., S. 137.
26 Vgl. Kühling/Buchner (Hrsg.), DS-GVO – Datenschutz-Grundverordnung – Kommentar, Art. 5 Rn. 57.
27 Vgl. Roßnagel, ZD 8/18, 341.
28 Vgl. Härting, a.a.O., S. 28.

rung« den »Maßstab« für den Umfang der Verarbeitung personenbezogener Daten bilden. Die Verarbeitung ist auf das notwendige und geringstmögliche Maß zu beschränken. Es dürfen nur Daten gespeichert werden, die zur Zweckerreichung geeignet sind. Daraus ergeben sich klare und eindeutige Löschungsfristen.

▸ Richtigkeit

Nach Art. 5 Abs. 1d DS-GVO müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Daten müssen die Realität repräsentieren und diese nicht verfälschen.[29] Bereits bei der Erhebung ist auf die Richtigkeit der Daten zu achten. Richtig bedeutet, der Wahrheit entsprechend.[30] Zudem sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden[31]. Als Maßstab für die Richtigkeit sind die Zwecke der Verarbeitung von zentraler Bedeutung. Der Grundsatz der Richtigkeit stärkt die Rechte der Betroffenen. Ergänzt wird der Grundsatz der Richtigkeit durch den in Art. 16 DS-GVO verankerten Berichtigungsanspruch von Betroffenen. Betroffene haben zudem nach Art. 18 Abs. 1a DS-GVO die Möglichkeit, die Richtigkeit der Daten zu bestreiten und die Einschränkung der Datenverarbeitung zu verlangen.[32]

DV-Tipp 6:
Grundsatz der Richtigkeit

Es ist zu vereinbaren, dass die Richtigkeit der Daten auch nach Abschluss der Dienstvereinbarung regelmäßig überprüft wird. Zudem sollte auf die Korrekturrechte der Beschäftigten verwiesen werden.

▸ Speicherbegrenzung

Nach Art. 5 Abs. 1e DS-GVO müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen nur dann länger gespeichert werden, wenn sie vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von der DS-GVO zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden.

Die Dauer der Speicherung der personenbezogenen Daten ist an den Vorgaben »Zweck«, »Identifizierbarkeit« und »Erforderlichkeit« geknüpft. Die Speicherbegrenzung ist nur dann anzuwenden, wenn eine Person identifiziert werden kann, also nicht zwingend bei tatsächlich anonymen Daten.

DV-Tipp 7:
Grundsatz der Speicherbegrenzung

In einer Dienstvereinbarung ist festzulegen, wann welche Daten zu löschen sind. Es ist eine Löschroutine zu verankern. Zudem ist zu prüfen und zu regeln, inwieweit mit Pseudonymisierung gearbeitet werden kann.

▸ Integrität und Vertraulichkeit

Nach Art. 5 Abs. 1f DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich dem Schutz

- vor unbefugter oder unrechtmäßiger Verarbeitung und
- vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder
- unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Der Grundsatz der Integrität und Vertraulichkeit wird durch die Art. 25 und Art. 32 DS-GVO konkretisiert.[33] Unter Umständen muss dieser Grundsatz durch eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO im Vorfeld der Verarbeitung überprüft werden.[34] In dem Fall müssen technische und organisatorische Maßnahmen nach Art. 32 DS-GVO, für die nach Art. 24 DS-GVO der Verantwortliche

29 Vgl. Auernhammer, a.a.O., Art. 5 Rn. 32.
30 Vgl. Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 5 Rn. 52.
31 Vgl. Erwägungsgrund 39, Satz 11; Härting, a.a.O., S. 28.
32 Vgl. Moos/Schefzig/Arning (Hrsg.), a.a.O., S. 69 f.
33 Vgl. Breyer, DUD 5/18, 314.
34 Hierzu Kiesche, PersR 4/2018, 25 ff.

Personenbezogene Daten der Beschäftigten haben auch die Personalratsmitglieder zu wahren.

zuständig ist, umgesetzt werden, um so eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten. Damit stellt der Grundsatz »Integrität und Vertraulichkeit« auf zu treffende technische und organisatorische Maßnahmen und eine funktionierende IT-Infrastruktur ab.

Unbefugte und unrechtmäßige Verarbeitung ist insbesondere dann gegeben, wenn Dritte, also Personen, die nicht dem Verantwortlichen zuzurechnen sind, auf personenbezogene Daten zugreifen. Dies ist aber selbst dann gegeben, wenn ein Beschäftigter des Verantwortlichen auf Daten zugreifen kann, die er in keiner Weise für die Erfüllung seiner Arbeitsaufgaben benötigt.

Unbeabsichtigter Verlust, unbeabsichtigte Zerstörung oder unbeabsichtigte Schädigung liegt vor, wenn Daten abhandenkommen oder beschädigt werden, auch wenn das unbeabsichtigt geschieht. Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen, unter anderem gemäß Art. 32 DS-GVO treffen.

DV-Tipp 8: Grundsatz der Integrität und Vertraulichkeit

In Dienstvereinbarungen sind konkrete Maßnahmen zum Datenschutz und zur Datensicherheit zu regeln. Die wichtigsten Vorgaben sind insbesondere in Art. 32 DS-GVO enthalten. Die konkreten Maßnahmen schließen gegebenenfalls unter anderem 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,
- 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 Evaluation der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

▸ Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung der oben genannten Grundsätze verantwortlich und muss dessen Einhaltung nachweisen (Art. 5 Abs. 2 DS-GVO). Wie die Dokumentation hinsichtlich der Rechenschaftspflicht erfolgt, obliegt dem Verantwortlichen. Es bietet sich an, die Umsetzung der Grundsätze der Verarbeitung nach Art. 5 DS-GVO im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu dokumentieren. ◁

DV-Tipp 9: Grundsatz der Rechenschaftspflicht

Bei einer Regelung eines IT-Systems im Rahmen einer Dienstvereinbarung ist eine Dokumentation der Verarbeitung personenbezogener Daten von zentraler Bedeutung. So könnte das Verzeichnis der Verarbeitungstätigkeiten beispielsweise als Anlage Bestandteil einer Dienstvereinbarung sein.

Bruno Schierbaum,
BTQ Niedersachsen GmbH,
Oldenburg.