WILLE // RECHTSANWÄLTE

WILLE RECHTSANWÄLTE PART.MBB // WILHELMSHÖHER ALLEE 23 // 34117 KASSEL

SACHBEARBEITER:
RA Roland Wille

AKTENZEICHEN:

DATUM:

Datenschutz, Kontrolle und Überwachung am Arbeitsplatz

- Was müssen Arbeitgeber ab 25.05.2018 beachten! -

Skript zum Vortrag 06.03.2018
Beschäftigtendatenschutz
Creditreform Kassel

RA Roland Wille
- Fachanwalt für Arbeitsrecht -

www.wille-rechtsanwaelte.de

WILLE RECHTSANWÄLTE PARTNERSCHAFT MBB
WILHELMSHÖHER ALLEE 23
34117 KASSEL
TEL.: 0561 / 70 97 5 0
0561 / 70 97 5 10
FAX: 0561 / 70 97 5 90
INFO@WILLE-RECHTSANWAELTE.DE
WWW.WILLE-RECHTSANWAELTE.DE

ROLAND WILLE
RECHTSANWALT UND FACHANWALT FÜR ARBEITSRECHT

DR. ANDREAS NODOUSHANI
RECHTSANWALT UND FACHANWALT FÜR BAU- UND ARCHITEKTENRECHT HANDELS- UND GESELLSCHAFTSRECHT

ANNI DEMUTH
RECHTSANWÄLTIN UND FACHANWÄLTIN FÜR FAMILIENRECHT UND FÜR MEDIZINRECHT

CARSTEN HAHN*
RECHTSANWALT UND FACHANWALT FÜR BAU- UND ARCHITEKTENRECHT

HARDY BUSSE*
RECHTSANWALT UND FACHANWALT FÜR ARBEITSRECHT

OLIVER DEMUTH*
RECHTSANWALT

*RECHTSANWALT IM ANGESTELLTENVERHÄLTNIS

PARTNERSCHAFT MBB
AG FRANKFURT A.M. PR 2355

Raiffeisenbank eG Baunatal (BIC: GENODEF1BTA) IBAN: DE26 5206 4156 0000 6764 70
Commerzbank Kassel (BIC: COBADEFFXXX) IBAN: DE87 5204 0021 0290 0090 00
Kasseler Sparkasse (BIC: HELADEF1KAS) IBAN: DE78 5205 0353 0000 1150 34

Gliederung

Datenschutz, Kontrolle und Überwachung am Arbeitsplatz

- Was müssen Arbeitgeber ab 25.05.2018 beachten! -

I. Überblick

1. EU-Datenschutz-Grundverordnung (DS-GVO)

Ab dem 25. Mai 2018 erlangt die EU-Datenschutz-Grundverordnung (DS-GVO) innerhalb der EU und damit auch in Deutschland Geltung. Die DS-GVO regelt als unmittelbar in den EU-Staaten anzuwendendes EU-Recht umfassend den Verbraucher- und Beschäftigtendatenschutz.

2. Öffnungsklausel der DS-GVO für den Beschäftigtendatenschutz

Die DS-GVO ermöglicht den EU-Mitgliedstaaten im Rahmen der Öffnungsklausel des Art. 88 DS-GVO die Möglichkeit durch nationale Rechtsvorschriften oder durch Kollektivvereinbarung spezifischere Vorschriften zum Beschäftigtendatenschutz zu regeln.

Von dieser Regelungskompetenz hat der deutsche Gesetzgeber Gebrauch gemacht mit der Novellierung des Bundesdatenschutzgesetzes (BDSG), welches gleichfalls mit Wirkung vom 25.05.2018 in seiner Neufassung (BDSG 2018) Geltung beansprucht.

3. Kollisionsregelungen zwischen DS-GVO und BDSG 2018

Nach § 1 Abs. 5 BDSG 2018 ist das BDSG nur insoweit anzuwenden, wenn nicht bereits unmittelbar eine entsprechende Regelung der DS-GVO unmittelbar gilt. Es gilt daher folgende Stufenfolge:

a) Regelung in DS-GVO ohne Öffnungsmöglichkeit für Mitgliedsstaaten
= unmittelbare Geltung der DS-GVO.

b) Regelungsgegenstand in DS-GVO mit Öffnungsklausel für Mitgliedsstaaten
= hier ist zu prüfen, ob der deutsche Gesetzgeber spezifischere Regelungen (z. B. im BDSG 2018) getroffen hat. Wenn ja, gelten diese nationalen, spezielleren Regelungen, beispielsweise des BDSG 2018. Wenn nein, gelten die Grundsätze des Regelungsbereichs der DS-GVO.

c) Fehlende Regelung in DS-GVO
= hier gelten weiterhin die gesetzlichen Regelungen auf nationaler Ebene, d. h. beispielsweise des BDSG in seiner jeweils gültigen Fassung, aber auch des TMG

(Telemediengesetz), TKG (Telekommunikationsgesetz), UWG (Gesetz gegen unlauteren Wettbewerb) oder auch des StGB (Strafgesetzbuch).

d) Kollektivrechtliche Vereinbarungen

= diese gelten kollektivrechtlich fort, sind aber auf Aktualisierungs- und Anpassungsbedarf im Hinblick auf die am 25.05.2018 geltenden Regelungen zum Beschäftigtendatenschutz zu überprüfen.

e) Übergeordnete Rechtsgrundsätze

= übergeordnete Rechtsgrundsätze, beispielsweise aus Art. 1, 2 GG (Grundgesetz) sowie Art. 8 der EMK (Europäische Menschenrechtskonvention) gelten unbeschadet der DS-GVO und einfach nationaler Gesetze fort und stehen weiterhin über bzw. neben den Neuregelungen der DS-GVO und des BDSG.

II. Allgemeine Datenschutzregelungen nach der DS-GVO/BDSG (2018)

1. Datenschutz als Grundrecht (Verbot mit Erlaubnisvorbehalt)

a) Artikel 8 EMK „Recht auf Achtung des Privat- und Familienlebens"

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

b) Artikel 16 AEUV (Vertrag über die Arbeitsweise der Europäischen Union)

Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

c) Artikel 1, 2 GG (Grundgesetz)

Art. 1 GG: Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlicher Gewalt (...).

Art. 2 GG: Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit (...).

Zwischenfazit:

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollen gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsortes gewahrt bleiben.

Die DS-GVO soll damit zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarktes sowie zum Wohlergehen natürlicher Personen beitragen (Art. 1 DS-GVO).

Aus diesen Grundsätzen des Anspruchs jeder natürlichen Person auf den Schutz seiner persönlichen Daten folgt das sog. Verbot der Datenverarbeitung mit Erlaubnisvorbehalt.

Beachte: Personenbezogene Datenverarbeitung ist verboten – es sei denn sie ist erlaubt.

2. Kernelemente der DS-GVO (Art. 5)

Kernelemente der DS-GVO sind

- **Rechtmäßigkeit:** Besteht eine Ermächtigungsgrundlage für die Datenverarbeitung?!
- **Zweckbindung:** Während der gesamten Dauer der Datenverarbeitung ist deren Erforderlichkeit und Verhältnismäßigkeit am Datenerhebungs- oder Nutzungszweck zu messen.
- **Transparenz:** Die Verarbeitung personenbezogener Daten muss für den Betroffenen nachvollziehbar und er hierüber informiert sein.
- **Datenminimierung:** Die Datenverarbeitung ist auf das notwendige Maß zu beschränken.
- **Richtigkeit:** Die verantwortlichen Unternehmen müssen für die Korrektheit der Daten sorgen, d. h. unrichtige Daten unverzüglich löschen oder berichtigen.
- **Integrität und Vertraulichkeit:** Daten müssen durch technische und organisatorische Maßnahmen vor unbefugter Verarbeitung, Zerstörung, Veränderung oder Verlust geschützt werden.
- **Speicherbegrenzung:** Personenbezogene Daten dürfen nur solange gespeichert werden, wie es für den Zweck (Zweckbindung) erforderlich ist.
- **Rechenschaftspflicht:** Wer personenbezogene Daten verarbeitet, ist gegenüber den betroffenen Rechteinhaber sowie den Aufsichtsbehörden zur Rechenschaft verpflichtet.

3. Sanktionsandrohung durch Bußgelder

Nach Art. 83 DS-GVO sollen die Aufsichtsbehörden sicherstellen, dass die Geldbußen für Verstöße „in jedem Fall wirksam, verhältnismäßig und abschreckend" sind.

Deshalb steigt gegenüber dem bisherigen Bußgeldrahmen im BDSG a. F. von € 300.000,00 der Bußgeldrahmen der DS-GVO auf bis zu 20 Mio. Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes des zu sanktionierenden Unternehmens.

Hierdurch soll eine abschreckende Wirkung auch für global in Deutschland agierende Konzerne (Facebook, Google & Co.) erreicht werden. Es bleibt abzuwarten, wie der Grundsatz der „Verhältnismäßigkeit" bei der Bußgeldbemessung gegenüber mittelständischen Unternehmen in der Praxis durch die Aufsichtsbehörden (Datenschutzbeauftragte der Länder) angewendet wird.

4. Anwendungsbereich

Unter die Regelung der DS-GVO fällt jedes Unternehmen (auch außerhalb der EU), welches personenbezogene Daten von EU-Bürgern verarbeitet. Hierbei ist unerheblich, ob die personenbezogenen Daten elektronisch oder körperlich, z. B. auf Karteikarten oder Papier, verarbeitet werden.

Es gilt insoweit das „Marktortprinzip", wonach die DS-GVO für alle Unternehmen gilt, die Leistungen für EU-Bürger anbieten und in diesem Zusammenhang deren personenbezogenen Daten „verarbeiten".

5. Was sind personenbezogene Daten?

Als „personenbezogene Daten" gelten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen" (Art. 4 Nr. 1 DS-GVO). Als identifizierbar ist jede Kennzeichnung oder Zuordnung zu verstehen, mit der eine bestimmte natürliche Person hinsichtlich ihrer persönlichen Merkmale identifiziert werden kann.

Beachte: Ist mit objektiv verfügbaren Mitteln herausfindbar, um wen es sich bei der Datenverarbeitung handelt, besteht ein Personenbezug.

6. Begriff der „Verarbeitung" von Daten

Der Begriff der „Verarbeitung" ist weit gefasst und beinhaltet letztlich jede Art des Umgangs mit personenbezogenen Daten, von der Erfassung und Erhebung über die Speicherung und Verwendung bis zur Löschung oder Vernichtung.

7. Rechenschaftspflicht – Verzeichnis von Verarbeitungstätigkeiten (VvV)

Unternehmen, die personenbezogene Daten verarbeiten, sind verpflichtet, die Einhaltung der DS-GVO nachzuweisen. Dies führt sowohl gegenüber den betroffenen Personen, deren Daten verarbeitet werden, als auch gegenüber den Aufsichtsbehörden (Landesdatenschutzbeauftragte) zu verstärkten Dokumentations- und Nachweispflichten.

Unabhängig von der Unternehmensgröße ist Rechenschaft über die Beachtung der Grundsätze der Datenverarbeitung (Art. 5 DS-GVO) abzulegen, einschließlich eines entsprechenden Auskunftsanspruchs seitens der betroffenen natürlichen Person, deren Daten verarbeitet werden.

Insbesondere ist hierbei die Rechtmäßigkeit und damit das Bestehen einer rechtlichen Ermächtigungsgrundlage für die Datenverarbeitung zu beachten.

Zur Erfüllung der Rechenschafts- und Dokumentationspflicht ist grundsätzlich ein **„Verzeichnis aller Verarbeitungstätigkeiten"** mit personenbezogenen Daten zu führen. Hierbei gilt das

Grundprinzip, dass jeder Verantwortliche und Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses verpflichtet ist, sofern er nicht von der Verpflichtung ausgenommen ist.

Verantwortlicher ist hierbei jeder für die Datenverarbeitung Verantwortliche, also Unternehmen, Freiberufler, Vereine etc..

Auftragsverarbeiter ist derjenige, der ohne eigenen Einfluss auf die Daten beispielsweise im Rahmen eines Dienstleistungsvertragsverhältnisses (z. B. für die Lohnbuchhaltung oder als externer IT-Dienstleister) personenbezogene Daten für den Verantwortlichen weisungsgebunden weiter verarbeitet.

Ausnahme (Art. 30 Abs. 5 DS-GVO):

Arbeitgeber mit weniger als 250 Mitarbeitern müssen kein Verzeichnis aller Verarbeitungstätigkeiten (VvV) führen. Diese Ausnahme gilt allerdings nur, soweit das „Kleinunternehmen"

- die Datenverarbeitung nur gelegentlich vornimmt (z. B. zu Zwecken der Lohnbuchhaltung),
- oder keine besonders sensitiven Daten gemäß Art. 9 Abs. 1 DS-GVO erhebt (z. B. Religionsdaten, Gewerkschaftszugehörigkeit, Gesundheitsdaten usw.) oder strafrechtliche Verurteilungen und Straftaten erfasst,
- oder aufgrund der Verarbeitung personenbezogener Daten keine besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen (z. B. aufgrund regelmäßig oder ständig durchgeführter Überwachungsmaßnahmen, wie beispielsweise ständige Videoüberwachung oder Scoring über EDV-gestützte Datenauswertung).

Problem in der Praxis: Trotz Befreiung von der Verpflichtung zur Führung eines „Verzeichnisses aller Verarbeitungstätigkeiten" bleibt die Rechenschaftspflicht und Nachweispflicht bestehen, dass die Datenverarbeitung unter Einhaltung der Vorgaben der DS-GVO im Übrigen erfolgt.

Praxistipp: Im Zweifel dürfte sich zur Erfüllung dieser Rechenschaftspflicht und bestehender Ermächtigungsgrundlagen für die Datenverarbeitung die „freiwillige" Führung eines Verzeichnisses der Verarbeitungstätigkeiten (Mindeststandard) empfehlen, vergleichbar des aus dem BDSG a. F. bekannten Verfahrensverzeichnisses (§ 4 g Abs. 2, 2 a BDSG a. F. „Übersicht").

8. Inhalt des Verzeichnisses von Verarbeitungstätigkeiten (VvV)

Die Zuständigkeit für die Führung eines „freiwilligen" oder verpflichtenden VvV liegt bei „dem Verantwortlichen", also der Geschäftsführung/Vorstand/Inhaber des Unternehmens bzw. der Körperschaft.

Beim VvV handelt es sich um eine Aufstellung der Verfahrensbeschreibungen aller im Unternehmen eingesetzten datenschutzrechtlich relevanten Verfahren und Abläufe.

Unter Verfahren ist dabei die Gesamtheit an Verarbeitungstätigkeiten zu verstehen, mit denen eine oder mehrere miteinander verbundenen Zweckbestimmungen realisiert werden sollen.

Beachte: Ein IT-System (z. B. Server, Software etc.) ist kein Verfahren, sondern lediglich ein Mittel (Tool, Application), um eine Verarbeitung durchzuführen.

Achtung: Das „Verzeichnis von Verarbeitungstätigkeiten" ist auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung zu stellen. Aufsichtsbehörde für den Datenschutz sind die Datenschutzbeauftragten der Länder (Ausnahme Bayern).

Praxistipp: Bestehen bislang keinerlei betriebliche Erfahrungen mit einer bisherigen „Übersicht" über die Verarbeitungstätigkeiten und den Anforderungen an die Erstellung eines „Verzeichnisses der Verarbeitungstätigkeiten" empfiehlt sich die Hinzuziehung externer Sachverständiger für Datenschutz; zumindest bei der erstmaligen Errichtung des VvV.

9. Auftragsverarbeitung von Daten für den Verantwortlichen durch Dritte

Die aus dem BDSG a. F. bekannte „Auftragsdatenverarbeitung" heißt begrifflich nach der DS-GVO und dem BDSG 2018 nunmehr ***„Auftragsverarbeitung"***.

Definition: Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

Kennzeichen hierfür ist die weisungsabhängige Datenverarbeitung im Auftrag für den Verantwortlichen im Sinne einer „verlängerten Werkbank".

Beispiele:

- Externe Lohnbuchhaltung und Abrechnungserstellung,
- externer IT-Dienstleister,
- Werbeadressenverarbeitung durch Dritte,
- Auslagerung des eigenen Telekommunikationsanlagenbetriebes (Problem: Cloud-Computing),
- Datenträgerentsorgung und Aktenvernichtung mit personenbezogenen Dateninhalt,
- Erhebung von Personaldaten im Rahmen einer Mitarbeiterbefragung durch Fremdfirma.

Beachte: Keine Auftragsverarbeitung ohne Vertrag!

Zwingend ist zwischen dem Verantwortlichen und dem Auftragsverarbeiter ein schriftlicher Vertrag zu schließen, in dem Rechte und Pflichten (insbesondere Sorgfaltspflichten des Dritten) sowie Maßnahmen zur Sicherstellung der Einhaltung der Pflichten geregelt sind.

Achtung: Neu ist die umfassende Haftung des Auftragsverarbeiters neben dem Verantwortlichen, in dessen Auftrag die Datenverarbeitung erfolgt; einschließlich der Möglichkeit einer gesamtschuldnerischen Haftung beider (Art. 32 DS-GVO).

10. Datenschutzbeauftragte/r

a) Bisherige Rechtslage (§§ 4 d, f BDSG a. F.)

Bereits bislang mussten solche Daten(auftrags)verarbeiter (z. B. Unternehmen, Freiberufler, Vereine usw.) einen Datenschutzbeauftragten bestellen, sofern sie

- personenbezogene Daten geschäftsmäßig verarbeiten,
- oder automatisierte Verarbeitungen vornehmen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen,
- oder mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind,
- oder mindestens 20 Personen mit der Verarbeitung, Nutzung oder Erhebung personenbezogener Daten auf andere Weise (manuelle Verfahren) beschäftigt sind.

b) Rechtslage ab 25.05.2018 (Art. 37-39 DS-GVO)

Nach der ab 25.05.2018 geltenden Rechtslage hat der Verantwortliche/Auftragsverarbeiter einen Datenschutzbeauftragten zu benennen, **wenn**

- im Unternehmen mindestens 10 Personen regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind,
- oder personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für die Zwecke der Markt- und Meinungsforschung verarbeitet werden,
- oder die Hauptaufgabe des Unternehmens in einer umfangreichen Verarbeitung besonderes sensitiver Datenkategorien (z. B. Gesundheitsdaten, strafrechtliche Verurteilungen etc.) besteht.

c) „Person" des Datenschutzbeauftragten

Grundsätzlich kann sowohl ein interner Mitarbeiter/in zum Datenschutzbeauftragten bestellt werden oder sich hierbei eines externen Dienstleisters oder externen Datenschutzbeauftragten bedient werden.

Zu beachten ist, dass der Datenschutzbeauftragte über eine angemessene berufliche Qualifikation und entsprechendes Fachwissen im Bereich Datenschutzrecht und Datenschutzpraxis verfügen muss und darüber hinaus (insbesondere als interner DSB) zeitlich und hinsichtlich seiner Zugriffsrechte zur tatsächlichen Kontrolle des betrieblichen Datenschutzes in der Lage sein muss.

Beachte: Der Datenschutzbeauftragte (DSB) genießt, wie bisher, besonderen Kündigungsschutz (§§ 6 Abs. 4, 38 Abs. 3 BDSG 2018). Dies jedenfalls dann, soweit eine Pflicht zur Bestellung des Datenschutzbeauftragten besteht.

Beachte: Erfolgt die Bestellung zum DSB nicht nur zeitlich befristet, stellt die Bestellung eine Arbeitsvertragsänderung dar, in deren Folge der Widerruf der Bestellung nur im Wege der Änderungskündigung und gemessen an deren Anforderungen möglich ist.

Praxistipp: Im Hinblick auf die unabhängig wahrzunehmenden Aufgaben, den besonderen Kündigungsschutz und die gesteigerten Haftungsrisiken nicht gesetzeskonformer Datenverarbeitung sprechen viele Argumente für das „Outsourcing" des Datenschutzbeauftragten auf einen externen DSB.

Hinweis: Folgende Personen können aufgrund möglichen Interessenkonfliktes nicht zum Datenschutzbeauftragten bestellt werden:

- Unternehmensinhaber/GF/Vorstand,
- Leiter IT-Abteilung, Leiter Personalabteilung, Leiter Rechtsabteilung,
- externe Rechtsanwälte, Steuerberater oder Wirtschaftsprüfer, sofern sie bereits in dieser Funktion für das Unternehmen tätig sind.

Besteht im Rahmen einer Unternehmensgruppe eine **„Konzernstruktur"**, besteht grundsätzlich die Möglichkeit für solche Unternehmensgruppen, einen gemeinsamen Datenschutzbeauftragten im Sinne eines **„Konzerndatenschutzbeauftragten"** zu bestellen. Voraussetzung hierfür ist, dass er von jeder Niederlassung aus leicht erreicht werden kann und die jeweiligen unternehmensbezogenen Aufgaben eines Datenschutzbeauftragten tatsächlich erfüllen kann.

Beachte: Auch im Konzern oder der Struktur einer Unternehmensgruppe bedarf die Übermittlung und Verarbeitung personenbezogener Daten innerhalb unterschiedlicher Unternehmen einer jeweiligen Rechtsgrundlage.

Hinweis: Besteht die Verpflichtung zur Benennung eines Datenschutzbeauftragten, sind dessen Kontaktdaten im Unternehmen und nach außen (z. B. Homepage) zu veröffentlichen und (unaufgefordert) der zuständigen Aufsichtsbehörde für den Datenschutz (z. B. Datenschutzbeauftragte der Länder) mitzuteilen.

11. Verletzung des Schutzes personenbezogener Daten

Definition: Die Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der (Daten-) Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Der Verantwortliche muss eine Verletzungshandlung des Schutzes personenbezogener Daten unaufgefordert und unverzüglich an die Aufsichtsbehörde melden (Art. 33 Abs. 1 DS-GVO).

Unterlässt der Verantwortliche die Meldung, droht ein erhebliches Bußgeld. Dies gilt auch dann, wenn die Verletzungshandlung nicht zu einem nachweisbaren Schaden für betroffene Personen geführt hat (Art. 83 DS-GVO).

Praxistipp: Stellen Sie als Verantwortlicher eine Verletzungshandlung des Schutzes personenbezogener Daten fest, ist diese nicht „unter den Teppich zu kehren", sondern der Aufsichtsbehörde unverzüglich zu melden.

Daneben ist vom Verantwortlichen bei einer Verletzungshandlung zugleich zu prüfen, ob „voraussichtlich ein hohes Risiko für die Verletzung persönlicher Rechte und Freiheiten" der betroffenen Person/en prognostisch besteht. Ist von einem entsprechend hohen Risiko auszugehen, ist gleichfalls der/die betroffene Person/en ebenfalls über die Verletzungshandlung zu informieren (Art. 34 Abs. 1 DS-GVO). Diese Information muss in „klarer und einfacher Sprache die Art der Verletzung und des Schutzes personenbezogener Daten" beschreiben. Darüber hinaus ist der Betroffene über folgendes zu informieren:

- Namen und Kontaktdaten des Datenschutzbeauftragten oder der sonstigen Anlaufstelle,
- Beschreibung der wahrscheinlichen Folgen der Verletzungen des Schutzes personenbezogener Daten,
- Beschreibung der vom Verantwortlichen ergriffenen Maßnahmen zur Behebung oder Abmilderung der Folgen der Verletzungshandlung.

III. Beschäftigtendatenschutz im Arbeitsverhältnis

1. Rechtmäßigkeit der Datenverarbeitung (Art. 6 DS-GVO)

Für die Rechtmäßigkeit der Datenverarbeitung bedarf es einer Rechts- oder Ermächtigungsgrundlage. Dieser bedarf es sowohl für die Datenerhebung dem Grunde nach, als auch insbesondere für den inhaltlichen und zeitlichen Umfang der Datenverarbeitung infolge des Grundsatzes „Verbot mit Erlaubnisvorbehalt".

Nach Art. 6 DS-GVO ist die Verarbeitung nur rechtmäßig, wenn mindestens **eine** der nachstehenden Bedingungen erfüllt ist:

a) Einwilligung
b) Zweck einer Vertragserfüllung/vorvertraglichen Maßnahme
c) Erfüllung einer rechtlichen Pflicht des Verantwortlichen
d) Schutz lebenswichtiger Interessen
e) Aufgaben im Bereich der öffentlichen Sicherheit
f) Wahrung berechtigter Interessen, unter Berücksichtigung der Erforderlichkeit und der Abwägung der Verhältnismäßigkeit.

a) Einwilligung

Völlig neue Anforderungen werden an die Einwilligung gestellt. Diese ist auf Basis der DS-GVO nur dann wirksam, wenn

- sie freiwillig abgegeben wird, d. h. ohne Zwang oder Druck, wie beispielsweise im Zusammenhang mit einem Arbeitsvertragsschluss;
- sie für einen transparent dargestellten hinreichend bestimmten (konkretisierten) Fall oder Zweck abgegeben wird;
- der Einwilligende klar und verständlich über den konkreten Zweck und die Erforderlichkeit der Datenverarbeitung informiert wurde;
- eine Information über das jederzeitige (grundlose) Widerrufsrecht enthalten ist;
- eine eindeutig bestätigende Handlung durch den Einwilligenden vorliegt, z. B. in einer schriftlichen Erklärung oder bei Erklärungen im Internet nach dem sog. „Opt-In-Verfahren".

b) Zweck einer Vertragserfüllung

Personenbezogene Daten dürfen verarbeitet werden, soweit sie zur Erfüllung eines Vertrages notwendig sind. Sind beispielsweise für die Abwicklung eines Kaufvertrages die persönlichen Kontaktdaten, einschließlich der Bankverbindung oder für einen Vertragsschluss die Geschäftsfähigkeit erforderlich, dürfen zur Vertragsabwicklung die jeweiligen personenbezogenen Daten erhoben und verarbeitet werden.

c) Erfüllung einer rechtlichen Pflicht des Verantwortlichen

Soweit der Verantwortliche selbst eine rechtliche Pflicht zu erfüllen hat, für die die Erhebung und Verarbeitung personenbezogener Daten erforderlich ist, so ist die Datenverarbeitung rechtmäßig.

Insofern darf der Arbeitgeber für den Abschluss eines Arbeitsvertrages alle personenbezogenen Daten abfragen, die für die ordnungsgemäße sozialversicherungsrechtliche und lohnbuchhalterische sowie steuerrechtliche Anmeldung und Erfassung erforderlich sind. Dies schließt das Geburtsdatum, die Bankverbindung und soweit der Mitarbeiter kirchensteuerpflichtig ist, auch die Zugehörigkeit zu einer steuerlich zu erfassenden Religionsgemeinschaft ein.

d) Wahrung berechtigter Interessen des Verantwortlichen

Personenbezogene Daten dürfen auch zur Wahrung der rechtlichen Interessen des Verantwortlichen verarbeitet werden, sofern nicht demgegenüber die Interessen der betroffenen Person dagegenstehen und überwiegen. Bei dieser Interessenabwägung ist auf die vernünftigen Erwartungen einer betroffenen Person abzustellen.

2. Regelung der Datenverarbeitung durch Kollektivvereinbarungen

Mit Art. 88 DS-GVO und § 26 BDSG (2018) sind erstmals Regelungen gesetzlich aufgenommen worden, wonach die Rechtmäßigkeit einer Datenverarbeitung (auch) auf eine Kollektivvereinbarung (Betriebsvereinbarung/Dienstvereinbarung) gestützt werden kann.

Achtung: Kollektivrechtliche Vereinbarungen im Zusammenhang mit der Verarbeitung personenbezogener Daten von Arbeitnehmern dürften in der Regel der echten Mitbestimmung nach § 87 BetrVG unterliegen (z. B. § 87 Abs. 1 Nr. 6 BetrVG).

Praxistipp: Soweit für technische Überwachungseinrichtungen bislang im Betrieb noch keine Kollektivvereinbarungen bestehen (z. B. für offene Videoüberwachung), ist der Abschluss einer entsprechenden Betriebs- oder Dienstvereinbarung nunmehr für Arbeitgeber dringend empfehlenswert.

Beachte: Auch Betriebsvereinbarungen dürfen nicht gegen das Grundrecht der freien Entfaltung der Persönlichkeit und das allgemeine Persönlichkeitsrecht verstoßen (§ 75 Abs. 2 BetrVG; Art. 2 Abs. 1 GG).

3. Begriff der „Beschäftigten“

Der Begriff des „Beschäftigten“ umfasst gemäß § 26 Abs. 8 BDSG (2018):

- Stellenbewerber und Personen, deren Beschäftigungsverhältnis beendet ist,
- Arbeitnehmer einschließlich Leiharbeitnehmer im Verhältnis zum Entleiher,
- Auszubildende im Sinne des BBiG,
- Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben oder zur Arbeitserprobung,
- in Behindertenwerkstätten Beschäftigte,
- Freiwillige nach dem Bundesfreiwilligendienstgesetz/Jugendfreiwilligendienstgesetz,
- in Heimarbeit Beschäftigte oder ihnen Gleichgestellte sowie Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnlich anzusehen sind,
- Beamte, Richter und Soldaten sowie Zivildienstleistende.

IV. Einzelfragen vom BEM bis Videoüberwachung

1. Betriebliches Eingliederungsmanagement (BEM)

Erkrankt ein Arbeitnehmer innerhalb von 12 Monaten länger als sechs Wochen ununterbrochen oder wiederholt, ist der Arbeitgeber unter Beteiligung des Betriebsrates verpflichtet, ein betriebliches Eingliederungsmanagement (BEM) durchzuführen (§ 167 Abs. 2 SGB IX – vormals § 84 Abs. 2 SGB IX).

Hierin ist zu klären, wie die Arbeitsunfähigkeit möglichst überwunden werden kann und mit welchen Leistungen oder Hilfen erneute Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz

erhalten werden kann. Bei schwerbehinderten Menschen kann ggf. das Integrationsamt eingeschaltet werden und Unterstützungsleistungen gewähren.

Die im BEM-Verfahren erhobenen personenbezogenen Daten unterliegen einer strengen Zweckbindung und dürfen daher nicht anderweitig vom Arbeitgeber „verwertet" werden, z. B. zur Vorbereitung einer personenbedingten Kündigung (Art. 5 b DS-GVO).

Damit sind erhöhte Anforderungen an das BEM-Verfahren gestellt, um die Datenschutzvorgaben einzuhalten.

Hiernach gilt zu beachten:

a)

Der/Die Betroffene ist umfassend über Sinn, Zweck und Erforderlichkeit des BEM und der hierzu erhobenen Daten zu informieren und muss in die Durchführung des BEM und eine damit verbundene Datenverarbeitung ausdrücklich einwilligen. Hierbei ist auf das jederzeitige Widerrufsrecht hinzuweisen und bei Einbeziehung des Betriebsrates vom Betroffen auch in dessen Einbeziehung einzuwilligen.

b)

BEM-Akten sind getrennt von den sonstigen Personalakten zu führen und ggf. einer durch BV/DV eingerichteten BEM-Stelle zuzuweisen.

c)

Aufgrund der ohnehin verpflichtenden Einbeziehung des Betriebsrates empfiehlt sich der Abschluss einer BV/DV für die Durchführung des BEM-Verfahrens.

d)

Der Arbeitgeber ist gehalten und berechtigt, auch gegen den Willen des Betroffenen diejenigen Daten zum BEM-Verfahren selbst zu verwahren (oder in der Personalakte zu führen), die der Arbeitgeber benötigt, um die ordnungsgemäße Durchführung eines BEM-Verfahrens in einem späteren Kündigungsschutzprozess dokumentieren zu können.

2. Überwachung E-Mail-Account/Handynutzung

Hat der Arbeitgeber die private Nutzung des dienstlichen E-Mail-Accounts sowie eines etwaigen Diensthandys gestattet, bedarf der Zugriff auf den E-Mail-Account oder die Handynutzungsdaten des Betroffenen einer ausdrücklichen Einwilligung. Dies folgt aus dem Schutz der Vertraulichkeit der persönlichen Daten im Rahmen privater Kommunikationsdaten.

Anderenfalls kann beim Arbeitgeberzugriff, z. B. bei Abwesenheit des Arbeitnehmers, auf den E-Mail-Account und die Handynutzungsdaten sowohl eine Verletzungshandlung nach den

Datenschutzbestimmungen der DS-GVO/BDSG vorliegen, als auch eine Verletzungshandlung nach dem TMG (Telemediengesetz), dem TKG (Telekommunikationsgesetz) und ggf. sogar nach § 203 StGB (Verletzung Fernmeldegeheimnis).

Praxistipp: Will der Arbeitgeber ohne gesonderte Einwilligung auf den dienstlichen E-Mail-Account von Mitarbeitern beispielsweise bei Abwesenheit zugreifen, ist die private Mitnutzung des dienstlichen E-Mail-Accounts strikt zu untersagen.

Hinweis: Ein ständiger Überwachungsdruck, z. B. durch Mitlesen („Key-Logger") ist als Persönlichkeitsrechtsverletzung gleichwohl unzulässig (BAG vom 27.07.2017 - 2 AZR 681/16 -).

3. Internetnutzung

Ohne konkreten und begründeten Verdacht einer Straftat oder einer schweren arbeitsvertraglichen Pflichtverletzung ist der Arbeitgeber nicht berechtigt, Aufzeichnungen und Speicherungen der Tastatureingaben eines Arbeitnehmers am dienstlichen Computer (z. B. mit Hilfe eines „Key-Loggers") vorzunehmen (s. o. BAG vom 27.07.2017).

Praxistipp: Sowohl aufgrund der Anforderungen an den Arbeitgeber als „Verantwortlichen" für die Sicherstellung der Datensicherheit, als auch im Hinblick auf Grenzfragen dazu, ob ein Arbeitgeber selbst „Telekommunikationsanbieter" wird, wenn er seinen Beschäftigten die private Mitnutzung dienstlicher Telekommunikationsmedien ermöglicht, empfiehlt sich die Privatnutzung des Internets mit dienstlich gestellten Arbeitsmitteln (PC, Tablet, Handy, etc.) ausdrücklich zu untersagen.

4. Fotonutzung und Geburtsdaten

Auch die betriebsinterne und erst recht nach außen öffentliche Nutzung von persönlichen Mitarbeiterdaten, wie beispielsweise Fotos und Geburtsdaten bedürfen der Einwilligung des Betroffenen (mit jederzeitiger Widerrufsmöglichkeit).

5. Mitarbeiterumfragen

Für Mitarbeiterumfragen durch den Arbeitgeber gilt, dass Freiwilligkeit und eine Einwilligung des Betroffenen vorliegen muss (Art. 7, 13 DS-GVO).

Da bei nicht anonymisierten Mitarbeiterumfragen ein „Beteiligungsdruck" nie ganz auszuschließen ist, welcher der tatsächlichen Freiwilligkeit entgegensteht, ist anonymen Mitarbeiterumfangreichen der Vorzug zu geben.

Diese müssen allerdings bei Befragung einzelner Mitarbeitergruppen sicherstellen, dass keine Identifizierbarkeit einzelner Mitarbeiter aufgrund geringer Gruppengröße möglich sind. In der Regel setzt dies Befragungsgruppen von jedenfalls mehr als fünf Personen (beispielsweise einer Abteilung) voraus.

Beachte: Führt ein externer Dienstleister die Mitarbeiterbefragung durch, liegt ein Fall der Auftragsverarbeitung vor, für die ein entsprechender Vertrag zur Einhaltung der Datenschutzbestimmungen erforderlich ist.

6. Videoüberwachung offen

Videoüberwachung greift grundsätzlich besonders tief in das Persönlichkeitsrecht ein. Neben dem Maßstab der Zweckbindung, Erforderlichkeit und Verhältnismäßigkeit unterliegen daher Videoüberwachungsmaßnahmen einer vom Verantwortlichen vorab durchzuführenden „Datenschutz-Folgenabschätzung" (DSFA gemäß Art. 35 DS-GVO). Diese „ersetzt" die frühere Vorabkontrolle nach dem BDSG a. F..

Die offene Videoüberwachung ist als präventive Schutzmaßnahme zusätzlich am Maßstab der Erforderlichkeit nach § 26 Abs. 1 S. 1 BDSG (2018) zu messen.

Die Videoüberwachung ist daher räumlich und zeitlich sowie hinsichtlich ihrer technischen Ausgestaltung auf einem verhältnismäßig angemessenen Schutzzweck zu beschränken und ggf. Schutzmaßnahmen zu ergreifen, die einem „ständigen Überwachungsdruck" entgegenstehen.

Beachte: Insbesondere eine permanente Livebild-Auswertung erzeugt regelmäßig einen unangemessenen Überwachungsdruck.

Praxistipp: Zeitlich begrenze Aufzeichnung und Speicherung ohne Bildauswertung mit automatischer Löschung nach 48/72 Stunden, soweit kein konkreter Verdacht auf Straftat oder schwere Pflichtverletzung vorliegt.

Hinweis: Die offene Videoüberwachung muss für Beschäftigte und Dritte bei Zutritt in den Überwachungsbereich offen kenntlich gemacht werde (z. B. Hinweisschild).

Achtung: Die technische Überwachung höchstpersönlicher Lebensbereiche (Duschen, Toiletten, Sozialräume) ist generell unzulässig.

Praxistipp: Zur „Verbreiterung" der Ermächtigungsgrundlage empfiehlt sich für die Einführung und Ausgestaltung offener Videoüberwachung auf dem Unternehmensgelände der Abschluss einer Betriebsvereinbarung/Dienstvereinbarung.

7. Videoüberwachung verdeckt

Die verdeckte Videoüberwachung ist zusätzlich am Maßstab des § 26 Abs. 1 S. 2 BDSG (2018) zu messen. Hiernach müssen folgende Voraussetzungen erfüllt sein:

- Es müssen tatsächliche (konkrete) Anhaltspunkte für den Verdacht einer Straftat aufgrund dokumentierter Anhaltspunkte vorliegen;
- zusätzlich muss sich der Verdacht auf eine bestimmte oder eingrenzbar mehrere bestimmte Personen beziehen;
- zusätzlich muss die verdeckte Videoüberwachung erforderlich, angemessen und verhältnismäßig sein; d. h. mildere Mittel müssen (erfolglos) zuvor ausgeschöpft sein;
- Umfang und Ausdehnung der verdeckten Videoüberwachung müssen gemessen am Maßstab der Verhältnismäßigkeit erforderlich und angemessen sein.

Beachte: Auch hier gilt, dass eine Live-Überwachung (Kamera-Monitor-Prinzip) im Regelfall einen besonders schwerwiegenden Persönlichkeitseingriff darstellt und daher einer besonderen Rechtfertigung hinsichtlich der Erforderlichkeit bedarf.

Hinweis: Für verdeckte Audioaufzeichnungen (Telefonmithören) gelten generell die gleichen Grundsätze wie für die verdeckte Videoüberwachung.

Impressum:

Urheber/Herausgeber:	Wille Rechtsanwälte Partnerschaft mbB, Wilhelmshöher Allee 23, 34117 Kassel, RA Roland Wille, Fachanwalt für Arbeitsrecht
Copyright:	Der Inhalt dieses Skriptes/Vortragsunterlage ist urheberrechtlich geschützt. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen.
Stand:	06.03.2018