EMPFEHLUNG ZUR REGELUNG DER TECHNISCHEN KONTROLLE UND ÜBERWACHUNG IM BESCHÄFTIGUNGSKONTEXT

VERFASSER

Dipl.-Jur. Falk Hagedorn

Das Projekt ist durch das Programm Grundrechte und Unionsbürgerschaft von der Europäischen Union kofinanziert.

DEZEMBER 2012

Content

ANMERKUNG: Die nachfolgenden Bestimmungen wurden im Rahmen des EU-Projektes „Datenschutz am Arbeitsplatz“[1] entwickelt.[2] Sie basieren auf dem „Universal code of conduct on the protection of personal data acquired through monitoring by technical means in employment context“ und *transformieren dessen Vorgaben in deutsches Recht.[3] Hierbei erheben sie keinen Anspruch auf Vollständigkeit, sondern dienen vielmehr als Anregung für die Erstellung von Betriebsvereinbarungen[4] oder allgemein für Leitlinien, die innerbetrieblich den Beschäftigtendatenschutz und insbesondere die Frage der Kontrolle und Überwachung von Beschäftigten ausgestalten.[5] Insofern ist der Anwender angehalten, aktuelle Entwicklungen - insbesondere im Datenschutzrecht und Arbeitsrecht - stetig zu verfolgen und in seinem Regelwerk umzusetzen. Es wird empfohlen, einen Ansprechpartner für den Beschäftigtendatenschutz zu benennen und diesen mit Befugnissen auszustatten, die der Förderung einer vorbildlichen Verwendung personenbezogener Beschäftigtendaten dient. Hiervon unberührt bleiben Stellung und Aufgaben bestellter Datenschutzbeauftragter.*

1. Hintergrund, Zielsetzung der Vereinbarung

1.1.

Die anhaltenden Veränderungen in der Informationstechnologie ziehen notwendigerweise auch Veränderungen in der Arbeitswelt und damit auch bei den dafür geschaffenen Bestimmungen zum Schutz personenbezogener Daten von Beschäftigten nach sich. Der Einsatz zeitgemäßer und leistungsfähiger IuK-Technik in Unternehmen wirft im Beschäftigungskontext eine Vielzahl von Fragestellungen auf, die bislang auf gesetzgeberischer Ebene nicht oder nur unzureichend geklärt wurden.

Abgesehen von einigen wenigen bereichsspezifischen Regelungen, bemisst sich der Schutz der personenbezogenen Daten von Beschäftigten in Deutschland derzeitig an den Vorgaben allgemeiner Gesetze wie etwa dem Bundesdatenschutzgesetz, dem Telekommunikationsgesetz, dem Telemediengesetz und dem Betriebsverfassungsgesetz.

---

[1] Weitere Informationen zum Projekt stehen Ihnen unter http://www.pawproject.eu zur Verfügung.

[2] Verfasser: Dipl.-Jur. Falk Hagedorn, Wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsrecht der Georg-August-Universität Göttingen, Lehrstuhl Prof. Dr. Wiebe, LL.M. (Bürgerliches Recht , Wettbewerbs- und Immaterialgüterrecht, Medien- und Informationsrecht).

[3] Die Bestimmungen des „Universal code of conduct on the protection of personal data acquired through monitoring by technical means in employment context“ wurden teilweise unter Berücksichtigung des „ILO Code of practice on the protection of worker’s personal data“ sowie insbesondere nach Maßgabe der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr *(Amtsblatt Nr. L 281 vom 23.11.1995, S. 31 - 50) geschaffen.*

[4] Eine Regelung mittels Betriebsvereinbarung bietet sich allein schon deshalb an, weil Arbeitgeber und Betriebsrat nach § 75 Abs. 2 S. 1 BetrVG eine Fürsorgepflicht trifft, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern.

[5] In Betrieben, in denen kein Betriebsrat besteht, hat der Arbeitgeber anderweitig die ausreichende Berücksichtigung der Rechte und Interessen der Beschäftigten bezüglich einer Verwendung derer personenbezogener Daten sicherzustellen.

Aufgrund der defizitären Rechtslage und dem hieraus erwachsenden Regelungs- und Verbesserungsbedarf besteht nach wie vor das praktische Bedürfnis, einerseits die Persönlichkeitsrechte der Beschäftigten zu schützen und anderseits dem Arbeitgeber die Wahrung seiner Rechte zu ermöglichen.

1.2.

Vor diesem Hintergrund verfolgt diese Vereinbarung das Ziel, für die Privatwirtschaft Vorgaben dafür zu schaffen, durch den Einsatz moderner IuK-Technik bereits bestehende oder drohende Spannungslagen im Arbeitsverhältnis interessengerecht aufzulösen.

Dementsprechend bezwecken die nachfolgenden Regelungen zum einen, Beschäftigte vor der unrechtmäßigen Verwendung ihren personenbezogenen Daten zu schützen. Zum anderen soll ebenso das Informationsinteresse des Arbeitgebers gewürdigt werden.

Die Vereinbarung schafft Rahmenbedingungen für ein Datenschutz-Managementsystem (DSMS), das Arbeitgebern die Verwendung personenbezogener Daten im Beschäftigungskontext ermöglicht. Gleichzeitig soll sie ermöglichen, unternehmensinterne Rahmenbedingungen zur Beurteilung der Konformität nebst möglicher Auditierung und Zertifizierung des DSMS des Arbeitgebers in Übereinstimmung mit den Vorgaben des „Universal code of conduct on the protection of personal data acquired through monitoring by technical means in employment context“ zu schaffen.

Die Vereinbarung trägt dem Umstand Rechnung, dass sich die Parteien des Arbeitsverhältnisses zwar rechtlich als gleichwertige Vertragspartner gegenüberstehen, faktisch der Arbeitgeber aber meist aufgrund wirtschaftlicher und struktureller Überlegenheit eine übergeordnete Stellung einnimmt. Angesichts nach wie vor anhaltendender Datenschutzskandale fokussiert sich die Vereinbarung insbesondere darauf, Rahmenbedingungen für Kontroll- und Überwachungsmaßnahmen im Beschäftigungskontext zu schaffen.

Die Vereinbarung soll als Grundlage dafür dienen, ein vertrauensvolles Arbeitsklima zwischen Arbeitgebern und Beschäftigten am Arbeitsplatz zu unterstützen und den Betriebsfrieden zu sichern. Dementsprechend sollen die mit dem Einsatz von IuK-Technik angestrebten Ziele hierbei stets in Kooperation zwischen Arbeitgeber- und Beschäftigtenseite verwirklicht werden. Bei der Zusammenarbeit sollen dabei die Interessen aller Beteiligten in angemessener Art und Weise Berücksichtigung finden.

2. Geltungsbereich

2.1. Räumlicher Geltungsbereich

Diese Vereinbarung findet im Geltungsbereich des BetrVG im gesamten Unternehmen XY[6] Anwendung. Sie findet gleichermaßen Anwendung auf die Nutzung von IuK-Technik in- und außerhalb der Betriebsstätten.

2.2. Sachlicher Geltungsbereich

Diese Vereinbarung und ihre Anlagen regeln allgemeingültige und verbindliche Standards für den Einsatz von IuK-Technik am Arbeitsplatz und hiermit zusammenhängender Fragen der Kontrolle und Überwachung im Beschäftigungskontext. Sie stellen Grundsätze für die Entwicklung, Einführung, Anwendung und Weiterentwicklung von IuK-Technik auf, von denen Auswirkungen auf die Persönlichkeitsrechte von Beschäftigten zu erwarten sind.[7] Die Grundsätze gelten auch für Daten in Papierform.

2.3. Persönlicher Geltungsbereich[8]

Diese Vereinbarung und ihre Anlagen finden Anwendung auf sämtliche Beschäftigten des Unternehmens XY [9] mit Ausnahme der leitenden Angestellten i.S.v. § 5 Abs. 3 BetrVG. Das Unternehmen stellt sicher, dass leitende Angestellte über den Inhalt dieser Vereinbarung und deren Anlagen informiert werden und die darin niedergelegten Standards beachten. Das Unternehmen lässt sich die Kenntnisnahme des Inhalts der Vereinbarung und ihrer Anlagen sowie die Verpflichtung zur Einhaltung der in ihr niedergelegten Standards schriftlich bestätigen.

3. Begriffsbestimmungen

Datenschutzrechtliche Begriffsbestimmungen, die auf diese Vereinbarung anzuwenden sind, enthält Anlage 1.

---

[6] Name und Rechtsstellung des Unternehmens einfügen.

[7] Es wird empfohlen, die in der Vereinbarung aufgestellten Grundsätze als Basis für eine vorbildliche Verwendung von personenbezogenen Beschäftigtendaten zu verwenden.

[8] Sprachlich vereinfachende Bezeichnungen (z. B. „Beschäftigte“) beziehen sich auf Frauen und Männer in gleicher Weise.

[9] Name und Rechtsstellung des Unternehmens einfügen.

4. Allgemeine Grundsätze

4.1.

Bei der Verwendung personenbezogener Beschäftigtendaten sind die allgemeinen datenschutzrechtlichen Grundsätze zu wahren. Insbesondere sind folgende Grundsätze zu berücksichtigen:

1) Verbot mit Erlaubnisvorbehalt;
2) Direkterhebung;
3) Datensparsamkeit;
4) Datenvermeidbarkeit;
5) Transparenz;
6) Zweckbindung;
7) Erforderlichkeit.

Eine Erläuterung dieser Grundsätze sowie nähere Aussagen zu der Gewährleistung eines umfassenden Beschäftigtendatenschutzes enthält Anlage 2.

4.2.

Der Arbeitgeber muss grundsätzliche Anforderungen an Datenverarbeitungssysteme vorgeben. Hierzu muss er insbesondere folgende Punkte sicherstellen:

1) klare Strukturierung verwendeter Systeme
2) transparente, abschließende und vollständige Dokumentation der verwendeten Systeme und
3) abschließende und vollständige Festschreibung von Zugriffsberechtigungen und Schnittstellen zu anderen Systemen.

5. Rechtsgrundlage für die Verwendung von personenbezogenen Beschäftigtendaten; besondere Arten personenbezogener Daten; Beweislastverteilung

5.1.

Personenbezogene Beschäftigtendaten dürfen nur auf Grundlage einer eindeutigen Rechtsgrundlage verwendet warden.

5.2.

Die Verwendung besonderer Arten personenbezogener Daten i. S. d. Anlage 1 Nr. 2 erfordert eine gesonderte Prüfung und Darlegung der Rechtsgrundlage.

5.3.

Der Arbeitgeber trägt die Beweislast für die Notwendigkeit einer Datenverwendung und deren Rechtsgrundlage.

6. Spezielle Anforderungen an die Einwilligung eines Beschäftigten

6.1.

Eine informierte Einwilligung gemäß §§ 4, 4a BDSG kann nur eine Verwendung von personenbezogenen Beschäftigtendaten legitimieren, wenn sie auf der freien Entscheidung des Beschäftigten beruht. Freiwilligkeit liegt in diesem Sinne vor, wenn die Einwilligung nicht in einer Zwangslage oder unter Druck getroffen wurde. Das Freiwilligkeitskriterium bedarf im Beschäftigungskontext insbesondere der genauen Prüfung, wenn die Machtverhältnisse unausgeglichen sind.

6.2.

Um die Beschäftigten zu schützen, muss der Arbeitgeber daher die Datenverwendung auf Grundlage der Einwilligung des Beschäftigten nur unter strenger Beachtung folgender Voraussetzungen in Betracht ziehen.

1) Bevor der Beschäftigte einwilligt, muss der zuständige Betriebsrat über den konkreten Regelungstatbestand umfassend informiert werden und der Bitte um Einholung einer Einwilligung ausdrücklich zustimmen.
2) Der Beschäftigte muss vor Abgabe seiner eindeutigen[10] Einwilligung darauf hingewiesen werden, dass seine Erklärung freiwillig[11] ist und er im Falle der Einwilligung diese später ohne Angaben von Gründen widerrufen kann, ohne dass ihm hieraus negative Konsequenzen drohen.
3) Der Beschäftigte muss vor Abgabe der Einwilligung in geeigneter Weise über deren Bedeutung informiert werden.[12]

[10] Eindeutigkeit i. d. S. liegt vor, wenn keine Zweifel daran bestehen, dass eine Einwilligung vorliegt und welchen Inhalt diese Einwilligung hat.
[11] Dies bedeutet, der Beschäftigte muss sich bei der Erklärung seines Einverständnisses darüber bewusst sein, dass er seine Daten nicht mitteilen muss und demensprechend die Einwilligung verweigern kann. Insbesondere liegt keine Freiwilligkeit vor, wenn der Beschäftigte getäuscht oder gezwungen wurde, sozialem Druck ausgesetzt war oder die Verweigerung der Einwilligung für ihn mit Nachteilen verbunden ist.
[12] Inhalt und Umfang der Information hängen vom jeweiligen Verwendungszweck ab.

4) Dem Beschäftigten muss tatsächlich die Möglichkeit eingeräumt werden, seine Einwilligung zu verweigern.
5) Die Einwilligung muss schriftlich erfolgen.
6) Die Aufklärung des Beschäftigten über die Bedeutung seiner Einwilligung, deren Freiwilligkeit sowie der Möglichkeit zum Widerruf der Einwilligung sind bezogen auf den konkreten Regelungstatbestand zu protokollieren.

7. Zwecke der Datenverwendung

7.1.

Vor der Erhebung personenbezogener Daten muss der Zweck ihrer weiteren Verarbeitung und Nutzung eindeutig, verbindlich und abschließend bestimmt werden. Weitere Ausführungen zu möglichen Zweckbestimmungen im Beschäftigungskontext enthält Anlage 3. Die Beschäftigten und ihre Interessenvertretungen sind über die Zwecke der Datenverarbeitung und -nutzung angemessen zu informieren. Zu Zwecken der Beweissicherung müssen Zwecke der Datenverwendung protokolliert warden.

7.2.

Soweit geregelte Verfahren oder Prozesse durchgeführt werden, werden die Zwecke und Ziele hierauf bezogen bestimmt.

7.3.

Die Zweckbestimmung erfolgt

1) in Einklang mit gesetzlichen Bestimmungen und
2) unter bestmöglicher Wahrung der Persönlichkeitsrechte der Beschäftigten.

7.4.

Werden konkrete Arbeitsaufgaben durchgeführt oder konkrete Arbeitsaufträge erledigt, dürfen personenbezogene Beschäftigtendaten nur verarbeitet oder genutzt werden, wenn es die Verarbeitung oder Nutzung vor der Erhebung dieser Daten eindeutig legitimiert.

7.5.

Die Verwendung von personenbezogenen Beschäftigtendaten auf Vorrat ist verboten.[13]

[13] Vgl. hierzu grundsätzlich BVerfGE 65, 1, 46.

7.6.

Besondere Zweckbindungen[14] sind beim Umgang mit personenbezogenen Beschäftigtendaten entsprechend zu beachten.

7.7.

Personenbezogene Beschäftigtendaten sind sofort zu löschen, wenn sie für den bestimmten Zweck nicht mehr erforderlich sind.

8. Grundsatz enger Auslegung der Zweckbestimmung

8.1.

Die Zweckbestimmung ist eng auszulegen.

8.2.

Jede konkrete Verwendung von personenbezogenen Beschäftigtendaten muss sich einer dokumentierten Zweckbestimmung zweifelsfrei zuordnen lassen. Bestehen Zweifel daran, dass die Zweckbestimmung die betreffende Verwendung erfasst, ist von einer Verwendung der betreffenden personenbezogener Beschäftigtendaten abzusehen.

9. Zweckänderung

Die nachträgliche Änderung der Zweckbestimmung ist grundsätzlich verboten. Ausnahmsweise ist eine Änderung der Zweckbestimmung erlaubt, wenn

1) dies unter Wahrung datenschutzrechtlicher Vorgaben erforderlich ist,
2) die Interessenvertretungen beteiligt und kollektivrechtliche Verfahren durchgeführt werden und
3) die betroffenen Beschäftigten vorher schriftlich[15] über die Zweckänderung informiert werden.

Erfolgt eine Zweckänderung, um eine gesetzlich erlaubte interne Sachverhaltsaufklärung durchzuführen, ist die vorherige Information der betroffenen Beschäftigten entbehrlich, wenn

[14] Vgl. hierzu §§ 31 und 39 BDSG.
[15] Die Schriftform kann auch mittels E-Mail gewahrt werden.

hierdurch die Durchführung gefährdet wird. Die Information der betroffenen Beschäftigten ist dann umgehend nach Aufklärung des Sachverhalts vorzunehmen.

10. Trennungsgebot

10.1.

Personenbezogene Beschäftigtendaten, die zu unterschiedlichen Zwecken erhoben wurden, sind vollständig getrennt nach dem jeweiligen Zweck ihrer Erhebung zu verarbeiten und zu nutzen.

10.2.

Die verantwortliche Stelle muss durch geeignete technische und organisatorische Maßnahmen[16] die Einhaltung des Trennungsgebotes sicherstellen.[17]

11. Informationspflichten

11.1.

Der Arbeitgeber verpflichtet sich, eine angemessene, regelmäßige und aktuelle Entwicklungen berücksichtigende Information aller Beschäftigten über deren Persönlichkeitsrechtsschutz im Beschäftigungskontext sicherzustellen.

11.2.

Die Information umfasst insbesondere auch die Einführung oder Änderung EDV-bezogener Verhaltensregeln, Kontroll- und Überwachungspotentialen des Arbeitgebers sowie kollektivrechtliche Bestimmungen. Die Betriebsparteien treffen die Auswahl eines geeigneten

[16] Zu den besonderen datenschutzrechtlichen Anforderungen an die Gestaltung der innerbetrieblichen Organisation vgl. allgemein § 9 S. 1 BDSG nebst Anlage. Die Anlage zu § 9 S. 1 BDSG spezifiziert die Sicherheits- und Schutzanforderungen des BDSG. Nach S. 2 der Anlage zu § 9 S. 1 BDSG sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Einhaltung des Gebots der Datentrennung geeignet sind. Zu beachten ist, dass nach § 9 S. 2 BDSG Maßnahmen nur erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

[17] Die Einhaltung des Trennungsgebots kann etwa durch die Speicherung von Daten auf verschiedenen Servern oder auch durch logische Trennung sichergestellt werden. Hierbei bestimmt die Art der gespeicherten Daten, welche Trennung sinnvoll und angezeigt ist. Um eine Vermischung mit anderen Datensätzen zu verhindern, sollten hochsensible Daten generell auf eigenen Servern verarbeitet werden.

Informationsmediums (z. B. Information per Intranet oder betrieblichen Informationsbroschüren) in gemeinsamer Absprache.

11.3.

Der Arbeitgeber verpflichtet sich, an die Beschäftigten eine jährliche und vollständige Übersicht über Systeme und Verfahren zu veröffentlichen, in denen personenbezogene Beschäftigtendaten verarbeitet warden.

11.4.

Vor der Durchführung von Kontroll- und Überwachungsmaßnahmen sind die Beschäftigten hierüber rechtzeitig und umfassend in sprachlich angemessener, insbesondere klarer und verständlicher Weise zu informieren. Die Informationspflichten des Unternehmens erstrecken sich hierbei insbesondere auf folgende Angaben:

1) Zweck und Gründe der Maßnahme
2) Dauer und Umfang der Maßnahme
3) angewandte Methoden und eingesetzte Technik
4) Art der erhobenen Daten und Dauer ihrer Speicherung
5) geplante weitere Datenverarbeitung und -nutzung und
6) Rechte und Pflichten im Zusammenhang mit den Maßnahmen.

11.5.

Verstöße mit Relevanz für den Persönlichkeitsrechtsschutz im Beschäftigungskontext sind den Beschäftigten unverzüglich mitzuteilen. Entsprechende Unterlagen sind den Beschäftigten auf deren Verlangen zur Verfügung zu stellen. Bestimmungen zum Geheimnisschutz bleiben hiervon unberührt. Drohen schwerwiegende Beeinträchtigungen der Rechte oder schutzwürdiger Interessen der Beschäftigten, muss der Arbeitgeber darüber hinaus auch die zuständige Aufsichtsbehörde unverzüglich unterrichten. § 42a S. 3-4 und 6 BDSG findet entsprechende Anwendung.

12. Heimliche Maßnahmen

12.1.

Heimliche Maßnahmen zur Kontrolle und Überwachung von Beschäftigten[18] verfügen über eine besonders hohe Eingriffsintensität und sollten selbst im Fall ihrer rechtlichen Zulässigkeit nur als ultima ratio in Betracht gezogen warden.

12.2.

Heimliche Maßnahmen können in absolut engen Ausnahmefällen zulässig sein, wenn

1) der zu dokumentierende konkrete[19] Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung[20] im Zusammenhang mit dem Beschäftigungsverhältnis zu Lasten des Arbeitgebers besteht,
2) weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind,
3) die heimliche Maßnahme praktisch das einzig verbleibende Mittel darstellt und
4) die heimliche Maßnahme insgesamt verhältnismäßig ist.[21]

12.3.

Die hierfür erforderlichen Prozesse, Instrumente und Methoden sind unter Einbeziehung der Interessenvertretung auszuwählen und auszugestalten. Insbesondere ist sicherzustellen, dass die heimliche Maßnahme nur für eine zuvor festgelegte, angemessene Dauer stattfindet. Die Auswertung der betreffenden Daten muss durch einen Dritten erfolgen, der weder an der Entscheidungsfinden zur Vornahme einer heimlichen Maßnahme noch an deren Durchführung beteiligt war.

12.4.

Bestätigt sich der konkrete Verdacht i. S. d. Abs. 2 Nr. 1 nicht, sind die durch die heimliche Maßnahme erlangten Daten unverzüglich zu löschen.

---

[18] Z. B. heimliche Videoüberwachung. Im Einzelnen wird die Zulässigkeit von heimlichen Maßnahmen im jeweiligen stark kontrovers diskutiert. Im Sinne eines vorbildlichen Beschäftigtendatenschutzes sollten derartige Maßnahmen vorzugsweise unterbleiben.

[19] Der Verdacht muss in persönlicher, räumlicher und funktionaler Hinsicht ausreichend konkretisiert sein.

[20] Das Gesetzt regelt in § 32 Abs. 1 S. 2 BDSG lediglich die Verfolgung konkreter Verdachtsfälle („zur Aufdeckung von Straftaten“). Nach herrschender Meinung bildet § 32 Abs. 1 S. 1 BDSG die Rechtsgrundlage für Maßnahmen zur (i.d.R. verdachtsunabhängigen) Prävention von Straftaten im Zusammenhang mit dem Beschäftigungsverhältnis (sog. Korruptionsbekämpfung). Rein präventive Maßnahmen sehen sich datenschutzrechtlichen Durchführungsrisiken ausgesetzt und sollten genauestens auf ihre Zulässigkeit hin rechtlich überprüft werden. Es wird dringend empfohlen, das weitere Verfahren mit der zuständigen Aufsichtsbehörde abzustimmen und von deren Vorgaben abhängig zu machen.

[21] Vgl. grundlegend zur heimlichen Videoüberwachung BAG, NZA 2003, 1187, 1193.

12.5.

Über die generelle Möglichkeit, heimliche Maßnahmen zur Kontrolle und Überwachung von Beschäftigten durchzuführen, sind die Beschäftigten zu informieren. Über konkrete Maßnahmen sind die betroffenen Beschäftigten so bald als möglich zu informieren.

13. Sicherheitsaspekte

13.1.

Der Arbeitgeber muss die Informationssicherheit gewährleisten, indem er technische und organisatorische Maßnahmen[22] trifft, die das im Unternehmen benötigten Maß an Vertraulichkeit, Verfügbarkeit und Integrität der zu verarbeitenden Daten sicherstellen.

13.2.

Hierzu muss der Arbeitgeber insbesondere ein Informationssicherheits-Managementsystem (ISMS) implementieren. Das ISMS dient dazu, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten ISMS sind unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation aufzustellen.[23]

13.3.

Dem Arbeitgeber obliegt es, Prozesse und Verfahren[24] für einen rechtskonformen Umgang mit personenbezogenen Beschäftigten vorzugeben.[25]

---

[22] Vgl. zu § 9 S.1 BDSG nebst Anlage bereits Fn. 16.

[23] Vgl. allgemein hierzu „Leitfaden Informationssicherheit - IT-Grundschutz kompakt“ des BSI, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile). Vgl. ferner zu den allgemeinen Anforderungen an ein ISMS etwa die IT-Grundschutz-Standards des BSI (abrufbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html) oder den BITKOM- und DIN-Kompass zur IT-Sicherheitsstandards, „Kompass der IT-Sicherheitsstandards - Leitfaden und Nachschlagewerk“, 4. Auflage (abrufbar unter: http://www.nia.din.de/cmd?level=tpl-artikel&languageid=de&cmstextid=kompass).

[24] Z. B. Vier-Augen-Prinzip als Maßnahme organisatorischer Art. Dieses Prinzip zielt darauf ab, das Risiko von Fehlern und Missbrauch zu reduzieren. Hierzu werden an wichtigen Entscheidungen und kritischen Tätigkeiten stets mehrere Personen beteiligt, anstatt die Kompetenz in einer Person zu zentralisieren. Vgl. hierzu weiterführend https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m04/m04129.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf?__blob=publicationFile.

14. Datengeheimnis, Schulung, Belehrung und Verpflichtung

14.1.

Personenbezogene Beschäftigtendaten müssen vertraulich behandelt werden. Sie unterliegen dem Datengeheimnis (§ 5 BDSG), das den bei der Datenverarbeitung beschäftigten Personen die unbefugte Verwendung personenbezogener Beschäftigtendaten untersagt (§ 5 S. 1 BDSG). Die bei der Datenverarbeitung beschäftigten Personen sind nach entsprechender Belehrung bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten (§ 5 S. 2 BDSG) und gem. § 4g Abs. 1 S. 4 Nr.2 BDSG zu unterweisen. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort (§ 5 S. 3 BDSG).

14.2.

Der Verpflichtung muss eine angemessene und sachgerechte Schulung vorangehen. Die Schulung dient zum bedarfsgerechten Erwerb fachlicher Qualifizierungen der Beschäftigten. Sie zielt darauf ab, neben allgemeinem datenschutzrechtlichem und arbeitsrechtlichem Grundlagenwissen insbesondere auch Wissen über die rechtmäßige Verwendung von personenbezogenen Beschäftigtendaten. In jedem Fall ist sicherzustellen, dass die Schulung umfangreiche Kenntnisse über die Kontrolle und Überwachung von Beschäftigten vermittelt.

14.3.

Vor Eintritt des Bedarfsfalls muss der Arbeitgeber konkrete Qualifizierungsmaßnahmen entwickeln und den Betriebsrat hierüber informieren. Sofern und soweit erforderlich, stimmen Arbeitgeber und Betriebsrat ein Qualifizierungskonzept ab.[26]

14.4.

Die für die Teilnahme an den Qualifizierungsmaßnahmen erforderliche Arbeitszeit ist den Beschäftigten einzuräumen. Nach Möglichkeit sollen die Qualifizierungsmaßnahmen während der regelmäßigen, betriebsüblichen Arbeitszeit stattfinden. Die zur Teilnahme an den Qualifizierungsmaßnahmen erforderlichen Kosten trägt der Arbeitgeber.

---

[25] Denkbar sind hier etwa Rollen- und Berechtigungskonzepte, Schutzbedarfsfestellungen, Risikoanalysen sowie Bestimmungen zur Datensicherung.

[26] Inhalte eines Qualifizierungskonzeptes können u.a. sein: Kursziele, Kerninhalte, Teilnehmer, Termine und Ort der Qualifizierungsmaßnahme.

15. Dokumentation der Datenverarbeitung

15.1.

Der Arbeitgeber muss den Umgang mit personenbezogenen Beschäftigtendaten umfassend dokumentieren. Hier zu stellt er sicher, dass eine Aufstellung über sämtliche Stellen und Systeme erstellt wird, in und mit denen personenbezogene Beschäftigtendaten verwendet werden. Diese Aufstellung wird um weitere Informationen[27] zu einen Verfahrensverzeichnis ergänzt.[28]

15.2.

Das Verfahrensverzeichnis muss so verwaltet werden, dass jedermann in geeigneter Weise hierin einsehen kann.

16. Audit

16.1.

Um die Rechtskonformität des Umgangs mit personenbezogenen Beschäftigtendaten mit den Anforderungen dieser Vereinbarung sicherzustellen, werden die für den Beschäftigtendatenschutz relevanten DV-Prozesse regelmäßig auditiert. Ebenso werden Maßnahmen überprüft, die diesbezüglich das Datenschutzniveau nachhaltig sichern und verbessern können. Der Arbeitgeber verfasst einen detaillierten Bericht, um die Bewertung der Rechtskonformität zu ermöglichen und zu unterstützen.

16.2.

Um Interessenkollisionen zu vermeiden, werden Audits vorzugsweise von einem betriebsfremden Dritten durchgeführt, der über die notwendige Fachexpertise[29] verfügt. Alternativ können Audits auch betriebsintern erfolgen, sofern der Arbeitgeber sicherstellt, dass die Durchführung der Datenschutz-Audits durch eine unabhängige und weisungsfreie Institution erfolgt, die die notwendige Fachexpertise aufweist.[30] In beiden Fällen erfolgt die Auswahl in gemeinsamer Absprache der Betriebsparteien.

---

[27] Art der gespeicherten Daten, Zweckbestimmungen, Zugriffsberechtigungen etc.

[28] Als Hilfe für die Erstellung kann der Praxisleitfaden der BITKOM dienen (abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Verfahrensverzeichnis_V_2.0.pdf).

[29] Insbesondere sollte sichergestellt werden, dass es sich bei dem Dritten um einen zertifizierten Fachauditor (Zertifizierung nach ISO/IEC 27001) handelt, der zudem vertiefte Kenntnisse über die Verwendung personenbezogener Beschäftigtendaten nachweisen kann.

[30] Zu den Anforderungen siehe bereits Fn. 29.

16.3.

Das Ergebnis jedes Audits wird in einem Auditbericht festgehalten und den Betriebsparteien dauerhaft zur Verfügung gestellt. Im Einzelnen muss der Auditbericht mindestens folgende Punkte umfassend abhandeln und erörtern:

1) Ist-Zustand des Datenschutzniveaus;
2) diesbezügliche Risikoeinschätzung;
3) Hinweise auf etwaige Schutzlücken und/oder Verbesserungspotential und
4) daraus abgeleitete Umsetzungsmaßnahmen mit Terminsetzung (Maßnahmenplan).

17. Rechte der Beschäftigten

17.1.

Jeder Beschäftigte hat nach Maßgabe von § 34 BDSG ein Recht auf Auskunft und Erläuterung über alle zu seiner Person gespeicherten Daten (Auskunftsanspruch). Der Arbeitgeber hat hierfür einen Ansprechpartner zu benennen. Das Recht des Beschäftigten auf Akteneinsicht bleibt vom Auskunftsanspruch unberührt.

17.2.

Jeder Beschäftigte hat nach Maßgabe von § 35 BDSG einen Anspruch auf Berichtigung, Löschung und Sperrung seiner personenbezogenen Daten.

18. Beteiligungsrechte des Betriebsrats

18.1.

Der Arbeitgeber gewährleistet durch geeignete Prozessgestaltung, dass der Betriebsrat seine Beteiligungsrechte umfassend und so früh wie möglich wahrnehmen kann.[31]

[31] Dem Betriebsrat stehen – abhängig vom zugrunde liegenden Sachverhalt – nach dem BetrVG verschiedenste Beteiligungsrechte zu (vgl. hier insbesondere §§ 81 Abs. 1 Nr. 1, 87 Abs. 1 Nr. 6, 94 BetrVG). Diese Rechte müssen auch im Beschäftigungskontext gewährt werden (vgl. § 32 Abs. 3 BDSG).

18.2.

Hierbei muss er insbesondere darauf achten, die Wahrnehmung der Mitbestimmungsrechte bei der Einführung und Anwendung von IuK-Technik zu Zwecken der Kontrolle und Überwachung von Mitarbeitern zu gewährleisten.

19. Verstöße, Auslegung der Vereinbarung

19.1.

Soweit ein zuständiger Betriebsrat einen Verstoß gegen diese Vereinbarung rügt, obliegt es dem Arbeitgeber, dies zu widerlegen. Die abschließende Feststellung, ob ein Verstoß vorliegt, trifft eine unabhängige Einigungsstelle.[32]

19.2.

Wird ein Verstoß festgestellt, muss dieser unverzüglich abgestellt werden.

Zuwiderhandlungen gegen diese Vereinbarung werden bei zu vertretenem Tun/Unterlassen[33] mit individuellen arbeits-/vertragsrechtlichen Konsequenzen geahndet. Dies gilt ebenso für verantwortliche Vorgesetzte, soweit deren zu vertretenes Tun/Unterlassen zum Verstoß beigetragen hat. Über weitere Konsequenzen eines festgestellten, vom Arbeitgeber zu vertretenen Verstoßes entscheidet die vorbezeichnete unabhängige Einigungsstelle[34].

19.3.

Die unterzeichnenden Parteien verpflichten sich, bei Streitigkeiten um die Auslegung und Anwendung dieser Vereinbarung unverzüglich Verhandlungen mit dem Ziel einer einvernehmlichen Regelung aufzunehmen. Im Zweifel sind die Bestimmungen dieser Vereinbarungen im Sinne einer datenschutzfreundlichen Verwendung von personenbezogenen Beschäftigtendaten auszulegen. Wird über einzelne Fragen kein Einvernehmen erzielt, ist die vorbezeichnete unabhängige Einigungsstelle[35] anzurufen.

---

[32] Bezeichnung einfügen. Sofern nicht vorhanden, wird empfohlen, vorzugsweise eine betriebliche, unabhängige Einigungsstelle einzurichten, um Streitigkeiten direkt vor Ort klären zu können. Die unterzeichnenden Parteien sollten hierzu entsprechende Regelungen treffen (Besetzung, Geschäftsordnung, Vorsitz nach Rotationsprinzip, Entscheidungsfindung etc.).

[33] Das Dulden einer Handlung stellt ebenso ein Unterlassen da.

[34] Bezeichnung einfügen.

[35] Bezeichnung einfügen.

20. Salvatorische Klausel

20.1.

Sollte eine Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden oder sollte die Vereinbarung eine Regelungslücke enthalten, so berührt dies nicht die Wirksamkeit der Vereinbarung im Übrigen.

20.2.

Die unterzeichnenden Parteien verpflichten sich, in einem solchen Fall eine Neuregelung herbeizuführen, damit ein der unwirksamen oder undurchführbaren Bestimmung oder ein der Regelungslücke möglichst nahekommendes, den beabsichtigten Vereinbarungszweck erreichendes Ergebnis rechtswirksam erzielt wird.

21. Inkrafttreten, Kündigung, Geltungsdauer, Schriftform, Anlagen

21.1.

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft.

21.2.

Sie ist beidseitig mit einer Frist von drei Monaten jeweils zum Quartalsende kündbar, erstmals jedoch zum XXX[36].

21.3.

Bis zum Abschluss einer neuen Vereinbarung gelten die Regelungen dieser Vereinbarung weiter.

21.4.

Alle in der Vereinbarung genannten Anlagen sind Bestandteile derselben.

Ergänzungen und Änderungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für das Absehen vom Schriftformerfordernis. Anlagen:

1) Anlage 1 Begriffsbestimmungen

[36] Datum einfügen.

2) Anlage 2 Erläuterung der allgemeinen datenschutzrechtlichen Grundsätze, Gewährleistung eines umfassenden Beschäftigtendatenschutzes
3) Anlage 3 Ausführungen zur Zweckbestimmung im Beschäftigungskontext

[Ort, Datum, Unterschriften der Parteien]

Anlage 1 - Begriffsbestimmungen

Soweit in dieser Anlage nicht definiert, gelten die Begriffsbestimmungen des BDSG in der geltenden Fassung.

1. *Personenbezogene Daten* sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener). Personenbezogene Beschäftigtendaten sind Einzelangaben über persönliche oder sachliche Verhältnisse eines bestimmten oder bestimmbaren Beschäftigten. Daten sind personenbezogen, wenn sie eindeutig einem Beschäftigten zuzuordnen sind oder diese Zuordnung zumindest mittelbar erfolgen kann (personenbeziehbare Daten).

2. *Besondere Arten personenbezogener D*aten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

3. *Beschäftigte* sind alle natürlichen Personen, die bei einem Arbeitgeber beschäftigt sind. Der Begriff ist weit zu verstehen[37] und umfasst neben Arbeitnehmern u. a. auch zur Berufsausbildung beschäftigte Personen, arbeitnehmerähnliche Personen, Bewerber sowie Personen, deren Beschäftigungsverhältnis beendet ist.[38]

4. *Verwendung* ist jede Erhebung, Verarbeitung und Nutzung von Daten.

5. *Automatisierte Verwendung* ist die Verwendung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

6. *Verwendung auf Vorrat* ist jede Verwendung personenbezogener Beschäftigtendaten ohne abschließende Festlegung von Ziel und Zweck.

7. *IuK-Technik* ist sämtliche Technik im Bereich der Informationsverarbeitung und Kommunikation.

8. *Kontroll- und Überwachungsmaßnahmen* sind solche Maßnahmen, die den Einsatz von IuK-Technik zu Zwecken der Kontrolle und Überwachung von Beschäftigten vorsehen. IuK-Technik kann z.B. zur Kontrolle und Überwachung der E-Mail- und Internetnutzung, sozialer Netzwerke, mittels optisch-elektronischer Einrichtungen (Videoüberwachung), mittels Zutritts-/Zugangskontrollsystemen (RFID, Abgleich biometrischer Daten) und auch außerhalb des Betriebsgeländes (GPS-/GSM-Ortung) eingesetzt werden.[39]

---

[37] Vgl. weitergehend das divergierende Verständnis im Datenschutz-, Arbeits- und Betriebsverfassungsrecht.

[38] Der Status des Beschäftigten erstreckt sich damit auf alle Phasen des Beschäftigungsverhältnisses (Anbahnungs-, Durchführungs-, Beendigungsphase). Zu beachten ist, dass das zugrunde gelegte Begriffsverständnis abhängig vom Rechtsgebiet divergiert (vgl. etwa die Definitionen im Datenschutzrecht, Sozialversicherungsrecht, Arbeitsrecht und Betriebsverfassungsrecht).

[39] Vgl. zum Persönlichkeitsrechtsschutz im Beschäftigungskontext ausführlich *Hagedorn*, „Datenschutz am Arbeitsplatz – Länderbericht Bundesrepublik Deutschland“ (Stand: Juni 2011), abrufbar unter: http://www.pawproject.eu.

Anlage 2 - Erläuterung der allgemeinen datenschutzrechtlichen Grundätze, Gewährleistung eines umfassenden Beschäftigtendatenschutzes

1. Allgemeine datenschutzrechtliche Grundsätze

Bei der Verwendung personenbezogener Beschäftigtendaten sind folgende Grundsätze zu beachten:

a) *Verbot mit Erlaubnisvorbehalt* (§ 4 Abs. 1 BDSG)

Der Umgang mit personenbezogenen Daten ist grundsätzlich verboten. Eine Ausnahme besteht nur dann, wenn es für die Verwendung eine ausdrückliche gesetzliche Grundlage gibt oder Beschäftigte in die Verwendung ihrer personenbezogenen Daten eingewilligt haben.

b) *Direkterhebung* (§ 4 Abs. 2 S. 1 BDSG, sog. „offene Erhebung")

Personenbezogene Daten sind grundsätzlich beim Beschäftigten selbst und mit dessen Mitwirkung zu erheben. Ausnahmen vom Direkterhebungsgrundsatz sind etwa denkbar, wenn eine Rechtsvorschrift die anderweitige Erhebung vorschreibt oder die Erhebung beim Beschäftigten selbst einen unverhältnismäßig hohen Aufwand erfordern würde.

c) *Datenvermeidung und Datensparsamkeit* (§ 3a BDSG)

Die Verwendung personenbezogener Beschäftigtendaten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten sind, so wenig personenbezogene Daten wie möglich zu verwenden. Insbesondere sind personenbezogene Beschäftigtendaten zu anonymisieren (§ 3 Abs. 6 BDSG) oder zu pseudonymisieren (§ 3 Abs. 6a BDSG), soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

d) *Transparenz*

Für den Beschäftigten muss die Verwendung seiner personenbezogenen Daten transparent sein. Dies setzt die Kenntnis der Struktur der Datenverarbeitung, der Datenverarbeitungsprozesse, der eingesetzten Technik sowie der Datenströme voraus. Mit anderen Worten soll der Beschäftigte wissen, dass Daten über ihn erhoben werden und welche Daten zu welchem Zweck bei welcher Stelle und aus welchem Grund gespeichert werden. Eine heimliche Datenerhebung ist grundsätzlich unzulässig und nur in Ausnahmefällen unter sehr strengen Voraussetzungen möglich. Der Grundsatz der Direkterhebung (s. o.), Informationspflichten des Arbeitgebers sowie der Auskunftsansprüche von Beschäftigten dienen zur Herstellung der Transparenz.

e) *Zweckbindung*

Jeder Verwendung von personenbezogenen Beschäftigtendaten muss ein bestimmter legitimer Zweck zugrunde liegen. Personenbezogene Beschäftigtendaten dürfen grundsätzlich nur für Zwecke verarbeitet oder genutzt werden, für die sie erhoben wurden. Ausnahmsweise kann sich die Zulässigkeit einer Zweckänderung aus der Einwilligung von Beschäftigten ergeben.

f) *Erforderlichkeit*

Die Verwendung personenbezogener Beschäftigtendaten muss tatsächlich notwendig sein, d. h. auf das erforderliche Maß begrenzt werden. Weitestgehend wird das Merkmal der Erforderlichkeit in dem Sinne verstanden, dass eine Verhältnismäßigkeitsprüfung vorzunehmen ist. Der Prüfung ist dabei ein subjektiver Maßstab zugrunde zu legen, mithin muss sie am konkreten Einzelfall und unter Würdigung der konkreten Gegebenheiten erfolgen. Der Begriff der Erforderlichkeit ist gerade im Beschäftigungskontext stark umstritten, weshalb die Verwendung personenbezogener Beschäftigtendaten besonders gründlich unter Erforderlichkeitsgesichtspunkten geprüft werden sollte.

2. Gewährleistung eines umfassenden Beschäftigtendatenschutzes

a) Der Arbeitgeber hat die Einhaltung der datenschutzrechtlichen Grundsätze nach Maßgabe eines vorbildlichen Beschäftigtendatenschutzes sicherzustellen. Hierbei bekennt er sich dazu, den Schutz personenbezogener Beschäftigungsdaten in allen Phasen des Beschäftigungsverhältnisses (mithin von dessen Anbahnung bis nach dessen Beendigung) zu gewährleisten.

b) Der Arbeitgeber verpflichtet sich, Bewerber nur auf Grundlage von solchen Daten auszuwählen, die unmittelbar und persönlich vom jeweiligen Bewerber stammen.

Neben den üblichen Bewerbungsunterlagen können etwa Daten herangezogen werden, die der Bewerber dem Arbeitgeber zum Abruf bereitgestellt hat (z. B. Einstellen von Daten in eine Jobbörse) oder eigens an einen Personalvermittler zu dem Zweck überlassen hat, die Daten an den Arbeitgeber weiterzugeben. Über die Umstände der Verwendung der Bewerberdaten (automatisierte Verwendung, unternehmensweite Verwendung etc.) sind die Bewerber bereits in der Stellenausschreibung zu informieren. Die Zulässigkeit der Weitergabe von Bewerberdaten in Abweichung von der ursprünglichen Stellenausschreibung ist von der Einwilligung des Bewerbers abhängig. Bei Initiativbewerbungen müssen Bewerber über den Umgang mit Bewerberdaten informiert werden und die Möglichkeit erhalten, innerhalb einer angemessenen Frist der Verarbeitung und Nutzung ihrer Daten zu widersprechen. Wird ein Bewerber abgelehnt, sind ihm seine Unterlagen unverzüglich zurückzureichen und müssen die seine Bewerberdaten unverzüglich gelöscht werden, es sei denn, der Bewerber stimmt einer längerfristigen Speicherung seiner Daten zwecks etwaiger späterer Einstellung ausdrücklich zu.

c) Der Arbeitgeber verpflichtet sich, personenbezogene Daten ausgeschiedener Beschäftigter nach Beendigung des Beschäftigungsverhältnisses unverzüglich zu löschen bzw. datenschutzrechtskonform zu entsorgen.

d) Stehen gesetzliche Anforderungen oder vertragliche Aufbewahrungspflichten der Löschung der personenbezogenen Daten entgegen, müssen die Daten für andere Zwecke gesperrt werden.

Anlage 3 - Ausführungen zur Zweckbestimmung im Beschäftigungskontext

Die Verwendung personenbezogener Beschäftigtendaten richtet sich meist nach der datenschutzrechtlichen Generalklausel des § 32 BDSG.[40]

Hiernach ist eine Datenverwendung entweder *„für Zwecke des Beschäftigungsverhältnis“* denkbar, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich[41] ist (Grundtatbestand, § 32 Abs. 1 S. 1 BDSG). In Relation zu dem Grundtatbestand stellt § 32 Abs. 1 S. 2 BDSG[42] schärfere Anforderungen, wenn die Zulässigkeit der Datenverwendung *„zur Aufdeckung von Straftaten“*[43] in Frage steht. Von der gesetzlichen Formulierung sind neben Straftaten, die im Zusammenhang mit der Arbeitsaufgabe verübt werden auch solche erfasst, die nur bei Gelegenheit der Beschäftigung begangen werden.[44]

Rein vertragsbrüchiges oder ordnungswidriges Verhalten fällt hingegen nach dem gesetzgeberischen Willen in den Anwendungsbereich von § 32 Abs. 1 S. 1 BDSG, der sonstige Rechtsverstöße regelt.[45] Nach § 32 Abs. 2 BDSG findet schließlich Abs. 1 auch auf die manuelle Datenverarbeitung Anwendung.[46] Laut Gesetzesbegründung werden insofern die *Grundsätze des Datenschutzes im Arbeitsverhältnis* aufgegriffen.[47] Dadurch unterfallen jegliche Datensammlungen mit Beschäftigtenbezug (z.B. Aufzeichnungen von Führungskräften und Interviewern aus Bewerbungs- und Jahresführungsgesprächen sowie sämtliche Notizen zum Leistungsverhalten) dem Schutzbereich des § 32 Abs. 1 BDSG.[48]

Da viele Einzelfragen umstritten sind, fällt es insgesamt äußerst schwer, eindeutige und zuverlässige Aussagen über zulässige Verwendungszwecke im Beschäftigungskontext zu treffen. In jedem Fall ist es angezeigt, die Zulässigkeit arbeitgeberseitiger Maßnahmen genauestens zu überprüfen. Dies gilt vor allem vor dem Hintergrund, dass das Kontroll- und Überwachungspotential des Arbeitgebers auch und gerade maßgeblich von der Entscheidung abhängt, in welchem Umfang der Arbeitgeber als Inhaber der betrieblichen Mittel den Beschäftigten die Nutzung der Informations- und Kommunikationsmittel erlaubt.[49]

---

[40] Zu dessen Konkurrenzverhältnis zu § 28 BDSG vgl. *Hagedorn*, a. a. O., S. 19.
[41] Vgl. allgemein zum datenschutzrechtlichen Grundsatz der Erforderlichkeit Anlage 1 Nr. 1 lit. f.
[42] Vom Wortlaut her ist die Regelung § 100 Abs. 3 S. 1 TKG nachempfunden; inhaltlich entspricht sie den Anforderungen, die seitens der Rechtsprechung an eine verdeckte Überwachung von Arbeitnehmern gestellt wurden, Thüsing, NZA 2009, 865, 868 unter Rückgriff auf *BAG*, NZA 2003, 1193 und NZA 2008, 1187.
[43] Z. B. Diebstahl und Korruptionsfälle, BT-Drs. 16/13657, S. 36. Zu der Frage, in welchem Verhältnis § 32 Abs. 1 S. 1 und S.2 BDSG stehen, siehe Franzen, RdA 2010, 257, 260 f.
[44] Deutsch/Diller, DB 2009, 1462, 1462.
[45] BT-Drs. 16/13657, S. 36; Schmidt, RDV 2009, 193, 195 zu den problematischen Aspekten der Regelung.
[46] Vgl. zu der Ausweitung des Anwendungsbereichs des BDSG auch § 8 Abs. 1 BewachV.
[47] BT-Drs. 16/13657, S. 37 unter Rückgriff auf BAGE 54, 365; 119, 238.
[48] Wank, in: ErfK zum Arbeitsrecht, § 32 BDSG Rn. 2.
[49] Zu beachten ist in diesem Kontext, dass sich das Mitbestimmungsrecht des Betriebsrates nicht auf die Frage der Erlaubnis der Privatnutzung an sich erstreckt, LAG Hamm, NZA-RR 2007, 20, 21 f.; Ernst, NZA 2002, 585, 586; Lindemann/Simon, BB 2001, 1950, 1954.

Es wird insbesondere empfohlen, soweit erforderlich zunächst ein Konzept zur Ausgestaltung der Nutzung von betrieblichen Informations- und Kommunikationsmitteln zu entwickeln. Darüber hinaus sollte generell zur Schonung der Persönlichkeitsrechte von Beschäftigten so weit wie möglich auf technische Kontroll- und Überwachungsmaßnahmen verzichtet werden.[50]

[50] Dies hängt von der Beurteilung der Gesamtumstände im Einzelfall ab. Denkbar wäre, nicht nur an die rechtliche Zulässigkeit von Kontroll- und Überwachungsmaßnahmen anzuknüpfen, sondern weitergehende Aspekte zu berücksichtigen (z.B. ob die Durchführung der Maßnahme im Einzelfall auch geboten erscheint). Zu der unterschiedlichen rechtlichen Behandlung von dienstlicher und privater Nutzung der Informations- und Kommunikationsmitteln sowie generell zu der Zulässigkeit technischer Kontroll- und Überwachungsmaßnahmen im Beschäftigungskontext vgl. *Hagedorn*, a. a. O., insbes. S. 21 ff.