datenschutz-berater.de

49. Jahrgang

DSB 07-08/2025

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz
Schriftleitung: Prof. Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Stichwort des Monats

Datenschutz im Fokus

Rechtsprechung

Service

ISSN 0170-7256

dfv Mediengruppe

Nina Diercks

Vorbereitung ist alles – auch in Sachen interne Ermittlungen unter dem Aspekt Beschäftigtendatenschutz

Interne Ermittlungen sind kein beliebtes Thema in Unternehmen. Davon abgesehen, dass es rein zwischenmenschlich Angenehmeres gibt als gegen den Kollegen oder die Kollegin zu ermitteln, ist es auch juristisch ein nicht ganz einfaches Feld. Dabei ist es umso wichtiger, sich als Unternehmen bereits vor der allerersten internen Ermittlung gerade mit der datenschutzrechtlichen Seite zu beschäftigen. Denn hier wird die Grundlage dafür gelegt, dass im Fall der Fälle alles „glatt" geht und das Unternehmen nicht in eine selbstgegrabene Grube fällt. Oder anders ausgedrückt: Es wird der Grundstein dafür gelegt, dass das Unternehmen nicht selbst Gegenstand eines (datenschutzrechtlichen) Verfahrens aufgrund unzulässiger interner Ermittlungen wird.

Der grundlegende Interessenskonflikt bei internen Ermittlungen

„Vorsicht ist besser als Nachsicht" – dieses sehr alte Sprichwort bewahrheitet sich auch heute in den Fällen, in denen Unternehmen Kenntnis davon erlangen, dass Mitarbeitende gegen Pflichten oder Gesetze verstoßen haben. Dies gilt noch mehr, wenn diese Kenntnis erst durch eine Meldung von Ermittlungsbehörden entsteht. Schließlich werden in all diesen Fällen interne Ermittlungen in Form der internen Überprüfung des Sachverhaltes erforderlich. Das geht wiederum wesentlich leichter, wenn man als Unternehmen bereits präventiv Maßnahmen ergriffen hat, interne Ermittlungen unkompliziert, d. h. ohne datenschutzrechtliche Stolpersteine, führen zu können. Anders ausgedrückt: Mögliche interne Ermittlungen sollten im Rahmen der eigenen Compliance-Struktur nicht nur stets mitgedacht, sondern vor allem vorbereitet sein.

Was heißt dies? Nun, internen Ermittlungen ist immer ein Interessenskonflikt inhärent. Auf der einen Seite steht das Unternehmen mit seinem Recht am eingerichteten und ausgeübten Gewerbebetrieb und damit dem Recht, diesen laufenden Betrieb zu schützen, Angriffe sowie den Abfluss von Informationen (sprich Geschäftsgeheimnissen) unterbinden oder jedenfalls schnellstmöglich erkennen und aufklären zu können. Auf der anderen Seite stehen die Beschäftigten, ihre personenbezogenen Daten, ihr Recht auf informationelle Selbstbestimmung und damit ihr allgemeines Persönlichkeitsrecht.

Interne Ermittlungen stellen selbstverständlich einen Eingriff in ebendiese Rechte dar. Wenn wir uns aber an die Grundrechtsvorlesungen erinnern möchten, ist ein Eingriff immer nur dann ein Problem, wenn er nicht gerechtfertigt werden kann. Und einfachgesetzlich ist in Bezug auf Datenverarbeitungen mit der DSGVO zu fragen, ob die Datenverarbeitung erforderlich, also verhältnismäßig war.

Kann keine Rechtsgrundlage oder keine Verhältnismäßigkeit bei einer Datenverarbeitung auf eben jener Rechtsgrundlage erkannt werden, drohen bekanntermaßen Schadensersatzansprüche des Betroffenen nach Art. 82 DSGVO sowie Bußgelder nach Art. 83 DSGVO.

Dies vorausgeschickt, stellen sich sofort die folgenden Fragen: Welche Rechtsgrundlagen stehen zur Datenverarbeitung bei (vorbereitenden) internen Ermittlungen zur Verfügung? Wann sind (vorbereitende) interne Ermittlungen und die damit verbundenen Datenverarbeitungen rechtbzw. verhältnismäßig? Wie kann der Interessenskonflikt aufgelöst werden? Und gab es nicht noch das Problem, dass jeder Arbeitgeber zum Telekommunikationsanbieter würde, sobald er private Nutzungen der IT-Infrastruktur seiner Mitarbeiter erlaubte, somit per se Verstöße gegen das Fernmeldegeheimnis vorlägen, damit die Verwirklichung von Straftatbeständen im Raum und alle Geschäftsführer und Vorständen bereits mit einem Bein im Gefängnis stünden? Dazu der Reihe nach.

Vorab darf aber schon jetzt zum einen mitgeteilt werden, dass sich kein geschäftsführendes Organ um Gefängnisaufenthalte (jedenfalls nicht wegen privater Nutzung der IT-Infrastruktur) sorgen muss. Und zum anderen, dass die Regelung von privater Nutzung der IT-Infrastruktur in Unternehmen eine sehr gute Idee zur Vorbereitung interner Ermittlungen ist.

Rechtsgrundlagen zur Datenverarbeitung bei internen Ermittlungen

Naheliegend scheint auf den ersten Blick auf § 26 Abs. 1 Satz 2 BDSG als Rechtsgrundlage zu sein. Dieser besagt, dass Beschäftigtendaten zur Aufdeckung von Straftaten verarbeitet werden dürfen, sofern „tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an

dem Ausschluss der Verarbeitung nicht überwiegt". Bereits aus dem Wortlaut wird jedoch ersichtlich, dass § 26 Abs. 1 Satz 2 BDSG gerade nicht zur abstrakten Vorbereitung interner Ermittlungen heranzuziehen ist, sondern vielmehr erst in Situationen greifen kann, in denen bereits eine mögliche Straftat im Raum steht. Dies wird auch von der arbeitsrechtlichen Rechtsprechung gestützt, die ebenfalls Ermittlungen „ins Blaue hinein" untersagt (BAG, Urt. v. 21.11.13 – 2 AZR 797/11).

Bis vor Kurzem wurde weitgehend vertreten, dass (präventive) interne Ermittlungsmaßnahmen auf die Rechtsgrundlage des § 26 Abs. 1 Satz 1 BDSG zu stützen seien. So weit, so zutreffend. Allerdings hat der EuGH die im Wortlaut des § 26 Abs. 1 Satz 1 BDSG fast identische Regelung des § 23 HDSIG für unanwendbar erklärt, da es sich bei dieser nationalen Regelung nicht um eine Spezifizierung im Sinne des Art. 88 DSGVO handele (EuGH, Urt. v. 30.3.23 – C-34/21). Demnach ist auch der § 26 Abs. 1 Satz 1 BDSG als unanwendbar anzusehen.

Gerade weil diese Norm aber nach dem EuGH keinen eigenen Anwendungsbereich hat, bleibt hier – so auch der EuGH – der Rückgriff auf Art. 6 Abs. 1 lit. b DSGVO. Art 6 Abs. 1 lit. b DSGVO stellt die maßgebliche Rechtsgrundlage für präventive interne Ermittlungen dar. Nach ständiger Rechtsprechung des BAG ist im Arbeitsverhältnis die Erforderlichkeit des Art. 6 Abs. 1 lit. b DSGVO in Erfüllung des Verhältnismäßigkeitsgrundsatzes zu sehen.

Und für die Fälle, bei denen kein Zweck der Vertragsdurchführung in Betracht kommt, etwa bei Datenverarbeitungen zur Aufrechterhaltung der IT-Sicherheit, stehen – wie bisher auch – Art. 6 Abs. 1 lit. c oder lit. f DSGVO zur Verfügung.

Wann sind interne Ermittlungen und die damit verbundenen Datenverarbeitungen verhältnismäßig?

Die Antwort wäre recht einfach, wenn in einem Unternehmen nur dienstbezogene personenbezogene Daten vorhanden wären. Dann wäre die Verarbeitung – machen wir es so kurz – dieser Daten auch zu Zwecken der (präventiven) internen Ermittlungen zulässig, da sie verhältnismäßig wäre bzw. kein schutzwürdiges, überwiegendes Interesse der Beschäftigten zu erkennen wäre.

Der Konjunktiv Irrealis wird hier aber nicht ohne Grund verwendet. Denn die Realität in der weit überwiegenden Anzahl von Unternehmen sieht auch im Jahr 2025 noch so aus, dass im Ergebnis eine ungeregelte private Nutzung der IT-Infrastruktur erfolgt und damit zwischen dienstlichen Emails und Daten auch private Nachrichten, Dokumente und Seitenaufrufe zu finden sind.

Das Problem: Die (ungeregelte) private Nutzung von IT-Infrastrukturen

Die Regelung der privaten Nutzung von betrieblicher IT-Infrastruktur ist immer noch ein Reizthema in Unternehmen. Sei es, weil das Vertändeln von Arbeitszeit befürchtet wird (als ob man nicht auch in der Teeküche oder beim Blick aus dem Fenster seine Zeit vertrödeln könnte) oder weil aufgrund einer Erlaubnis der privaten Nutzung eine Compliance-Problematik eben vor dem Hintergrund des informationellen Selbstbestimmungsrechts der Beschäftigten befürchtet wird.

So weit, so fast richtig. Das größte Compliance-Problem ist nämlich die ungeregelte private Nutzung. Sehr vereinfacht ausgedrückt liegt in diesem Fall nämlich das vom Mitarbeiter eingescannte Ultraschallbild seines Kindes neben der Personalplanung 2026. Großartig! So kann die Personalabteilung doch gleich die Elternzeit des Mitarbeiters sinnvoll einplanen.

Lassen wir den Sarkasmus beiseite. Rechtlich betrachtet liegt in einer solchen – ungeregelten – Privatnutzung ein erhebliches Compliance-Problem. Denn jedem Zugriff auf Unternehmensdaten liegt zugleich eine potenzielle Verletzung des Rechts auf informationelle Selbstbestimmung der Mitarbeiter inne. Gibt es doch ein berechtigtes Interesse seitens des Unternehmens darauf Unternehmensdaten zu verarbeiten, nicht aber private Daten. Und das gilt natürlich auch, wenn wir über interne Ermittlungen sprechen. Ungeregelte private Nutzungen und damit private Daten können internen Untersuchungen im Weg stehen. Dabei ist es gleichgültig, ob wir über den Einsatz von technischen Hilfssystemen zur Kenntniserlangung von Pflichtverstößen oder aber über die „klassische" erste interne Ermittlung nach Kenntniserlangung sprechen.

Mit technischen Hilfssystemen sind unter anderem solche wie Compliance- und Fraud-Monitoring-Systeme (CFM-Systeme) und Intrusive-Detection-Systeme (IDS) gemeint. Erstere analysieren stetig im Unternehmen vorhandene Daten (insb. in Buchhaltung und Controlling) auf Anzeichen für Fehlverhalten und dienen der Erfüllung von gesetzlichen Compliance-Pflichten, etwa aus § 91 Abs. 2 AktG, § 130 OWiG). Letztere prüfen die Netzwerke ständig auf Angriff und/oder möglichen internen Missbrauch (bspw. hohe Datenabflüsse zu ungewöhnlichen Zeiten), dienen der Sicherstellung der eigenen System-Integrität und damit der Erfüllung von Art. 32 DSGVO durch das Vorhalten von technischen Maßnahmen zur Datensicherheit.

Wenn nur dienstliche personenbezogene Daten im (virtuellen) Raum stünden, wäre all dies datenschutzrechtlich unproblematisch und auch arbeitsrechtlich in Bezug auf unzulässige Leistungs- und Verhaltenskontrollen leicht zu regeln.

Bei einer ungeregelten privaten Nutzung der IT-Infrastruktur bleibt es aber datenschutzrechtlich dabei: An jeder Ecke droht die Verletzung von Rechten der Mitarbeiter (vgl. dazu schon LAG Berlin-Brandenburg, Urt. v. 16.2.11 – 4 Sa 2132/10, welches nur aufgrund der geregelten Privatnutzung keinen Verstoß gegen das allgemeine Persönlichkeitsrecht der Klägerin erkannte).

Zwar kennt das deutsche Arbeits- bzw. Zivilrecht kein Beweisverwertungsverbot unzulässig erlangter Beweise wie das Strafrecht (BAG, Urt. v. 29.6.23 – 2 AZR 296/22). Aber die oben schon erwähnten potenziellen Verstöße gegen das Persönlichkeits- und damit das Datenschutzrecht mitsamt ihren möglichen Konsequenzen verbleiben.

Die vermeintliche Lösung: Das Verbot der privaten Nutzung

Die vermeintliche Lösung liegt auf der Hand. Die private Nutzung der IT-Infrastruktur wird verboten. Schon liegen keine störenden privaten Daten in den Unternehmenssystemen. Auf dienstliche Daten darf schließlich grundsätzlich nach Belieben zugegriffen werden.

Das Problem ist hierbei allerdings, dass ein solches Verbot nachgehalten und durchgesetzt werden müsste. Es müsste stichprobenartige Prüfungen ob der Einhaltung geben. Bei Verstößen müssten die Beschäftigten entsprechend arbeitsrechtlich abgemahnt werden. Dies passiert in der Unternehmenspraxis jedoch nicht. Daraus folgt – sehr verkürzt – die Erlaubnis der privaten Nutzung durch betriebliche Übung. Und damit ist die ungeregelte private Nutzung, der compliance-technische worst case der Nutzung der IT-Infrastruktur, wieder fröhlich durch die Hintertür ins Unternehmen marschiert.

Damit wird klar: Das Verbot der privaten Nutzung ist im Regelfall keine Lösung. (Der Autorin ist kein einziges Unternehmen bekannt, das ein Verbot der privaten Nutzung nachhält.)

Die Lösung: Die geregelte private Nutzung

Daraus folgt, dass zur Vermeidung dieser compliance-technisch schwierigen Situation der ungeregelten Nutzung die einfache Lösung auf der Hand liegt: Der Regelung der privaten Nutzung der IT-Infrastruktur.

Die Mär vom Arbeitgeber als Telekommunikationsanbieter

An dieser Stelle müssen wir auf die Mär vom Arbeitgeber als Telekommunikationsanbieter eingehen und mit ebendieser aufräumen. Denn ebendiese Mär sorgt nach wie vor dafür, dass Unternehmen vor einer geregelten privaten Nutzung zurückschrecken.

In der einschlägigen Kommentarliteratur fand sich lange die Auffassung, dass der Arbeitgeber, wenn er die private Nutzung der IT-Infrastruktur erlaubte, zum Telekommunikationsanbieter werde und somit die Gefahr bestünde, er würde – strafrechtlich relevant – das Telekommunikationsgeheimnis verletzen. Dies, obwohl bereits in den Jahren 2010 bis 2012 herrschende Rechtsprechung war, dass der Arbeitgeber eben nicht zum Telekommunikationsanbieter wird (LAG Niedersachsen, Urt. v. 31.5.10, 12 – Sa 875/09; LAG Berlin-Brandenburg, Urt. v. 16.2.11 – 4 Sa 2132/10; LAG Hamm, Urt. v. 10.7.12 14 – Sa 1711/10).

Dennoch wird immer wieder und durchaus auch heute noch in einschlägigen Schulungen eben davor gewarnt und das Szenario des Geschäftsführers, der sich strafbar mache, aufgezogen. Daraus resultiert die recht verbreitete Auffassung, eine geregelte private Nutzung sei keine Lösung. Das Risiko sei doch viel zu groß! Gute Nachrichten. Die vorstehende Auffassung lässt sich mit der jüngeren Rechtsprechung, der heutigen Literatur und auch den aktuellen Behördenauffassungen wirklich nur noch als abseitige Mindermeinung vertreten.

Nicht nur kommt die jüngere Rechtsprechung (LAG Rheinland-Pfalz, Urt. v. 24.1.19 – 5 Sa 226/18; LG Erfurt, Urt. v. 28.04.21 – 1 HK O 43/20 mit intensiver Auseinandersetzung zum damaligen § 3 TKG) weiterhin zu dem Ergebnis, dass der Arbeitgeber nicht zum TK-Anbieter wird. Auch die Literatur sieht wahlweise den Arbeitgeber nicht als TK-Anbieter und/oder sieht aufgrund des Vorrangs der DSGVO vor dem TDDDG den Anwendungsbereich nicht als eröffnet an.

Wen das nicht überzeugt, der sei auf Munz, in: Taeger/Gabel/Munz, 4. Aufl. 2022, DSGVO-BDSG-TTDSG, § 3 TTDSG Rn. 25 verwiesen, der statuiert: „[…] liegt die Lösung in klaren Bedingungen zur Nutzung der Kommunikationssysteme zu privaten Zwecken, die den Mitarbeitern zu vermitteln und ggf. mit den Mitarbeitern zu vereinbaren sind. Da – nach ganz herrschender Auffassung – der Arbeitgeber die private Nutzung grundsätzlich verbieten kann, muss es ihm auch möglich sein, die private Nutzung zu gestatten unter der Bedingung, dass ihm gleichzeitig die Rechte zustehen, welche er hätte, wenn nur die dienstliche Nutzung erlaubt wäre."

Damit sind wir dann auch beim dem pragmatischen Vorgehen des LfDI Baden-Württemberg, der im Ratgeber Beschäftigtendatenschutz aus dem April 2020 zwar noch erklärte, die Aufsichtsbehörden hielten das (damalige) TKG für anwendbar, aber im Anschluss ausführte: „Mit unserer unterstützenden Beratung hat das Unternehmen mit dem Betriebsrat eine entsprechende Betriebsvereinbarung abgeschlossen, auf deren Grundlage die Beschäftigten jetzt wirksam in die Erhebung, Verarbeitung und

Nutzung ihrer personenbezogenen IuK-Daten einwilligen konnten."

Im Jahr 2024 riet dann auch die LDI NRW mittels ihres Tätigkeitsberichts 2024 dazu, Vereinbarungen zur betrieblichen und/oder privaten Nutzung der Infrastruktur zu treffen und merkte dabei an, dass Arbeitgeber, die die private Nutzung erlaubten, nicht zum TK-Anbieter würden.

Zwischenfazit

Datenverarbeitungen zu Zwecken der (vorbereitenden) internen Ermittlungen wären grundsätzlich verhältnis- und damit rechtmäßig im datenschutzrechtlichen Sinne, wenn im Unternehmen ausschließlich personenbezogene Daten mit Dienstbezug verarbeitet würden.

Dies ist aber nur in idealen Welten der Fall. In der Realität werden betriebliche IT-Infrastrukturen auch zu privaten Zwecken genutzt. Damit liegen streng genommen private und dienstliche Daten – mindestens aus Sicht der IT – direkt nebeneinander. Damit kann und wird die Datenverarbeitung zu Zwecken der internen Ermittlung stets Gefahr laufen, unzulässige Eingriffe, d. h. Verletzungen der Persönlichkeitsrechte der Beschäftigten, darzustellen. Dem kann allerdings abgeholfen werden, indem die private Nutzung der IT-Infrastruktur geregelt und auf diesem Wege die Rechte des Unternehmens und die Persönlichkeitsrechte in einen verhältnismäßigen Ausgleich gebracht werden.

Doch nicht nur das. Zeitgleich stellen Richtlinien oder Betriebsvereinbarungen, die die Nutzung der IT-Infrastruktur regeln, organisatorische Maßnahmen im Sinne von Art. 32 DSGVO dar, die ein Verantwortlicher (der Arbeitgeber) ohnehin vorhalten muss. Und all dem steht auch nicht (mehr) die Mär vom Arbeitgeber als TK-Anbieter im Weg.

Schaffung der Verhältnismäßigkeit über Betriebsvereinbarungen oder Richtlinien

Wenn mittels Betriebsvereinbarungen oder Richtlinien ein verhältnismäßiger Ausgleich auch in Bezug auf interne Ermittlungen zwischen den berechtigten Interessen von Unternehmen und Beschäftigten geschaffen werden soll, dann muss eine solche Betriebsvereinbarung oder Richtlinie insbesondere Regelungsabschnitte

- zur IT- und Datensicherheit (etwa Passwortmanagement, Speichermanagement, Datenklassifizierung),
- zur privaten Nutzung der IT-Infrastruktur (Umfang, Pflicht zur Kennzeichnung, Speicherplätze, Zugriffsregelungen bei Abwesenheit von Beschäftigten) und
- ein Verbot der Nutzung privater Devices vorsehen;
- Zwecke zu Datenverarbeitungen insbesondere im Bereich der IT-Sicherheit und präventiver Analysen darlegen sowie
- einen konkreten Prozess unter Einbeziehung von Datenschutzbeauftragten und ggf. Betriebsräten zur Auswertung von Daten beim Einsatz von präventiv wirkenden Systemen sowie im Falle des Verdachts auf Pflichtverletzungen oder Straftaten vorhalten.

Durch diesen Aufbau werden einerseits Rechte und Pflichten für die Beschäftigten und andererseits klare zweckgebundene Eingriffe und Prozesse definiert. Im Fall von Verstößen gegen die Pflichten liegt also bereits ein definierter, zweckgebundener Prozess unter Einbeziehung von Datenschutzbeauftragten und Betriebsräten vor. Hierdurch werden die Interessenslagen des Unternehmens und der Beschäftigten in Ausgleich gebracht.

Weitere To-dos in der Praxis

Voraussetzung für die Schaffung oder Überarbeitung einer solchen Betriebsvereinbarung oder Richtlinie zur Nutzung der IT-Infrastruktur, welche auch die private Nutzung umfasst und insoweit die unproblematische interne Ermittlung unterstützt, ist stets eine vorgehende Analyse des Ist-Zustandes im Unternehmen.

Diese Analyse ist zum einen auf existierende, interne Ermittlung unterstützende Systeme und deren Datenverarbeitungen zu richten. Im besten Fall sind diese bereits im Verzeichnis für Verarbeitungstätigkeiten nach Art. 30 DSGVO aufgenommen, die entsprechenden Datenverarbeitungen und ihre Zwecke dort beschrieben. Zum anderen müssen bestehende Richtlinien und Betriebsvereinbarungen zu den Themen IT-Infrastruktur und private Nutzung gesichtet und geprüft werden.

Zu vermeiden sind schließlich sich widersprechende Betriebsvereinbarungen bzw. Richtlinien.

Fazit

Die Regelung der (privaten) Nutzung der IT-Infrastruktur über eine entsprechende Richtlinie oder Betriebsvereinbarung ist ein ganz wesentlicher Baustein im hauseigenen Compliance-System, um internen Ermittlungen mindestens aus datenschutzrechtlicher Sicht entspannt entgegensehen zu können.

Autorin: **Nina Diercks, M. Litt (University of Aberdeen) ist seit 2010 als Rechtsanwältin im IT-, Datenschutz- und Arbeitsrecht tätig und führt die Kanzlei Diercks in Hamburg. Daneben veröffentlicht sie Fachbeiträge und betreibt den Blog Diercks Digital Recht.**