BRANDI
RECHTSANWÄLTE

DER MITARBEITEREXZESS

Informationen zum Datenschutz I Oktober 2025

Einleitung

Unternehmen setzen auf umfassende Compliance-Maßnahmen wie die Durchführung von Schulungsmaßnahmen oder die Erarbeitung von Datenschutzkonzepten, um eine datenschutzkonforme Verarbeitung personenbezogener Daten – insbesondere auch durch ihre Mitarbeitenden – sicherzustellen. Dennoch kann es vorkommen, dass Mitarbeitende ohne beruflichen Anlass auf personenbezogene Daten zugreifen. So ist es denkbar, dass Beschäftigte aus reiner Neugier etwa das Kaufverhalten des Nachbarn in den internen Systemen einsehen oder Kontoinformationen von Familienmitgliedern abrufen. Solche Handlungen verstoßen regelmäßig gegen den Grundsatz der Zweckbindung aus Art. 5 Abs. 1 lit. b) DS-GVO. Verarbeiten Mitarbeitende die Daten für eigene Zwecke, stellt sich die Frage, wann das eigenmächtige Handeln dem Unternehmen zugerechnet wird und wer gegebenenfalls für den Datenschutzverstoß haftet.

Wenn Mitarbeitende ihre Befugnisse überschreiten

Grundsätzlich haften Unternehmen für Datenschutzverstöße ihrer Mitarbeitenden. Dies folgt aus dem im europäischen Recht etablierten funktionalen Unternehmensbegriff, wonach das Unternehmen als wirtschaftliche Einheit aller für Sie tätigen Organisationsstrukturen angesehen wird. Im Normalfall entscheidet das Unternehmen über die Zwecke und die Mittel der Verarbeitung von personenbezogenen Daten und ist deshalb datenschutzrechtlich Veranwortlicher im Sinne der DS-GVO; Handlungen von Mitarbeitenden werden diesem grundsätzlich zugerechnet.

Eine Ausnahme besteht in der Konstellation eines sogenannten Mitarbeiterexzesses. Ein solcher liegt nach der Datenschutzkonferenz, dem Gremium der deutschen Datenschutzaufsichtsbehörden, dann vor, wenn die Handlungen der Beschäftigten bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können (vgl. DSK, Entschließung v. 3.4.2019). Es kommt insofern darauf an, ob das Handeln objektiv im Aufgabenbereich des Mitarbeitenden liegt. Unerheblich ist, ob das Handeln subjektiv von eigenen Interessen geleitet ist. Handelt der Mitarbeitende bei der Begehung eines Datenschutzverstoßes außerhalb seiner beruflichen Tätigkeit und der ihm zugewiesenen Aufgaben und damit objektiv nicht für seinen Arbeitgeber, liegt ein Mitarbeiterexzess vor.

Die Frage nach der Verantwortlichkeit

Stellt sich ein Sachverhalt als Mitarbeiterexzess dar, wirft dies die Frage auf, welche Partei in welchem Stadium als datenschutzrechtlich Verantwortlicher einzustufen ist. An diese Einordnung knüpfen weitreichende Konsequenzen: Der Verantwortliche hat insbesondere die Betroffenenrechte zu erfüllen, haftet auf Schadensersatz nach Art. 82 DS-GVO und ist Adressat möglicher Bußgelder.

Wer datenschutzrechtlich Verantwortlicher ist, ergibt sich allgemein aus Art. 4 Nr. 7 DSGVO. Hiernach ist „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet […]. Ob sich Mitarbeitende im Falle des Exzesses zu Verantwortlichen im Sinne der DS-GVO aufschwingen, wird von Gerichten und Aufsichtsbehörden teilweise unterschiedlich beurteilt. Die bayrischen Aufsichtsbehörden lehnen (im Gegensatz zu den meisten anderen Aufsichtsbehörden) eine eigene Verantwortlichkeit des Mitarbeitenden in solchen Fällen ab; der Mitarbeitende würde nicht grundsätzlich über Zwecke und Mittel der Abfragesysteme entscheiden, sondern lediglich die ihm zur Verfügung gestellten Abfragesysteme für private Zwecke nutzen. Eine eigene Verantwortlichkeit des Mitarbeitenden bestünde erst dann, wenn dieser die Daten mittels arbeitgeberfremder Ressourcen weiterverarbeitet (vgl. BayLfD, Gemeinsame Verantwortlichkeit – Orientierungshilfe, S. 43f.). Anders sieht es das OLG Stuttgart und schließt sich damit der Mehrheit der Aufsichtsbehörden an: Bereits in dem Moment, in dem der Mitarbeitende überhaupt nicht betrieblich veranlasst tätig wird, begründet er eine eigene Entscheidungsmacht über Zwecke und Mittel der Datenverarbeitung und ist damit Verantwortlicher (vgl. OLG Stuttgart, Beschl. v. 25.2.2025 – 2 ORbs 16 Ss 336/24).

Im Falle eines Mitarbeiterexzesses liegt somit nach überwiegender Ansicht eine datenschutzrechtliche Verantwortlichkeit des Mitarbeitenden vor.

Haftung für Schadensersatz

Entsteht einem Betroffenen infolge eines Datenschutzverstoßes ein Schaden und hat der Verantwortliche den Verstoß zu verschulden, haftet dieser hierfür nach Art. 82 DS-GVO. Steht die den Datenschutzverstoß verursachende Handlung im Bezug zu der Tätigkeit des Mitarbeitenden im Betrieb, so haftet das Unternehmen als verantwortliche Stelle gegenüber dem Betroffenen. Ein Mitarbeiterexzess liegt in dieser Konstellation nicht vor. Liegt jedoch ein Mitarbeiterexzess vor und erfolgt etwa die Verarbeitung zu rein privaten Zwecken, haftet – sofern man der Auffassung der Mehrheit der Aufsichtsbehörden und des OLG Stuttgart folgt – der Mitarbeitende als Verantwortlicher selbst; der Verstoß wird ihm zugerechnet.

Für Betroffene ist dies misslich, da Unternehmen im Gegensatz zu ihren Mitarbeitenden häufig zahlungsfähiger sind. Unter Umständen kann dass Unternehmen dennoch (zusätzlich) in die Haftung genommen werden. Nach Art. 82 Abs. 2 S. 1 DS-GVO haftet jeder an der Verarbeitung beteiligte Verantwortliche für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wurde. Das Unternehmen muss hierfür nicht die schadensverursachende Datenschutzverletzung selbst vorgenommen haben. Insoweit kann die (rechtmäßige) Offenlegung der Daten an den Mitarbeitenden grundsätzlich als Verursachungsbeitrag ausreichen. Das Unternehmen kann sich aber nach Art. 82 Abs. 3 DS-GVO exkuplieren und von der Haftung befreien, indem es nachweist, nicht für den Schaden verantwortlich zu sein. Entlastend können hier bespielsweise die hinreichende Kontrolle des Mitarbeitenden, die ordnungsgemäße Erfüllung der Rechenschaftspflichten, die Durchführung von Schulungen sowie die Implementierung geeigneter technischer und organisatorischer Maßnahmen sein. Um diese Maßnahmen nachweisen zu können, ist im Unternehmen auf eine ordnungsgemäße Dokumentation datenschutzrechtlicher Prozesse zur Erfüllung der eigenen Rechenschaftspflicht zu achten. Eine Zurechnung kann dagegen erfolgen, wenn das (unzulässige) Handeln im Unternehmen gebilligt wird.

Meldepflicht des Unternehmens

Weiterhin kann die unbefugte Verwendung von personenbezogenen Daten durch den Mitarbeitenden eine Meldepflicht des Unternehmens auslösen. Nach Art. 33 DS-GVO sind Verantwortliche grundsätzlich dazu verpflichtet, eine Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde zu melden. Was unter einer solchen Verletzung zu verstehen ist, definiert Art. 4 Nr. 12 DS-GVO: Danach ist hierunter unter anderem eine „Verletzung der Sicherheit, die ob unbeabsichtigt oder unrechtmäßig, […] zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“ zu verstehen. Nutzt der Mitarbeitende die Daten für eigene, unternehmensfremde Zwecke, ist hierin eine unbefugte Offenlegung zu sehen, da die Daten grundsätzlich nur für die Zwecke verarbeitet werden dürfen, zu denen sie erhoben wurden (Zweckbindungsgrundsatz, Art. 5 Abs. 1 lit. b) DS-GVO).

Eine Meldung der Datenpanne an die Aufsichtsbehörde muss dann nicht erfolgen, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Person führt. In die Risikobewertung fließen die Umstände des Einzelfalls ein, etwa die Art beziehungsweise Sensibilität und der Umfang der Daten, die Schwere der Folgen für den Betroffenen und ihre Eintrittswahrscheinlichkeit.

Darüber hinaus ist der von der Datenschutzverletzung Betroffene gem. Art. 34 DS-GVO über diese zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Fazit

Ein Mitarbeiterexzess liegt vor, wenn ein Mitarbeitender unbefugt Daten für nicht unternehmensbezogene Zwecke verarbeitet. Nach überwiegender Auffassung wird er in diesem Fall selbst zum Verantwortlichen, sodass Ansprüche auf Schadensersatz nach Art. 82 DS-GVO in erster Linie ihn treffen. Das Unternehmen kann allerdings unter Umständen mithaften.

Das Unternehmen hat die Möglichkeit, sich hinsichtlich der Haftung zu entlasten. Hierfür ist es Unternehmen anzuraten, geeignete Sicherungsmaßnahmen zu ergreifen und zu dokumentieren. In Betracht kommen hier regelmäßig Konzepte für das Berechtigungsmanagement, sowie die Durchführung von Sensibilisierungs- oder Schulungsmaßnahmen.

Zudem kann eine Datenschutzverletzung durch einen Mitarbeitenden eine Meldepflicht des Unternehmens gegenüber der Aufsichtsbehörde und im Falle eines hohen Risikos auch eine Benachrichtigungspflicht gegenüber den Betroffenen begründen.

Marc-Levin Joppek

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Marc-Levin Joppek
Wissenschaftlicher Mitarbeiter

T +49 521 96535 - 890
F +49 521 96535 - 113
E levin.joppek@brandi.net