Neben jüngst ergangen Entscheidungen der Datenschutzbehörden und Gerichte werfen auch die Pläne der Bundesregierung ihre Schatten voraus. Mit unserem Update möchten wir Sie sowohl über einige spannende vergangene als auch zukünftige Entwicklungen im Datenschutzrecht informieren.

Pläne der „Ampel"

Die „Ampelparteien" haben sich in ihrem Koalitionsvertrag im Bereich des Datenschutzrechts insbesondere Folgendes vorgenommen:

- Institutionalisierung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) im BDSG.
- Stärkung des Beschäftigtendatenschutzes.
- Schaffung eines Straftatbestands für die rechtswidrige De-Anonymisierung personenbezogener Daten.
- Beschleunigung der Verabschiedung der E-Privacy-Verordnung.
- Einsatz für den **Abschluss eines Abkommens mit den USA**, um einen rechtssicheren und datenschutzkonformen Datentransfer auf europäischem Schutzniveau zu ermöglichen.

Während die Pläne zum Beschäftigtendatenschutz und die (mögliche) Verabschiedung der E-Privacy-Verordnung Unternehmen in der kommenden Legislaturperiode unter Umständen vor neue Herausforderungen stellen, wäre ein Datenschutzabkommen mit den USA eine enorme Erleichterung im Umgang mit Datentransfers in die USA und der Nutzung amerikanischer Dienstleister (z. B. Zoom, WhatsApp und Google-Dienste). Denn nach dem Status quo ist die Übermittlung personenbezogener Daten an Empfänger in den USA nur mit großem Aufwand datenschutzkonform möglich (Abschluss Standardvertragsklauseln, Überwachung Einhaltung eines ausreichenden Datenschutzniveaus, zusätzliche Sicherheitsmaßnahmen wie Verschlüsselung).

Ob ein derartig ambitioniertes Abkommen tatsächlich geschlossen werden kann, bleibt angesichts der immer wieder kritisch hinterfragten geltenden amerikanischen „Überwachungsgesetze" allerdings abzuwarten.

DSK: IT-Sicherheitsstandards stehen nicht zur Disposition des Betroffenen

Am 24. November 2021 hat sich die (DSK) zu der umstrittenen Frage geäußert, ob Verantwortliche auf ausdrücklichen Wunsch des Betroffenen von den nach Art. 32 DSGVO geforderten Standards

zur Sicherheit der Verarbeitung personenbezogener Daten zu ihren Lasten abweichen dürfen und festgehalten, dass der einzuhaltende Sicherheitsstandard **nicht zur Disposition des Betroffenen** steht.

Relevanz hat dieser Beschluss beispielsweise im Bereich der E-Mail-Kommunikation. Denn nach Ansicht der Datenschutzbehörden bieten gänzlich unverschlüsselte E-Mails keinen angemessenen Sicherheitsstandard für die Übermittlung personenbezogener Daten und sensible Daten (u. a. Gesundheitsdaten) sollen ohnehin nur mit einer Ende-zu-Ende Verschlüsselung oder einer qualifizierten Transportverschlüsselung (z. B. DANE oder DNSSEC) übermittelt werden dürfen.

Praktisch bedeutet der Beschluss, dass die durchaus übliche (ausdrückliche oder konkludente) Einwilligung eines Betroffenen in unverschlüsselte E-Mail Kommunikation (datenschutzrechtlich) keine Grundlage dafür bietet, per E-Mail zu kommunizieren, soweit personenbezogene Daten übermittelt werden und die Anforderungen an die Verschlüsselung nicht erfüllt sind. Insbesondere E-Mail-Kommunikation muss also zukünftig (noch sorgfältiger) in Bezug auf ihre datenschutzrechtliche Zulässigkeit überprüft werden.

Kontrolle der 3-G Regelungen im Betrieb

Mit Inkrafttreten der Neufassung des § 28b Infektionsschutzgesetzes (IfSG) ist eine gesetzliche Grundlage zur Kontrolle des „3-G"-Status von Beschäftigten geschaffen worden, die eine Arbeitsstätte betreten wollen. Die Frage, ob anstatt der täglichen Sichtkontrolle beim Zugang zur Arbeitsstätte auch eine (dauerhafte) **Speicherung des Status** in Betracht kommt, ist noch offen. Konkretes hierzu kann gemäß Abs. 6 der Vorschrift in einer Verordnung des Bundesministeriums für Arbeit und Soziales geregelt werden, die soweit bekannt bisher nicht erlassen worden ist.

Sofern nicht in einer etwaigen Verordnung abweichend geregelt, reicht es nach Ansicht der DSK (Anwendungshilfe vom 20.12.2021) grundsätzlich aus, dass der Arbeitgeber entsprechende Nachweisdokumente bei Betreten der Arbeitsstätte sichtet und überprüft. Eine Speicherung von Daten (insbesondere Nachweisen) sei hingegen nicht erforderlich. Der Dokumentationspflicht sei genüge getan, wenn regelmäßig dokumentiert wird, durch wen und mit welchen Mitteln eine Zugangskontrolle erfolgt.

Das Gesetz sieht allerdings vor, dass Mitarbeiter ihren Status beim Arbeitgeber hinterlegen können. Soweit von dieser Möglichkeit gebraucht gemacht werden soll, um die Abläufe zu vereinfachen, empfiehlt die DSK, hierfür die **Einwilligung** der Beschäftigten einzuholen. An eine Einwilligung im Beschäftigungskontext sind aufgrund des herrschenden Hierarchieverhältnisses jedoch besonders strenge Anforderungen zu stellen. Es ist in besonderem Maße darauf zu achten, die Freiwilligkeit der Erhebung zu betonen und in jedem Fall parallel die Möglichkeit anzubieten, den Status weiterhin täglich nachzuweisen. Zudem hat die Einwilligung schriftlich oder elektronisch zu erfolgen (§ 26 Abs. 2 BDSG).

Auch wenn das Fragerecht über den „3-G"-Status nun gesetzlich statuiert ist, kann den bisher verbleibenden Unsicherheiten hinsichtlich der Dokumentation und Vereinfachung dieser Kontrollen somit weiterhin nur durch einen gut abgestimmten und (rechtlich) überprüften Organisationsablauf begegnet werden.

Neues zur Schadensersatzpflicht bei DSGVO-Verstößen

Seit Inkrafttreten der DSGVO ist umstritten, ob ein Schadensersatzanspruch nach Art. 82 DSGVO einen konkreten (erheblichen) Schaden bei dem Betroffenen voraussetzt oder im Rahmen der möglichst effektiven Durchsetzung des Europarechts („effet utile") schon der Verstoß gegen die Vorschriften der DSGVO allein einen Anspruch begründen kann.

Während ein Schadensersatzanspruch in der Vergangenheit teilweise abgelehnt wurde, soweit kein konkreter nicht nur unbedeutender (insbesondere persönlichkeitsrechtlicher) Schaden vorgetragen wurde (z. B. OLG München, 27.10.2021 – 20 U 7051/20 oder LG Essen, 23.09.2021 – 16 O 182/20), schließen sich die deutschen Gerichte in letzter Zeit vermehrt der Ansicht an, dass es der „effet utile" gebiete, den Schadensbegriff der

DSGVO weit auszulegen und **jeder DSGVO-Verstoß einen Schadensersatzanspruch begründe** – unabhängig von der Darlegung konkreter nachteiliger Konsequenzen für den Betroffenen (z. B. LAG Niedersachen, 22.10.2021, 16 Sa 761/20, LAG Hessen oder LG Mainz, 12.11.2021 – 3 O 12/21). Die Frage, ob der Schadensersatzanspruch konkrete Folgen für den Betroffenen voraussetzt, die über den durch den Verstoß hervorgerufenen „Ärger" hinausgehen, ist bisher nicht höchstrichterlich geklärt.

Vor diesem Hintergrund hat das Landgericht Saarbrücken diese und andere Fragen in Bezug auf Art. 82 DSGVO mit Beschluss vom 22.11.2021 (5 O 151/19) dem **EuGH** vorgelegt (Rechtssache C-741/21). Die Kernfrage nach der Erforderlichkeit konkreter Konsequenzen hatte im April 2021 auch der Österreichische Oberste Gerichtshof (OGH) nach Luxemburg adressiert und zudem angefragt, ob „unerhebliche" Schäden den Anspruch ausschlössen, soweit ein konkreter Schaden Voraussetzung für den Anspruch sei (Rechtssache C-300/21).

Das Deutsche Bundesarbeitsgericht (BAG) geht bisher davon aus, dass ein Anspruch auf Schadensersatz nach der DSGVO keine weiteren (erheblichen) Konsequenzen auf Seiten des Betroffenen voraussetzt, hat dem EuGH aber Fragen zur Bedeutung des Verschuldens in diesem Zusammenhang vorgelegt. (Vorlagebeschluss vom 26.08.2021 –Rechtssache C-667/21).

Die Entscheidungen(en) des EuGHs in diesen Rechtssachen werden in der Praxis richtungsweisende Bedeutung haben. Denn sollte sich die Rechtsauffassung durchsetzen, dass allein der Verstoß gegen die DSGVO (unabhängig eines hieraus resultierenden konkreten Schadens) einen Schadensersatzanspruch des Betroffenen begründen kann, dürften derartige Ansprüche zukünftig deutlich an Bedeutung gewinnen. In diesem Fall könnten beispielsweise schon vermeintliche Bagatellverstöße (z. B. fehlerhafte Informationen oder Auskünfte) zu (Sammel-)Klagen Betroffener führen.

Die wechselhafte Rechtsprechung und die hieraus resultierenden Vorlagen an den EuGH zeigen, dass das Datenschutzrecht nach wie vor ständigen Entwicklungen unterworfen ist und Datenschutzmanagement und DSGVO-Compliance nie abgeschlossene Themen darstellen werden. Um Risiken zu reduzieren, ist daher jederzeit eine sorgfältige Beobachtung der aktuellen Entwicklungen erforderlich. Gleichzeitig gilt es, pragmatische Lösungen zu entwickeln, um trotz der zahlreichen rechtlichen Vorgaben handlungsfähig zu bleiben.

Kontakt

Sollten Sie zu diesen und anderen datenschutzrechtlichen Themen Fragen haben, beraten wir Sie gerne.

Bei Bedarf wenden Sie sich bitte an:

Andrea Ringle

Partnerin, Rechtsanwältin,
Fachanwältin für Gewerblichen Rechtsschutz

Büro Hamburg
+49-40-35006-151
Andrea.Ringle@BRL.de

Ingwert Liesch

Rechtsanwalt, Datenschutzbeauftragter (TÜV)

Büro Hamburg
+49-40-35006-151
Ingwert.Liesch@BRL.de

Diese von BRL BOEGE ROHDE LUEBBEHUESEN herausgegebene Mandanteninformation enthält auszugsweise eine Auswahl an Gesetzesänderungen, Entscheidungen der Rechtsprechung und Auffassungen der Behörden und ersetzt nicht die Beratung im Einzelfall.

Für die Richtigkeit wird eine Haftung nicht übernommen. Für weitere Informationen wenden Sie sich bitte an:

BRL BOEGE ROHDE LUEBBEHUESEN
Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern mbB

© BRL BOEGE ROHDE LUEBBEHUESEN

BRL

Hamburg
Jungfernstieg 30
20354 Hamburg
+49 40 35006-0

Berlin
Pariser Platz 4A
10117 Berlin
+49 30 565556-0

Dortmund
Lübkestraße 3
44141 Dortmund
+49 231 108771-0

Bochum
Meinolphusstraße 6-10
44789 Bochum
+49 234 610688-0

Hannover
Gellertstraße 6
30175 Hannover
+49 511 543688-31

Frankfurt
Westhafenplatz 1
60327 Frankfurt
+49 69 12007471-10

München
Arnulfstraße 122/126
80636 München
+49 89 272755-125

info@BRL.de
www.BRL.de

PGW

PGW Bielefeld *
Adenauerplatz 7
33602 Bielefeld
+49 521 96464-0

mail@PGW_Partner.de
www.PGW-Partner.de

* *Die Kanzlei PGW in Bielefeld hat sich Mitte 2021 der BRL Gruppe angeschlossen und wird bis Mitte 2022 mit dieser rechtlich verschmelzen*

Internationales Netzwerk

MOORE BRL
www.Moore-BRL.de