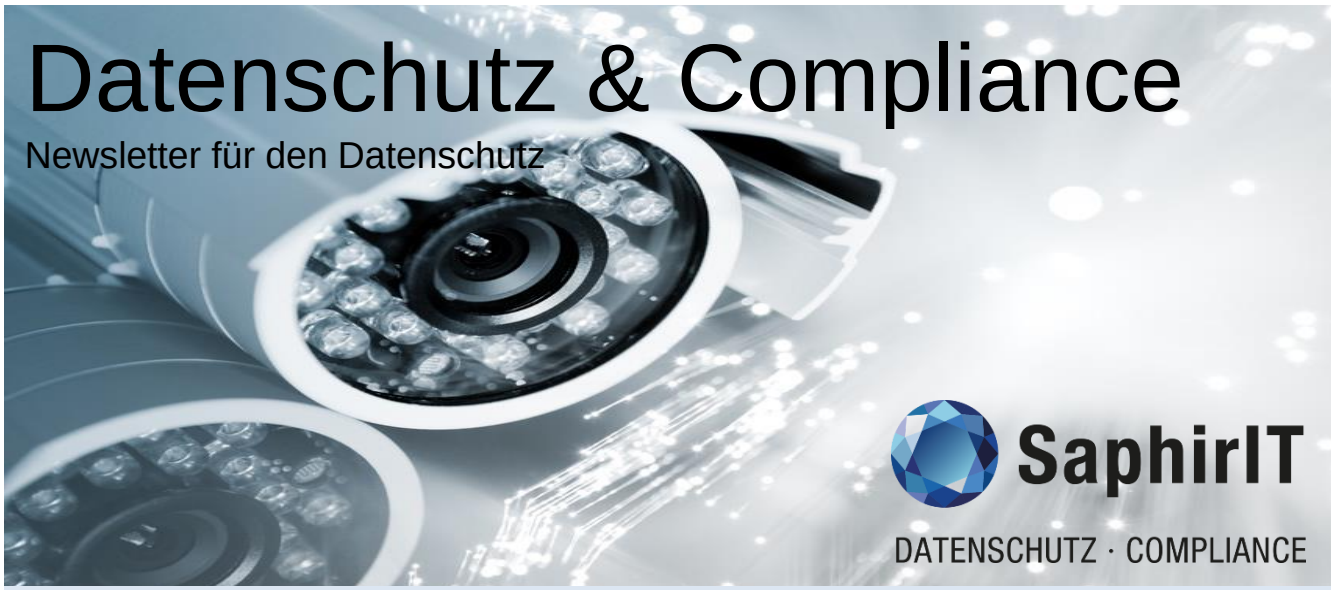


**Ausgabe Juli 2021** | Seite 234 - 238

INHALT

SEITE 234
**Betriebsrätemodernisierungsgesetz Datenschutzrechtliche Verantwortlichkeit des Betriebsrats**

SEITE 237
**Vereinigtes Königreich ist sicheres Drittland -Europäische Kommission erlässt Angemessenheitsbeschluss**

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Juli 2021.

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
*Ihre SaphirIT GmbH*

# Betriebsrätemodernisierungsgesetz

## Datenschutzrechtliche Verantwortlichkeit des Betriebsrats

Am 18.06.2021 ist das neue Betriebsrätemodernisierungsgesetz in Kraft getreten.

Unter anderem regelt dies nunmehr im neuen § 79a BetrVG das datenschutzrechtliche Verhältnis zwischen Betriebsrat und Arbeitgeber.

Wichtig ist dies deshalb, da bisher nicht geklärt war, ob der Betriebsrat selbst verantwortlich für die Verarbeitung personenbezogener Daten ist, oder ob er als Teil des Arbeitgebers der Verantwortlichkeit des Arbeitgebers unterfällt.

Bereits in unserem Newsletter April 2020 hatten wir auf die Problematik hingewiesen und dargestellt, dass eine einheitliche Rechtsprechung bisher nicht vorlag. Das Bundesarbeitsgericht (BAG) hatte die Frage zuletzt ausdrücklich offengelassen (BAG, Beschl. v. 09.04.2019, Az. 1 ABR 51/17).

Der neue § 79a BetrVG bringt nun Licht ins Dunkel.

## Betriebsverfassungsgesetz § 79a Datenschutz

Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Arbeitgeber und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. § 6 Absatz 5 Satz 2, § 38 Absatz 2 des Bundesdatenschutzgesetzes gelten auch im Hinblick auf das Verhältnis der oder des Datenschutzbeauftragten zum Arbeitgeber.

Bereits vor der Gesetzesänderung war klar, dass der Betriebsrat, unabhängig davon ob er als eigener Verantwortlicher zu sehen ist oder nicht, datenschutzrechtliche Vorgaben einzuhalten hat. § 79a S. 1 BetrVG hat demnach lediglich klarstellende Wirkung.

§ 79a S. 2 BetrVG konkretisiert die Datenschutzgrundverordnung (DSGVO) dahingehend, dass die datenschutzrechtliche Verantwortlichkeit beim Arbeitgeber liegt.

Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet ist der Arbeitgeber der für die Verarbeitung Verantwortliche.

Somit ist nun durch das Gesetz geklärt, dass der Betriebsrat selbst nicht als Verantwortlicher im Sinne der DSGVO gilt. Für den Arbeitgeber ergeben sich hieraus Pflichten denen er nachkommen muss.

1. Der Betriebsrat ist nicht verpflichtet ein eigenes Verzeichnis von Verarbeitungstätigkeiten zu führen. Daher ist der Arbeitgeber dazu verpflichtet die Verarbeitungstätigkeiten des Betriebsrats in seinem Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren.

2. Arbeitgeber und Betriebsrat sind dazu verpflichtet sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften zu unterstützen. Insbesondere bei Auskunftsansprüchen ist dies der Gesetzesbegründung zufolge vorgeschrieben.

3. Bezüglich des Datenschutzbeauftragten stellt die Gesetzesbegründung klar, dass die Aufgaben des Datenschutzbeauftragten auch gegenüber dem Betriebsrat als Teil der verantwortlichen Stelle bestehen. Der Betriebsrat kann demnach, soweit erforderlich, die Beratung durch den Datenschutzbeauftragten in Anspruch nehmen.

Etwaigen Konflikten wird dahingehend aus dem Weg gegangen, dass der Datenschutzbeauftragte dem Arbeitgeber gegenüber zur Verschwiegenheit bezüglich Informationen die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen, verpflichtet ist.

Sowohl der Betriebsrat als auch der Arbeitgeber dürften ein hohes Interesse daran haben die Rahmenbedingungen der Zusammenarbeit zu regeln, sodass es nicht zu Konflikten kommt.

Folgende Fragen können in diesem Zusammenhang relevant sein:

- Wer stellt in welcher Form Informationen zur Verfügung, die zur Erstellung der Verarbeitungsbeschreibungen der Prozesse des Betriebsrats im Verzeichnis von Verarbeitungstätigkeiten notwendig sind?
- Wie informiert der Betriebsrat Personen (z.B. Beschäftigte) die sich mit Fragen an ihn wenden und die eine weitere Datenerhebung nach sich ziehen?
- Wie werden neue Betriebsratsmitglieder über die Verarbeitung der sie betreffenden personenbezogenen Daten informiert?
- Wie wird sichergestellt, dass der Betriebsrat ausreichende Kenntnisse hat, um seine datenschutzrechtlichen Aufgaben erfüllen zu können?
- Inwiefern ist eine spezielle datenschutzrechtliche Schulung der Mitglieder des Betriebsrats erforderlich bzw. sinnvoll?
- Ist der Betriebsrat in der Lage die technischen und organisatorischen Maßnahmen, die teilweise eigenverantwortlich umgesetzt werden müssen, umzusetzen?
- Wie erfolgt die Absicherung des Betriebsratsbüros oder die Nutzung der IT-Infrastruktur des Arbeitgebers?
- Wie werden Unterlagen des Betriebsrats vernichtet?
- Wie erfolgt die Kommunikation innerhalb des Betriebsrats? Werden Messenger verwendet?
- Wer gibt Auskunft, wenn eine betroffene Person ihren Auskunftsanspruch geltend macht? Muss der Arbeitgeber hier mit einbezogen werden?
- Wie werden Datenpannen in der Sphäre des Betriebsrates behandelt?
- Wie kann der Datenschutzbeauftragte des Unternehmens auch den Betriebsrat unterstützen?

Da es viele Schnittstellen zwischen Arbeitgeber und Betriebsrat gibt, kann es sinnvoll sein die gegenseitige Unterstützung beispielsweise in einer Rahmenbetriebsvereinbarung zu regeln. Ziel sollte es sein zwischen allen Beteiligten einen Konsens herzustellen.

Auch hinsichtlich der Haftung ergeben sich Besonderheiten für den Arbeitgeber. Zur Haftung des Betriebsrats selbst enthält § 79a BetrVG keine Regelung.

Grundsätzlich ist der Arbeitgeber der Verantwortliche, weshalb ihm auch mögliche Bußgelder bei Verstößen durch den Betriebsrat drohen. Der Arbeitgeber hat daher durchaus ein berechtigtes Interesse daran, dass der Betriebsrat ein umfassendes Schutzniveau, insbesondere bei der Weitergabe von sensiblen Beschäftigtendaten an den Betriebsrat, gewährleistet.

Gemäß Art. 82. Abs. 3 DSGVO kann eine Haftung des Verantwortlichen jedoch ausscheiden, wenn dieser nachweisen kann, dass er nicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Demnach dürfte davon auszugehen sein, dass ein Arbeitgeber, der dem Betriebsrat aufgrund seiner Unabhängigkeit als Strukturprinzip der Verfassung keine Vorgaben zum Datenschutz machen kann, nicht für Datenschutzverstöße des Betriebsrats haften muss.

Sollten Sie zu dieser Problematik Fragen haben oder Hilfe bei der Erstellung einer Rahmenbetriebsvereinbarung haben sprechen Sie uns gerne an.

# Vereinigtes Königreich ist sicheres Drittland

## Europäische Kommission erlässt Angemessenheitsbeschluss

Die Europäische Kommission hat am 28.06.2021 das Vereinigte Königreich kurz vor Ablauf der Übergangsphase, die Ende Juli endete zum sicheren Drittland erklärt. Durch den erlassenen Angemessenheitsbeschluss bleibt die Übermittlung personenbezogener Daten auch nach dem Brexit möglich.

Seit dem 01.01.2021 ist das Vereinigte Königreich nicht mehr Mitglied der Europäischen Union. Folglich gilt es als Drittland und die Art. 44ff. Datenschutzgrundverordnung (DSGVO) sind zu beachten. Diese Vorschriften sollen sicherstellen, dass Daten auch dann noch einem angemessenen Schutz unterliegen, wenn Unternehmen oder andere Einrichtungen nicht mehr der DSGVO unterliegen. Es soll dennoch ein angemessenes Datenschutzniveau bestehen.

Für Drittländer stellt ein Angemessenheitsbeschluss die einfachste Möglichkeit dar ein angemessenes Datenschutzniveau zu gewährleisten. Die EU-Kommission kann nach ausführlicher Prüfung beschließen, dass das Datenschutzniveau im Drittland dem Standard der DSGVO entspricht.

Besteht ein Angemessenheitsbeschluss ist ein ungehinderter Datenverkehr von einem EU-Land in das betreffende Drittland möglich.

Da das Vereinigte Königreich jahrelang Mitglied der Europäischen Union war und bis zuletzt dort die DSGVO Anwendung fand, ist es nicht verwunderlich, dass der britische Datenschutz dem der DSGVO in vielen Zügen ähnelt.

Dennoch gab es auch Kritik am Erlass des Angemessenheitsbeschlusses. Insbesondere wurden Bedenken dahingehend geäußert, ob die dort geltenden Gesetze ausreichend regulieren, dass ein Datentransfer von dem Vereinigten Königreich in andere Drittstaaten ebenfalls ein hinreichendes Datenschutzniveau für personenbezogene Daten und Betroffenenrechte gewährleisten. Der Rechtsgedanke der Art. 44ff. DSGVO müsse sich auch im Vereinigten Königreich wiederfinden.

Zudem wurde gerügt, dass es Ausnahmeregelungen für die Zwecke der Einwanderungskontrolle gebe, wodurch Betroffenenrechte eingeschränkt würden. Aus diesem Grund werden Datenübermittlungen zu diesem Zweck derzeit vom Angemessenheitsbeschluss ausgenommen.
Schließlich sind noch die Überwachungsgesetze (wie z.B. der Investigatory Powers Act von 2016) des Vereinigten Königreichs problematisch. Diese erlauben britischen Geheimdiensten ausgeweitete Überwachungsbefugnisse.

Wichtig ist, dass ein einmal erteilter Angemessenheitsbeschluss nicht für immer gilt. Die EU-Kommission muss alle vier Jahre erneut prüfen, ob das Drittland weiterhin ein angemessenes Datenschutzniveau gewährleisten kann. Es besteht daher durchaus die Möglichkeit, dass die EU-Kommission in vier Jahren zu einem anderen Ergebnis kommt.

Bis dahin gilt der Angemessenheitsbeschluss jedoch und ein sicherer Datentransfer in das Vereinigte Königreich ist sichergestellt.

Zwar ist für den Datentransfer nun keine Genehmigung mehr erforderlich; die Prüfung, ob die allgemeinen datenschutzrechtlichen Voraussetzungen für eine Datenübertragung erfüllt sind, ist davon jedoch unabhängig. Diese Prüfung ist durch den Verantwortlichen immer durchzuführen.



SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de