

Datenschutz im Betriebsratsbüro

Helene Baumgartner (AK Wien)
Sebastian Klocker (ÖGB)
Thomas Riesenecker-Caba (FORBA)



FORBA



ÖGB



Inhalt

BETRIEBSRAT UND DATENSCHUTZ	4
BEGRIFFSERKLÄRUNGEN ZUM VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN	6
HANDLUNGSEMPFEHLUNGEN ZUR UMSETZUNG DER DATENSCHUTZ- RECHTLICHEN ANFORDERUNGEN	9
DOKUMENTATION (PROTOKOLLIERUNG) DER VORGENOMMENEN ÄNDERUNGEN	14
ALLGEMEINE ANGABEN ZUM/ZUR VERANTWORTLICHEN NACH ARTIKEL 4 UND ARTIKEL 30 DSGVO	15
ERSTELLUNG VON DATENSCHUTZ- UND DATENSICHERHEITSMABNAHMEN	17
IT-SICHERHEIT IM BETRIEBSRAT: VEREINBARTE MASSNAHMEN ZUR IT- UND DATENSICHERHEIT	21
DATENBLATT ZU EINER KONKRETEN VERARBEITUNGSTÄTIGKEIT (SYSTEM) NACH ARTIKEL 30 DSGVO	22
ZUM ABSCHLUSS	28



IMPRESSUM

Herausgeber: Österreichischer Gewerkschaftsbund, 1020 Wien, Johann-Böhm-Platz 1,
Tel.: 01/534 44-0, Fax: 01/534 44-204, E-Mail: oegb@oegb.at, Web: www.oegb.at
ZVR 576 439 352

Hersteller: Verlag des Österreichischen Gewerkschaftsbundes GmbH, 1020 Wien,
Johann-Böhm-Platz 1, Tel.: 01/662 32 96, Fax: 01/662 32 96-39793,
Vorbehaltlich Satz- und Druckfehler.



Betriebsrat und Datenschutz

Seit 25. Mai 2018 gilt EU-weit ein einheitliches Datenschutzrecht, die Datenschutz-Grundverordnung (DSGVO). Da die DSGVO zahlreiche „Öffnungsklauseln“ enthält, die den nationalen Gesetzgeber verpflichten und/oder berechtigen, bestimmte Angelegenheiten gesetzlich näher zu regeln, gibt es neben der DSGVO in Österreich ein nationales Datenschutzgesetz - das „Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz - DSG)“. Neben der DSGVO und dem DSG kann es auch in anderen Gesetzen Regelungen zum Datenschutz geben.

Warum Datenschutz für den Betriebsrat wichtig ist

Als Betriebsrat¹ verarbeitest du regelmäßig persönliche Daten der Belegschaft. Deswegen gilt: Du bist datenschutzrechtlich selbst verantwortlich und musst die Anforderungen der DSGVO einhalten.

Das Verarbeitungsverzeichnis – das Herzstück der Dokumentation

Eine deiner zentralen Aufgaben ist die Führung eines **Verzeichnisses aller Datenverarbeitungen** (kurz: **Verarbeitungsverzeichnis**). Darin wird festgehalten, welche Daten der Betriebsrat wofür nutzt. Dieses Verzeichnis muss auf Nachfrage der Datenschutzbehörde vorgelegt werden.

So dokumentierst du richtig (Nachweispflicht)

Diese Broschüre unterstützt dich bei der Erstellung der notwendigen datenschutzrechtlichen Dokumente.

Als Verantwortlicher musst du die folgenden Unterlagen ausfüllen und sicher dokumentieren, um die Einhaltung deiner Verpflichtungen jederzeit nachweisen zu können.

Konkret bedeutet das:

- Speichere die elektronischen Dokumente in einem **Datenschutzordner** am Betriebsrats-PC.
- Sorge auch für eine Ablage der wichtigen Unterlagen in **ausgedruckter Form**.

Beachte bitte, dass die Dokumentationsunterlagen im Betriebsratsbüro

aufliegen müssen, aktuell zu halten sind und die Datenschutzbehörde zur Überprüfung der Einhaltung des Datenschutzrechts Einsicht nehmen kann. Deiner oder deinem Arbeitgeber:in und einer oder einem möglicherweise eingerichteten Datenschutzbeauftragten sind diese Unterlagen jedoch **NICHT** vorzulegen. Beide haben kein Recht auf Einsicht in diese Dokumentation des Betriebsrates. Unabhängig vom Datenschutzrecht gilt für dich und alle anderen Mitglieder des Betriebsrats folgende gesetzliche Verschwiegenheitspflicht²:

„Die Mitglieder und Ersatzmitglieder des Betriebsrates sind verpflichtet, über alle in Ausübung ihres Amtes bekanntgewordenen Geschäfts- und Betriebsgeheimnisse, insbesondere über die ihnen als geheim bezeichneten technischen Einrichtungen, Verfahren und Eigentümlichkeiten des Betriebes Verschwiegenheit zu bewahren. Werden im Zuge der Mitwirkung in personellen Angelegenheiten Mitgliedern des Betriebsrates persönliche Verhältnisse oder Angelegenheiten der Arbeitnehmer bekannt, die ihrer Bedeutung oder ihrem Inhalt nach einer vertraulichen Behandlung bedürfen, so haben sie hierüber Verschwiegenheit zu bewahren.“

Weitere Informationen findest du unter:

- Beschäftigtendatenschutz. Handbuch für die betriebliche Praxis. ÖGB-Verlag, 2020, <https://shop.oegbverlag.at/beschaefigtendatenschutz-9783990464052>
- Die europäische Datenschutzgrundverordnung aus Arbeitnehmer:innen-sicht, GPA, 2024, <https://tinyurl.com/bdrckk9y>
- AK Portal: „Datenschutz für Betriebsräte“ https://www.arbeiterkammer.at/service/betriebsrat/rechteundpflichtendesbetriebsrates/Datenschutz_fuer_Betriebsraete.html
- Verarbeitung von personenbezogenen MitarbeiterInnen-Daten. Mitbestimmung und Datenschutz. Praktische Gewerkschaftsarbeit 5, ÖGB-Verlag, 2025, <https://www.voegb.at/skripten-und-broschueren/praktische-gewerkschaftsarbeit/verarbeitung-von-personenbezogenen-mitarbeiterinnen-daten>

¹ Es wird in der Regel der Begriff Betriebsrat als Körperschaft verwendet, wenn einzelne Personen des Betriebsrates angesprochen sind, verwenden wir „Mitglied des Betriebsrates“ gemäß § 115 ArbVG

² Gemäß § 115 ArbVG.

Begriffserklärungen zum Verzeichnis der Verarbeitungstätigkeiten

Hier findest du die wichtigsten Begriffe und Artikel der Datenschutz-Grundverordnung (DSGVO). Konkrete Begriffsbestimmungen findet man im Artikel 4 DSGVO.

DSGVO	VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Downloadmöglichkeit unter: https://dsb.gv.at/rechte-pflichten/rechtsquellen
DSG	Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999, idgF., Downloadmöglichkeit unter: https://dsb.gv.at/rechte-pflichten/rechtsquellen
Datenschutzbehörde	Von Österreich gemäß Artikel 51 DSGVO eingerichtete unabhängige staatliche Stelle www.dsb.gv.at
Datenschutzbeauftragte:r	Stelle bei der oder dem Arbeitgeber:in (kann auch extern vergeben sein), die unter bestimmten Voraussetzungen ³ verpflichtend einzurichten ist. Die Stellung und die Aufgaben einer oder eines Datenschutzbeauftragten sind in Artikel 38 und 39 DSGVO beschrieben. Der Betriebsrat benötigt keine:n rechtlich verpflichtende:n Datenschutzbeauftragte:n! Aus rechtlichen Gründen empfiehlt es sich, die für den Datenschutz zuständige Person nicht als „Datenschutzbeauftragte:r“ zu bezeichnen.

³ Artikel 37 DSGVO.

Verantwortliche:r	<i>Die natürliche oder juristische Person, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Da der Betriebsrat Daten von Beschäftigten verarbeitet, ist es somit jedes Mitglied des Betriebsrats.</i>
Verarbeitung	<i>Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie: das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.</i> Also jede Tätigkeit, die du mit personenbezogenen Daten durchführst – egal ob digital oder auf Papier – von der Erhebung über die Speicherung bis hin zum Löschen oder der Weitergabe.
Verzeichnis der Verarbeitungstätigkeiten	Dokumentation der (elektronischen oder nicht elektronischen) personenbezogenen Datenverarbeitungen.
Besondere Kategorien von Daten	Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Die wichtigsten DSGVO-Artikel für deine Betriebsratsarbeit

Die Links zu den rechtlichen Grundlagen finden sich auch auf der Webseite der österreichischen Datenschutzbehörde unter <https://www.dsb.gv.at/> (Bereich Rechte&Pflichten/Rechtsquellen)

Artikel 4 DSGVO	In diesem Artikel finden sich die Definitionen, die in der DSGVO Anwendung finden.
Artikel 5 DSGVO	Dieser Artikel beschreibt die Grundsätze, die bei personenbezogener Datenverarbeitung einzuhalten und zu dokumentieren sind.
Artikel 6 DSGVO	Dieser Artikel regelt, unter welchen Bedingungen die Verarbeitung von personenbezogenen Daten rechtmäßig erfolgt.
Artikel 9 DSGVO	Auch die DSGVO kennt besonders schutzwürdige (bisher sensible) Daten. Der Umgang mit diesen besonderen Kategorien von Daten ist in diesem Artikel beschrieben.
Artikel 30 DSGVO	Dieser Artikel beschreibt die Anforderungen an ein Verzeichnis von Verarbeitungstätigkeiten.
Artikel 32 DSGVO	Dieser Artikel beschreibt Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen (TOMs) zur Sicherheit der Verarbeitung.

Handlungsempfehlungen zur Umsetzung der datenschutzrechtlichen Anforderungen

Folgender **Ablauf** wird zur Planung und Umsetzung der datenschutzrechtlichen Anforderungen vorgeschlagen:

A. Klärung der Zuständigkeit = Verantwortlichkeit

Die DSGVO verlangt zwingend eine:n Verantwortliche:n (Art. 4 Nr. 7 DSGVO), die oder der klar benannt werden kann – zum Beispiel, um Bußgelder oder Klagen korrekt zu adressieren. In Österreich ist die Betriebsratskörperschaft aber keine eigene juristische Person, sondern nur ein Organ der Belegschaft.

Wichtig: Trotz dieser juristischen Feinheit muss klar sein, wer für die Einhaltung der Datenschutzpflichten zuständig ist. Um hier Rechtssicherheit zu schaffen, empfehlen wir, die Zuständigkeit – inklusive der nötigen Kompetenzen und Ressourcen – wie folgt festzulegen:

1. Obwohl der Betriebsrat keine eigene juristische Person ist, werden die BR-Körperschaft und ihre Mitglieder in der Praxis als Verantwortliche im Sinne der DSGVO behandelt. Das bedeutet, das gesamte Gremium und jedes Mitglied tragen die Verantwortung für die Einhaltung der Pflichten. Das Gremium sollte per Beschluss festlegen, welches Mitglied sich primär als Ansprechperson für die Belegschaft um das Thema Datenschutz kümmert und die notwendigen Richtlinien vorbereitet. Gibt es keinen Beschluss bzgl. einer zuständigen Person, ist es im Zweifel die oder der Betriebsratsvorsitzende.
2. Haltet intern fest (am besten per Beschluss), dass jedes Betriebsratsmitglied, das sich nicht an die vereinbarten Datenschutzregeln hält – zum Beispiel, indem es eigenmächtig Daten verarbeitet oder weitergibt – selbst zur oder zum Verantwortlichen wird.
3. Gibt es einen Betriebsratsfonds, gilt das hier beschriebene Vorgehen gleichermaßen für die Datenverarbeitung des Betriebsratsfonds (hier ist der Betriebsratsfonds Verantwortlicher iSd DSGVO).

B. Betroffene ermitteln

Bevor der Betriebsrat mit der Datenverarbeitung beginnt, muss er genau klären, wessen Daten er verarbeitet. Diese Personengruppen werden in der DSGVO „betroffene Personen“ genannt. Typische Kategorien Betroffener sind: aktive Beschäftigte, ausgeschiedene Beschäftigte, Arbeitgeber:in, externe Dritte.

C. Bestandsaufnahme: Welche Daten nutzen wir wofür?

Dies ist der zentrale Schritt für das Verarbeitungsverzeichnis. Der Betriebsrat muss für jede Tätigkeiten klären, welche Daten er hat, wo diese gespeichert sind und wofür sie genutzt werden.

Stelle dir für jede Verarbeitungstätigkeit (z. B. Prüfung der Lohnverrechnung) folgende Fragen:

- **Welche Daten?** Welche konkreten Kategorien von Daten verarbeitest du (z. B. Name, Gehalt, Krankenstandstage)?
- **Wofür? (Zweckbindung)** Was ist der genaue Zweck der Verarbeitung (z. B. Kontrolle der korrekten Einstufung)?
- **Wo liegen diese Daten?** Liegen die Daten elektronisch oder auf Papier vor? Speicherst du sie auf betriebsratseigenen Rechnern oder Ablagesystemen oder arbeitest du auf IT-Systemen, die dein:e Arbeitgeber:in zur Verfügung stellt? (Wichtig für die Zuständigkeit wesentlicher Sicherheitsfragen.)

D. Unterscheidung der Datenarten

Es muss geklärt werden, ob **besondere Kategorien von Daten**⁴ (das sind besonders sensible Informationen wie z. B. Gesundheit, Gewerkschaftszugehörigkeit) verarbeitet werden, da diese grundsätzlich strenger geschützt sind als nicht-sensible Daten (z. B. Gehaltsdaten).

E. Empfänger:innenkreise auflisten: Wer bekommt welche Daten?

Die Stellen, an die Daten weitergegeben oder offengelegt werden, sind aufzulisten. Darunter fällt auch die Übermittlung an andere Organe der

⁴ Früher hat man diese Daten als „sensible Daten“ bezeichnet. Diesen Begriff kennt die DSGVO nicht mehr. Vgl. Artikel 9 DSGVO.

Belegschaft (Jugendvertrauensrat, andere Betriebsratsgremien im Unternehmen, ...) oder auch die Übermittlung an AK/ÖGB usw.

F. Rechtsgrundlage prüfen: Ist die Datenverwendung erlaubt?

Jede Datenverarbeitung braucht eine Rechtsgrundlage (die „Erlaubnis“ aus der DSGVO). Für die Betriebsratsarbeit kommen hauptsächlich diese zwei Grundlagen in Frage:

- **Gesetz, Kollektivvertrag oder Betriebsvereinbarung:** Der Betriebsrat ist mit einer Reihe von Rechten/Pflichten ausgestattet. Dies betrifft auch Daten, die die oder der Arbeitgeber:in aufgrund des ArbVG (z. B. Lohnkontrolle), eines Kollektivvertrags (KollV) oder einer Betriebsvereinbarung (BV) an den Betriebsrat übermittelt. Hier ist die Rechtsgrundlage bereits durch die gesetzliche oder vertragliche Pflicht gegeben.
- **Zustimmung der Beschäftigten:** Für alle Daten, deren Verarbeitung nicht durch Gesetz, KollV oder BV gedeckt ist, braucht es die freiwillige und informierte Zustimmung der jeweiligen Beschäftigten.

G. Verarbeitungsverzeichnis erstellen und pflegen

Alle nun erhobenen Informationen sind im „**Verzeichnis von Verarbeitungstätigkeiten**“ festzuhalten.

Wichtig: Dieses Dokument muss aktuell gehalten werden.

H. Lösch- und Aufbewahrungsfristen festlegen

Daten dürfen nicht unbegrenzt gespeichert werden. Es muss für jede Datenverarbeitung festgelegt werden, wann die Daten gelöscht oder vernichtet werden. Bei der Festlegung der Fristen gelten folgende Grundsätze:

- **Zweckbindung:** Daten dürfen nur so lange aufbewahrt werden, wie sie für den ursprünglichen Zweck (z. B. für eine laufende Kontrolle oder eine laufende Klage) gebraucht werden bzw. wie es gesetzlich vorgeschrieben ist.
- **Datenminimierung:** Nur die zwingend notwendigen Daten sollen gespeichert werden und müssen gelöscht werden, sobald der Zweck erfüllt ist.

I. Datensicherheitsmaßnahmen festlegen und dokumentieren

Es müssen technische und organisatorische Maßnahmen getroffen werden, um die Daten sicher zu verarbeiten und vor Missbrauch zu schützen. Diese getroffenen Maßnahmen sind (z. B. im Verarbeitungsverzeichnis) festzuhalten.

Wichtig: Diese Maßnahmen sind bei der Verarbeitung besonderer Daten-Kategorien (ehemals sensible Daten) gemäß Art 9 DSGVO besonders streng zu wählen!

Konkrete Sicherheitsmaßnahmen (Beispiele):

- **Zugriffskontrolle:** Konzepte für Berechtigungen und Zugriffe definieren (Wer darf wann auf welche Daten zugreifen?).
- **Verschleierung:** Nutzung von Pseudonymisierung (Ersetzen des Namens durch ein Pseudonym) oder Anonymisierung von Daten, wo dies möglich ist.
- **Schulung & Geheimhaltung:** Regelmäßige Datenschuttschulungen für Mitglieder und Mitarbeiter:innen des Betriebsrats sowie die Geheimhaltungserklärung der administrativen Beschäftigten im BR-Büro.

J. Regelmäßige Überprüfung der getroffenen Maßnahmen!

K. Externe Dienstleister:innen erfassen und Verträge schließen

Wenn der Betriebsrat Aufgaben oder IT-Services an externe Dienstleister:innen (Bezeichnung in der DSGVO ist „Auftragsverarbeiter“) auslagert (z. B. IT-Wartung, Cloud-Speicher), muss mit diesen ein Vertrag abgeschlossen werden.

Wichtig für den Vertrag:

Es muss ein **schriftlicher Vertrag** mit der oder dem Dienstleister:in abgeschlossen werden, der **Datenschutz und Datensicherheit** gewährleistet. Dieser Vertrag muss dem Betriebsrat auch **Kontrollrechte** bei der oder dem Dienstleister:in sichern.

L. Betroffenenrechte: Abläufe für Anfragen festlegen

Jede betroffene Person (also jede Person, deren Daten der Betriebsrat verarbeitet) hat Rechte nach der DSGVO. Es müssen im Betriebsrat interne

Abläufe festgelegt werden, um diese Anfragen fristgerecht und korrekt beantworten zu können.

Diese Rechte sind unter anderem zu beachten:

- **Auskunft:** Das Recht auf Auskunft darüber, welche Daten der Betriebsrat verarbeitet.
- **Berichtigung:** Das Recht auf Korrektur falscher Daten.
- **Löschung:** Das Recht auf Löschung der Daten, wenn kein Zweck mehr vorliegt.



Dokumentation (Protokollierung) der vorgenommenen Änderungen

Wir empfehlen, alle Änderungen, die in der Dokumentation zur Erfüllung der Anforderungen des Datenschutzrechts erfolgen, zu dokumentieren (Nachweis der Änderungen).

[illegible]

gegebenenfalls neue Zeilen einfügen

Dieses Protokoll speichern und regelmäßig (halbjährlich bis jährlich) ausdrucken und zur schriftlichen Dokumentation beifügen.

Allgemeine Angaben zur oder zum Verantwortlichen nach Artikel 4 und Artikel 30 DSGVO

Beachtet, dass sich die Kontaktdaten nach einer Betriebsratswahl ändern könnten und dann in diesem Dokument angepasst werden müssen. Dokumentiert daher Änderungen immer auch in der „*Dokumentation (Protokollierung) der vorgenommenen Änderungen*“.

1. Verantwortliche:r	... Arbeiter:innen-/Angestellten-Betriebsrat der ...
2. Anschrift	
3. Kontaktdaten	
Telefon	
Mobiltelefon	
E-Mail	
4. Für Datenschutz im Betriebsrat zuständige Person	Name der zuständigen Person (wenn keine bestimmt wurde, die oder der Betriebsrats-Vorsitzende)
5. Etwaige Vertreter:in der zuständigen Person	

Erhebt in einem ersten Schritt alle unterschiedlichen Verarbeitungstätigkeiten, die durch den Betriebsrat vorgenommen werden.

Empfehlungen zu einer Gliederung und Unterteilung der möglichen Verarbeitungstätigkeiten erhältst du bei deiner Interessenvertretung.

Erklärung (Kurzinfo) zu den Anforderungen an die Rechenschaftspflicht nach Artikel 5 der Datenschutz-Grundverordnung (DSGVO)

Jede Verarbeitungstätigkeit ist im Hinblick auf die folgenden Grundsätze zur Verarbeitung personenbezogener Daten zu überprüfen.

Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 DSGVO

Wenn du personenbezogene Daten verarbeitest, darf das nur unter Beachtung der folgenden Grundsätze erfolgen:

Rechtmäßige Verarbeitung (1a): Wenn personenbezogene Daten verarbeitet werden, bedarf dies einer Rechtsgrundlage, nämlich (Pflicht-)Befugnis des Betriebsrates nach ArbVG, KollV oder BV, Einwilligung der Betroffenen, Vertrag oder überwiegendes Interesse (das wäre zu begründen!).

Verarbeitung nach Treu und Glauben (1a): Die geplante Datenverarbeitung muss (gegenüber den Betroffenen) fair und ausgewogen sein.

Transparenz gegenüber Betroffenen (1a): Alle Personen, deren Daten verarbeitet werden, sind darüber zu informieren (z. B. schriftliches Informationsblatt bei Einstellung, Hinweis in BR-Zeitung, Intranetseite des BR).

Zweckbindung (1b): Die Zwecke, warum Daten verarbeitet werden, sind möglichst präzise zu definieren. Daten die für einen bestimmten Zweck erhoben wurden, dürfen auch nur für diesen Zweck verarbeitet werden.

Datenminimierung (1c): Es dürfen nur Daten verarbeitet werden, die zur Erreichung des Zwecks unbedingt notwendig sind.

Richtigkeit (1d): Die gespeicherten Daten müssen richtig sein und aktuell gehalten werden.

Speicherbegrenzung (1e): Daten dürfen nur so lange gespeichert werden, wie dies zur Erreichung der Zwecke notwendig erscheint. Sobald der Zweck erfüllt ist und keine festgelegten Aufbewahrungsfristen mehr gelten, müssen die Daten gelöscht werden.

Die Fristen sind im Verarbeitungsverzeichnis (siehe dazu das Musterdatenblatt ab Seite 22) anzuführen.

Integrität und Vertraulichkeit (1f): Jede:r Verantwortliche muss angemessene Maßnahmen zur Datensicherheit treffen. Hinweise zur Definition von technischen und organisatorischen Maßnahmen zur Datensicherheit sind im nächsten Kapitel beschrieben.

Erstellung von Datenschutz- und Datensicherheitsmaßnahmen

Bei der Verarbeitung von personenbezogenen Daten sind auch die Anforderungen zur Daten- und IT-Sicherheit zu prüfen und zu dokumentieren (im Betrieb können die betrieblich vereinbarten Maßnahmen auch in anderslautenden Dokumenten wie z. B. „IT-Policy“ oder „IT-Sicherheitsleitlinien“ veröffentlicht sein). Die in Folge angeführten Textbausteine dienen dabei zur Orientierung und können für die Dokumentation der eigenen Maßnahmen zur IT-Sicherheit nach Prüfung im Betriebsrat verwendet werden.

Folgende Checkliste zur IT-Sicherheit kann für die Betriebsratsarbeit und die Arbeit im Betriebsratsbüro – zusätzlich zu den betrieblichen Anforderungen (sofern vorhanden) – von der oder dem BR-Zuständigen für Datenschutz herangezogen werden.

Organisatorische Sicherheitsmaßnahmen

- Personenbezogene Daten und vertrauliche Dokumente (von Beschäftigten, von der oder dem Arbeitgeber:in, von Dritten) dürfen nicht auf privaten Geräten gespeichert werden, außer es wurde ausdrücklich gestattet und es sind zusätzliche Sicherheitsmaßnahmen zum Schutz dieser Daten und Dokumente vereinbart worden.
- Neue Software und neue Apps, die vom BR installiert werden, sind auf Geräten, auf denen sich personenbezogene Daten von Beschäftigten befinden, nur nach Prüfung zu verwenden. Die Geschäfts-/Nutzungsbedingungen der Software bzw. der Apps sind im Hinblick auf die Anforderungen der DSGVO zu prüfen und abzulegen.
- Das Speichern von personenbezogenen Daten und/oder Dokumenten bei externen Cloud-Anbietern ist nur nach Prüfung der datenschutzrechtlichen Anforderungen (z. B. es wurde eine Lizenz käuflich erworben und der Cloud-Anbieter verpflichtet sich zur Einhaltung der Bestimmungen der DSGVO) gestattet. Es ist ein Auftragsvertragsvertrag abzuschließen.
- Daten/Dokumente von Beschäftigten oder Informationen aus dem Betriebsrat, die sich auf (privaten) Geräten des Betriebsrates befinden, sind

regelmäßig zu sichern, damit diese nicht verloren gehen können. Nicht mehr notwendige Daten/Dokumente sind zu löschen.

- Es wird eine Unterscheidung in zwei Stufen von Daten/Informationen getroffen:
 - **öffentliche Daten/Dokumente:** Diese können ohne Einschränkung betrieblich verwendet und veröffentlicht werden (z. B. Speiseplan der Kantine).
 - **vertrauliche Daten/Dokumente:** Diese dürfen nur von ausgewählten Mitgliedern des Betriebsrates verwendet werden (Informationen von oder über einzelne Beschäftigte).
- Die Betroffenenrechte (z. B. gegenüber Beschäftigten) sind im Sinne der rechtlichen Anforderungen zu erfüllen. Die betroffenen Personen werden darüber und über ihre Rechte gemäß DSGVO (z. B. auch in Formularen) informiert.
- Die im Betriebsrat vereinbarten und getroffenen Maßnahmen werden dokumentiert und regelmäßig auf ihre Anwendbarkeit geprüft.

Personelle Sicherheitsmaßnahmen

- Für dienstliche Geräte (von der oder dem Arbeitgeber:in zur Verfügung gestellt) wie PC, Laptop, Smartphone, Datenträger (z. B. USB-Stick) sind die im Betrieb definierten Regelungen – z. B. betreffend Passwortgestaltung, Virenschutz oder Datensicherung – einzuhalten.
- Geräte für die Betriebsratsarbeit sind zu schützen (z. B. Passwort, Multi-Faktor-Anmeldung, Ausloggen bei Verlassen des Arbeitsplatzes) und Zugangsdaten zu diesen Geräten dürfen nicht an Dritte weitergegeben werden.
- Die datenschutzrechtliche Aufgabenverteilung und Zuständigkeiten im Betriebsrat und im BR-Büro sind ausdrücklich festzuschreiben und zu dokumentieren.
- Betriebsräte unterliegen nach dem ArbVG einer gesetzlichen Verschwiegenheit, daher ist vor Weitergabe von Daten zu prüfen, ob dies im Sinne der gesetzlichen Bestimmungen auch zulässig ist. Ersatzmitglieder dürfen nur diejenigen Daten/Dokumente erhalten, die sie im Rahmen ihrer konkreten Vertretungstätigkeit benötigen.
- Mitarbeiter:innen im BR-Büro, die keine Tätigkeit als Betriebsrat ausüben, sind – zusätzlich zur betrieblichen Verschwiegenheit – gesondert

zur Geheimhaltung der im Arbeitsalltag bekannt werdenden Informationen zu verpflichten.

- Bei Ausscheiden aus dem Betriebsrat sind alle relevanten Daten und Dokumente, die während der BR-Tätigkeit entstanden bzw. bekannt geworden sind, sofern diese noch benötigt werden, nach Rücksprache mit der oder dem BR-Vorsitzenden und der oder dem Zuständigen für Datenschutz im BR zurückzugeben und erst dann zu löschen.
- Beim Ausscheiden aus dem Betriebsrat bzw. dem BR-Büro (bei Admin-Beschäftigten) sind die dienstlichen Betriebsmittel (PC, Laptop, Smartphone, aber auch Schlüssel/Zutrittskarten) zurückzugeben. Gegebenenfalls sind auf den Endgeräten befindliche Daten vor bzw. nach Übergabe an die oder den BR-Vorsitzende:n bzw. die für Datenschutz im BR zuständige Person zu löschen.
- Die oder der Zuständige für Datenschutz im Betriebsrat weist regelmäßig (1 bis 2 Mal pro Jahr) im Rahmen von BR-Sitzungen auf die Anforderungen zu Datenschutz und Datensicherheit und die vereinbarten Sicherheitsleitlinien (Spielregeln) hin.
- Bei Verlassen des Arbeitsplatzes und/oder des Büros ist der Systemzugang zu sperren und Papierdokumente vor dem Einblick Unberechtigter zu schützen bzw. zu versperren.
- Betriebsratsmitglieder und Mitarbeiter:innen im BR-Büro sind zum Datenschutz und zu den getroffenen Regelungen der Verarbeitung personenbezogener Daten zu schulen.

Technische Sicherheitsmaßnahmen

- Bei Geräten (PC, Laptop, Smartphone, Datenträger) und Programmen/Apps bzw. im Ablagesystemen (elektronisch und Handakte) ist zu prüfen, wer darauf Zugriff benötigt und die notwendigen Rechte sind zu vergeben und regelmäßig zu prüfen.
- Auf privaten Geräten, auf denen sich personenbezogene Daten/Dokumente befinden, sind die Zugriffsberechtigungen sowie die Betriebssoftware und der Virenschutz aktuell zu halten, Passwörter sind sicher zu gestalten und zu ändern, wenn die Gefahr besteht, dass Dritte davon Kenntnis erlangt haben. Wenn das System zusätzliche Sicherheitsvorkehrungen (Multi-Faktor-Authentifizierung) anbietet, sind diese zu nutzen.
- In öffentlichen WLANs (die oft nicht ausreichend gesichert sind) ist be-

sondere Vorsicht im Umgang mit personenbezogenen Daten geboten, bei Arbeiten oder Telefonieren im öffentlichen Raum (z. B. im Zug, im Kaffeehaus) sind die betrieblichen Daten zu schützen (z. B. Blickschutz für das Display).

- › Bei Datenübermittlung sind vertrauliche Daten, wenn technisch möglich, zu schützen (Verschlüsselung, Dateien mit Passwortschutz).
- › Daten auf mobilen Datenträgern (z. B. USB-Stick) können leicht verloren gehen und sind daher besonders zu schützen.
- › Beim Öffnen von E-Mail-Anhängen bzw. dem Anklicken eines Links in E-Mails oder im Internet ist darauf zu achten, dass keine Gefahr für die betriebliche Infrastruktur entstehen kann.
- › Als besonders schutzwürdig eingestufte Datenverarbeitungen sind zu protokollieren, dabei soll erfasst werden, wer wann aus welchem Grund die Datenverarbeitung durchgeführt hat (durch die Software oder händisch zu dokumentieren).
- › Die Verwaltung von Schlüsseln/Zutrittskarten zum BR-Büro und zu versperrbaren Kästen mit Dokumenten ist zu dokumentieren.
- › BR-Dokumente und Daten sind gesichert zu speichern und nach Zweckerreichung zu löschen bzw. zu vernichten.

IT-Sicherheit im Betriebsrat: Vereinbarte Maßnahmen zur IT- und Datensicherheit

Folgende Maßnahmen zur IT-Sicherheit wurden in der Sitzung vom [Datum einfügen] vereinbart:

Beschreibung der Maßnahmen zur IT-Sicherheit (kann aus vorheriger Checkliste übernommen werden)

- › Maßnahme 1
- › Maßnahme 2
- › Maßnahme 3
- › Maßnahme 4
- › Maßnahme 5
- › Maßnahme 6
- › Maßnahme 7
- › Maßnahme 8
- › Maßnahme 9
- › Maßnahme 10

gegebenenfalls neue Zeilen einfügen

ausgefüllt von

Name einfügen

Ort einfügen

Datum einfügen

Dieses Dokument wird in Folge als Nachweis bzw. Dokumentation der Einhaltung der datenschutzrechtlichen Vorgaben benötigt und ist daher nach dem Befüllen zu speichern und gegebenenfalls auszudrucken.

Datenblatt zu einer konkreten Verarbeitungstätigkeit (System) nach Artikel 30 DSGVO

Bitte beachtet, dass sich der Umfang an Daten, die für einen gewissen Zweck verarbeitet werden, auch ändern kann und dieses Dokument/dieses File entsprechend anzupassen ist.

- Wir empfehlen daher die Tatsache, dass Änderungen vorgenommen wurden, in der Übersicht „*Dokumentation (Protokollierung) der vorgenommenen Änderungen*“ festzuhalten.
- Für jede Verarbeitungstätigkeit muss ein gesondertes Datenblatt erstellt werden.
- Empfehlungen zu einer Gliederung und Unterteilung der möglichen Verarbeitungstätigkeiten erhältst du bei deiner Interessenvertretung.
- Ab der nächsten Seite findet sich ein Muster zur Beschreibung einer konkreten Verarbeitungstätigkeit.

Dieses Dokument wird in Folge als Nachweis bzw. Dokumentation der Einhaltung der datenschutzrechtlichen Vorgaben benötigt und ist daher nach dem Befüllen zu speichern und gegebenenfalls auszudrucken.

Verzeichnis Verarbeitungstätigkeit

1.	Datenblatt Nummer	*hier einfügen*	Fortlaufende Nummer
2.	Datenblatt zur Verarbeitungstätigkeit	*hier einfügen*	Beschreibung der konkreten Verarbeitungstätigkeit
3.	Sind bei dieser Verarbeitungstätigkeit personenbezogene Daten der Beschäftigten in einem System gespeichert, das die oder der Arbeitgeber:in zur Verfügung stellt?	o ja	Arbeitgeber:in ist primär für die Datensicherheit (Artikel 32 DSGVO) verantwortlich und der Betriebsrat muss sich an Datenschutzrecht und betriebliche Vorgaben (z. B. IT-Policy) halten. Zusätzliche Maßnahmen laut Checkliste sind zu prüfen
		o nein	Betriebsrat muss sich als Verantwortlicher um Datensicherheit (Artikel 32 DSGVO) kümmern (siehe Checkliste)
		o teils/teils	Betriebsrat muss sich als Verantwortlicher bei seinen „Systemen“ um Datensicherheit (Artikel 32 DSGVO) kümmern (siehe Checkliste)
4.	Zwecke der Verarbeitung	*hier einfügen*	
5.	Herkunft der Daten	o von der oder dem Arbeitgeber:in o von den Beschäftigten o von Dritten	
6.	Getroffene technische und organisatorische (inkl. personelle) Maßnahmen zur Datensicherheit (Artikel 30 und 32 DSGVO)	vereinbarte Maßnahmen laut Checkliste	

7.	Betroffene Gruppen, von denen Daten für diese Verarbeitungstätigkeit verarbeitet werden	- o aktive Beschäftigte - o ehemals Beschäftigte - o Familienangehörige - o Arbeitgeber:in - o Dritte (z. B. Vertragspartner:innen) und zwar: *hier einfügen*	
8.	Rechtsgrundlage der Verarbeitung (gemäß Artikel 6 DSGVO)	- o Einwilligung der betroffenen Person(en) - o Erfüllung eines Vertrages (z. B. ermäßigte Bestellung über BR-Büro) - o Erfüllung einer rechtlichen Verpflichtung (z. B. [Kontroll] Befugnis laut ArbVG, KollIV oder BV)	
9.	Wird der Betriebsrat bei der Datenverarbeitung durch eine:n Auftragsverarbeiter:in unterstützt und werden Daten bei dieser oder diesem verarbeitet?	- o ja - o nein	wenn ja, Angaben zu der oder dem Auftragsverarbeiter:in und zum geschlossenen Vertrag
10.	Findet eine Speicherung von Daten außerhalb der EU statt (z. B. Cloud-Lösung, bei der Daten nicht in einem Rechenzentrum innerhalb der EU liegen)?	- o ja - o nein	wenn ja, Angaben zu der oder dem Auftragsverarbeiter:in und zum geschlossenen Vertrag

Neben diesen Angaben sind die Daten(kategorien) je Verarbeitungstätigkeit näher zu beschreiben (siehe Folgeseite). Datenkategorien sind z. B. Name, Adresse, Kostenstelle.

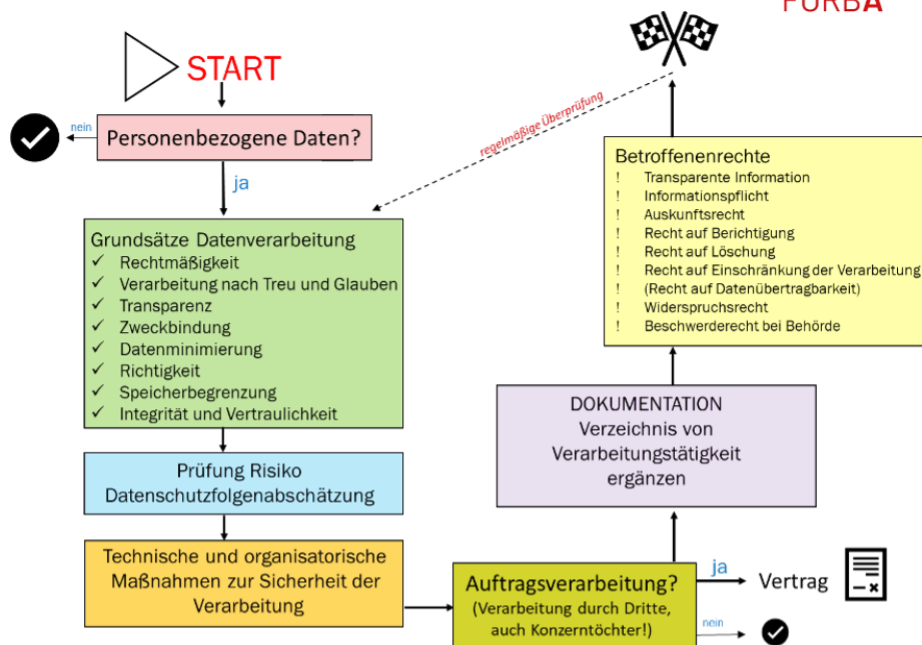
[illegible]

Zum Abschluss

Diese Publikation beschreibt die wesentlichen Schritte zur Erfüllung der Dokumentationspflichten nach den datenschutzrechtlichen Anforderungen, ersetzt jedoch nicht die Beratung im Einzelfall.

Hier nochmals eine Übersicht der wesentlichen Schritte zur datenschutzkonformen Verarbeitung von personenbezogenen Daten.

Datenschutzkonforme Datenverarbeitung



Informiert euch bei eurer Fachgewerkschaft oder Arbeiterkammer regelmäßig über weitere Unterlagen und Publikationen bzw. besucht die Webseite der österreichischen Datenschutzbehörde und abonniert deren Newsletter unter <https://www.dsb.gv.at/ueber-die-datenschutzbehoerde/newsletter>.

Notizen

[illegible]

Notizen

[illegible][illegible]

