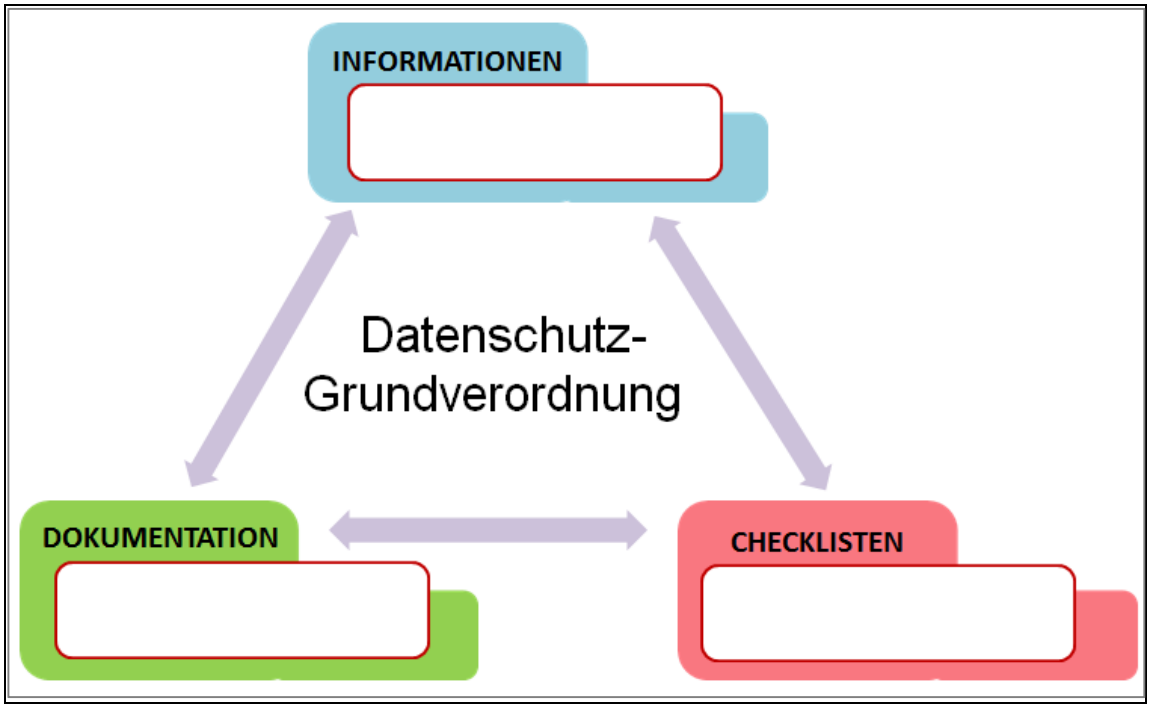
Betriebsratsarbeit im Zeichen der EU Datenschutz-Grundverordnung

GÖD

Mai 2018

Betriebsratsarbeit im Zeichen der EU Datenschutz-Grundverordnung

Checklisten, Informationsblätter und Musterformulare zur Erfüllung der rechtlichen Pflichten



Ein Projekt der Arbeiterkammer Wien und des Österreichischen Gewerkschafts-bundes (ÖGB)

durchgeführt von der Forschungs- und Beratungsstelle Arbeitswelt (FORBA)

Jänner 2018

Inhalt

INFORMATION ZU DEN VORLIEGENDEN DOKUMENTEN (INFO 1)

Ab 25. Mai 2018 gilt EU-weit ein einheitliches Datenschutzrecht, die Datenschutz-Grundverordnung (DS-GVO).

Da die DS-GVO zahlreiche "Öffnungsklauseln" enthält, die den nationalen Gesetzgeber verpflichten und/oder berechtigen, bestimmte Angelegenheiten gesetzlich näher zu regeln, gibt es neben der DS-GVO in Österreich weiterhin ein nationales Datenschutzgesetz. Dieses ebenfalls ab 25. Mai 2018 gültige Gesetz lautet "Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz - DSG)".

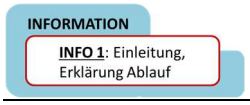
Inwieweit konkrete Maßnahmen des neuen Datenschutzrechts auch Sie als Betriebsrat/BR-Körperschaft treffen, können Sie in der Checkliste „*CHECK 1: Prüfung der Verantwortung*“ erkennen.

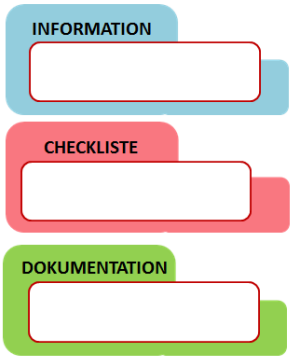
Wenn das Resultat der Prüfung in der Checkliste „*CHECK 1: Prüfung der datenschutzrechtlichen Anforderungen an Verantwortliche gemäß DS-GVO und DSG*“ ergeben hat, dass Sie als Betriebsrat (Betriebsratskörperschaft) Verantwortlicher im Sinne des Datenschutzrechts sind, lesen Sie bitte zuerst „*INFO 3: Handlungsempfehlungen zur Umsetzung der datenschutzrechtlichen Anforderungen*" zur Erstellung eines Informationssicherheits- und Datenschutz-Managementsystems.

ACHTUNG: Ein in Ihrem Betrieb möglicherweise vorhandener Betriebsrats-Fonds gilt ebenfalls als eigener Verantwortlicher im Sinne des Datenschutzrechts. Es kann jedoch das hier vorgeschlagene Vorgehen angewendet werden.

Diese Publikation unterstützt Sie in der Durchführung der notwendigen Schritte zur Erfüllung der Anforderungen des Datenschutzrechts.

Die folgenden Unterlagen sind daher von Ihnen als datenschutzrechtlicher Verantwortlicher in ihrer Rolle als Betriebsrat/Betriebsratskörperschaft zu befüllen und als Nachweis der Einhaltung der datenschutzrechtlichen Verpflichtungen zu dokumentieren (d.h. Speichern der elektronischen Dokumente in einem Datenschutzordner am Betriebsrats-PC und Ablage in ausgedruckter Form).





In dieser Publikation finden sich drei Arten von Dokumenten (jeweils farblich unterscheidbar), die entweder

1. zur *Information* dienen,
2. durchzuführende Prüfschritte beschreiben (*Checkliste*) oder
3. Vorlagen zur *Dokumentation* nach Datenschutzrecht enthalten

Die folgenden notwendigen Unterlagen werden in dieser Publikation beschrieben und stehen auch zum Download (DOKU 1 bis 4 als Word- und Excel-Vorlage) zur Verfügung.

INFO 1:	Einleitung, Erklärung Ablauf
CHECK 1:	Prüfung der Verantwortung
INFO 2:	Begriffe, Definitionen
INFO 3:	Handlungsempfehlungen
DOKU 1:	Änderungen, Historie
DOKU 2:	Allgemeine Angaben zum Verantwortlichen und Grundsätze Datenverarbeitung
CHECK 2:	Prüfung von organisatorischen, personellen und technischen Maßnahmen zur IT-Sicherheit
INFO 4:	Mögliche Maßnahmen zur IT-Sicherheit
DOKU 3:	Beschreibung der Maßnahmen zur IT-Sicherheit
DOKU 4:	Verzeichnis Verarbeitungstätigkeiten, für jede Verarbeitungstätigkeit, die in DOKU 2 angeführt ist, ist ein eigenes Blatt auszufüllen.

Bei weiteren Fragen wenden Sie sich bitte an Ihre Fachgewerkschaft oder Arbeiterkammer.

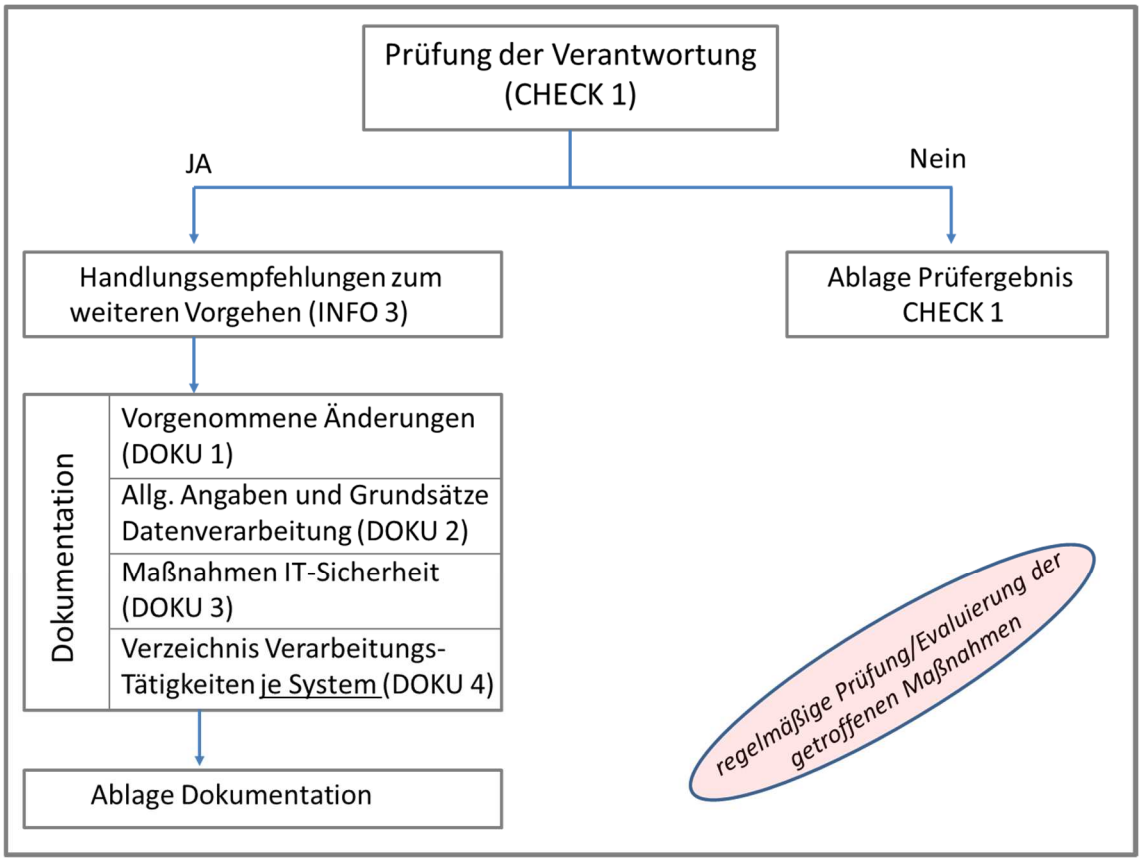
Einzelne Begriffe werden unter „*INFO 2: Informationen und Begriffserklärungen zum Verzeichnis der Verarbeitungstätigkeiten*“ näher ausgeführt. In den verschiedenen Unterlagen sind Begriffe, die erklärt werden, jeweils durch das Symbol [>>] gekennzeichnet.

Beachten Sie bitte, dass die Dokumentationsunterlagen (DOKU 1 – 4) im Betriebsratsbüro aufliegen müssen und die [>>] Datenschutzbehörde zwecks Überprüfung der Einhaltung des Datenschutzrechts Einsicht nehmen kann.

Ihrem Arbeitgeber und einem möglicherweise eingerichteten [>>] Datenschutzbeauftragten sind diese Unterlagen jedoch NICHT vorzulegen. Beide haben kein Recht auf Einsicht in diese Dokumentation des Betriebsrates.

Bitte beachten Sie weiters, dass gemäß § 115 ArbVG für Mitglieder des Betriebsrates eine gesetzliche Verschwiegenheitspflicht gilt.

Überblick des Ablaufes



PRÜFUNG DER DATENSCHUTZRECHTLICHEN ANFORDERUNGEN AN VERANTWORTLICHE GEMÄSS DS-GVO UND DSG (CHECK 1)

Beantworten Sie bitte die folgenden Fragen, wobei unter "Daten von Beschäftigten" (Beschäftigte = Arbeitnehmer/innen und Beschäftigte im BR-Büro) Informationen zu diesen Personen wie Name, Adresse, Telefonnummer oder Dokumente (Beitritt Gewerkschaft, Anmeldung Betriebsausflug, Dienstzettel, Arbeitsverträge) verstanden werden.

	JA	NEIN
1) Haben Sie als Betriebsrat Daten von Beschäftigten auf einem der folgenden GERÄTE gespeichert? (bitte je Geräteart beantworten)		
a) PC oder Laptop, der vom Arbeitgeber zur Verfügung gestellt wird?		
b) ihrem privaten PC oder Laptop?		
c) einem PC oder Laptop - vom Betriebsrat (bzw. BR-Fonds) auf eigene Rechnung angeschafft?		
d) Smartphone oder Tablet, das vom Arbeitgeber zur Verfügung gestellt wird?		
e) privates Smartphone oder Tablet?		
f) einem Smartphone oder Tablet - vom Betriebsrat (bzw. BR-Fonds) auf eigene Rechnung angeschafft?		
2) Speichern Sie als Betriebsrat Daten von Beschäftigten auf externen Festplatten, USB-Sticks oder auf externen Datensicherungssystemen (z.B. Cloudlösungen wie Dropbox)?		

	JA	NEIN
3) Nutzen Sie als Betriebsrat zur Kommunikation mit Beschäftigten einen oder mehrere der in Folge angeführten DIENSTE?		
a) Mailingsystem, das der Arbeitgeber zur Verfügung stellt?		
b) privat genutztes Mailsystem (z.B. Webmail)?		
c) Messenger (wie z.B. WhatsApp)?		
d) soziale Medien (wie z.B. Facebook)?		
e) Datenanwendung im Internet (Cloudlösung, wie z.B. Dropbox)?		
4) Besitzen Sie Dokumente oder Listen auf Papier (z.B. Ausdrucke) mit Beschäftigtendaten, die in Ordnern im Betriebsratsbüro abgelegt sind?		

Haben Sie **zumindest eine der Fragen mit JA beantwortet**, sind Sie in Ihrer Rolle als Betriebsrat datenschutzrechtliche/r [>>] Verantwortliche/r und haben die Bestimmungen der Datenschutz-Grundverordnung und des Datenschutzgesetzes zu erfüllen. Dies beinhaltet weiters das Führen eines [>>] Verzeichnisses von Verarbeitungstätigkeiten, wobei diese Unterlage Sie dabei unterstützt.

INFORMATIONEN UND BEGRIFFSERKLÄRUNGEN ZUM VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN (INFO 2)

Dieses Informationsblatt beschreibt die wichtigsten Begriffe und Artikel der Datenschutz-Grundverordnung (DS-GVO).

Begriffserklärung (diese Begriffe sind im Dokument mit [>>] angeführt)

DS-GVO	"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: http://tinyurl.com/DSGVO-2018"
DSG	Datenschutzgesetz - DSG in der Fassung Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, Downloadmöglichkeit unter: http://tinyurl.com/RIS-DSG2018
Datenschutzbehörde	von Österreich gemäß Artikel 51 DS-GVO eingerichtete unabhängige staatliche Stelle
Datenschutzbeauftragte/r	Stelle beim Arbeitgeber (kann auch extern vergeben sein), die unter bestimmten Voraussetzungen (siehe Artikel 37 DS-GVO) verpflichtend einzurichten ist. Stellung (in Artikel 38) und Aufgaben (in Artikel 89) sind in der DS-GVO beschrieben. Der Betriebsrat benötigt keinen gesetzlich verpflichtenden Datenschutzbeauftragten!
Verantwortliche/r	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

Verarbeitung	jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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
Verzeichnis der Verarbeitungstätigkeiten	Dokumentation der (elektronischen oder nicht elektronischen) personenbezogenen Datenverarbeitungen eines Verantwortlichen.
besondere Kategorien von Daten	personenbezogener 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

Verweis datenschutzrechtliche Regelung

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

Artikel 4 DS-GVO	In diesem Artikel finden sich die Definitionen, die in der DS-GVO Anwendung finden.
Artikel 5 DS-GVO	Dieser Artikel beschreibt die Grundsätze, die bei personenbezogener Datenverarbeitung einzuhalten und zu dokumentieren sind.

Artikel 6 DS-GVO	Dieser Artikel regelt, unter welchen Bedingungen die Verarbeitung von personenbezogenen Daten rechtmäßig erfolgt.
Artikel 30 DS-GVO	Dieser Artikel beschreibt die Anforderungen an ein Verzeichnis von Verarbeitungstätigkeiten.
Artikel 9 DS-GVO	Auch die DS-GVO kennt besonders schutzwürdige (bisher sensible) Daten. Der Umgang mit diesen besonderen Kategorien von Daten ist in diesem Artikel beschrieben.
Artikel 32 DS-GVO	Dieser Artikel beschreibt Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen (TOMs) zur IT-Sicherheit.

HANDLUNGSEMPFEHLUNGEN ZUR UMSETZUNG DER DATENSCHUTZRECHTLICHEN ANFORDERUNGEN (INFO 3)

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

A. **Klärung der Zuständigkeit = Verantwortlichkeit** (die DS-GVO bringt keine Klarheit, da die Betriebsratskörperschaft keine juristische Person, sondern nur das Organ der teilrechtsfähigen Körperschaft „Belegschaft" ist), wir empfehlen die Zuständigkeit für die Einhaltung und Durchführung der datenschutzrechtlichen Verpflichtungen (klarerweise samt den entsprechenden Kompetenzen) wie folgt festzulegen

   1. Körperschaft ist Verantwortlicher iSd DS-GVO (vormals datenschutzrechtlicher Auftraggeber nach DSG 2000), im Betriebsrats-Gremium ist mit Beschluss festzulegen, wer sich um Datenschutz kümmert. Diese Person hat die Kompetenz/Zuständigkeit Richtlinien (siehe DOKU 3) zu erarbeiten, die verantwortliche Person und die Richtlinien können allenfalls im Gremium beschlossen werden. Gibt es diesen Beschluss bzgl. verantwortlicher Person im Betriebsrat nicht, ist es im Zweifel der/die Betriebsratsvorsitzende/r.
   2. Klarstellung im Betriebsrat, dass jemand, der sich nicht an dieses *Konzept des Datenschutzmanagements* hält (kann ebenfalls mit Beschluss gefasst werden), so zB eigenmächtig Daten verarbeitet, selbständiger Verantwortlicher ist.
   3. Gibt es einen BR-Fonds, sollte dieses Datenschutzmanagement-konzept gleichermaßen für die Datenverarbeitung des BR-Fonds zur Anwendung gelangen (hier ist der BR-Fonds Verantwortlicher iSd DS-GVO).

B. Auflistung: **Welche Daten** hat der Betriebsrat? Was macht er damit? (Welche Datenverarbeitungen? Für welche Zwecke?) elektronisch – nicht elektronisch? Auf Systemen des AG oder auf eigenen Systemen? (notwendig für DOKU 2 und 4)

C. Unterscheidung: Welche Datenarten: „besondere Kategorien von Daten" (vormals sensible Daten, zB Gesundheitsdaten) – nicht sensible Daten (zB Gehaltsdaten)

D. **Betroffene ermitteln** (aktive Mitarbeiter, ausgeschiedene AN, AG, externe Dritte)

E. **Empfängerkreise auflisten** (das bedeutet Offenlegung von Daten, Übermittlung an Dritte, Übermittlung an andere Organe der Belegschaft, Übermittlung an AK/ÖGB usw)

F. **Prüfung der Grundsätze für die Verarbeitung personenbezogener Daten** insb. Rechtmäßigkeit: rechtliche Grundlage der Datenverwendung (zB ArbVG für vom AG übermittelte Daten im Rahmen einer auf dem ArbVG, KollV oder BV basierenden Datenverarbeitung, Zustimmung der AN für sonstige Daten)

G. Festhalten der vorgenannten Erhebungen im „**Verzeichnis von Verarbeitungstätigkeiten**“ (vormals Meldung an das DVR) – ist klarerweise aktuell zu halten!

H. NEU: **Löschfristen** aufnehmen (dabei die Grundsätze der Datensparsamkeit und Datenminimierung sowie Zweckbindung beachten)!

I. I**mplementierung von Datensicherheitsmaßnahmen** plus Dokumentation im Verarbeitungsverzeichnis (zB Anonymisierung oder Pseudonymisierung von Daten, Berechtigungs- und Zugriffskonzepte definieren, Datenschutzschulungen der Mitglieder und Mitarbeiter des BR, Geheimhaltungserklärung der Mitarbeiter des BR in Bezug auf Informationen des BR), das gilt natürlich in besonderem Maße für besondere Kategorien von Daten (vormals: sensible Daten)

J. NEU: regelmäßige **Evaluierung der getroffenen Maßnahmen**!

K. **Auftragsverarbeiter erfassen** (zB ausgelagerte Dienstleistungen und IT-Services) und in Verträgen mit diesen eigene Datenschutz- und Datensicherheitspflichten an diese überbinden (mit entsprechenden Kontrollrechten)

L. **Standardisierung des Umganges mit Begehren von der Datenverarbeitung betroffenen Personen**: a) Auskunft b) Berichtigung c) Löschung

DOKUMENTATION (PROTOKOLLIERUNG) DER VORGENOMMENEN ÄNDERUNGEN (DOKU 1)

Dokumentieren Sie alle Änderungen, die Sie in Ihrer Dokumentation zur Erfüllung der Anforderungen des Datenschutzrechts durchführen (Nachweis der Änderungen).

Datum	wer hat geändert	was wurde geändert
		gegebenenfalls neue Zeilen einfügen

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

ALLGEMEINE ANGABEN ZUM/ZUR VERANTWORTLICHEN NACH ARTIKEL 4 UND ARTIKEL 30 DS-GVO (DOKU 2)

Beachten Sie, dass sich die Kontaktdaten nach einer Betriebsratswahl ändern könnten und dann in diesem Dokument angepasst werden müssen. Dokumentieren Sie daher Änderungen immer auch in der „*Dokumentation (Protokollierung) der vorgenommenen Änderungen* (DOKU 1)“.

1. Verantwortliche/r:	… Arbeiter/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, der/die Betriebsrats-Vorsitzende)
5. Etwaige Vertreter/in der zuständigen Person	

Übersicht der Verarbeitungstätigkeiten und Nachweis (siehe Erklärung unten) **zur Einhaltung der Grundsätze zur Verarbeitung personenbezogener Daten** (Rechenschaftspflicht nach Artikel 5 Abs. 2 DS-GVO)**.**

Wenn die Grundsätze geprüft wurden, bitte abhaken ☒

Bezeichnung der Verarbeitungs-tätigkeit (System)	rechtmäßige Verarbeitung (1a)	Verarbeitung nach Treu und Glauben (1a)	Transparenz gegenüber Betroffenen (1a)	Zweckbindung (1b)	Datenminimierung (1c)	Richtigkeit (1d)	Speicherbegrenzung (1e)	Integrität und Vertraulichkeit (1f)	**Anmerkung**
1) ...									weitere Informationen sind im Dokument Verzeichnis Verarbeitungs-tätigkeiten (DOKU 4) beschrieben
2) …									
3) …									
4) …									
5) …									
6) ….									
7) ….									
8) ….									

Bezeichnung der Verarbeitungs-tätigkeit (System)	rechtmäßige Verarbeitung (1a)	Verarbeitung nach Treu und Glauben (1a)	Transparenz gegenüber Betroffenen (1a)	Zweckbindung (1b)	Datenminimierung (1c)	Richtigkeit (1d)	Speicherbegrenzung (1e)	Integrität und Vertraulichkeit (1f)	**Anmerkung**
									weitere Informationen sind im Dokument Verzeichnis Verarbeitungs-tätigkeiten (DOKU 4) beschrieben
gegebenenfalls weitere Zeilen einfügen									

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

Als Verantwortlicher haben Sie je Verarbeitungstätigkeit in der obigen Darstellung eine eigene Zeile auszufüllen und die Einhaltung der Grundsätze zur Verarbeitung personenbezogener Daten (siehe unten) zu überprüfen.

Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 DS-GVO

Wenn Sie personenbezogene Daten verarbeiten, darf das nur unter Beachtung der folgenden Grundsätze erfolgen.

Wenn Sie dies geprüft haben, haken Sie das bitte in der betreffenden Zeile und beim zutreffenden Grundsatz ab ☒

rechtmäßige Verarbeitung (1a): Wenn Sie personenbezogene Daten verarbeiten, bedarf dies einer Rechtsgrundlage, nämlich (Pflicht)Befugnis des Betriebsrates nach ArbVG, KollV oder Betriebsvereinbarung, Einwilligung des Betroffenen, Vertrag, überwiegendes Interesse (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 Sie verarbeiten sind darüber zu informieren (z.B. schriftliches Informationsblatt bei Einstellung, Hinweis in BR-Zeitung, Intranetseite des BR, persönliches Gespräch).

Zweckbindung (1b): Die Zwecke, warum Sie Daten verarbeiten sind möglichst präzise zu definieren.

Datenminimierung (1c): Es dürfen nur Daten verarbeitet werden, die zur Zweckerreichung notwendig sind.

Richtigkeit (1d): Die gespeicherten Daten müssen richtig sein und im Falle einer Änderung auf den richtigen Stand gebracht werden.

Speicherbegrenzung (1e): Daten dürfen nur so lange gespeichert werden, wie dies zur Erreichung der Zwecke notwendig erscheint. Dies ist in der jeweiligen Zusatzdokumentation (Datenblatt) anzuführen. Danach sind die Daten physisch zu löschen.

Integrität und Vertraulichkeit (1f): Jeder Verantwortlicher muss angemessene Maßnahmen zur Datensicherheit treffen. Dazu liegt eine Checkliste vor und Hinweise zur Definition von technischen und organisatorischen Maßnahmen zur Datensicherheit.

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

PRÜFUNG DER ORGANISATORISCHEN, PERSONELLEN UND TECHNISCHEN SICHERHEITSMASSNAHMEN ZUR IT-SICHERHEIT (CHECK 2)

Die folgenden Kriterien sind für dienstlich zur Verfügung gestellte Systeme und Geräte bzw. privat (z.B. über BR-Fonds) angeschaffte Systeme und Geräte immer dann zu prüfen, wenn in der jeweiligen Spalte bei der jeweiligen Prüfung (dienstlich, privat) ein X steht.

Das Prüfergebnis liefert Hinweise, inwieweit Maßnahmen zur IT-Sicherheit im Betriebsrat zu ergreifen sind. Die Dokumente (INFO 4 und DOKU 4) bieten dabei Unterstützung.

	Prüfkriterium zur Sicherheit der Verarbeitung (Quelle: Pollirer, Dako Nr. 2 + 3 /2016, adaptiert von AK/ÖGB/FORBA, 08/2017)		
		Dienstliches System bzw. Gerät	Privates System bzw. Gerät
	Organisatorische Sicherheitsmaßnahmen (systemunabhängig)		
O1	Hat der Betriebsrat eine für alle Mitglieder des Betriebsrates, sowie Beschäftigte im BR-Büro verständliche, aktuelle Sicherheitsleitlinie („Information Security Policy“)?	X	X
	Anmerkung: Das Fehlverhalten der „eigenen Leute“ stellt eines der größten Risken für den Datenschutz und die eingesetzte IT dar. Die Sicherheitsleitlinie („Information Security Policy“) schafft Abhilfe, da sie Vorgaben enthält, wie mit Daten, IT (PC, Smartphone etc) und Internet umzugehen ist.		
O2	Verfügt der Betriebsrat über ein Informationssicherheits- und Datenschutz-Managementsystem?	X	X
	Anmerkung: Die Aufgabe des Informationssicherheits- und Datenschutz-Managementsystems ist es, sowohl Gefahren für die Informationssicherheit als auch Bedrohungen des Datenschutzes von BR-Daten durch klare Regeln abzuwehren.		

		Dienst-liches System bzw. Gerät	Privates System bzw. Gerät
O3	Werden vom Betriebsrat externe Service-Anbieter (Cloud, Webmail, Dropbox etc) in Anspruch genommen?	X	X
	Anmerkung: Wenn Service-Anbieter (Auftragsverarbeiter) in Anspruch genommen werden, müssen diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten; den BR trifft eine diesbezügliche Prüfpflicht. Dieser kann er nachkommen, indem er sich vom Service-Anbieter dessen Sicherheitskonzept vorlegen lässt. Insofern ist auch zu prüfen, inwiefern die entsprechenden Verträge bzw Geschäftsbedingungen (AGB) im Internet ausgestaltet sind. Bei Service-Anbietern in Nicht-EU-Staaten ist unter Umständen die Genehmigung der Datenschutzbehörde (DSB) einzuholen, wenn die Server nicht in der EU stehen.		
O4	Werden sowohl Software auf den privaten Endgeräten wie auch selbst oder im Auftrag des Betriebsrates entwickelte Programme einer geregelten Abnahme- und Freigabeprozedur im Sinne von Datenschutz und Daten-sicherheit unterzogen?	X	X
	Anmerkung: Ohne Überprüfung der Software (zB Apps) kann nicht beurteilt werden, ob die Software frei von Viren und in der eingesetzten Betriebssystemumgebung überhaupt lauffähig ist.		
O5	Existiert für BR-Daten ein schriftliches Datensicherungs-konzept?		X
	Anmerkung: Voraussetzung für jede Notfallvorsorge sind die Planung und Durchführung regelmäßiger Datensicherungen (Back-up). Daher ist in schriftlicher Form festzulegen, welche Daten, von wem zu welchem Zeitpunkt gesichert werden müssen und welche Datensicherungsmethoden dabei eingesetzt werden.		
O6	Verfügt der Betriebsrat über eine Dokumentation der getroffenen Informationssicherheits- und Datenschutz-maßnahmen?	X	X
	Anmerkung: Diese Dokumentation stellt nicht nur im Anlassfall eine hilfreiche und notwendige Grundlage dar, sondern dient auch der entsprechenden Information der „eigenen Leute“.		

		Dienstliches System bzw. Gerät	Privates System bzw. Gerät
O7	Wurde im Betriebsrat eine Klassifizierung der verarbeiteten Daten in Bezug auf ihre Vertraulichkeit (Informationssicherheit) und die Datenschutzanforderungen durchgeführt?	X	X
	Anmerkung: Diese Klassifizierung ist eine wesentliche Voraussetzung für die Auswahl adäquater Sicherheitsmaßnahmen. Eine Klassifizierung im Sinne der Informationssicherheit umfasst die Stufen „betriebsöffentlich – BR-intern – vertraulich – geheim“. Eine Klassifizierung im Sinne des Datenschutzes kann folgende Stufen umfassen: „besondere Kategorien von Daten (sensible Daten) – nicht-sensible Daten“.		

	Prüfkriterium zur Sicherheit der Verarbeitung (Quelle: Pollirer, Dako Nr. 2 + 3 /2016, adaptiert von AK/ÖGB/FORBA, 08/2017)		
		Dienstliches System bzw. Gerät	Privates System bzw. Gerät
	Personelle Sicherheitsmaßnahmen (systemunabhängig)		
P1	Wurde die Aufgabenverteilung und Zuständigkeit bei der Datenverarbeitung im Betriebsrat und hinsichtlich der Beschäftigten im BR-Büro ausdrücklich festgelegt?	X	X
	Anmerkung: Eine klare und eindeutige Aufgabenverteilung und Regelung der entsprechenden Zuständigkeiten unterstützt Informationssicherheit und Datenschutz.		
P2	Werden die Beschäftigten im BR-Büro zur Einhaltung einschlägiger Gesetze, Vorschriften und interner Richtlinien schriftlich verpflichtet?	X	X
	Anmerkung: Beschäftigte im BR-Büro sind nicht nur auf die Einhaltung des Datengeheimnisses zu verpflichten, sondern auch zur Einhaltung der verschiedenen BR-Richtlinien (wie zB PC-Benutzerregeln, Regeln für die Benutzung von Internet und E-Mail, Passwortrichtlinie, Bring Your Own Device-Richtlinie).		

		Dienst-liches System bzw. Gerät	Privates System bzw. Gerät
P3	Wird das Verarbeiten von Daten an das Vorliegen gültiger genereller Richtlinien bzw spezieller Vorgaben im Einzelfall seitens des im Betriebsrat für zuständig erklärten Mitgliedes gebunden (im Zweifel der BRV)?	X	X
	Anmerkung: Die Zuständigkeit für die Einhaltung und Durchführung datenschutz-rechtlicher Verpflichtungen (samt den entsprechenden Kompetenzen) ist im BR-Gremium mit Beschluss festzulegen. Gibt es diesen Beschluss nicht, ist im Zweifel der BRV zuständig.		
P4	Gibt es im Betriebsrat eine Richtlinie, wie beim Aus-scheiden von Mitgliedern im Betriebsrat oder Beschäftigten im BR-Büro vorzugehen ist? (Insb Löschung BR-relevanter Informationen auf eigenen Geräten bzw Löschung BR-relevanter Daten vor Rück-gabe von Endgeräten an den Arbeitgeber!)	X	X
	Anmerkung: Bei personellen Veränderungen innerhalb der BR-Körperschaft bzw beim Ausscheiden von Beschäftigten im BR-Büro, sind von diesen sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (mobile Geräte, Speichermedien usw) zurückzufordern. Des Weiteren sind sämtliche Zugangs- und Zugriffsberechtigungen zu sperren bzw zu löschen.		
P5	Werden die Mitglieder des Betriebsrates und die Beschäftigten im BR-Büro im Rahmen von Schulungen auf die Gefahren im Umgang mit Daten und IT-Systemen sowie über Gegenmaßnahmen bei Gefährdung der Systeme/Daten geschult?	X	X
	Anmerkung: Die „eigenen Leute“ sind über Informationssicherheit und Datenschutz im BR-Büro zu belehren.		
P6	Werden die Mitglieder im Betriebsrat sowie die Beschäftigten im BR-Büro über die Gefahren von Social Engineering-Angriffen (zB Vorgabe falscher Identität) aufgeklärt?	X	X
	Anmerkung: Gute "Social Engineers" können unter Umständen zu verschiedensten unerlaubten Handlungen, insb zu Verstößen gegen den Datenschutz und Sicherheits-auflagen oder Richtlinien bewegen.		

		Dienstliches System bzw. Gerät	Privates System bzw. Gerät
P7	Wurden alle Mitglieder des Betriebsrates und die Beschäftigten im BR-Büro in der Auswahl sicherer Passwörter geschult?	X	X
	Anmerkung: Die Auswahl eines guten und sicheren Passwortes ist wichtig für die Sicherheit und Vertraulichkeit der Daten.		
P8	Wurde im Betriebsrat eine Clear Desk-/Clear Screen-Policy eingeführt?	X	X
	Anmerkung: Alle Mitglieder des Betriebsrates und alle Beschäftigten im BR-Büro sollten dazu angehalten werden, bei Abwesenheit vertrauliche Unterlagen zu verschließen und sich vom PC abzumelden.		
P9	Gibt es ein Entsorgungskonzept für Datenträger und Papierdokumente?	X	X
	Anmerkung: Datenträger und Papierdokumente mit vertraulichen Inhalten müssen auf sichere Art entsorgt werden. So sind Papierdokumente mit einem Shredder oder über ein geprüftes Entsorgungsunternehmen zu vernichten. Bei Datenträgern muss sichergestellt sein, dass diese physisch vernichtet (zerstört) werden.		

	Prüfkriterium zur Sicherheit der Verarbeitung (Quelle: Pollirer, Dako Nr. 2 + 3 /2016, adaptiert von AK/ÖGB/FORBA, 08/2017)		
		Dienstliches System bzw. Gerät	Privates System bzw. Gerät
	Technische Sicherheitsmaßnahmen (je Verarbeitungstätigkeit zu prüfen!)		
T1	Wurde für alle relevanten Datenverarbeitungen und Datenträger ein wirksames Zugriffskontrollsystem eingerichtet?	X	X
	Anmerkung: Der Zugriff auf Daten und Programme und der Schutz der Datenträger vor Einsicht und Verwendung durch Unbefugte sind zu definieren. In Bezug auf die einzelnen Datenverarbeitungen ist der personifizierte passwortgeschützte Zugriff (Überprüfung der Identität des jeweiligen Nutzers) auf die einzelnen Informationen und sind Berechtigungen, insb Lesen, Schreiben, Löschen, Übermitteln im jeweiligen System zu regeln.		
T2	Ist auf privaten Geräten, die von BR-Mitgliedern genutzt werden, sichergestellt, dass die Betriebssystemkomponenten, Internetbrowser und andere Software auf allen IT-Systemen laufend aktualisiert werden?		X
	Anmerkung: Aktualisierungen (Updates) sollen Fehler beseitigen und für mehr Sicherheit sorgen. Ohne Updates kann jedes internetfähige Endgerät zum Angriffsziel von Viren oder Spionagetools werden.		
T3	Werden Daten auf den Endgeräten (PC, Laptop, Smartphone, Tablet) bei besonderen (sensiblen) Datenverarbeitungen verschlüsselt und werden die Verschlüsselungspasswörter sicher hinterlegt?	X	X
	Anmerkung: Gelangen gespeicherte Daten in die Hände Unbefugter, so kann daraus großer Schaden entstehen.		
T4	Findet die Übertragung von BR-Daten außerhalb betrieblicher Netzwerke (über mobile IT-Geräte) in verschlüsselter Form statt (zB https, End-to-End-Verschlüsselung bei Apps)?	X	X
	Anmerkung: Durch den Einsatz von mobilen IT-Geräten entstehen spezielle Risken, insb durch Einschleppen von Schadsoftware. Bei nichtverschlüsselter Übertragung (zB ungesichertes WLAN) können vertrauliche BR-Daten in falsche Hände geraten.		

		Dienst-liches System bzw. Gerät	Privates System bzw. Gerät
T5	Gibt es eine Regelung, dass für verschiedene Daten-verarbeitungen unterschiedliche Passwörter verwendet werden müssen?	X	X
	Anmerkung: Für die Anmeldung bei Internetdiensten wie zB Webmail, Facebook oder E-Banking sollte niemals nur ein einziges Passwort verwendet werden. Wird eine dieser Websites gehackt, kann der Angreifer Zugriff auf die Anmeldedaten erhalten und diese bei anderen Datenverarbeitungen ausprobieren und somit Zugang zu Informationen erhalten. Bei einer größeren Anzahl von verschiedenen Passwörtern empfiehlt sich der Einsatz eines Passwort-Safes (Passwortmanagement-Software). Diese Software verwaltet und generiert auf Wunsch auch Kennwörter und schützt diese in einer Datenbank.		
T6	Sind auf privaten Geräten, die von BR-Mitgliedern genutzt werden, Virenschutzprogramme installiert und werden diese auch laufend aktualisiert?		X
	Anmerkung: Zur Abwehr von Schadprogrammen müssen alle privaten IT-Geräte des Betriebsrates mit Antivirus-Software ausgestattet sein.		
T7	Wurde die Benutzung von Wechselmedien (zB USB-Stick, externe Festplatte, CD-ROM) im Betriebsrat geregelt?	X	X
	Anmerkung: Die Verwendung von Wechselmedien bringt einige Risken wie das Starten fremder Betriebssysteme, die unbefugte Installation unerwünschter Software oder Schadsoftware sowie das unberechtigte Kopieren von BR-Daten mit sich und muss entsprechend geregelt werden.		
T8	Wird auf privaten Geräten, die von BR-Mitgliedern genutzt werden, ein gewartetes Firewallsystem betrieben?		X
	Anmerkung: Jede Kommunikation zwischen Unternehmensnetz und Internet muss ausnahmslos über die Firewall geführt werden.		

		Dienst-liches System bzw. Gerät	Privates System bzw. Gerät
T9	Wurde im Betriebsrat eine Social-Media-Strategie eingeführt, welche die Nutzung Sozialer Netzwerke regelt?	X	X
	Anmerkung: Den durchaus wünschenswerten Vorteilen im Bereich der Kommunikation durch die Nutzung Sozialer Netzwerke (Facebook, Twitter etc) sind potenzielle Risken wie Datenabflüsse (Dritte erhalten Einsicht), Einschleusen von Schadsoftware usw gegenüberzustellen. Es ist unumgänglich, eine geeignete Strategie zu entwickeln und umzusetzen.		
T10	Gibt es im Betriebsrat eine Protokollierungspflicht für Änderungen, Abfragen und Übermittlungen bei besonders sensiblen Datenverarbeitungen (zB von Gesundheitsdaten)?	X	X
	Anmerkung: Sensible Daten sind besonders schützenswert, daher ist deren Verwendung an zusätzliche datenschutzrechtliche Verpflichtungen (Datensicherheitsmaßnahmen) gebunden.		
T11	Erfolgt im Betriebsrat eine rechtssichere Archivierung relevanter Geschehnisse (zB Ablage von Protokollen)?	X	X
	Anmerkung: Eine rechtssichere Archivierung von Dokumenten gewährleistet eine fälschungssichere Ablage (zB für eine spätere allfällige Vorlage bei Gericht oder Behörde relevant).		
T12	Wurde ein Schließplan oder Zutrittsberechtigungskonzept (Verteilung der Schlüssel zum BR-Büro und zu den Kästen im BR-Büro bzw der Zutrittsberechtigungen über Chip) erstellt?	X	
	Anmerkung: Alle Maßnahmen und Informationen, die im Zusammenhang mit der Schlüsselvergabe bzw einem Zutrittsberechtigungskonzept stehen, müssen in einem Schließplan des Betriebsrates dokumentiert werden bzw im Berechtigungskonzept des Arbeitgebers seitens des Betriebsrates überprüft werden.		

INFORMATIONSBLATT ZUR ERSTELLUNG EINES INFORMATIONS-SICHERHEITS- UND DATENSCHUTZ-MANAGEMENTSYSTEMS (INFO 4)

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 zB *IT-Policy* oder *IT-Sicherheitsleitlinien* veröffentlicht sein).

Wir empfehlen die in der Checkliste "*Prüfung der organisatorischen, personellen und technischen Sicherheitsmaßnahmen zur IT-Sicherheit (CHECK 2)*" angeführten Prüfschritte durchzuführen und daraus abgeleitete Maßnahmen und Regeln für die BR-Körperschaft zu beschreiben.

Die in Folge angeführten Textbausteine dienen dabei zur Orientierung und können für die Dokumentation der eigenen Maßnahme zur IT-Sicherheit (DOKU 3) nach Prüfung im Betriebsrat verwendet werden.

Folgende Vorschläge zur IT-Sicherheit können für die Betriebsratsarbeit und die Arbeit im Betriebsratsbüro - zusätzlich zu den betrieblichen Anforderungen (sofern vorhanden) - vom BR-Zuständigen für Datenschutz erlassen werden.

Organisatorische Sicherheitsmaßnahmen

- Personenbezogene Daten und vertrauliche Dokumente (von Arbeitnehmer/innen, vom Arbeitgeber, 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 wird, sind auf Geräten, auf denen sich personenbezogene Daten von Mitarbeiter/innen befinden, nur nach Prüfung zu verwenden. Die Geschäfts-/Nutzungsbedingungen sind im Hinblick auf die Anforderungen der DSGVO/des DSG zu prüfen und abzulegen.
- Das Speichern von personenbezogenen Daten und/oder Dokumenten bei externen Cloudanbietern ist nur nach Prüfung der datenschutzrechtlichen Anforderungen gestattet.
- Daten/Dokumente von Mitarbeiter/innen 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.

- Daten/Dokumente werden in folgende Sicherheitsklassen unterteilt:
  a) *öffentliche Daten/Dokumente*: diese können ohne Einschränkung betrieblich verwendet und veröffentlicht werden
  b) *interne Daten/Dokumente*: diese stehen nur innerhalb des Betriebsrates zur Verfügung und dürfen nur nach Prüfung an berechtigte Dritte weitergegeben werden
  c) *vertrauliche Daten/Dokumente*: diese dürfen nur von ausgewählten Mitgliedern des Betriebsrates verwendet werden
  d) *geheime Daten/Dokumente*: diese stehen ausschließlich vorab definierten Personen zur Verfügung und sind betrieblich besonders zu schützen
- Die Betroffenenrechte (z.B. gegenüber Mitarbeiter/innen) sind im Sinne der rechtlichen Anforderungen zu erfüllen. Die betroffenen Personen werden darüber und über ihre Rechte gemäß Datenschutzrecht (z.B. auch in Formularen) informiert.
- Die im Betriebsrat vereinbarten und getroffenen Maßnahmen werden dokumentiert (siehe DOKU 3) und regelmäßig auf ihre Anwendbarkeit geprüft (Evaluierung).

Personelle Sicherheitsmaßnahmen

- Für dienstliche Geräte (vom Arbeitgeber zur Verfügung gestellt) wie PC, Laptop, Smartphone, Datenträger (z.B. USB) sind die im Betrieb definierten Regelungen - z.B. bzgl. Passwortgestaltung, Virenschutz oder Datensicherung einzuhalten.
- Geräte für die Betriebsratsarbeit sind zu schützen (z.B. Passwort, 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 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, wenn sie diese 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 gewordenen 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 dem/der BR-Vorsitzende/r und dem/der 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 den/die BR-Vorsitzende/n bzw. die für Datenschutz im BR zuständige Person zu löschen.
- Der Zuständige für Datenschutz im Betriebsrat weist regelmäßig (2-3/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 den getroffenen Regelungen der Verarbeitung personenbezogener Daten zu schulen.

Technische Sicherheitsmaßnahmen (je Verarbeitungstätigkeit zu prüfen!)

- 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.
- In öffentlichen WLANs (die oft nicht ausreichend gesichert sind) ist besondere Vorsicht im Umgang mit personenbezogenen Daten walten zu lassen, bei Arbeiten oder Telefonieren im öffentlichen Raum sind die betrieblichen Daten zu schützen.
- Bei Datenübermittlung (E-Mail, Messenger wie WhatsApp oder soziale Medien wie Facebook) sind vertrauliche Daten, wenn technisch möglich, zu schützen (Verschlüsselung, zip-Dateien mit Passwortschutz, Dokument mit Kennwortschutz).

- Daten auf mobilen Datenträgern (z.B. USB) können leicht verloren gehen und sind daher besonders zu schützen.
- Beim Öffnen von Mailanhängen bzw. dem Anklicken eines Links in 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, auch hinsichtlich der Person des auf die Daten Zugreifenden (etwa 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 (DOKU 3)

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

Beschreibung der Maßnahmen zur IT-Sicherheit

- Maßnahme 1
- Maßnahme 2
- Maßnahme 3
- Maßnahme 4
- Maßnahme 5
- Maßnahme 6
- Maßnahme 7
- Maßnahme 8
- Maßnahme 9
- Maßnahme 10
- Maßnahme 11
- Maßnahme 12
- Maßnahme 13

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 auszudrucken.

DATENBLATT ZU EINER KONKRETEN VERARBEITUNGSTÄTIGKEIT (SYSTEM) NACH ARTIKEL 30 DS-GVO (DOKU 4)

Bitte beachten Sie, dass sich die Daten ändern können und dieses Dokument/dieses File entsprechend anzupassen ist.

Dokumentieren Sie daher die Tatsache, dass Sie Änderungen vorgenommen haben in „*Dokumentation (Protokollierung) der vorgenommenen Änderungen (DOKU 1)*“

Für jede Verarbeitungstätigkeit, die in „*Allgemeine Angaben zum/zur Verantwortlichen nach Artikel 4 und Artikel 30 DS-GVO (DOKU 2)*“ angeführt ist, muss ein gesondertes Datenblatt erstellt werden

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 auszudrucken.

Verzeichnis Verarbeitungstätigkeit

1.	**Datenblatt Nummer**	*hier einfügen*	Nummer aus Dokument „Allgemeine Angaben zum/zur Verantwortlichen nach Artikel 4 und Artikel 30 DS-GVO (DOKU 2)“ übernehmen.
2.	**Datenblatt zur Verarbeitungstätigkeit**	*hier einfügen*	Bezeichnung aus Dokument „Allgemeine Angaben zum/zur Verantwortlichen nach Artikel 4 und Artikel 30 DS-GVO (DOKU 2)“ übernehmen.
3.	**Sind bei dieser Verarbeitungstätigkeit personenbezogene Daten der Beschäf-tigten in einem System gespeichert, das der Arbeitgeber zur Verfügung stellt?**	☐ ja	Arbeitgeber ist für die [>>] Datensicherheit (Artikel 32 DS-GVO) verantwortlich und der Betriebsrat muss sich an Datenschutzrecht und betriebliche Vorgaben (z.B. IT-Policy) halten.
		☐ nein	Betriebsrat muss sich als Verantwortlicher um Datensicherheit (Artikel 32 DS-GVO) kümmern (siehe CHECK 2 und INFO 4 bzw. DOKU 3)
		☐ teils/teils	Betriebsrat muss sich als Verantwortlicher bei seinen "Systemen" um Datensicherheit (Artikel 32 DS-GVO) kümmern (siehe CHECK 2 und INFO 4 bzw. DOKU 3)

4.	**Zwecke der Verarbeitung**	*hier einfügen*	
5.	**Herkunft der Daten**	☐ vom/von Arbeitgeber/in	
		☐ von den Arbeitnehmer/innen	
		☐ von Dritten	
6.	**Getroffene technische und organisatorische (inkl. personelle) Maßnahmen zur Datensicherheit (Artikel 30 und 32 DS-GVO)**	Siehe DOKU 3	
7.	**Betroffene Gruppen, von denen Daten für diese Verarbeitungstätigkeit verarbeitet werden**	☐ aktive Beschäftigte	
		☐ ehemals Beschäftigte	
		☐ Familienangehörige	
		☐ Arbeitgeber	
		☐ Dritte (z.B. Vertragspartner) und zwar: *hier einfügen*	
8.	**Rechtsgrundlage der Verarbeitung (gemäß Artikel 6 DS-GVO)**	☐ Erfüllung einer rechtlichen Verpflichtung (z.B. [Kontroll]Befugnis laut ArbVG, KollV oder Betriebsvereinbarung)	
		☐ Einwilligung der betroffenen Person(en)	
		☐ Erfüllung eines Vertrages (z.B. ermäßigte Bestellung über BR-Büro)	

9.	**Wird der Betriebsrat bei der Datenverar-beitung durch einen Auftragsverarbeiter unterstützt und werden Daten bei diesem verarbeitet?**		wenn ja, Angaben zum Auftragsverarbeiter und zum geschlossenen Vertrag
10.	**Findet eine Speicherung von Daten außerhalb der EU statt? (z.B. Cloudlösung bei der Daten nicht in einem Rechenzentrum innerhalb der EU liegen)**		wenn ja, Angaben zum Auftragsverarbeiter und zum geschlossenen Vertrag

Neben diesen Angaben sind die Daten(kategorien) je Verarbeitungstätigkeit näher zu beschreiben (siehe Folgeseite/n)

11. **Überblick Daten(kategorien)**

Kategorie(n) personenbezogener Daten	Herkunft	[>>] besondere Kategorie (j/n)	wer erhält im Betriebsrat Zugriff auf diese Information / dieses Datum	wird diese Information / dieses Datum an Dritte - außerhalb des Betriebsrates übermittelt (wenn ja, Angabe der Stelle)	Löschfristen	Anmerkungen

Kategorie(n) personenbezogener Daten	Herkunft	[>>] besondere Kategorie (j/n)	wer erhält im Betriebsrat Zugriff auf diese Information / dieses Datum	wird diese Information / dieses Datum an Dritte - außerhalb des Betriebsrates übermittelt (wenn ja, Angabe der Stelle)	Löschfristen	Anmerkungen

Kategorie(n) personenbezogener Daten	Herkunft	[>>] besondere Kategorie (j/n)	wer erhält im Betriebsrat Zugriff auf diese Information / dieses Datum	wird diese Information / dieses Datum an Dritte - außerhalb des Betriebsrates übermittelt (wenn ja, Angabe der Stelle)	Löschfristen	Anmerkungen

ZUM ABSCHLUSS

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

Informieren Sie sich bei Ihrer Fachgewerkschaft oder Arbeiterkammer regelmäßig über weitere Unterlagen und Publikationen bzw. besuchen Sie die Webseite der österreichischen Datenschutzbehörde und abonnieren deren Newsletter unter https://www.dsb.gv.at/newsletter.