Datenschutz

Infoblatt Februar 2026

Der Schutz personenbezogener Daten ist auch für die Interessenvertretung ein wichtiges Thema!

Datenschutz ist kein Hindernis, sondern Voraussetzung für faire und transparente Mitbestimmung. Er schützt Persönlichkeitsrechte und hilft, Kontrolle und Transparenz in der digitalen Arbeitswelt zu sichern. Betriebs- und Personalräte sind damit wichtige Akteure für gelebten Beschäftigtendatenschutz.

Zuständig für den Datenschutz in einem Unternehmen oder einer Behörde ist nach Artikel 4 der Datenschutzgrundverordnung (DSGVO) der oder die **„Verantwortliche“**. Das ist die Firmenleitung, die Geschäftsführung, der oder die Bürgermeister*in – und nicht die Interessenvertretung.

Betriebs- und Personalräte verarbeiten selbst personenbezogene Daten und müssen die datenschutzrechtlichen Bestimmungen einhalten. Verantwortlicher für die Einhaltung der Datenschutzvorschriften im gesamten Unternehmen, auch wenn personenbezogene Daten im Büro der Interessenvertretung verarbeitet werden, bleibt jedoch der Arbeitgeber.

Aber: Die datenschutzrechtliche Verantwortlichkeit des Arbeitgebers beschneidet nicht die **institutionelle Unabhängigkeit der Interessenvertretung**. Daher muss sie selbst die datenschutzrechtlichen Vorschriften einhalten. Der Arbeitgeber muss jedoch zugleich in der Lage sein, seinen Pflichten als Verantwortlicher nachzukommen.

www.arbeitnehmerkammer.de

Arbeitnehmerkammer
Bremen

Als Interessenvertretung den Datenschutz gewährleisten, aber unabhängig bleiben?

Wie gelingt nun dieser Spagat? Eine Lösung wäre es, dem/der Datenschutzbeauftragten des Betriebs Zutritt zum Büro der Interessenvertretung zu gewähren, um den Datenschutz zu überprüfen. Manche Interessenvertretungen halten das für keine gute Lösung.

Zwar ist die oder der Datenschutzbeauftragte zur Vertraulichkeit verpflichtet (§ 79a BetrVG), berichtet jedoch gleichzeitig an die oberste Managementebene. In den Räumen der Interessenvertretung befinden sich besonders sensible Daten, etwa wenn sich eine beschäftigte Person über eine vorgesetzte Person beschwert.

Wir empfehlen eine gute Zusammenarbeit mit dem oder der Datenschutzbeauftragten. Um ganz unabhängig zu bleiben, möchten einige Interessenvertretungen sich doch lieber selbst um den Datenschutz im eigenen Büro kümmern.

Welche personenbezogenen Daten kommen bei der Interessenvertretung an?

Manche der personenbezogenen Daten kommen vom Arbeitgeber, andere von den Beschäftigten und manche erzeugt die Interessenvertretung selbst.

Zu nennen sind zum Beispiel:

- Vorlagen von Dienststelle oder Arbeitgeber im Rahmen der Beteiligungsrechte
- Informationen, die die Interessenvertretung von sich aus anfordert
- Kenntnisse über Mitarbeitende, die im Zuge eines Gesprächs bei der Interessenvertretung ankommen
- Informationsbeschaffung durch die Interessenvertretung selbst (zum Beispiel durch eine Befragung der Beschäftigten)
- Protokolle, Mitschriebe in Arbeitsgruppen

Was sind „personenbezogene Daten“?
Definition nach DSGVO Artikel 4:

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“

Was sind die relevantesten Datenschutz-Regelungen?

- Das relevanteste „Gesetz“ in diesem Zusammenhang ist eine Verordnung der Europäischen Union: die **Datenschutzgrundverordnung (DSGVO)**. Sie gilt in der gesamten Europäischen Union und ist die übergreifende Regelung. In dieser Verordnung sind auch die Grundsätze geregelt.
- Die Bundesregierung hat ein eigenes **Bundesdatenschutzgesetz (BDSG)** veröffentlicht. Dieses gilt für die nichtöffentlichen Stellen (also zum Beispiel Unternehmen), für die öffentlichen Stellen des Bundes und immer dann, wenn kein Landesdatenschutzgesetz verabschiedet wurde, auch für die öffentlichen Stellen der Länder.
- Wenn ein Land ein eigenes **Landesdatenschutzgesetz (LDSG)** verabschiedet hat, dann gilt jedoch dieses für die öffentlichen Stellen der Länder. Das BDSG gilt dann nur noch ergänzend in den Bereichen, in denen das LDSG keine Regelung getroffen hat. Das bremische Landesgesetz heißt „Bremisches Gesetz zur Ausführung der Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680“. Die Kurzform lautet BremDSGVOAG.
- Zentral sind zudem das **Betriebsverfassungsgesetz (BetrVG)** und die **Personalvertretungsgesetze (zum Beispiel BPersVG oder LPersVG)**. In ihnen ist geregelt, dass die Interessenvertretungen darüber zu wachen haben, dass die zugunsten der Beschäftigten und Bediensteten geltenden Gesetze unter anderem zum Datenschutz eingehalten werden.

Welche Datenschutzgrundsätze sind zwingend einzuhalten?

In Artikel 5 DSGVO sind neun Grundsätze für die Verarbeitung personenbezogener Daten genannt, die alle auch im Büro der Interessenvertretung eingehalten werden müssen.

- **Rechtmäßigkeit**
  Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn es dafür eine klare rechtliche Grundlage gibt. Dazu zählen zum Beispiel Einwilligungen, gesetzliche Vorgaben oder berechtigte Interessen des Gremiums. Auch eine Dienst- oder Betriebsvereinbarung eignet sich als rechtliche Grundlage, jedoch nur dann, wenn sie vollumfänglich DSGVO-konform ausgestaltet ist. Ohne eine Rechtsgrundlage nach Artikel 6 DSGVO ist die Datenverarbeitung unzulässig (Artikel 6 und 9 DSGVO).

- **Treu und Glaube (Fairness)**
  Die Verarbeitung muss fair und nachvollziehbar sein – gegenüber den Beschäftigten darf nichts „hintenrum“ passieren. Interessenvertretungen sollten offen und verantwortungsvoll mit den Daten umgehen. Die betroffenen Personen dürfen nicht überrascht oder benachteiligt werden.

- **Transparenz**
  Die Beschäftigten müssen wissen, wer ihre Daten verarbeitet, zu welchem Zweck und mit welchen Rechten. Das geht zum Beispiel über verständliche Datenschutzhinweise, die Kommunikation im Gremium oder über Transparenzregeln in einer Vereinbarung (Artikel 12 bis 14 DSGVO).

- **Zweckbindung (Zweckbestimmung)**
  Daten dürfen nur für vorher festgelegte, konkrete Zwecke genutzt werden – zum Beispiel zur Wahlvorbereitung oder zur Beratung im Einzelfall. Eine spätere Nutzung zu anderen Zwecken ist nur dann erlaubt, wenn eine neue rechtliche Grundlage vorliegt. Die Zwecke müssen dokumentiert und nachvollziehbar sein.

- **Datenminimierung**
  Es dürfen nur so viele Daten wie nötig verarbeitet werden. Die Interessenvertretung sollte sich fragen: Welche Daten brauchen wir wirklich? Alles, was nicht erforderlich ist, darf nicht verarbeitet werden.

- **Richtigkeit**
  Die gespeicherten Daten müssen korrekt und aktuell sein. Falsche oder veraltete Informationen müssen berichtigt oder gelöscht werden (Artikel 16 DSGVO).

- **Speicherbegrenzung**
  Personenbezogene Daten dürfen nicht „für immer“ aufbewahrt werden. Sie müssen gelöscht oder anonymisiert werden, sobald sie für den Zweck nicht mehr gebraucht werden. Dazu gehören klare Löschfristen und eine regelmäßige Überprüfung (Artikel 17 DSGVO).

- **Integrität und Vertraulichkeit (Sicherheit)**
  Daten müssen vor unbefugtem Zugriff, Verlust oder Veränderung geschützt werden. Das betrifft sowohl digitale Systeme als auch Papierunterlagen. Maßnahmen wie Passwörter, Verschlüsselung und verschlossene Schränke sind Pflicht.

- **Rechenschaftspflicht**
  Die Interessenvertretung muss jederzeit nachweisen können, dass sie sich an die Datenschutzgrundsätze hält. **Das bedeutet: Datenschutz muss dokumentiert, organisiert und überprüfbar sein.** Auch interne Absprachen oder Verfahren gehören dazu.

Wie kann die Interessenvertretung nachweisen, dass sie den Datenschutz einhält?

Kein Gesetz liefert exakte Vorgaben darüber, wie die Interessenvertretungen den Datenschutz einzuhalten und zu dokumentieren hat. Wir schlagen daher zur fortlaufenden Dokumentation des Datenschutzes ein **Datenschutzkonzept** im Büro der Interessenvertretung vor.

In diesem Datenschutzkonzept werden wichtige Informationen zur Verarbeitung personenbezogener Daten beschrieben. Nach Sichtung des Konzepts sollte unter anderem bekannt sein, **welche Daten zu welchem Zweck mit welcher Begründung wie lange verarbeitet werden.** Die Einhaltung der datenschutzrechtlichen Grundsätze kann mithilfe des Konzepts überprüft werden.

DSGVO Artikel 4 Definition: „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“

Achtung bei besonders schützenswerten Daten!
Die Verarbeitung dieser Daten sollte sehr sorgfältig betrachtet werden. „Besonders schützenswerte Daten“ heißen laut Artikel 9 DSGVO „besondere Kategorien personenbezogener Daten“ und sind 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“.

Das Datenschutzkonzept

Das hier vorgeschlagene Konzept gliedert sich in vier Abschnitte.

Abschnitt 1: Dokumentation

Was hat die Interessenvertretung unternommen, um den Datenschutz im eigenen Büro auf sichere Füße zu stellen? Hat sie eine für den Datenschutz zuständige Person im Gremium? Welche Workshops wurden besucht? Wann gab es einen Austausch mit dem oder der Datenschutzbeauftragten? Wann immer etwas zum Thema Datenschutz anfällt, sollte es chronologisch und fortlaufend notiert werden. Dabei kann es sich um eine Buchanschaffung handeln, um den regelmäßigen gemeinsamen Termin im Gremium zur Auffrischung des Wissens oder um einen gemeinsamen Datenlöschtag zum Jahresende.

Abschnitt 2: Bestandsaufnahme

So manche Interessenvertretung stellt sich die Frage: „Welche Daten verarbeiten wir eigentlich?“ Zum Verständnis ist obige Definition von „Verarbeitung“ wichtig. Es handelt sich im weitesten Sinne um das **„Haben“** von Daten. Eine Bestandsaufnahme ist sinnvoll für eine Interessenvertretung, die sich in Sachen Datenschutz gut aufstellen möchte. Es ergibt Sinn, sich die eigenen Räumlichkeiten, Aktenschränke, Laufwerke anzusehen und der Frage nachzugehen, ob das, was sich dort angesammelt hat, wirklich noch datenschutzrechtlich in Ordnung ist. Maßstab dabei sind die oben genannten Grundsätze. Diese müssen alle eingehalten werden.

Als Hilfestellung für eine Bestandsaufnahme sollen folgende Fragen dienen. **Die Auflistung ist nicht abschließend, sie dient allein zur Orientierung.**

1. **Organisatorische Grundlagen**
- Gibt es eine Geschäftsordnung oder interne Richtlinie zum Thema Datenschutz?
- Sind Aufgaben und Verantwortlichkeiten beim Umgang mit personenbezogenen Daten klar geregelt?
- Ist eine Person aus dem Gremium für das Thema verantwortlich?

2. **Bestandsaufnahme der Datenverarbeitung**
- Existiert ein vollständiges Verzeichnis der Verarbeitungstätigkeiten?
- Sind alle Prozesse erfasst, bei denen personenbezogene Daten verarbeitet werden (zum Beispiel Mitgliederverwaltung, Beschwerden, Protokolle)?

3. **Technisch-organisatorische Maßnahmen (TOM)**
- Welche technischen Maßnahmen sind ergriffen worden?
  Mit technischen Maßnahmen sind Schutzvorkehrungen gemeint, die mit IT oder Technik umgesetzt werden – zum Beispiel hat das Büro der Interessenvertretung ein Schloss, das nur mit einem Schlüssel geöffnet werden kann.
- Welche organisatorischen Maßnahmen werden angewendet?
  Mit einer organisatorischen Maßnahme sind Regelungen gemeint, die den datenschutzkonformen Umgang steuern. Wird zum Beispiel eine Liste geführt, wer den Schlüssel für das Büro erhalten hat, dann ist das eine organisatorische Maßnahme.
- Wie werden besonders schützenswerte Daten aufbewahrt?
- Wer hat Zugriff darauf?

4. **Informationspflichten und Transparenz**
- Werden die Beschäftigten klar über die Datenverarbeitung ihrer personenbezogenen Daten im Büro der Interessenvertretung informiert?
- Ist geregelt, wie Auskunftsersuchen oder Löschanfragen bearbeitet werden?

5. **Schulung und Sensibilisierung**
- Sind alle Mitglieder der Interessenvertretung über den Datenschutz informiert?
- Gibt es regelmäßige Auffrischungen oder Informationsrunden zum Thema?

6. **Datenschutzverletzungen**
- Gibt es einen Ablaufplan für den Fall einer Datenschutzverletzung?
- Wie und wann wird der oder die Datenschutzbeauftragte informiert?

7. **Kommunikation und E-Mails**
- Werden personenbezogene Daten verschlüsselt per E-Mail versendet (zum Beispiel sensible Anhänge)?
- Wird bei E-Mail-Verteilern auf den Datenschutz geachtet (zum Beispiel „Bcc“ statt „An“)?

8. **Aufbewahrung und Löschung**
- Gibt es klare Regeln zur Aufbewahrung und Löschung personenbezogener Daten?
- Werden nicht mehr benötigte Daten regelmäßig gelöscht oder anonymisiert?

Abschnitt 3: Geschäftsordnung Datenschutz

Aus der Bestandsaufnahme lassen sich Regeln ableiten, wie konkret zu verfahren ist. Diese sollten verschriftlicht werden. Denkbar ist es, sie in einer Geschäftsordnung Datenschutz niederzuschreiben, die dann für die Dauer der Amtszeit der Interessenvertretung Gültigkeit hat (vergleiche hierzu § 36 BetrVG und § 38 BremPersVG).

Abschnitt 4: Verzeichnis der Verarbeitungstätigkeiten

Die DSGVO ist in Artikel 30 eindeutig: Jede*r Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten. Wenn sich die Interessenvertretung eigenständig um den Datenschutz in ihrem Büro

kümmert, drängt sich ein **eigenes Verzeichnis** auf. Dazu ist wichtig zu wissen, welche Verarbeitungen im Büro überhaupt stattfinden.

Zur Orientierung **drei Beispiele**:

- Gremienkommunikation: Jede Interessenvertretung, egal welcher Größe und wie viele Ausschüsse sie hat, muss kommunizieren und dabei auch personenbezogene Daten verarbeiten.
- Betriebsrats- oder Personalratswahlen: Um diese zu organisieren, werden auch Beschäftigtendaten verarbeitet. Es werden Listen mit Namen erstellt, Einladungen per E-Mail versendet.
- BEM-Verfahren: Auch hier werden Namen und personenbezogene Sachverhalte verarbeitet. Zudem werden hier besonders schützenswerte Daten verarbeitet.

Damit ein Verzeichnis der Verarbeitungstätigkeiten den gesetzlichen Vorgaben entspricht, muss es zu den einzelnen Verarbeitungstätigkeiten (wie zum Beispiel der Gremienkommunikation) mehrere Informationen enthalten. Diese sind in Artikel 30 der DSGVO aufgeführt:

- Warum werden die Daten verarbeitet? Was ist der Zweck der Verarbeitung?
- Welche Personen sind betroffen? Wessen Daten werden verarbeitet? Hier sind Kategorien zu nennen, also nicht die konkreten Namen einzelner Personen, sondern zum Beispiel „Beschäftigte“ oder „Schwerbehinderte“.
- Welche personenbezogenen Daten werden verarbeitet? Auch hier geht es nicht um Einzeldaten, sondern um die Kategorien wie zum Beispiel „Name“, „Adresse“.
- Wer bekommt die Daten? An wen werden Daten weitergegeben? (zum Beispiel Mitglieder des Personalrats)
- Werden Daten ins Ausland geschickt? (Drittlandübermittlung)
- Wann werden die Daten gelöscht? Wie lange werden die Daten aufbewahrt?
- Wie werden die Daten geschützt?

Als hilfreich hat sich erwiesen, zu den einzelnen Verarbeitungen noch einfache Erklärungen zu notieren, was warum wozu gemacht wird.

Die Bundesbeauftragte für den Datenschutz hat ein **Muster** (siehe QR-Code) veröffentlicht. Dieses ist zwar für die Verantwortlichen verfasst, eignet sich aber gut zur Orientierung.

Fazit:
Datenschutz im Büro der Interessenvertretung ist nicht immer ein Thema, das Begeisterung auslöst. Es wirkt manchmal sperrig, technisch oder bürokratisch. Aber genau hier liegt der Wert: Ein strukturierter Umgang mit den anvertrauten personenbezogenen Daten schützt nicht nur die Beschäftigten, sondern auch die Arbeit der Interessenvertretung selbst. Klar geregelte Zugriffsrechte, dokumentierte Abläufe und ein bewusstes Umgehen mit Informationen schaffen Vertrauen – nach innen und außen. Datenschutz ist damit nicht nur Pflicht, sondern kann auch ein Werkzeug sein, um professionelle und verlässliche Gremienarbeit zu sichern.

Infoblätter und weitere Informationen unter
➔ *arbeitnehmerkammer.de/betriebs-personalraete*

Wir sind für Sie erreichbar:

Mitbestimmung und Technologieberatung
☎ 0421.3 63 01-938/-957/-961 in Bremen
☎ 0471.9 22 35-22/-24/-31 in Bremerhaven
@ mitbestimmung@arbeitnehmerkammer.de
www.arbeitnehmerkammer.de/mitbestimmung

Impressum

Herausgeberin:
Arbeitnehmerkammer Bremen
Mitbestimmung und Technologieberatung
Bürgerstraße 1, 28195 Bremen
☎ 0421.3 63 01-959

Autor: Steffen Andreae
Layout: GfG/Gruppe für Gestaltung, Bremen
Druck: Druckerei Wellmann

Stand: Februar 2026

Arbeitnehmerkammer
Bremen