Vorbemerkung zur Auftragsverarbeitungsvereinbarung (AVV)

Das Programm „Betriebsratswahl 2026“ ist als Formulargenerator für die Wahlvorstände der Betriebsratswahlen 2026 im Geltungsbereich des deutschen Betriebsverfassungsgesetzes (BetrVG) vorgesehen. Dazu muss mit dem Bund-Verlag eine AVV abgeschlossen werden. (Dies erfolgt online, vor Aufrufen der Software, durch einfache Bestätigung des AVV-Textes per „Klick“).

Verantwortlicher im Sinne des Datenschutzrechts ist der Arbeitgeber, in dessen Betrieb die Betriebsratswahl stattfindet und für die „Betriebsratswahl 2026“ genutzt wird.

Das Programm "Betriebsratswahl 2026” für die Online-Nutzung in der Cloud (Software as a Service - SaaS) vorgesehen. Ist eine Eingabe der personenbezogenen Daten in den Cloudserver nicht gewünscht, kann der Wahlvorstand der Betriebsratswahl auch alle im Programm bereitgestellten Formulare als Leervorlagen auf den eigenen Rechner herunterladen, mit Microsoft Office oder kompatiblen Programmen bearbeiten und lokal speichern.

Auftragsverarbeitungsvereinbarung

für die Online-Nutzung der von der Bund-Verlag GmbH unter https://br-wahl2026.bund-verlag.de bereitgestellten Software „Betriebsratswahl 2026“ im vorgesehenen Nutzungszeitraum 1.8.2025 bis 30.6.2029.

Standardvertragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der 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)] sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II

PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von

beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens [eine Woche] im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der

Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679].

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter

bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 o in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I

Liste der Parteien

Verantwortlicher: Siehe Vorbemerkung Seite 1.

Auftragsverarbeiter: Bund-Verlag GmbH, vertreten durch den Geschäftsführer Jürgen Scholl, Emil-von-Behring-Str. 14, 60439 Frankfurt, E-Mail juergen.scholl@bund-verlag.de,Internet: www.bund-verlag.de.

Datenschutzbeauftragter des Auftragsverarbeiters:

Herr Markus Strauss, tacticx Consulting GmbH Walbecker Straße 53, 47608 Geldern, E-Mail datenschutz@bund-verlag.de, Internet: www.tacticx.de

Unterschrift und Beitrittsdatum: Frankfurt, 1. Juli 2025.

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Wahlvorstände, Wahlbewerberinnen und Wahlbewerber im Rahmen der Betriebsratswahlen 2026 und weiterer Betriebsratswahlen nach Maßgabe des BetrVG, Kategorien personenbezogener Daten, die verarbeitet werden.

Für das Cloud-Verfahren werden gemäß Art. 28 DSGVO personenbezogene Daten verarbeitet:

a. über Wahlbewerberinnen und Wahlbewerber (Vorname, Nachname, Geburtsdatum, Art der Beschäftigung im Betrieb, Geschlecht, ggf. Listenzugehörigkeit sowie das Wahlergebnis).
b. Verarbeitet werden zudem die Kontakt- und Kommunikationsdaten zu Mitgliedern des Wahlvorstands, des Betriebsrats (bzw. Gesamt- und Konzernbetriebsrats) und des Betriebs (bzw. Unternehmens und Konzerns) (in der Regel Name, Vorname, Standort), sofern sie von dem Nutzer eingegeben werden. Diese Daten werden zum Ersetzen der Platzhalter in den entsprechenden Formularen verarbeitet.

Betroffene haben ein Recht auf Auskunft, auf Berichtigung oder Löschung, sowie auf Widerspruch gemäß den Regelungen der DSGVO (Art. 15-18, 19,20, 21 DSGVO). Entsprechende Ansprüche sind direkt gegen den beim Auftraggeber bestehenden Wahlvorstand geltend zu machen. Wegen möglicher Datenschutzverstöße kann sich ein Betroffener an die für den Arbeitgeber zuständige Datenschutzaufsichtsbehörde im entsprechenden Bundesland wenden.

Art der Verarbeitung

Der Transfer der Daten zum Server des Auftragnehmers erfolgt über das Internet in verschlüsselter Form. Der Auftragnehmer ergreift die zur Wahrung der Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit erforderlichen Maßnahmen (Art. 32 DSGVO). Die Eingabe und Verarbeitung der Daten finden durch die Nutzer der Software „Betriebsratswahl 2026“ selbst statt.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Zweck der Datenverarbeitung ist allein die informationstechnische Unterstützung von Betriebsratswahlen. Rechtsgrundlage für die Verarbeitung ist § 18 BetrVG in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO.

Die Software unterstützt den Wahlvorstand beim Vorbereiten und Durchführen der Betriebsratswahlen. Eingaben personenbezogener Daten ermöglichen ein automatisiertes Berechnen der Sitzverteilung im neu gewählten Betriebsrat. Die personenbezogenen Daten werden in die vom Wahlvorstand verwendeten Formulare importiert, so dass zwingende Eingaben nicht mehr manuell vorzunehmen sind.

Dauer der Verarbeitung und Löschung

Die Software wird während der Wahlvorbereitung und -durchführung genutzt; der Nutzer kann in der Software jederzeit alle von ihm eingegebenen Daten und Datensätze löschen; ansonsten erfolgt die Löschung aller Daten aller Nutzer durch den Bund-Verlag am 1.7.2029.

Eine manuelle Löschung der Daten und Datensätze durch den Kunden ist während der Nutzung jederzeit möglich, es gibt einen entsprechenden „Löschen"-Button in der Software.

Das Löschdatum seitens des Bund-Verlags als Auftragnehmer „1.7.2029" folgt der gesetzlichen Aufgabenstellung, die mit dem Produkt erfüllt werden soll: Bei normalem Verlauf endet die vierjährige Amtszeit eines im Frühjahr 2026 gewählten Betriebsrats gemäß § 21 BetrVG im Frühjahr 2030, spätestens am 31.5.2030.

Das heißt, der amtierende Betriebsrat bestellt üblicherweise im dritten Quartal 2029 den Wahlvorstand für die nächste Wahl. Ab diesem Zeitpunkt ist eine Speicherung der alten Daten nicht mehr erforderlich, und die Software steht nicht mehr zur Verfügung, also löscht der Bund-Verlag dann auch vereinbarungsgemäß die alten Daten.

ANHANG III

Technische und organisatorische Maßnahmen

I. Vertraulichkeit gem. Art. 32 Abs. 1 lit b) DSGVO

1. Zutrittskontrolle

Technische Maßnahmen

- Chipkarten / Transpondersysteme
- Manuelles Schließsystem
- Elektronische Türöffner
- Serverraum mit Schutzvorkehrungen
- Schließsystem mit Codesperre
- Türen mit Knauf Außenseite
- Generalschlüssel
- Videoüberwachung des Serverraums
- Schutzvorkehrungen für Backups

Organisatorische Maßnahmen

- Schlüsselverwaltung / Dokumentation der
- Schlüsselvergabe (RFID-Chips) durch Personalabteilung/Geschäftsführung
- Bewachung außerhalb der Betriebszeiten
- Sorgfalt bei Auswahl Reinigungsdienste
- Zugang zum Serverraum für dritte nur unter Aufsicht
- Schutzkonzept für Backups

2. Zugangskontrolle

Technische Maßnahmen

- Login mit Benutzername + Passwort
- Login mit biometrischen Daten
- Anmeldung Tablet, Handy
- Single Sign-On
- Multi-Faktor-Authentifizierung
- Anti-Viren-Software
- Anti-Virus-Software Clients
- Anti-Virus-Software mobile Geräte
- Firewall (Hardware, Software, Multilayer)
- Intrusion Detection/Prevention System
- Mobile Device Management
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung der internen Notebook SSDs

- Verschlüsselung von Smartphones
- Verschlüsselung von Tablet
- BIOS Schutz (separates Passwort)
- Automatische Desktopsperre

Organisatorische Maßnahmen

- Zentrale Verwaltung von
- Benutzerberechtigungen
- Begrenzung der Anzahl befugter Benutzer
- Autorisierungsprozess für
- Zugangsberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe
- Sichere Dokumentation und Aufbewahrung der Passwörter
- Richtlinie „Sicheres Passwort“; regelmäßige Änderung von Kennwörtern
- Richtlinie „Löschen / Vernichten“
- Richtlinie „Clean desk“
- Allg. Richtlinie zur IT-Sicherheit
- Mobile Device Policy (Betriebsvereinbarung)
- Anleitung „Manuelle Desktopsperre“
- Vertraulichkeitsverpflichtung der zur Verarbeitung personenbezogener Daten befugten Personen

3. Zugriffskontrolle

Technische Maßnahmen

- Aktenshredder (mind. Stufe 3, crosscut)
- Externer Aktenvernichter (DIN 66399, entspricht alt: DIN 32757)
- Physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf
- Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten auf Fileserver und Sharepoint.
- Verschlüsselung von CD/ DVD, externen
- Festplatten, USB-Sticks; mobile Speichermedien werden möglichst selten benutzt
- Sichtschutzfolien für öffentliche/mobile
- Bildschirme Personalbereich
- Mobile Device Management-System
- Nicht-reversible Löschung von Datenträgern

Organisatorische Maßnahmen

- Einsatz Berechtigungskonzepte (differenzierte
- Berechtigungen: Profile/ Rollen)
- Minimale Anzahl an Administratoren
- Datenschutztresor
- Verwaltung Benutzerrechte durch
- Administratoren;
- Löschkonzept mit Löschfristen und Anweisungen ist vorhanden und wird fortgeschrieben.
- Genehmigungsroutinen (Zeichnungsrichtlinie)
- Vier-Augen-Prinzip

4. Trennungskontrolle

Technische Maßnahmen

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme /
- Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter
- Anwendungen
- Datensätze sind mit Zweckattributen versehen

Organisatorische Maßnahmen

- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten

4. **Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**

Organisatorische Maßnahmen

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
- Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation

5. **Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**

Technische Maßnahmen

- Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones s.o.
- Verschlüsselung von mobilen Speichermedien (CD/DVD, USB-Stick, externen Festplatten)
- Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)

- Gesichertes WLAN (WPA3, VLAN separiert, WAN separiert)

Organisatorische Maßnahmen

- Verschlüsselte Aufbewahrung von Passwörtern
- Verschiedene Passwörter zur Verschlüsselung

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1. **Weitergabekontrolle**

Technische Maßnahmen

- Bereitstellung über verschlüsselte Verbindungen u.a. TLS, sftp, ipSec
- Einsatz von VPN

Organisatorische Maßnahmen

- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- Zugriffsrechtekonzept

2. **Eingabekontrolle**

Technische Maßnahmen

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Auditing (Filezugriff)

Organisatorische Maßnahmen

- Klare Zuständigkeiten für Löschungen

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. **Verfügbarkeitskontrolle**

Technische Maßnahmen

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher Serverraum
- Schutzsteckdosenleisten Serverraum
- Serverraum klimatisiert
- USV im Serverraum
- Alarmmeldung bei Zutritt zu Serverraum
- Datenschutztresor (S60DIS, S120DIS,
- andere geeignete Normen mit Quelldichtung etc.)

- RAID-System / Festplattenspiegelung
- Videoüberwachung Serverraum
- regelmäßige Backups
- Trennung von Webserver/Webapplikationen und Geschäftsanwendungen

Organisatorische Maßnahmen

- Backup & Recovery-Konzept (ausformuliert)
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur
- Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an
- einem sicheren Ort außerhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Existenz eines Notfallplans (z.B. BSI IT-
- Grundschutz 100-4)
- Getrennte Partitionen für Betriebssysteme und Daten

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

1. Datenschutz-Management

Technische Maßnahmen

- Dokumentiertes Sicherheitskonzept und internes Datenschutzhandbuch
- Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind.
- jährlich durchgeführt
- Regelmäßige Datenschutz-Schulungen der Mitarbeiter

Organisatorische Maßnahmen

- Externer Datenschutzbeauftragter: Herr Markus Strauss, tacticx Consulting GmbH Walbecker Straße 53, 47608 Geldern, datenschutz@bund-verlag.de
- Interner Datenschutz-Koordinator als Ansprechpartner
- Datenschutz-E-Mail-Postfach: datenschutz@bund-verlag.de
- Mitarbeiter geschult und auf Vertraulichkeit verpflichtet
- Interner Informationssicherheits-Beauftragter
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Die Organisation kommt den Informations- pflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

2. Incident-Response-Management

(Unterstützung bei der Reaktion auf Sicherheitsverletzungen)

Technische Maßnahmen

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)

Organisatorische Maßnahmen

- Dokumentierter Prozess zur Erkennung und Meldung von Informationssicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Dokumentierte Vorgehensweise zum Umgang mit Datenschutzvorfällen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Einbindung von Datenschutzbeauftragtem und Informationssicherheitsbeauftragtem in Sicherheitsvorfälle und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem

3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO (Privacy-by-design / Privacy-by-default)

Technische Maßnahmen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

Organisatorische Maßnahmen

- Der Datenschutzbeauftragte wird in neue Prozesse zur Verarbeitung personenbezogener Daten frühestmöglich eingebunden.

4. Auftragskontrolle (Outsourcing an Dritte)

Organisatorische Maßnahmen

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln

ANHANG IV

Liste der Unterauftragsverarbeiter

Der Verantwortliche genehmigt die Inanspruchnahme folgender Unterauftragsverarbeiter des Auftragsverarbeiters Bund-Verlag GmbH:

Der Auftragsverarbeiter Bund Verlag GmbH stellt sicher, dass die Unterauftragnehmer vertraglich zur Einhaltung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO verpflichtet sind und dass ihnen mindestens die gleichen datenschutzrechtlichen Pflichten auferlegt sind wie dem Auftragsverarbeiter gegenüber dem Verantwortlichen.

1. Firma Treml & Sturm Datentechnik GmbH

Die Firma ist technischer Dienstleister für Infrastruktur und Hosting mit Rechenzentrumsbetrieb in Offenbach am Main, Deutschland; sie betreibt als Unterauftragnehmerin den Server des Auftragnehmers Bund-Verlag GmbH, auf dem die Software Betriebsratswahl 2026 gehostet wird, in Frankfurt am Main. Die Firma übernimmt übernimmt den technischen Betrieb der Serverinfrastruktur (Hosting), einschließlich Rechenzentrumsbetrieb, physischer Sicherheit, Systemverfügbarkeit und Basisadministration.

Die Treml & Sturm Datentechnik GmbH erbringt ausschließlich infrastrukturelle Leistungen und nimmt keine eigenständige inhaltliche Verarbeitung der personenbezogenen Daten (Anhang II) vor. Ein Zugriff auf personenbezogene Daten kann ausschließlich im Rahmen des technischen Betriebs oder der Störungsbehebung erfolgen und nur auf dokumentierte Weisung des Auftragsverarbeiters.

Anschrift: Mühlheimer Straße 209,
63075 Offenbach am Main
Online: https://treml-sturm.com/home/
Datenschutz: https://treml-sturm.com/datenschutz/

2. Firma Druckerei C.H.Beck Nördlingen

Die Druckerei C. H. Beck übernimmt die Pflege und Wartung der Formular-Generator-Software auf einem separaten Windows-Server, der im Rechenzentrum von Dienstleister 1 (Firma Treml & Sturm Datentechnik GmbH) betrieben wird und im Eigentum des Auftragsverarbeiters Bund-Verlag GmbH steht. Die Druckerei C. H. Beck hat im Rahmen ihrer Wartungs- und Supporttätigkeiten Zugriff auf die Serverumgebung und damit potenziell auf verschlüsselt gespeicherte personenbezogene Daten der Kunden. Der Zugriff erfolgt ausschließlich nach Weisung des Auftragsverarbeiters Bund-Verlag GmbH und unter Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen (insbesondere Verschlüsselung, Zugriffskontrolle, Protokollierung).

Anschrift: Bergerstr. 3-5, 86720 Nördlingen, Deutschland

Online: https://www.becksche.de/Home

Kontakt zu Datenschutz und Compliance Management:

https://www.becksche.de/CHBeck/Datenschutz