Vorbemerkung zum Auftragsverarbeitungsvertrag (AVV)

Die Software-Pakete „Betriebsratswahl 2022“ und „JAV-Wahl 2022“ können jeweils alternativ auf zwei Arten genutzt werden:

1. Online in der Cloud. Dazu muss mit dem Bund-Verlag der nachstehende AVV abgeschlossen werden. (Dies erfolgt online, vor Aufrufen der Software, durch einfache Bestätigung des AVV-Textes per „Klick“).
2. Auf einem dem Wahlvorstand zugänglichen Rechner oder Server. Dazu muss die Software heruntergeladen und installiert werden. Eine Speicherung der Daten erfolgt ausschließlich auf dem lokalen Rechner, so dass keine Auftragsverarbeitung von Daten durch den Bund-Verlag stattfindet und kein AVV zu schließen ist.

Verantwortlicher im Sinne des Datenschutzrechts ist und bleibt In beiden Fällen der Arbeitgeber.

Auftragsverarbeitungsvertrag

1. für die Online-/Cloud-Nutzung der von der Bund-Verlag GmbH unter <https://br-wahl2022.bund-verlag.de/> bereitgestellten Software „Betriebsratswahl 2022“ im vorgesehenen Nutzungszeitraum 1.8.2021 bis 31.5.2025.
2. für die Online-/Cloud-Nutzung der von der Bund-Verlag GmbH unter <https://jav-wahl2022.bund-verlag.de> bereitgestellten Software »JAV-Wahl 2022« im vorgesehenen Nutzungszeitraum 1.5.2022 bis 1.5.2024.

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 personenbezogener 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.

Auftragsverarbeiter:

1. Name: Bund-Verlag GmbH
Anschrift: Emil-von-Behring-Str. 14, 60439 Frankfurt

Name, Funktion und Kontaktdaten der Kontaktperson:

- Rainer Jöde, Geschäftsführer, rainer.joede@bund-verlag.de
- **Datenschutzbeauftragter:** Rechtsanwalt Jan-Alexander Fortmeyer, Fachanwalt für Urheber- und Medienrecht, Zeppelinallee 21, 60325 Frankfurt am Main, Tel 069 - 713 731 8-0, Fax -50

Unterschrift und Beitrittsdatum:

Für die Software »Betriebsratswahl 2022«: Frankfurt, 1. September 2021.

Für die Software »JAV-Wahl 2022«: Frankfurt, 1. Mai 2022.

ANHANG II

Beschreibung der Verarbeitung

1. Für die Software »Betriebsratswahl 2022«

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Wahlvorstände, Wahlbewerberinnen und Wahlbewerber im Rahmen der Betriebsratswahlen 2022 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 Cloudanbieter erfolgt über das Internet in verschlüsselter Form (AES Schlüssellänge 128 Bit). Der Cloudanbieter ergreift die zur Wahrung der Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit erforderlichen Maßnahmen (Art. 32 DSGVO).

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 zudem in die vom Wahlvorstand zu verwendenden Formulare importiert, so dass zwingende Eingaben nicht mehr manuell vorzunehmen sind.

Dauer der Verarbeitung

Während der Wahlvorbereitung und -durchführung; der Nutzer kann jederzeit alle von ihm eingegebenen Daten löschen; ansonsten Löschung aller Daten aller Nutzer durch die Bund-Verlag GmbH am 30.9.2025.

2. Für die Software »JAV-Wahl 2022«

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Wahlvorstände, Wahlbewerberinnen und Wahlbewerber im Rahmen der JAV-Wahlen 2022 und späterer JAV-Wahlen nach Maßgabe des BetrVG

Kategorien personenbezogener Daten, die verarbeitet werden

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

- c. über Wahlbewerberinnen und Wahlbewerber (Vorname, Nachname, Geburtsdatum, Art der Beschäftigung im Betrieb, Geschlecht, ggf. Listenzugehörigkeit sowie das Wahlergebnis).*
- d. Verarbeitet werden zudem die Kontakt- und Kommunikationsdaten zu Mitgliedern des Wahlvorstands, der JAV (bzw. Gesamt- und Konzern-JAV) 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 Cloudanbieter erfolgt über das Internet in verschlüsselter Form (AES Schlüssellänge 128 Bit). Der Cloudanbieter ergreift die zur Wahrung der Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit erforderlichen Maßnahmen (Art. 32 DSGVO).

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

Zweck der Datenverarbeitung ist allein die informationstechnische Unterstützung von JAV-Wahlen. 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 JAV-wahlen. Die personenbezogenen Daten des Wahlvorstands werden zudem in die von ihm zu verwendenden Formulare importiert.

Dauer der Verarbeitung

Während der Wahlvorbereitung und -durchführung; der Nutzer kann jederzeit alle von ihm eingegebenen Daten löschen; ansonsten Löschung aller Daten aller Nutzer durch die Bund-Verlag GmbH am 30.9.2024.

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret beschrieben werden; eine allgemeine Beschreibung ist nicht ausreichend.

Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☒ Schlüsselverwaltung / Dokumentation der Schlüsselvergabe(Chips)
☐ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption
☐ Biometrische Zugangssperren	☐ Pförtner / Werkschutz
☒ Chipkarten / Transpondersysteme	☐ Besucherbuch / Protokoll der Besucher

☐ Manuelles Schließsystem	☐ Mitarbeiter- / Besucherausweise
☐ Sicherheitsschlösser	☐ Besucherregelung / Begleitung durch Mitarbeiter / Besucherausweis
☒ Elektronische Türöffner teilweise	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☒ Bewachung außerhalb der Betriebszeiten
☐ Absicherung der Gebäudeschächte	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Türen mit Knauf Außenseite	☐ Sperrbereiche
☒ Generalschlüssel	
☐ Klingelanlage mit Kamera	
☒ Videoüberwachung der Eingänge Im Serverraum	
☐ Vergitterte Fenster/Türen	
☐ Zaunanlagen	
☒ Spezielle Schutzvorkehrungen Serverraum Videoüberwachung im Serverraum	
☒ Spezielle Schutzvorkehrungen Backups	

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von Call-Back-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Zentrale Verwaltung von Benutzerberechtigungen
☒ Login mit biometrischen Daten Anmeldung Tablet, Handy, einzeln verwaltet durch den MA	☒ Autorisierungsprozess für Zugangsberechtigungen

☒ Single Sign-On teilweise	☒ Erstellen von Benutzerprofilen
☐ Zwei-Faktor-Authentifizierung (TAN, Token, Chipkarten, etc.)	☒ Zentrale Passwortvergabe
☒ Anti-Viren-Software Server Kaspersky	☒ sichere Dokumentation und Aufbewahrung der Passwörter
☒ Anti-Virus-Software Clients s.o.	☒ Richtlinie „Sicheres Passwort“
☒ Anti-Virus-Software mobile Geräte Kaspersky- in der Einführung	☒ Richtlinie „Löschen / Vernichten“
☒ Firewall Watch Guard, Windows/Linux Firewall	☒ Richtlinie „Clean desk“
☒ Intrusion Detection/Prevention Systeme s.o.	☒ Allg. Richtlinie zur IT-Sicherheit
☒ Mobile Device Management Kaspersky-in der Einführung	☒ Mobile Device Policy BV
☒ Einsatz VPN bei Remote-Zugriffen	☒ Anleitung „Manuelle Desktopsperre“
☒ Verschlüsselung von Datenträgern Notebooks	☒ Begrenzung der Anzahl befugter Benutzer
☐ Verschlüsselung Smartphones	☒ Kennwortverfahren (regelmäßige Änderungen)
☐ Gehäuseverriegelung	
☐ BIOS Schutz (separates Passwort) Ggf. in der Einführung	
☐ Sperre externer Schnittstellen (USB)	
☒ Automatische Desktopsperre	
☒ Verschlüsselung von Notebooks / Tablet	
☒ Nicht-reversible Vernichtung von Datenträgern	

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenshredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte (differenzierte Berechtigungen)
☒ Externer Aktenvernichter (DIN 66399, alt: 32757)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern	☒ Datenschutztresor
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten teilweise	☒ Verwaltung Benutzerrechte durch Administratoren
☒ Verschlüsselung von CD/ DVD, externen Festplatten und/ oder Laptops	☐ Auswertungen von Datenverarbeitungen
☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbaren Datenträger	☒ Autorisierungsprozess für Berechtigungen
☒ Mobile Device Management-System	☒ Genehmigungsrouinen (Zeichnungsrichtlinie)
☒ Nicht-reversible Löschung von Datenträgern	☒ Profile/ Rollen
☒ Sichtschutzfolien für öffentliche/mobile Bildschirme Personalbereich	☒ Vier-Augen-Prinzip
	☐ Funktionstrennung „Segregation of Duties“

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Datensätze sind mit Zweckattributen versehen

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

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

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
☐ getrennte Speicherung von Zusatzinformationen zur Identifikation	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐ Verschlüsselung von Zusatzinformationen zur Identifikation	☒ Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation
☐ Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation	☐ Autorisierungsprozess oder Genehmigungsprotokolle für Berechtigungen auf die Zusatzinformationen zur Identifikation
	☐ Vier-Augen-Prinzip für Identifikation

Weitere Maßnahmen:

Es findet keine Pseudonymisierung statt.

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

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones s.o. teilweise	☒ Verschlüsselte Aufbewahrung von Passwörtern
☒ Verschlüsselung von mobilen Speichermedien (CD/DVD, USB-Stick, externen Festplatten) mobile Speichermedien selten benutzt	☒ Verschiedene Passwörter zur Verschlüsselung
☐ Verschlüsselung von Dateien	
☐ Verschlüsselung von Systemen/ Anlagen	
☐ Verschlüsselung von E-Mail und E-Mail-Anhängen	
☒ Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)	
☒ Gesichertes WLAN	

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

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

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen

☐ Protokollierung der Zugriffe und Abrufe Logfiles Implementierung der Auditing in der Prüfung	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☒ Zugriffsrechtekonzept

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten Logfiles Bund online, NTX, easy Archiv	☐ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☒ Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

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

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☐ Serverraumüberwachung Temperatur und Feuchtigkeit wird eingeführt	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Schutzsteckdosenleisten Serverraum	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschrift 100-4)
☒ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ RAID System / Festplattenspiegelung	
☒ Videoüberwachung Serverraum	
☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen

☐ Software-Lösungen für Datenschutz-Management im Einsatz	☒ Externer Datenschutzbeauftragter Rechtsanwalt Jan-Alexander Fortmeyer, Fachanwalt für Urheber- und Medienrecht, Zeppelinallee 21, 60325 Frankfurt am Main , Tel 069 - 713 731 8-0, Fax -50
☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☐ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
☒ Anderweitiges dokumentiertes Sicherheits-Konzept	☐ Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Weitere Maßnahmen:

Informationssicherheitsbeauftragter in Planung.

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

☒ Einsatz von Virens Scanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Intrusion Prevention System (IPS)	☐ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Weitere Maßnahmen:

Keine weiteren Maßnahmen vorhanden.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy-by-design / Privacy-by-default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ der Datenschutzbeauftragte wird in neue Prozesse zur Verarbeitung personenbezogener Daten frühestmöglich eingebunden.
☒ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen vgl. arbeitrecht.de Prüfung der Einführung der Selbstlöschung vgl. nextcloud	

Weitere Maßnahmen: -

Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen
☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln

☐ Schriftliche Weisungen an den Auftragnehmer
☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐ Regelung zum Einsatz weiterer Subunternehmer
☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter)Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

ANHANG IV

Liste der Unterauftragsverarbeiter

(ERLÄUTERUNG:

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7 Buchstabe a, Option 1).)

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: Fa. Treml & Sturm Datentechnik GmbH,

Anschrift: Mühlheimer Straße 209, 63075 Offenbach am Main

2. Name: Fa. Druckerei C.H.Beck

Anschrift: Bergerstr. 3-5, 86720 Nördlingen