Vertrag zur Auftragsverarbeitung (§ 30 DSG-EKD)

WICHTIG Bitte füllen Sie die Formularfelder und den Anhang 1 dieses Vertragsmusters aus. Berücksichtigen Sie bitte auch die grau hinterlegten Bearbeitungshinweise und löschen diese nach Abschluss der Bearbeitung.

Anschließend können Sie dieses Vertragsmuster zur weiteren Bearbeitung an Ihren Auftragsverarbeiter weiterleiten, damit dieser die erforderlichen Angaben in den Anhängen 2 und 3 macht.

zwischen

**<[Verantwortlicher], [Anschrift]>**

– nachfolgend „Verantwortlicher“ genannt –

und

**<[Auftragsverarbeiter], [Anschrift]>**

– nachfolgend „Auftragsverarbeiter“ genannt

und gemeinsam als „Vertragsparteien“ bezeichnet – wird Folgendes vereinbart:

##### § 1 Vorbemerkungen

Werden in diesem Vertrag die in dem Kirchengesetz über den Datenschutz in der Evangelischen Kirche in Deutschland (DSG-EKD) definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie im DSG-EKD.

##### § 2 Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben.

##### § 3 Weisungen der Verantwortlichen

1. Der Verantwortliche ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts verantwortlich. 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 eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.
2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestim­mungen der Union oder eines Mitgliedstaats verstößt.

##### § 4 Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter trifft mindestens die im Anhang 3 aufgeführten technischen und organisa­torischen Maßnahmen, um die Sicherheit der personen­bezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemes­senen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implemen­tierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach den §§ 13, 14 DSG-EKD) sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
2. Die im Anhang 3 aufgeführten Maßnahmen sind an technische und organisato­rische Weiterentwick­lungen anzupassen, sofern diese Anpassungen mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter wesentliche Anpassungen dem Verantwortlichen unaufgefordert mit.

##### § 5 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutz­recht­lichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungs­bereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.
2. 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 die zur Verarbeitung der erhal­tenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflich­tet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
3. Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauf­tragten für den Datenschutz und teilt dessen Kontaktdaten dem Verantwortlichen unaufgefordert mit.
4. Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundes­republik Deutschland, in einem Mitgliedstaat der Europäischen Union oder inner­halb des Europäischen Wirtschaftsraums. Jede Datenübermittlung durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich aufgrund dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt.

HINWEIS Der nachfolgende Absatz ist nur dann in den Vertrag zu übernehmen, wenn im Rahmen der Auftragsverarbeitung Daten verarbeitet werden, die in den Schutzbereich des § 203 StGB fallen bzw. einem Berufsgeheimnis unterliegen. Ist dies nicht der Fall, sollte dieser Absatz gestrichen werden.

1. Sofern der Auftragsverarbeiter Daten des Verantwortlichen im Auftrag verarbeitet, die dem Schutz­bereich des § 203 StGB bzw. einem Berufsgeheimnis unterliegen, darf der Auftragsverarbeiter nur dann auf derartige Daten zugreifen, soweit dies im Einzelfall erforderlich ist. Der Auftragsverarbeiter verpflichtet sich in diesem Zusammenhang, alle Personen, die im Rahmen der beauftragten Tätigkeit die in Satz 1 genannten Daten verarbeiten, auf die Geheimhaltung nach § 203 StGB zu verpflichten. Dem Auftragsverarbeiter ist bekannt, dass hinsichtlich der Daten, die dem Schutzbereich des § 203 StGB unterliegen, ein Zeugnisverweigerungsrecht nach § 53a StPO besteht. Über die Ausübung des Rechtes auf Zeugnisverweige­rung entscheidet der Berufsgeheimnisträger der Verantwortlichen. Dem Auftrags­verarbeiter ist bekannt, dass die dem Berufsgeheimnis unterliegenden Daten, die sich im Gewahrsam des Auftragsverarbeiters zur Erhebung, Verarbeitung oder Nutzung befinden, dem Beschlagnahmeverbot des § 97 Abs. 1, 3 StPO unterliegen. Einer Sicherstellung ist zu widersprechen. Der Verantwortliche ist unverzüglich zu informieren, wenn eine Beschlagnahme der Daten zu erwarten ist oder bevorsteht.

##### § 6 Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung aller gesetzlichen Pflich­ten, wirkt auf Anfrage an der Erstellung und Aktualisierung des Verzeichnisses der Verarbeitungstätig­keiten des Verantwortlichen und bei der Erstellung einer Datenschutz-Folgenabschätzung sowie der erforderlichen Konsul­tation der Aufsichtsbehörden mit. Er hat dem Verantwortlichen alle erforder­lichen Informationen auf Anfrage zur Verfügung zu stellen. Der Auftragsverarbeiter unterstützt zudem bei der Prüfung von Datenschutzverletzungen und der Umset­zung etwaiger Meldepflichten. Schließlich unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem er den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind.
2. Ferner unterstützt der Auftragsverarbeiter den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen. Er bearbeitet diese nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt. 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.

##### § 7 Berechtigung zur Begründung von Unterauftragsverhältnissen

1. Der Auftragsverarbeiter darf Unterauftragnehmer nur beauftragen, wenn der Verantwortliche dies vorher schriftlich genehmigt hat. Der Auftragsverarbeiter stellt die Informationen, die der Verantwort­liche benötigt, um über die Geneh­migung zu entscheiden, rechtzeitig, mindestens jedoch drei Wochen vor der Beauftragung des betreffenden Unterauftragsverarbeiters, zur Verfügung.

ACHTUNG Alternative Vertragsregelung. Falls diese eingesetzt werden soll, den vorstehenden Absatz löschen. Ansonsten den nachfolgenden Absatz streichen.

1. Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftra­gung von Unterauftragsverarbeitern, die in Anhang 2 aufgeführt sind. Der Auftragsverarbeiter unter­richtet den Verantwortlichen mindestens drei Wochen im Voraus schriftlich über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern, damit der Verant­wortliche vor der Beauftragung neuer Unterauftragsverarbeiter Einwände gegen diese Änderungen erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Wider­spruchsrechts zu entscheiden mit der Unterrichtung über die geplante Änderung zur Verfügung.
2. Ein Zugriff auf personenbezogene Daten durch den Unterauftragnehmer darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag mit dem Unterauftragnehmer sicherstellt, dass die in diesem Vertrag vereinbarten Rege­lungen auch gegenüber dem Unterauftragnehmer gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftrags­verarbeiters.
3. Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der EU-Datenschutz-Grund­verordnung (DSGVO) beinhaltet, die Einhaltung der Regelungen des Kapitels V der DSGVO sicher, indem geeignete Garantien gemäß Artikel 44ff. DSGVO getroffen werden.
4. Ferner führt der Auftragsverarbeiter, wenn infolge der Beauftragung eines Unter­auftragnehmers ein Drittlandbezug besteht, eine Risikoeinschätzung (sog. „Transfer Impact Assessment“) durch und stellt diese dem Verantwortlichen unaufgefordert zur Verfügung. Kommt der Auftragsverarbeiter zu dem Ergebnis, dass Maßnahmen getroffen werden müssen, um ein adäquates Schutzniveau zu erreichen, dann sind diese Maßnahmen von ihm bzw. vom Unterauftragnehmer zu ergreifen.

HINWEIS Der nachfolgende Absatz ist nur dann in den Vertrag zu übernehmen, wenn im Rahmen der Auftragsverarbeitung Daten verarbeitet werden, die in den Schutzbereich des § 203 StGB fallen bzw. einem Berufsgeheimnis unterliegen. Ist dies nicht der Fall, sollte dieser Absatz gestrichen werden.

1. Der Auftragsverarbeiter hat die Verpflichtung der weiteren mitwirkenden Personen und der Unter­auf­tragnehmer auf die Geheimhaltung gem. § 203 StGB und § 5 Abs. 5 dieses Vertrages sicherzustellen.

##### § 8 Kontrollrechte des Verantwortlichen

1. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfü­gung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder unmittelbar aus dem DSG-EKD oder anderen Gesetzen hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsver­arbeiter ebenfalls die Prüfung der unter diesen Vertrag 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.
2. 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.
3. Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

##### § 9 Mitzuteilende Verstöße

1. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bereits bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.
2. Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:
   * Beschreibung der Art der Verletzung, der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
   * Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
   * Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
   * Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

##### § 10 Beendigung des Auftrags

1. Nach Abschluss der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dies gilt auch für etwaige Sicherungs­kopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen.
2. Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestim­mungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der verein­barten Beendigung des Auftrags nicht zugemutet werden kann. Ein schwer­wiegender Verstoß liegt insbe­sondere vor, wenn der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde, die seine Pflichten gemäß dieses Vertrages, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

##### § 11 Schlussbestimmungen

1. Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.
2. Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.
3. Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirk­samkeit des Vertrags im Übrigen nicht.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Verantwortlicher

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Auftragsverarbeiter

##### Anhang 1

##### Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

|  |  |
| --- | --- |
| Gegenstand der Verarbeitung | <z.B. Akten- und Datenträgervernichtung> |
| Art und Zweck der Verarbeitung | <z.B. datenschutzkonforme Vernichtung von Schriftgut und Datenträgern nach der DIN 66399 zur Erfüllung der Löschpflichten nach dem DSG-EKD (Grundsatz der Speicherbegrenzung)> |
| Art der  personenbezogenen  Daten | <z.B. Beschäftigtendaten, Kundendaten, Lohn- und Gehaltsdaten, Bewerberdaten, Zahlungsdaten, Dienstleisterdaten> |
| Kategorien betroffener Personen | <z.B. Beschäftigte, Kunden, Dienstleister, Bewerber/innen, Kursteilnehmende> |

|  |  |
| --- | --- |
| Datenschutzbeauftragter des Verantwortlichen | <[Name Datenschutzbeauftragten des Verantwortlichen], [Anschrift], E-Mail: [E-Mail-Adresse] oder „Der Verantwortliche hat keinen Datenschutzbeauftragten bestellt.“> |
| Datenschutzbeauftragter des Auftragsverarbeiters | <[Name Datenschutzbeauftragte/r des Auftragsverarbeiters], [Anschrift], E-Mail: [E-Mail-Adresse] oder „Der Auftragsverarbeiter hat keinen Datenschutzbeauftragten bestellt.“> |

##### Anhang 2

##### Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

HINWEIS Diese Tabelle ist von bzw. mithilfe des Auftragsverarbeiters auszufüllen, wenn dieser zur Erfüllung des Vertrages ebenfalls Leistungen eines oder mehrerer Auftragsverarbeiter (sog. Unter­auftragnehmer) in Anspruch nimmt (vgl. hierzu § 7 des Vertrages). Bei Bedarf bitte weitere Zeilen an die Tabelle einfügen bzw. nicht benötigte Zeilen aus der Tabelle löschen.

|  |  |  |
| --- | --- | --- |
| Unterauftragnehmer | Verarbeitungsstandort | Art der Dienstleistung |
| <[Unterauftragnehmer, Anschrift]> | <[Anschrift Verarbeitungsstandort Unterauftragnehmer], falls die Verarbeitung nicht am Sitz des Unterauftragnehmers erfolgt oder „Verarbeitung erfolgt am Unternehmenssitz“*>* | <[Bezeichnung Dienstleistung]> |
| <[Unterauftragnehmer, Anschrift]> | <[Anschrift Verarbeitungsstandort Unterauftragnehmer], falls die Verarbeitung nicht am Sitz des Unterauftragnehmers erfolgt oder „Verarbeitung erfolgt am Unternehmenssitz“*>* | <[Bezeichnung Dienstleistung]> |
| <[Unterauftragnehmer, Anschrift]> | <[Anschrift Verarbeitungsstandort Unterauftragnehmer], falls die Verarbeitung nicht am Sitz des Unterauftragnehmers erfolgt oder „Verarbeitung erfolgt am Unternehmenssitz“*>* | <[Bezeichnung Dienstleistung]> |
| <wie oben> | <wie oben> | <wie oben> |
| <wie oben> | <wie oben> | <wie oben> |

Anhang 3

Technisch-organisatorische Maßnahmen zur IT‑Sicherheit (§ 27 DSG-EKD)

HINWEIS Sofern der Auftragsverarbeiter seine „technischen und organisatorischen Maßnahmen zur IT-Sicherheit“ nicht bereits selbst dokumentiert hat, ist es erforderlich, dass er die nachfolgenden Fragen so umfassend und detailliert wie möglich beantwortet (vgl. § 4 des Vertrages). Auf der Grundlage dieser Angaben ist dann zu prüfen, ob für die Auftragsverarbeitung ein ausreichendes Niveau zum Schutz personenbezogener Daten besteht.

1. Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

|  |  |
| --- | --- |
| 1. | ZutrittskontrollE Serverräume |
| 1.0 | Werden personenbezogene Daten der Verantwortlichen auf Servern gespeichert, die von Ihnen oder etwaigen Dienstleistern betrieben werden?  ja  nein |
|  | *Wenn 1.0 nein:* In diesem Fall müssen die weiteren Fragen zu A1 nicht beantwortet werden, sondern sogleich die Fragen ab A2. Auch die Fragen zu B1 und B2 entfallen. |
| 1.1 | Standort des Serverraums / Rechenzentrums (RZ).  <[Anschrift] des RZ> |
| 1.2 | Sind die personenbezogenen Daten auf mehr als einen Serverstandort bzw. Rechenzentrum verteilt (bspw. Backup-Server, Nutzung von Cloud-Dienstleistungen)?  ja  nein |
| 1.3 | *Falls 1.2 ja:* Machen Sie bitte die entsprechenden Standortangaben auch zu weiteren Servern.  Weitere Serverstandorte: <[Anschrift/en] weiterer Serverstandorte> |
| 1.4 | Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für alle im Einsatz befindlichen Rechenzentrum- bzw. Serverstandorte?  ja  nein |
| 1.5 | *Falls 1.4 nein:* Beantworten Sie bitte die Fragen 1.6 bis 1.21 und B für weitere Rechenzentrum- bzw. Serverstandorte. |
| 1.6 | Hat der Serverraum Fenster?  ja  nein |
| 1.7 | *Wenn 1.6 ja:* Wie sind die Fenster vor Einbruch geschützt?  vergittert  alarmgesichert  abschließbar  gar nicht  Sonstiges: <Andere Sicherungsmaßnahmen benennen> |
| 1.8 | Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?  ja  nein |
| 1.9 | *Wenn 1.8 ja:* Wer wird informiert, wenn die EMA auslöst (Mehrfachantworten möglich)?  beauftragter Wachdienst  Administrator  Leiter IT  andere Stelle: <[Stelle], die informiert wird, bspw. Geschäftsführung> |
| 1.10 | Ist der Serverraum videoüberwacht?  ja, ohne Bildaufzeichnung  ja, mit Bildaufzeichnung  nein |
| 1.11 | *Wenn 1.10 ja, mit Bildaufzeichnung:* Wie lange werden die Bilddaten gespeichert?  <Speicherdauer in Tagen angeben> Tage |
| 1.12 | Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne?  Anzahl der Personen: <Anzahl der Personen>  Funktion im Unternehmen: <Funktion/en des/der Zutrittsberechtigten> |
| 1.13 | Ist der Serverraum mit einem elektronischen Schließsystem versehen?  ☐ ja ☐ nein, mit mechanischem Schloss |
| 1.14 | *Wenn 1.13 ja:* Welche Zutrittstechnik kommt zum Einsatz? (Mehrfachantworten möglich)  RFID  PIN  Biometrie  Sonstiges: <andere Zutrittstechnik> |
| 1.15 | *Wenn 1.13 ja:* Werden die Zutrittsrechte personifiziert vergeben?  ja  nein |
| 1.16 | *Wenn 1.13 ja:* Werden die Zutritte zum Raum im Zutrittssystem protokolliert?  ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche  ja, aber nur erfolgreiche Zutritte  ja, aber nur erfolglose Zutrittsversuche  nein, das Schloss wird nur freigegeben oder nicht |
| 1.17 | *Wenn 1.16 ja:*  Wie lange werden die Zutrittsdaten ungefähr gespeichert?  <Speicherdauer in Tagen> Tage |
| 1.18 | *Wenn 1.13 nein:* Wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus?  Anzahl Schlüssel: <Anzahl>.  Aufbewahrungsort: <Ort>  Ausgabestelle: <Stelle> |
| 1.19 | Aus welchem Material besteht die Zugangstür zum Serverraum?  Stahl/Metall  sonstiges Material |
| 1.20 | Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt?  ja  nein |
| 1.21 | *Wenn 1.20 ja:* Was wird in dem Serverraum noch aufbewahrt?  Telefonanlage  Lagerung Büromaterial  Lagerung Akten  Archiv   Lagerung von IT-Ausstattung  Sonstiges: <Sonstiges> |
| 2. | ZUTRITTSKONTROLLMASSNAHMEN ZU BÜRORÄUMEN |
| 2.1 | Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: <Anschrift/en Standort/e> |
| 2.2 | Existiert ein Pförtnerdienst bzw. ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros?  ja  nein |
| 2.3 | Wird ein Besucherbuch geführt?  ja  nein |
| 2.4 | Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?  ja  nein |
| 2.5 | *Wenn 2.4 ja:* Wer wird informiert, wenn die EMA auslöst?  beauftragter Wachdienst  Administrator  Leiter IT  Sonstiges: <Stelle> |
| 2.6 | Werden das Bürogebäude bzw. seine Zugänge videoüberwacht?  ja, ohne Bildaufzeichnung  ja, mit Bildaufzeichnung  nein |
| 2.7 | *Wenn 2.6 ja (mit Bildaufzeichnung):* Wie lange werden die Bilddaten gespeichert?  <Speicherdauer in Tagen> Tage |
| 2.8 | Ist das Gebäude bzw. sind die Büroräume mit einem elektronischen Schließsystem versehen?  ja, Gebäude und Büroräume sind elektronisch verschlossen  ja, aber nur das Gebäude, nicht der Eingang zu den Büros bzw. zur Büroetage  ja, aber nur der Eingang zu den Büros bzw. zur Büroetage, nicht das Gebäude insgesamt  nein |
| 2.9 | *Wenn 2.8 ja:* Welche Zutrittstechnik kommt zum Einsatz (Mehrfachantworten möglich)?  RFID  PIN  Biometrie  Sonstiges: <Zutrittstechnik> |
| 2.10 | *Wenn 2.8 ja:* Werden die Zutrittsrechte personifiziert vergeben?  ja  nein |
| 2.11 | *Wenn 2.8 ja:* Werden die Zutritte im Zutrittssystem protokolliert?  ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche  ja, aber nur erfolgreiche Zutritte  ja, aber nur erfolglose Zutrittsversuche  nein, das Schloss wird nur freigegeben oder nicht |
| 2.12 | *Wenn 2.11 ja:* Wie lange werden diese Protokolldaten aufbewahrt?  <Aufbewahrungsdauer> Tage |
| 2.13 | *Wenn 2.11 ja:* Werden die Protokolle regelmäßig ausgewertet?  ja  nein, eine Auswertung wäre aber im Bedarfsfall möglich |
| 2.14 | Existiert ein mechanisches Schloss für die Gebäude bzw. die Büroräume?  ja  nein |
| 2.15 | *Wenn 2.14 ja:* Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus?  ja  nein Ausgabestelle: <Stelle> |
| 2.16 | Gibt es offizielle Zutrittsregelungen für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen?  nein  ja, betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen. |
| 3. | ZUGANGS- UND ZUGRIFFSKONTROLLMASSNAHMEN |
| 3.1 | Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen?  definierter Freigabeprozess  kein definierter Freigabeprozess, auf Zuruf  Sonstige Vergabeweise: <Verfahren> |
| 3.2 | Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert?  ja  nein |
| 3.3 | Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst?  ja  nein |
| 3.4 | Existieren verbindliche Passwortparameter im Unternehmen?  ja  nein |
| 3.5 | Passwort-Zeichenlänge: <Anzahl Zeichen>  Muss das Passwort Sonderzeichen enthalten?  ja  nein  Mindest-Gültigkeitsdauer in Tagen: <Dauer> |
| 3.6 | Zwingt das IT System den Nutzer zur Einhaltung der oben genannten Passwort-Vorgaben?  ja  nein |
| 3.7 | Wird der Bildschirm bei Inaktivität des Benutzers gesperrt?  Wenn ja, nach wieviel Minuten? <Dauer> Minuten |
| 3.8 | Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts?  Administrator vergibt neues Initialpasswort  keine |
| 3.9 | Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen?  ja, <Anzahl Versuche> Versuche  nein |
| 3.10 | *Wenn 3.9 ja:* Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde?  Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt  Die Zugänge bleiben für <Dauer der Sperre> Minuten gesperrt. |
| 3.11 | Wie erfolgt die Authentisierung bei Fernzugängen?  Authentisierung mit  Token  VPN-Zertifikat  Passwort |
| 3.12 | Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen?  ja, <Anzahl Anmeldeversuche> Versuche  nein |
| 3.13 | *Wenn 3.12 ja:* Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist?  Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt  Die Zugänge bleiben für <Dauer in Minuten> Minuten gesperrt. |
| 3.14 | Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt?  ja, nach <Dauer in Minuten> Minuten  nein |
| 3.15 | Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert?  ja  nein |
| 3.16 | *Wenn 3.15 ja:* Wird die Firewall regelmäßig upgedatet?  ja  nein |
| 3.17 | *Wenn 3.15 ja:* Wer administriert Ihre Firewall?  eigene IT  Externer Dienstleister |
| 3.18 | *Wenn ein externer Dienstleister zum Einsatz kommt:* Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten?  ja  nein, die Aufschaltung ist nur im Vier-Augen-Prinzip mit einem Mitarbeiter der eigenen IT möglich. |

|  |  |
| --- | --- |
| 4. | MASSNAHMEN ZUR SICHERUNG VON PAPIER-UNTERLAGEN, MOBILEN DATENTRÄGERN UND MOBILEN ENDGERÄTEN |
| 4.1 | Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke, Akten, Schriftwechsel) entsorgt?  Altpapier / Restmüll  Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist  Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden  Sonstiges: <Art der Entsorgung> |
| 4.2 | Wie werden nicht mehr benötigte Datenträger (z.B. USB-Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt?  Physische Zerstörung durch eigene IT  Physische Zerstörung durch externen Dienstleister  Löschen der Daten  Löschen der Daten durch <Anzahl> Überschreibungen  Sonstiges: <Art der Entsorgung> |
| 4.3 | Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks)  ja  nein |
| 4.4 | Dürfen die Mitarbeiter private Datenträger (z.B. USB-Sticks) verwenden?  generell ja  ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT  nein, alle benötigten Speichermedien werden vom Unternehmen gestellt |
| 4.5 | Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt?  Verschlüsselung der Festplatte  Verschlüsselung einzelner Verzeichnisse  keine Maßnahmen |
| 4.6 | Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)?  ja  nein |
| 5. | MASSNAHMEN ZUR SICHEREN DATENÜBERTRAGUNG |
| 5.1 | Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt?  gar nicht  nein, Datenübertragung erfolgt per MPLS  nur vereinzelt  per verschlüsselter Datei als Mailanhang  per PGP oder S/MIME  per verschlüsseltem Datenträger  per VPN  per https/TLS  per SFTP  Sonstiges: <Art der Verschlüsselung> |
| 5.2 | Wer verwaltet die Schlüssel bzw. die Zertifikate?  Anwender selbst  eigene IT  Externer Dienstleister |
| 5.3 | Werden die Übertragungsvorgänge protokolliert?  ja  nein |
| 5.4 | *Wenn 5.3 ja:* Wie lange werden diese Protokolldaten aufbewahrt?  <Dauer in Tagen> Tage |
| 5.5 | *Wenn 5.3 ja:* Werden die Protokolle regelmäßig ausgewertet?  ja  nein, eine Auswertung wäre aber im Bedarfsfall möglich |

1. Maßnahmen zur Sicherstellung der Verfügbarkeit

|  |  |
| --- | --- |
| 1. | Serveraum |
| 1.1 | Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür?  ja  nein |
| 1.2 | Ist der Serverraum mit Rauchmeldern ausgestattet?  ja  nein |
| 1.3 | Ist der Serverraum an eine Brandmeldezentrale angeschlossen?  ja  nein |
| 1.4 | Ist der Serverraum mit Löschsystemen ausgestattet (Mehrfachantworten möglich)?  ja, CO2 Löscher  ja, Halon-/Argon-Löschanlage  Sonstiges: <Art des Löschsystems> |
| 1.5 | Woraus bestehen die Außenwände des Serverraumes?  Massivwand (bspw. Beton, Mauer)  Leichtbauweise  Brandschutzwand (bspw. F90) |
| 1.6 | Ist der Serverraum klimatisiert?  ja  nein |
| 1.7 | Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)?  ja  nein |
| 1.8 | Wird die Stromversorgung des Serverraums zusätzlich über ein Dieselaggregat abgesichert?  ja  nein |
| 1.9 | Werden die Funktionalitäten unter 1.2, 1.3, 1.4, 1.6, 1.7 und 1.8 – sofern vorhanden – regelmäßig getestet?  ja  nein |
| 2. | BACKUP- UND NOTFALL-KONZEPT, VIRENSCHUTZ |
| 2.1 | Existiert ein Backupkonzept?  ja  nein |
| 2.2 | Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet?  ja  nein |
| 2.3 | In welchem Rhythmus werden Backups von Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden?  Echtzeitspiegelung  täglich  ein bis dreimal pro Woche  Sonstiges: <Speicherintervall> |
| 2.4 | Auf was für Sicherungsmedien werden die Backups gespeichert?  Zweiter redundanter Server  Sicherungsbänder  Festplatten  Sonstiges: <Art des Backups> |
| 2.5 | Wo werden die Backups aufbewahrt?  Zweiter redundanter Server steht an einem anderen Ort  Safe, feuerfest, datenträger- und dokumentensicher  einfacher Safe  Bankschließfach  abgeschlossener Aktenschrank/Schreibtisch  im Serverraum  Privathaushalt  Sonstiges: <Art der Aufbewahrung> |
| 2.6 | *Zu 2.5:* Im Falle eines Transports der Backups: Wie wird dieser durchgeführt?  Mitnahme durch einen Mitarbeitenden der IT-Abteilung, Geschäftsführung, Sekretariat  Abholung durch Dritte (bspw. Bankmitarbeitende, Wachunternehmen)  Sonstiges: <Art des Backups> |
| 2.7 | Sind die Backups verschlüsselt?  ja  nein |
| 2.8 | Befindet sich der Aufbewahrungsort der Backups in einem, vom primären Server aus betrachtet, getrennten Brandabschnitt bzw. Gebäudeteil?  ja  nein |
| 2.9 | Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement?  ja  nein  Prozess existiert, ist jedoch nicht dokumentiert |
| 2.10 | *Wenn 2.9 ja:* Wer ist für das Software- bzw. Patchmanagement verantwortlich?  Anwender selbst  eigene IT  Externer Dienstleister |
| 2.11 | Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekten, Brand oder Totalverlust)?  ja  nein |
| 2.12 | Sind die IT-Systeme technisch vor Datenverlusten bzw. unbefugten Datenzugriffen geschützt?  ja, mittels stets aktualisiertem  Virenschutz  Anti-Spyware  Spamfilter  nein |
| 2.13 | *Wenn 2.12 ja:* Wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich?  Anwender selbst  eigene IT  Externer Dienstleister |
| 3. | NETZANBINDUNG |
| 3.1 | Verfügt das Unternehmen über eine redundante Internetanbindung?  ja  nein |
| 3.2 | Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden?  ja  nein |
| 3.3 | Wer ist für die Netzanbindung des Unternehmens verantwortlich?  eigene IT  Externer Dienstleister |

1. Pseudonymisierung / Verschlüsselung

|  |  |
| --- | --- |
| 1. | Einsatz von Pseudonymisierung |
| 1.1 | Werden verarbeitete personenbezogene Daten pseudonymisiert?  ja, und zwar folgende: <Datenkategorien>  nein |
|  | *Wenn 1.1 nein:* In diesem Fall müssen die weiteren Fragen zu C1 nicht beantwortet werden, sondern sogleich die Fragen ab C2. |
| 1.2 | Werden Algorithmen zur Pseudonymisierung eingesetzt?  ja  nein |
| 1.3 | *Wenn 1.1 ja:* Welcher Algorithmus wird zur Pseudonymisierung eingesetzt?  <Algorithmus> |
| 1.4 | Erfolgt eine Trennung der Zuordnungsdaten und eine Aufbewahrung in getrennten Systemen?  ja  nein |
| 1.5 | Wie kann die Pseudonymisierung bei Bedarf rückgängig gemacht werden (Mehrfachantworten möglich)?  gemäß einem definierten Verfahren  im Mehr-Augen-Prinzip  Direktzugriff auf nicht pseudonymisierte Rohdaten  Auf Weisung des Vorgesetzten  Sonstiges: <anderes Verfahren> |
| 2. | EINSATZ VON VERSCHLÜSSELUNG |
| 2.1 | Werden verarbeitete personenbezogene Daten über die bereits beschriebenen Maßnahmen hinaus verschlüsselt?  ja, und zwar: <Datenkategorien>  nein |
|  | *Wenn 2.1 nein:* In diesem Fall müssen die weiteren Fragen zu C2 nicht beantwortet werden, sondern sogleich die Fragen ab D1. |
| 2.2 | Welche Arten der Verschlüsselung werden eingesetzt (Mehrfachantworten möglich)? Bei Mehrfachantworten beschreiben Sie bitte im Feld „Sonstige“, welche Art der Verschlüsselung für welche Daten eingesetzt wird.  Ende-zu-Ende-Verschlüsselung  Transportverschlüsselung  Data-at-Rest-Verschlüsselung  Sonstige: <Art der Verschlüsselung> |
| 2.3 | Welche kryptographischen Algorithmen werden zur Verschlüsselung oder für verschlüsselungsartige Maßnahmen (z.B. Hashen von Passwörtern) eingesetzt?  AES  SHA-256  RSA-2048 oder höher  Sonstige: <Algorithmus> |
| 2.4 | Wer hat Zugriff auf die verschlüsselten Daten?  Mitarbeitende aus den Abteilungen: <Stelle>  Insgesamt haben <Anzahl> Mitarbeitende Zugriff auf die verschlüsselten Daten |

1. Sonstige Maßnahmen

|  |  |
| --- | --- |
| 1. | Belastbarkeit |
|  | Es existieren Maßnahmen, die die Fähigkeit gewährleisten, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.  ja, <Maßnahmen beschreiben>  nein |
| 2. | WIEDERHERSTELLBARKEIT |
|  | Existieren Notfall- oder Recovery-Konzepte und Maßnahmen über B.2.11 hinaus, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen?  ja, <Maßnahmen beschreiben>  nein |
| 3. | VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER GETROFFENEN MASSNAHMEN |
| 3.1 | Existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung?  ja, <Maßnahmen beschreiben>  nein |
| 3.2 | *Wenn 3.1 ja:* In welchen Abständen finden die Überprüfungen statt?  Zeitraum: <Zeitraum> |
| 3.3 | *Wenn 3.1 ja:* Werden die Ergebnisse der Prüfungen dokumentiert?  ja  nein |
| 3.4 | Gibt es Zertifizierungen mit Bezug zu den technisch-organisatorischen Maßnahmen und wenn ja, welche?  ja, <Art der Zertifizierung/en>  nein |