**Mustervorlage Vereinbarung zur Auftragsverarbeitung gem. Art 28 DSGVO**



**Haftungsausschluss**

Das Dokument steht zur freien Verfügung und wird nur nach Bedarf an neue rechtliche Vorgaben angepasst. Wir achten selbstverständlich auf eine möglichst aktuelle Version unserer Mustervorlage. Dennoch übernehmen wir keinerlei Gewähr für die Aktualität, Richtigkeit und Vollständigkeit der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.  
Der Autor behält es sich ausdrücklich vor, Teile der Seiten oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

Vielen Dank für Ihr Verständnis.

Sie haben eine Frage zum Dokument? Dann [schreiben](https://vc-datenschutz.de/kontakt) Sie uns!

Ihr Team von Vetter Consulting

**Vereinbarung über Auftragsverarbeitung**

**gem. Art. 28 DS-GVO**

**Der Auftragnehmer:**

**verarbeitet für den Auftraggeber:**

personenbezogene Daten im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DS-GVO:

Hierzu wird folgende Zusatzvereinbarung geschlossen:

1. **Gegenstand der Vereinbarung**
2. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in Anlage 1 näher definiert.
3. Dauer der Auftragsverarbeitung

Die Auftragsverarbeitung beginnt am       und beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag vom      .

Die Auftragsverarbeitung ist befristet bis zum

Der Auftrag wird zur einmaligen Ausführung erteilt.

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von       zum       gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

Die Verpflichtungen zur Einhaltung des Datengeheimnisses und der Vertraulichkeit bestehen auch nach Beendigung dieser Vereinbarung fort.

1. Änderungen des Verarbeitungsgegenstandes, Verarbeitungsumfanges sowie Verfahrens­änderungen sind schriftlich zu vereinbaren.
2. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DS-GVO erfüllt sind.
3. **Pflichten des Auftragnehmers**
4. Der Auftragnehmer führt die Leistungen ausschließlich im Rahmen der getroffenen Vereinbarung und nach Weisung des Auftraggebers durch. Der Auftragnehmer ist verpflichtet, die getroffenen Weisungen unverzüglich zu dokumentieren. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen geltendes Recht verstößt. Alle Weisungsberechtigten sind in Anhang 1 aufgeführt.
5. Der Auftragnehmer verwendet Daten, die ihm im Rahmen der Erfüllung des Auftrages bekannt geworden sind, nur für die vereinbarten Vertragszwecke. Eine Verarbeitung oder Nutzung ohne Kenntnis des Auftraggebers oder zu eigenen Zwecken des Auftragnehmers ist nicht erlaubt. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
6. Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend Art. 32 DS-GVO zu. Die konkreten Vorgaben sind durch Anlage 2 geregelt. Der Auftragnehmer hat die Umsetzung der Maßnahmen zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Bestandteil des Vertrags.
7. Sofern ein betrieblicher Datenschutzbeauftragter (freiwillig oder verpflichtend) bestellt wurde, wird der Auftragnehmer diesen in Anlage 3 entsprechend benennen. Bei der Bestellung werden die gesetzlichen Anforderungen der Art. 37 bis 39 DS-GVO sowie der nationalen Regelungen entsprechend berücksichtigt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Hat der Auftragnehmer keinen Sitz innerhalb der EU, benennt er in Anlage 3 einen Vertreter in der Union gemäß Art. 27 DS-GVO.
8. Der Auftragnehmer verpflichtet sich, soweit rechtlich und tatsächlich möglich, den Verantwortlichen auch mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen zu unterstützen, die Betroffene zur Ausübung ihrer Rechte nach Art. 12-22 DS-GVO stellen. Dies betrifft insbesondere das Auskunftsrecht der Betroffenen (Art. 15 DS-GVO), das Recht auf Berichtigung unrichtiger personenbezogener Daten, das Recht der Betroffenen auf Löschung ihrer personenbezogenen Daten (Art. 17 DS-GVO) sowie das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO). Der Auftragnehmer darf Daten nur auf dokumentierte Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Er wird ferner keinerlei Auskunft über personenbezogene Daten an Dritte, aber auch nicht an den Betroffenen selbst erteilen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
9. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit schriftlich verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und darüber belehrt werden, dass die Verpflichtung auch nach Beendigung des Arbeitsverhältnisses weiter besteht. Die Verpflichtung umfasst auch die Betriebs- und Geschäftsgeheimnisse des Auftraggebers. Zur Wahrung des Fernmeldegeheimnisses entsprechend § 88 TKG hat der Auftragnehmer alle Personen (Arbeitnehmer), die auftragsgemäß auf Daten des Auftraggebers mittels Mittel der Telekommunikation wie Telefon oder E-Mail zugreifen können, auf das Fernmeldegeheimnis zu verpflichten und über die sich hieraus ergebenden Geheimhaltungspflichten zu belehren. Diese Verpflichtung gilt auch nach Beendigung des Arbeitsverhältnisses fort.
10. Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers sowie in Fällen eines Verstoßes gegen die in diesem Auftrag getroffenen Festlegungen. Er trifft umgehend die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und setzt sich unverzüglich mit dem Auftraggeber in Verbindung. Ebenso informiert er den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde oder anderer öffentlicher Stellen.
11. Darüber hinaus unterstützt der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei seinen Verpflichtungen aus Art. 33 DS-GVO (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) sowie aus Art. 34 DS-GVO (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person). Ebenso unterstützt er den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Durchführung der Datenschutz-Folgenabschätzung, einer ggf. erforderlichen Konsultation der Aufsichtsbehörde (Art. 35, 36 DS-GVO) sowie sonstigen behördlichen Anfragen und Kontrollen.
12. Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten das den Anforderungen des Art. 30 Abs. 2 DS-GVO genügt. Hinsichtlich des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers hat der Auftragnehmer den Auftraggeber auf Anforderung in dem ihm möglichen Umfang zu unterstützen.
13. Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten zur Verfügung zu stellen. Er erteilt auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.
14. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind.
15. **Pflichten des Auftraggebers**
16. Der Auftraggeber ist für die Einhaltung der jeweils einschlägigen Datenschutzgesetze sowie die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber geltend zu machen.
17. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
18. **Rechte des Auftraggebers / Kontrollen**
19. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Datenverarbeitung zu erteilen. Gleiches gilt für die Festlegung bzw. Fortschreibung der Datensicherungsmaßnahmen.
20. Der Auftraggeber oder ein Beauftragter des Auftraggebers kann sich nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen. Der Auftragnehmer hat die entsprechenden Kontrollen zu dulden und wird den Auftraggeber bei deren Durchführung unterstützen. Liegt hingegen ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrages beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers vor, so kann eine Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden.
21. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.
22. **Subunternehmer**
23. Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit schriftlicher Genehmigung des Auftraggebers vergeben werden. Dies und die nachfolgenden Regelungen gelten auch für den Subunternehmer.
24. Der Auftragnehmer hat den Auftraggeber ohne gesonderte Aufforderung über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subunternehmer zu informieren. Gegen solche Änderungen steht dem Auftraggeber ein Widerspruchsrecht zu.
25. Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen. Er hat sich vor Beginn der Datenverarbeitung durch den Subunternehmer und sodann regelmäßig von der Einhaltung der beim Subunternehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und die Ergebnisse zu dokumentieren. Dem Auftraggeber ist auf Verlangen der Prüfdokumentation zur Verfügung zu stellen.
26. Die Auftragsvergabe an Subunternehmer muss mittels eines schriftlichen Vertrages erfolgen. Die vertraglichen Vereinbarungen sind so zu gestalten, dass sie den Anforderungen dieser Vereinbarung entsprechen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.
27. Dem Auftraggeber sind unmittelbare Kontroll- und Überprüfungsrechte entsprechend § 4 dieser Vereinbarung auch gegenüber dem Subunternehmer einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
28. Sofern der Subunternehmer außerhalb eines in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stammt oder die Datenverarbeitung dort stattfindet, ist durch den Auftragnehmer darüber hinaus sicherzustellen, dass die Voraussetzungen der Art. 44 bis 49 DS-GVO erfüllt sind. Dies ist dem Auftraggeber gegenüber schriftlich vor Aufnahme der Tätigkeiten des Subunternehmers nachzuweisen.
29. Die Genehmigung zur Einschaltung der Dienstleister in Anlage 5 gilt als erteilt, sofern die vorstehenden Anforderungen erfüllt sind.
30. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten eines jeden Subunternehmers.
31. **Vertraulichkeit**
32. Die Parteien verpflichten sich, die ihnen während der Durchführung der Auftragsverarbeitung zur Kenntnis gelangten Informationen und Unterlagen, insbesondere Geschäfts- und Betriebsgeheimnisse des Vertragspartners streng vertraulich zu behandeln. Ebenso vertraulich zu behandeln sind der Gegenstand und Inhalt des Auftrages. Die Parteien sind verpflichtet, die zur Verfügung gestellten oder im Rahmen des Auftrages zur Kenntnis genommenen Daten und Informationen des Vertragspartners ausschließlich im Rahmen des Vertragszwecks zu verarbeiten und zu nutzen. Eine Verarbeitung oder Nutzung für eigene Zwecke sowie eine Weitergabe an Dritte ist nur nach schriftlicher Zustimmung des Vertragspartners zulässig.
33. Sofern zur Abwicklung des Auftrages die Einschaltung Dritter erforderlich ist, wird dafür Sorge getragen, dass die getroffenen Datenschutz- und Geheimhaltungsvereinbarungen von diesen Dritten ebenfalls strikt eingehalten werden. Die Einschaltung von Dritten erfordert das ausdrückliche Einverständnis des Vertragspartners.
34. Die vorstehenden Rechte und Pflichten gelten über die Dauer der Vereinbarung fort.
35. **Beendigung der Auftragsverarbeitung**
36. Nach Beendigung des Auftrages oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinem Besitz befindlichen Unterlagen, Datenträger oder sonstigen Ergebnisse auf Wunsch des Auftraggebers physisch zu löschen bzw. diesem restlos mit der Erklärung zurückgeben, dass sich keine weiteren Kopien beim Auftragnehmer oder bei Unterauftragnehmern befinden. Beim Auftragnehmer gespeicherte Daten sind physisch zu löschen. Die Löschung ist zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten bzw. zu löschen. Die jeweilige Löschung wird dem Auftraggeber unverzüglich und schriftlich bestätigt.
37. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus datenschutzrechtlich aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.
38. Der Auftraggeber ist berechtigt, die Einhaltung der vorstehenden Verpflichtungen, ggf. auch vor Ort, zu kontrollieren.

**§ 8. Haftung**

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechenden Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

**§ 9. Sonstiges, Allgemeines**

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.
2. Diese Vereinbarung zur Auftragsverarbeitung ersetzt eine ggf. zuvor getroffene Vereinbarung zur Auftragsdatenverarbeitung gem. Art 11 BDSG zwischen dem Auftraggeber und dem Auftragnehmer.
3. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
4. Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden oder die Vereinbarung eine Lücke enthalten, so bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Anstelle der unwirksamen oder fehlenden Bestimmung gilt eine wirksame Bestimmung als vereinbart, die dem von den Parteien Gewollten am nächsten kommt.

**§ 10 Gerichtsstand**

Es gilt deutsches Recht. Gerichtsstand ist Sitz des Auftraggebers.

*Ort/ Datum Ort/ Datum*

*Unterschrift (Auftragnehmer) Unterschrift (Auftraggeber)*

**Verarbeitungsinhalt und -Umfang**

(**Anlage 1)**

1. **Art / Gegenstand der Leistung**

*(bitte angeben, z.B. Dienstleistung IT-Support)*

1. **Zwecke der Datenverarbeitung**

*(bitte angeben, z.B. externe Dokumenten- bzw. Kundenverwaltung)*

1. **Personenkategorien**

*(bitte angeben, z.B. Mitarbeiter, Kunden, Bewerber)*

1. **Kategorien personenbezogener Daten**

*(bitte angeben, z.B. Personalstammdaten, Kommunikationsdaten, Name,*

*Adresse, Geburtsdatum)*

1. **Weisungsberechtigte und Weisungsempfangsberechtigte** 
   1. **Weisungsberechtigte Person (-en) des Auftraggebers:**

      *(Benennung namentlich oder per Funktion)*

* 1. **Weisungsempfangsberechtigte Person (-en) des Auftragnehmers:**

*(Benennung namentlich oder per Funktion)*

1. **Betriebliche Datenschutzbeauftragte** 
   1. **Datenschutzbeauftragter des Auftraggebers:**

Name:

Anschrift:

E-Mail:

Telefonnummer:

* 1. **Datenschutzbeauftragter des Auftragnehmers:**

Name:

Anschrift:

E-Mail:

Telefonnummer:

**Technische und organisatorische Maßnahmen (TOM)**

**i.S.d. Art. 32 DSGVO**

**(Anlage 2)**

der Organisation

Stand

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind **die** Maßnahmen, die in ihrem Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. **Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO**
   1. **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 | Schlüsselregelung / Liste |
| Automatisches Zugangskontrollsystem | Empfang / Rezeption / Pförtner |
| Biometrische Zugangssperren | Besucherbuch / Protokoll der Besucher |
| Chipkarten / Transpondersysteme | Mitarbeiter- / Besucherausweise |
| Manuelles Schließsystem | Besucher in Begleitung durch Mitarbeiter |
| Sicherheitsschlösser | Sorgfalt bei Auswahl des Wachpersonals |
| Schließsystem mit Codesperre | Sorgfalt bei Auswahl Reinigungsdienste |
| Absicherung der Gebäudeschächte |  |
| Türen mit Knauf Außenseite |  |
| Klingelanlage mit Kamera |  |
| Videoüberwachung der Eingänge |  |
|  |  |
|  |  |
|  |  |

* 1. **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 CallBack-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 | Verwalten von Benutzerberechtigungen |
| Login mit biometrischen Daten | Erstellen von Benutzerprofilen |
| Anti-Viren-Software Server | Zentrale Passwortvergabe |
| Anti-Virus-Software Clients | Richtlinie „Sicheres Passwort“ |
| Anti-Virus-Software mobile Geräte | Richtlinie „Löschen / Vernichten“ |
| Firewall | Richtlinie „Clean desk“ |
| Intrusion Detection Systeme | Allg. Richtlinie Datenschutz und / oder  Sicherheit |
| Mobile Device Management | Mobile Device Policy |
| Einsatz VPN bei Remote-Zugriffen | Anleitung „Manuelle Desktopsperre“ |
| Verschlüsselung von Datenträgern |  |
| Verschlüsselung Smartphones |  |
| Gehäuseverriegelung |  |
| BIOS Schutz (separates Passwort) |  |
| Sperre externer Schnittstellen (USB) |  |
| Automatische Desktopsperre |  |
| Verschlüsselung von Notebooks / Tablet |  |
|  |  |
|  |  |

* 1. **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** |
| Akten Schredder (mind. Stufe 3, cross cut) | Einsatz Berechtigungskonzepte |
| Externer Aktenvernichter (DIN 32757) | Minimale Anzahl an Administratoren |
| Physische Löschung von Datenträgern | Datenschutztresor |
| Protokollierung von Zugriffen auf  Anwendungen, konkret bei der Eingabe,  Änderung und Löschung von Daten | Verwaltung Benutzerrechte durch  Administratoren |
|  |  |
|  |  |

* 1. **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 Test-  Umgebung | Steuerung über Berechtigungskonzept |
| Physikalische Trennung (Systeme /  Datenbanken / Datenträger) | Festlegung von Datenbankrechten |
| Mandantenfähigkeit relevanter  Anwendungen | Datensätze sind mit Zweckattributen  versehen |
|  |  |
|  |  |

* 1. **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** |
| Im Falle der Pseudonymisierung:  Trennung der Zuordnungsdaten und Auf-  bewahrung in getrenntem und abge-  sicherten System (mögl. verschlüsselt) | Interne Anweisung, personenbezogene  Daten im Falle einer Weitergabe oder auch  nach Ablauf der gesetzlichen Löschfrist  möglichst zu anonymisieren / pseudonymi-  sieren |
|  |  |
|  |  |

1. **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
   1. **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** |
| E-Mail-Verschlüsselung | Dokumentation der Datenempfänger  sowie der Dauer der geplanten Über-  lassung bzw. der Löschfristen |
| Einsatz von VPN | Übersicht regelmäßiger Abruf- und  Übermittlungsvorgängen |
| Protokollierung der Zugriffe und Abrufe | 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 |  |
|  |  |
|  |  |

* 1. **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 | 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 Verar-  beitungen übernommen wurden |
|  | Klare Zuständigkeiten für Löschungen |

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

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

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Feuer- und Rauchmeldeanlagen | Backup & Recovery-Konzept (ausformuliert) |
| Feuerlöscher Serverraum | Kontrolle des Sicherungsvorgangs |
| Serverraumüberwachung Temperatur  und Feuchtigkeit | Regelmäßige Tests zur Datenwiederher-  Herstellung 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-Grundschutz 100-4) |
| Datenschutztresor (S60DIS, S120DIS,  andere geeignete Normen mit Quell-  dichtung etc.) | Getrennte Partitionen für Betriebs-  systeme und Daten |
| RAID System / Festplattenspiegelung |  |
| Videoüberwachung Serverraum |  |
| Alarmmeldung bei unberechtigtem Zutritt  zu Serverraum |  |
|  |  |
|  |  |
|  |  |

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

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Software-Lösungen für Datenschutz-  Management im Einsatz | Interner / externer Datenschutzbeauftragter  Name / Firma / Kontaktdaten |
| Zentrale Dokumentation aller Verfahrens-  weisen 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 Informations-  pflichten nach Art. 13 und 14 DSGVO nach |
|  | Formalisierter Prozess zur Bearbeitung von  Auskunftsanfragen seitens Betroffener ist  vorhanden |
|  |  |
|  |  |

* 1. **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 / Daten-  Pannen (auch im Hinblick auf Meldepflicht  gegenüber Aufsichtsbehörde) |
| Einsatz von Spamfilter und regelmäßige  Aktualisierung | Dokumentierte Vorgehensweise zum  Umgang mit Sicherheitsvorfällen |
| Einsatz von Virenscanner 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 Sicherheitsvor-  fällen und Datenpannen |
|  |  |
|  |  |
|  |  |

* 1. **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 |  |
| Einfache Ausübung des Widerrufrechts  des Betroffenen durch technische Maß-  nahmen |  |
|  |  |
|  |  |

* 1. **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.***

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  | Vorherige Prüfung der vom Auftrag-  nehmer getroffenen Sicherheitsmaß-  nahmen und deren Dokumentation |
|  | Auswahl des Auftragnehmers unter  Sorgfaltsgesichtspunkten (gerade in  Bezug auf Datenschutz und Datensicherheit |
|  | Abschluss der notwendigen Vereinbarung  zur Auftragsverarbeitung bzw. EU Standard-  Vertragsklauseln |
|  | Schriftliche Weisungen an den Auftrag-  nehmer |
|  | Verpflichtung der Mitarbeiter des Auftrag-  nehmers auf Datengeheimnis |
|  | Verpflichtung zur Bestellung eines Daten-  schutzbeauftragten durch den Auftrag-  nehmer bei Vorliegen Bestellpflicht |
|  | Vereinbarung wirksamer Kontrollrechte  gegenüber dem Auftragnehmer |
|  | Regelung zum Einsatz weiterer Sub-  unternehmer |
|  | Sicherstellung der Vernichtung von Daten  nach Beendigung des Auftrags |
|  | Bei längerer Zusammenarbeit: Laufende  Überprüfung des Auftragnehmers und  seines Schutzniveaus |

**Nennung der Subunternehmer:**

alternativ:

Hiermit versichern wir, keine Subunternehmer im Sinne einer

Auftragsverarbeitung einzusetzen.