

Vertrag zur Verarbeitung von Daten im Auftrag

Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

zwischen

siehe Angaben zum Auftraggeber

und

dilohver GmbH, Grünwalder Weg, 82041 Oberhaching

(gemeinsam nachfolgend: „die Parteien“)

Ziel dieses Vertrages

Aus diesem (Rahmen-) Vertrag zur Verarbeitung von Daten im Auftrag (nachfolgend Rahmenvertrag genannt) beabsichtigen die Parteien ihre datenschutzrechtlichen Rechte und Pflichten in Bezug auf die durch den Auftragnehmer im Auftrag des Auftraggebers verarbeiteten Daten zu regeln und somit die gesetzliche Anforderungen, insbesondere des Bundesdatenschutzgesetzes (BDSG) und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie zu erfüllen 95/46/EG (DSGVO) vgl. dort die Anforderungen des Art. 28 Abs. 3 DSGVO zu erfüllen.

Dieser (Rahmen-) Vertrag findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftraggebers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers im Auftrag des Auftragsgebers verarbeiten.

PRÄAMBEL

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1. GEGENSTAND

- 1.1 Gegenstand dieses Auftragsverarbeitungsvertrags ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.
- 1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in der Anlage unter der Ziffer 1.

2. ORT DER DATENVERARBEITUNG

Die vertraglich vereinbarte Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern sich aus der Anlage nichts anderes ergibt. Jede Verlagerung der Verarbeitung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in schriftlicher Form und darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

3. LAUFZEIT

- 3.1 Dieser Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Partei mit einer Frist von drei Monaten gekündigt werden. Soweit im Zeitpunkt der Kündigung noch ein Hauptvertrag oder mehrere Hauptverträge, bei denen der Auftragnehmer im Auftrag personenbezogene Daten des Auftraggebers verarbeitet, in Kraft sind, gelten die Bestimmungen dieses Vertrags bis zu der regulären Beendigung des Hauptvertrags/ der Hauptverträge fort.
- 3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

4. WEISUNG

- 4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.
- 4.2 Falls Weisungen, die unter Ziffer 1 der Anlage dieses Vertrags getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Vereinbarung in schriftlicher Form erfolgt.
- 4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrags und anschließend noch für drei Jahre aufzubewahren.
- 4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

- 4.5 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

- 5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.
- 5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgeabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.
- 5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

- 6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Auftraggeber Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.
- 6.2 Der Auftraggeber oder von ihm beauftragte Dritte sind – grundsätzlich nach Terminvereinbarung – berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen. Der Auftragnehmer ermöglicht dies und trägt dazu bei.
- 6.3 Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltung der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

Der Datenschutzbeauftragte wird dem Auftraggeber auf Nachfrage mitgeteilt, soweit für den Auftragnehmer ein Datenschutzbeauftragter bestellt sein muss oder freiwillig bestellt ist.

8. VERTRAULICHKEIT

- 8.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.
- 8.2 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

8.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen.

9. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (Anlagen, Seite 7)

9.1 Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Er gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und ein angemessenes Schutzniveau erreicht wird. Insbesondere hat der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen sicherzustellen.

9.2 Die vollständig ausgefüllte Vorlage für technische und organisatorische Maßnahmen in der Anlage 2 festgelegt.

9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage unter der Ziffer 5 vereinbarten Maßnahmen entsprechen.

10. INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS UND VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personengezogener Daten betreffen.

10.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.

10.3 Sollten die personenbezogenen Daten, die unter dieser Vereinbarung verarbeitet werden 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 relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

10.4 Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht festgestellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

10.5 Diese Ziffer 10 gilt entsprechend für Vorkommnisse bei Prozessen, die von Unterauftragnehmern ausgeführt werden.

11. UNTERAUFTRAGNEHMER

11.1 Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer erfolgt nur nach Zustimmung des Auftraggebers in schriftlicher oder elektronischer Form. Die Zustimmung des Auftraggebers ist vor Beginn der Beauftragung eines Unterauftragnehmers einzuholen.

11.2 Der Auftragnehmer hat vertraglich sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Subunternehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.

11.3 Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

- 11.4 Der Auftraggeber erteilt hiermit seine Zustimmung zur Beauftragung der in der Anlage unter der Ziffer 4 aufgeführten Unterauftragnehmer.
- 11.5 Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unterauftragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftraggeber nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

12. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

- 12.1 Der Auftragnehmer ist nach Abschluss, der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung erhalten hat, nach Wahl des Auftraggebers an den Auftraggeber zurückzugeben oder zu löschen. Dies schließt insbesondere die Ergebnisse der Datenverarbeitung, überlassene Dokumente und überlassene Datenträger und Kopien der personenbezogenen Daten mit ein. Die Pflicht zur Löschung oder Rückgabe besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort.
- 12.2 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind.
- 12.3 Die Vorgänge sind mit Angabe von Datum und durchführender Person zu protokollieren. Die Protokolle sowie ein Nachweis der Durchführung in schriftlicher Form sind dem Auftraggeber innerhalb von 48 Stunden nach Durchführung der Vorgänge zur Verfügung zu stellen.

13. HAFTUNG

Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

14. SCHLUSSBESTIMMUNGEN

- 14.1 Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten ausgeschlossen.
- 14.2 Für Änderungen oder Nebenabreden ist die Schriftform oder ein elektronisches Format erforderlich. Dies gilt auch für Änderungen dieses Formerfordernisses.
- 14.3 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht.

Unterschrift Auftraggeber



Unterschrift Auftragnehmer

Anlagen

Anlagen

- Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen – Eine ausführliche Auflistung der weiteren Datenarten siehe Anlage 3
- Anlage 2: Technische und organisatorische Maßnahmen
- Anlage 3: Weitere Auftragsverarbeiter

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung	Erbringung der beauftragten Dienstleistung gemäß Auftragsformular des Auftragnehmers, i.d.R. Durchführung der Lohn- und Gehaltsabrechnung sowie Tätigkeiten im direkten oder indirekten Zusammenhang mit dem Lohnsteuerabzug und der Lohnbuchführung. Erfüllung von vertraglichen Verpflichtungen und gesetzlichen Anforderungen.
Art und Umfang der Datenverarbeitung–	Automatisierte Verarbeitung: Alle Daten werden elektronisch erfasst, gespeichert und verarbeitet. Dies umfasst den Einsatz von Software für Lohn- und Gehaltsabrechnungen, die Datenbankverwaltung und den sicheren Austausch mit Dritten für die elektronische Übermittlung von Meldungen an Behörden, wie z.B. die Sozialversicherungsbehörden und das Finanzamt.
Art der Daten	<p>Mitarbeiterstammdaten: Name Anschrift Geburtsdatum Sozialversicherungsnummer Steueridentifikationsnummer Bankverbindung</p> <p>Beschäftigungsdaten: Anstellungsdatum Stellenbezeichnung Arbeitszeitmodell (Vollzeit, Teilzeit, Minijob, kurzfristig) Beschäftigter, Praktikant Tarifvertragliche Zugehörigkeit</p> <p>Lohn- und Gehaltsdaten: Bruttogehalt Zuschläge (z.B. Überstunden, Nachtarbeit) Abzüge (Steuern, Sozialversicherungsbeiträge) Nettogehalt</p> <p>Urlaubs- und Fehlzeiten: Urlaubsansprüche Krankheitszeiten Sonstige Fehlzeiten (z.B. Elternzeit)</p> <p>Sonstige relevante Informationen: Betriebliche Altersvorsorge Bonus- und Prämienzahlungen Fortbildungsmaßnahmen</p>
Kategorien betroffener Personen	Alle Angestellten des Auftraggebers, sowie ehemalige Mitarbeiter, die für Abrechnungen oder Nachfragen benötigt werden.

Anlage 2: Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen (TOM) sind zentral für die Datenschutzpraxis. Sie beschreiben Maßnahmen, die in erster Linie zum Schutz der verarbeiteten Daten ergriffen werden. Unterschieden werden technische Maßnahmen, die physisch umsetzbar sind, von organisatorischen Maßnahmen, die Verfahren, Abläufe und Handlungsanweisungen betreffen. Für diese TOM definiert das Standard-Datenschutz-Modell der deutschen Aufsichtsbehörden sieben Gewährleistungsziele. Die Checkliste zeigt übersichtlich eine Auswahl von Maßnahmen nach dem Standard-Datenschutz-Modell (SDM) auf:

- Maßnahmen zur Datenminimierung, wie z. B. die Implementierung von Sperr- und Löschroutinen
- Maßnahmen zur Transparenz, wie z. B. die Protokollierung von Zugriffen und Änderungen
- Maßnahmen zur Intervenierbarkeit, wie z. B. die Einrichtung einer Deaktivierungsmöglichkeit für einzelne Funktionalitäten

<p>1.0 Vertraulichkeit</p> <p>1.1 Zutrittskontrolle</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Alarmanlage</td> <td>Besucher in Begleitung</td> </tr> <tr> <td>Sicherheitsschlösser</td> <td>Sorgfalt bei Auswahl Reinigungsdienst</td> </tr> <tr> <td></td> <td>Clean-Desk-Policy</td> </tr> <tr> <td></td> <td>Kein Papier im Büro (Hinweis: digitaler Dienstleister)</td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	Alarmanlage	Besucher in Begleitung	Sicherheitsschlösser	Sorgfalt bei Auswahl Reinigungsdienst		Clean-Desk-Policy		Kein Papier im Büro (Hinweis: digitaler Dienstleister)	<p>1.2 Zugangskontrolle</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Login mit Benutzername + Passwort</td> <td>Verwalten von Benutzerberechtigungen</td> </tr> <tr> <td>2-Faktor-Identifizierung</td> <td>Erstellen von Benutzerprofilen</td> </tr> <tr> <td>2 Fach Login mit unterschiedlichem Passwort zum Zugang auf unseren Server</td> <td>Zentrale Passwortvergabe</td> </tr> <tr> <td>Anti-Viren-Software Laptops</td> <td>Richtlinie „Sicheres Passwort“</td> </tr> <tr> <td>Anti-Viren-Software Geschäftshandys</td> <td>Richtlinie „Sicheres Passwort“</td> </tr> <tr> <td>Firewall</td> <td>Richtlinie „Löschen / Vernichten“</td> </tr> <tr> <td>Mobile Device Management</td> <td>Richtlinie „Clean- Desk“</td> </tr> <tr> <td>Einsatz VPN bei Remote-Zugriffen</td> <td>Allg. Richtlinie Datenschutz und / oder Sicherheit</td> </tr> <tr> <td>Verschlüsselung von Datenträgern</td> <td>Mobile Device Policy</td> </tr> <tr> <td>Verschlüsselung Smartphones</td> <td>Anleitung „Manuelle Desktopsperr“</td> </tr> <tr> <td>Gehäuseverriegelung</td> <td></td> </tr> <tr> <td>BIOS Schutz (separates Passwort)</td> <td></td> </tr> <tr> <td>Sperre externer Schnittstellen (USB)</td> <td></td> </tr> <tr> <td>Automatische Desktopsperr</td> <td></td> </tr> <tr> <td>Verschlüsselung von Notebooks / Tablet</td> <td></td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen	2-Faktor-Identifizierung	Erstellen von Benutzerprofilen	2 Fach Login mit unterschiedlichem Passwort zum Zugang auf unseren Server	Zentrale Passwortvergabe	Anti-Viren-Software Laptops	Richtlinie „Sicheres Passwort“	Anti-Viren-Software Geschäftshandys	Richtlinie „Sicheres Passwort“	Firewall	Richtlinie „Löschen / Vernichten“	Mobile Device Management	Richtlinie „Clean- Desk“	Einsatz VPN bei Remote-Zugriffen	Allg. Richtlinie Datenschutz und / oder Sicherheit	Verschlüsselung von Datenträgern	Mobile Device Policy	Verschlüsselung Smartphones	Anleitung „Manuelle Desktopsperr“	Gehäuseverriegelung		BIOS Schutz (separates Passwort)		Sperre externer Schnittstellen (USB)		Automatische Desktopsperr		Verschlüsselung von Notebooks / Tablet	
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Alarmanlage	Besucher in Begleitung																																										
Sicherheitsschlösser	Sorgfalt bei Auswahl Reinigungsdienst																																										
	Clean-Desk-Policy																																										
	Kein Papier im Büro (Hinweis: digitaler Dienstleister)																																										
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen																																										
2-Faktor-Identifizierung	Erstellen von Benutzerprofilen																																										
2 Fach Login mit unterschiedlichem Passwort zum Zugang auf unseren Server	Zentrale Passwortvergabe																																										
Anti-Viren-Software Laptops	Richtlinie „Sicheres Passwort“																																										
Anti-Viren-Software Geschäftshandys	Richtlinie „Sicheres Passwort“																																										
Firewall	Richtlinie „Löschen / Vernichten“																																										
Mobile Device Management	Richtlinie „Clean- Desk“																																										
Einsatz VPN bei Remote-Zugriffen	Allg. Richtlinie Datenschutz und / oder Sicherheit																																										
Verschlüsselung von Datenträgern	Mobile Device Policy																																										
Verschlüsselung Smartphones	Anleitung „Manuelle Desktopsperr“																																										
Gehäuseverriegelung																																											
BIOS Schutz (separates Passwort)																																											
Sperre externer Schnittstellen (USB)																																											
Automatische Desktopsperr																																											
Verschlüsselung von Notebooks / Tablet																																											
<p>1.3 Zugriffskontrolle</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Aktenschredder (mind. Stufe 3, cross cut)</td> <td>Einsatz Berechtigungskonzepte</td> </tr> <tr> <td>Externer Aktenvernichter (DIN 32757)</td> <td>Minimale Anzahl an Administratoren</td> </tr> <tr> <td>Physische Löschung von Datenträgern</td> <td>Datenschutztesor</td> </tr> <tr> <td></td> <td>Verwaltung Benutzerrechte durch Administratoren</td> </tr> </tbody> </table> <p>1.4 Trennungskontrolle</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Trennung von Produktiv- und Testumgebung</td> <td>Festlegung von Datenbankrechten</td> </tr> <tr> <td>Physische Trennung (Systeme / Datenbanken / Datenträger)</td> <td>Datensätze sind mit Zweckattributen versehen</td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte	Externer Aktenvernichter (DIN 32757)	Minimale Anzahl an Administratoren	Physische Löschung von Datenträgern	Datenschutztesor		Verwaltung Benutzerrechte durch Administratoren	Technische Maßnahmen	Organisatorische Maßnahmen	Trennung von Produktiv- und Testumgebung	Festlegung von Datenbankrechten	Physische Trennung (Systeme / Datenbanken / Datenträger)	Datensätze sind mit Zweckattributen versehen	<p>1.5 Pseudonymisierung</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System</td> <td>Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.</td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.																						
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte																																										
Externer Aktenvernichter (DIN 32757)	Minimale Anzahl an Administratoren																																										
Physische Löschung von Datenträgern	Datenschutztesor																																										
	Verwaltung Benutzerrechte durch Administratoren																																										
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Trennung von Produktiv- und Testumgebung	Festlegung von Datenbankrechten																																										
Physische Trennung (Systeme / Datenbanken / Datenträger)	Datensätze sind mit Zweckattributen versehen																																										
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.																																										
<p>2.0 Integrität</p> <p>2.1 Weitergabekontrolle</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>E-Mail-Verschlüsselung</td> <td>Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen</td> </tr> <tr> <td>Einsatz von VPN</td> <td>Weitergabe in anonymisierter oder pseudonymisierter Form</td> </tr> <tr> <td>Sichere Transportbehälter</td> <td>Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen</td> </tr> <tr> <td>Bereitstellung über verschlüsselte Verbindungen wie z.B.: sftp, https</td> <td></td> </tr> </tbody> </table> <p>2.2 Eingangskontrolle</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Technische Protokollierung der Eingabe, Änderung und Löschung von Daten</td> <td>Übersicht welche Daten eingegeben, geändert oder gelöscht werden können</td> </tr> <tr> <td>Manuelle oder automatisierte Kontrolle der Protokolle</td> <td>Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)</td> </tr> <tr> <td></td> <td>Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts</td> </tr> <tr> <td></td> <td>Klare Zuständigkeiten für Löschungen</td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	E-Mail-Verschlüsselung	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen	Einsatz von VPN	Weitergabe in anonymisierter oder pseudonymisierter Form	Sichere Transportbehälter	Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen	Bereitstellung über verschlüsselte Verbindungen wie z.B.: sftp, https		Technische Maßnahmen	Organisatorische Maßnahmen	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht 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		Klare Zuständigkeiten für Löschungen	<p>3.0 Verfügbarkeit und Belastbarkeit</p> <p>3.1 Verfügbarkeitskontrolle</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Feuer- und Rauchmeldeanlagen</td> <td>Mit Sorgfalt ausgewählter externer Server sowie regelmäßige Tests zur Datenwiederherstellung</td> </tr> <tr> <td></td> <td>Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums</td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	Feuer- und Rauchmeldeanlagen	Mit Sorgfalt ausgewählter externer Server sowie regelmäßige Tests zur Datenwiederherstellung		Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums																
Technische Maßnahmen	Organisatorische Maßnahmen																																										
E-Mail-Verschlüsselung	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen																																										
Einsatz von VPN	Weitergabe in anonymisierter oder pseudonymisierter Form																																										
Sichere Transportbehälter	Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen																																										
Bereitstellung über verschlüsselte Verbindungen wie z.B.: sftp, https																																											
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht 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																																										
	Klare Zuständigkeiten für Löschungen																																										
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Feuer- und Rauchmeldeanlagen	Mit Sorgfalt ausgewählter externer Server sowie regelmäßige Tests zur Datenwiederherstellung																																										
	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums																																										
<p>4.0 Verfügbarkeit und Belastbarkeit</p> <p>4.1 Datenschutz-Maßnahmen</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Software-Lösungen für Datenschutz-Management im Einsatz</td> <td>Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet</td> </tr> <tr> <td>Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)</td> <td>Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich</td> </tr> </tbody> </table> <p>4.2 Incident-Response-Management</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Einsatz von Firewall und regelmäßige Aktualisierung</td> <td>Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)</td> </tr> <tr> <td>Einsatz von Spamfilter und regelmäßige Aktualisierung</td> <td>Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen</td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	Software-Lösungen für Datenschutz-Management im Einsatz	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich	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	<p>4.3 Datenschutzfreundliche Voreinstellungen</p> <table border="1"> <thead> <tr> <th>Technische Maßnahmen</th> <th>Organisatorische Maßnahmen</th> </tr> </thead> <tbody> <tr> <td>Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind.</td> <td></td> </tr> <tr> <td>Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen</td> <td></td> </tr> </tbody> </table>	Technische Maßnahmen	Organisatorische Maßnahmen	Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind.		Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen																									
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Software-Lösungen für Datenschutz-Management im Einsatz	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet																																										
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich																																										
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																																										
Technische Maßnahmen	Organisatorische Maßnahmen																																										
Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind.																																											
Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen																																											

Anlage 3: Weitere Auftragsverarbeiter

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
<p>Agenda Informationssysteme GmbH & Co. KG Oberastraße 14 83026 Rosenheim</p>	<p>Erfassung von Personaldaten: Die Software verarbeitet personenbezogene Daten von Mitarbeitern, wie Namen, Adressen, Geburtsdaten, Sozialversicherungsnummern, Steueridentifikationsnummern und Bankverbindungen.</p> <p>Erfassung von Arbeitszeitdaten: Die Software kann Arbeitszeitdaten, Überstunden, Urlaubs- und Krankheitszeiten sowie Abwesenheiten verarbeiten.</p> <p>Berechnung von Löhnen und Gehältern: Die Software führt Berechnungen durch, um Brutto- und Nettolöhne zu ermitteln, einschließlich der Abzüge für Steuern, Sozialversicherungsbeträge und andere Abgaben.</p> <p>Erstellung von Abrechnungen: Die Software generiert Lohn- und Gehaltsabrechnungen für die Mitarbeiter, die die berechneten Beträge und Abzüge ausweisen.</p> <p>Übermittlung von Daten: Die Software kann Daten an Finanzämter, Sozialversicherungsträger und andere</p>	<p>Berechnung von Löhnen und Gehältern: Die Software ermöglicht die automatisierte Berechnung von Brutto- und Nettolöhnen unter Berücksichtigung von Steuern, Sozialversicherungsbeiträgen und weiteren Abzügen.</p> <p>Erstellung von Abrechnungen: Die Software generiert Lohn- und Gehaltsabrechnungen für die Mitarbeiter, die die einzelnen Positionen und Abzüge klar auflisten.</p> <p>Dokumentation und Archivierung: Die Software sorgt für die ordnungsgemäße Dokumentation und Archivierung der Lohnabrechnungen und relevanten Daten, um gesetzlichen Anforderungen zu genügen.</p> <p>Meldungen an Behörden: Die Software kann die Erstellung von Meldungen an Finanzbehörden, Sozialversicherungsträger und andere relevante Institutionen unterstützen.</p> <p>Datenmanagement: Verwaltung von Mitarbeiterdaten, einschließlich persönlicher Informationen, Beschäftigungsdaten und Bankverbindungen, die für die Lohnabrechnung erforderlich sind.</p>	<p>Personenstammdaten: 1) Vorname und Nachname 2) Geburtsdatum 3) Adresse 4) Telefonnummer 5) E-Mail-Adresse</p> <p>Beschäftigungsdaten: 1) Personalnummer 2) Beschäftigungsbeginn und ende 3) Position/Titel</p> <p>Vergütungsdaten: 1) Brutto- und Nettogehalt 2) Zuschläge, z.B. Überstunden, Weihnachtsgeld 3) Abzüge, z.B. Steuern, Sozialversicherungsbeiträge</p> <p>Bankdaten: 1) Kontoinformationen für die Gehaltsüberweisung</p> <p>Urlaubs- und Fehlzeiten: 1) Urlaubsansprüche 2) Krankheitstage 3) sonstige Abwesenheiten</p> <p>Steuerdaten: 1) Steueridentifikationsnummer 2) Steuerklasse</p> <p>Sozialversicherungsdaten: 1) Sozialversicherungsnummer 2) Informationen zur Kranken- und Rentenversicherung</p>	<p>Identifikationsdaten: Name, Vorname, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Adresse.</p> <p>Beschäftigungsdaten: Personalnummer, Beschäftigungsart, Eintrittsdatum, Austrittsdatum, Abteilung, Position.</p> <p>Vergütungsdaten: Bruttogehalt, Nettogehalt, Zuschläge, Abzüge, Sozialversicherungsbeiträge.</p> <p>Zeiterfassungsdaten: Arbeitszeiten, Überstunden, Fehlzeiten, Urlaubsansprüche.</p> <p>Bankverbindungsdaten: Kontoinhaber, IBAN, BIC für die Gehaltsüberweisung.</p> <p>Steuerdaten: Steueridentifikationsnummer, Steuerklasse, Kirchensteuerpflicht.</p> <p>Sozialversicherungsdaten: Sozialversicherungsnummer, Angaben zur Krankenversicherung, Rentenversicherung.</p>

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
<p>IP-Projects GmbH & Co. KG Am Vogelherd 14 97295 Waldbrunn</p>	<p>Hosting der Webseite Die Daten, die auf dem Webspaces gespeichert sind (z. B. Webseiteninhalte, Benutzerinteraktionen), werden durch den Webhoster verarbeitet. Das Hosting umfasst in der Regel das Speichern von HTML-Dateien, Bildern, Datenbanken und anderen Webinhalten.</p> <p>Datenübertragungstool: Es handelt sich hierbei um ein Tool, bei dem die Daten SSL-verschlüsselt sicheren Übertragung von Daten. Es wird eine Verschlüsselung verwendet, um sicherzustellen, dass Daten während der Übertragung nicht abgefangen oder manipuliert werden.</p> <p>E-Mail-Server: Die E-Mails werden über einen E-Mail-Server verarbeitet, der sowohl die Sendung als auch den Empfang der Nachrichten ermöglicht. Dieser Server speichert die E-Mails und verwaltet sie, bis sie abgerufen oder gelöscht werden.</p>	<p>Bereitstellung und Betrieb des Webspaces Die Verarbeitung der Daten erfolgt zur Bereitstellung, Verwaltung und dem Betrieb des Webspaces, auf dem die Webseite des Auftraggebers gehostet wird. Dies umfasst das Speichern von Webseiteninhalten, Benutzerdaten, Interaktionen und Datenbanken sowie die Gewährleistung einer sicheren und funktionsfähigen Bereitstellung der Webseite.</p> <p>Datenübertragung und -austausch Die Verarbeitung erfolgt zur sicheren Übertragung von Daten über die zur Verfügung gestellten Datenübertragungstools. Dies schließt das Senden und Empfangen von Dateien sowie den Schutz und die Integrität der übermittelten Daten während des Übertragungsprozesses ein.</p> <p>Bereitstellung und Verwaltung von E-Mail-Diensten: Die Verarbeitung von E-Mail-Daten erfolgt zur Bereitstellung und Verwaltung der E-Mail-Kommunikationsinfrastruktur des Auftraggebers. Dies umfasst das Senden, Empfangen und Speichern von E-Mails sowie die Gewährleistung der Funktionsfähigkeit und Sicherheit des E-Mail-Systems.</p> <p>Erfüllung vertraglicher Pflichten: Die Verarbeitung personenbezogener und nicht personenbezogener Daten erfolgt zur Erfüllung der vertraglichen Pflichten.</p> <p>Einhaltung gesetzlicher Anforderungen: Die Verarbeitung erfolgt auch, um gesetzlichen Verpflichtungen nachzukommen, wie beispielsweise der Aufbewahrung von Daten zur Erfüllung steuerrechtlicher oder anderer gesetzlicher Vorschriften.</p>	<p>Kundendaten: Namen, E-Mail-Adressen, Telefonnummern und andere Kontaktdaten von Personen, die für den Auftraggeber tätig sind oder in der Kommunikation involviert sind.</p> <p>Benutzerdaten der Webseite: Daten, die von den Besuchern der Webseite des Auftraggebers übermittelt werden, wie z. B. IP-Adressen, Browser-Informationen, Nutzungsdaten und Interaktionen auf der Webseite (z. B. durch Cookies).</p> <p>E-Mail-Daten: Absender- und Empfängerinformationen, E-Mail-Inhalte, Betreffzeilen und Zeitstempel, die im Rahmen der E-Mail-Kommunikation verarbeitet werden.</p> <p>Vertragsdaten: Daten, die im Zusammenhang mit der Erfüllung des Vertrages stehen, wie z. B. Vertragsnummern, Rechnungsdaten, Zahlungsinformationen und Vereinbarungen über die bereitgestellten IT-Dienstleistungen. Technische Daten: Server- und Hosting-Daten, die im Zusammenhang mit der Webseite und den IT-Diensten verarbeitet werden, wie z. B. IP-Adressen, Protokoll Daten, Systemkonfigurationen, Backups und Fehlerprotokolle. Daten zu Webseiten-Interaktionen</p> <p>Cookies und Tracking-Daten: Daten, die über Cookies und ähnliche Technologien gesammelt werden, um das Nutzerverhalten auf der Webseite zu analysieren und die Benutzererfahrung zu verbessern. Sicherheits- und Protokoll Daten</p> <p>Kommunikationsdaten: E-Mails, Nachrichten und andere Kommunikationsformen. Diese Daten beinhalten sowohl den Inhalt als auch Metadaten (z. B. Zeitpunkt und Teilnehmer der Kommunikation).</p>	<p>Kunden des Auftraggebers (z. B. Mandanten oder Geschäftspartner)</p> <p>Mitarbeiter des Auftraggebers und des Auftragnehmers</p> <p>Webseitenbesucher die Interaktionen auf der Webseite des Auftraggebers durchführen, wie Interessenten, der Auftraggeber oder Mitarbeiter des Auftraggeber)</p> <p>E-Mail-Kommunikationspartner (Absender und Empfänger von E-Mails)</p> <p>Benutzer von Datenübertragungstools (z. B. Personen, die Daten über gesicherte Kanäle übertragen)</p>