Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

1. Allgemeines

1.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

1.2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

2.1. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

3.1. Der Auftraggeber ist Verantwortlicher i. S. v. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 2 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

3.2. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

3.3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z. B. E-Mail) erfolgen.

3.4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

3.5. Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese bei Abschluss eines Hauptvertrages für die Nutzung von Dienstleitungen oder Produkte des Auftragnehmers durch den Auftraggeber benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

3.6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

3.7. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen, 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 Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

4.2. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. 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.

4.3. Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese bei Abschluss eines Hauptvertrages für die Nutzung von Dienstleitungen oder Produkte des Auftragnehmers durch den Auftragnehmer benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

4.4. Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen gemäß Ziff. 9 dieses Vertrages.

4.5. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

4.6. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

4.7. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

4.8. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist grundsätzlich zulässig.

5. Datenschutzbeauftragter des Auftragnehmers

5.1. Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber auf Verlangen, den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

5.2. Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Kontrollbefugnisse

6.1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

6.2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes 1 erforderlich ist.

6.3. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

6.4. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i. S. d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

6.5. Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ zur Wahrung der Persönlichkeitsrechte von Beschäftigten des Auftragnehmers und etwaiger weiterer Personen im jeweiligen Haushalt primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 6 Abs. 3 und 4 zu treffenden Maßnahmen erfolgt.

7. Unterauftragsverhältnisse

7.1. Der Auftragnehmer ist berechtigt, die in der Anlage 2 zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

7.2. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 3 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

7.3. Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

7.4. Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag auf die Unterauftragnehmer zu übertragen und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit diesen

abzuschließen. Insbesondere gewährleistet der Auftragnehmer, dass die TOM des Unterauftragnehmers dem Schutzniveau der TOM aus Anlage 3 dieser Vereinbarung genügen.

7.5. Nicht als Unterauftragsverhältnisse i. S. d. Absätze 1 bis 4 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i. S. d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

8. Vertraulichkeitsverpflichtung

8.1. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

8.2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

9. Wahrung von Betroffenenrechten

9.1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

9.2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

9.3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

9.4. Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim Auftragnehmer geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Auftraggeber verantwortlich ist, ist der Auftragnehmer berechtigt, dem Betroffenen mitzuteilen, dass der Auftraggeber der Verantwortliche für die Datenverarbeitung ist. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

10. Geheimhaltungspflichten

10.1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz

oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

10.2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

11. Vergütung

11.1. Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

12. Technische und organisatorische Maßnahmen zur Datensicherheit

12.1. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

12.2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 3 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

13. Dauer des Auftrags

13.1. Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen oder Produkte des Auftragnehmers durch den Auftraggeber.

13.2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

14. Beendigung

14.1. Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

14.2. Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

15. Zurückbehaltungsrechte

15.1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

16. Schlussbestimmungen

16.1. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

16.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf diese Vereinbarung. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

16.3. Sollte eine Bestimmung dieser Bedingungen unwirksam sein oder werden, so bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Anstelle der unwirksamen Bestimmung gilt eine wirksame Bestimmung als vereinbart, die der von den Parteien gewollten Regelung wirtschaftlich am nächsten kommt; das gleiche gilt im Falle einer Vertragslücke.

16.4. Sämtliche in diesen Bedingungen genannten Anlagen sind verpflichtender Vertragsbestandteil.

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst grundsätzlich die folgenden Arbeiten und/oder Leistungen. Weitere Details zum Gegenstand und Zweck der Verarbeitung personenbezogener Daten sind dem jeweiligen Hauptvertrag zu entnehmen:

- *Wartung und Support der Software beim Auftraggeber, ggf. per Fernwartung*
- *Ggf. Installation und weitere Dienstleistungen in der Anwendungserstellung beim Auftraggeber*

2. Art(en) der personenbezogenen Daten

Folgende Datenarten können Gegenstand der Verarbeitung sein:

- *Vor- und Zunamen*
- *Kommunikationsdaten (z.B. Telefonnummer, E-Mail Adressen, Anschriften)*
- *Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Kundenhistorie)*
- *Personenstammdaten (z.B. Personalakten)*
- *Vertragsabrechnungs- und Zahlungsdaten*
- *Planungs- und Steuerungsdaten*
- *Leistungsdaten (z.B. aufgrund von Auswertungen)*
- *Gesundheitsdaten*

3. Kategorien betroffener Person

- *Interessenten und/oder Kunden des Auftraggebers*
- *Beschäftigte des Auftraggebers, auch ehemalige Beschäftigte*
- *Lieferanten/Dienstleister des Auftraggebers*
- *Patienten*

4. Datenschutzbeauftragter

Beim Auftragnehmer ist als Datenschutzbeauftragter bestellt:

Sven Bartsch, Secure Data GmbH
+49 7641 9563407, Datenschutzbeauftragter@intrexx.com

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Anlage 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Unterauftragnehmer	Art der Leistung
Continum AG Bismarckallee 7b-d | D-79098 Freiburg	Serverhosting
Amazon Web Services EMEA Sarl 38, avenue John F. Kennedy | L-1855 Luxembourg	Serverhosting
badenIT GmbH Tullastr. 61 | D-79108 Freiburg	Serverhosting

Anlage 3 – Technisch-organisatorische Maßnahmen

Datenschutz- und Datensicherheitskonzept

Die folgenden Maßnahmen beschreiben die im Rahmen der Auftragsverarbeitung getroffenen technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 DSGVO insbesondere unter den Gesichtspunkten der Schutzwerte: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- Vertraulichkeit:
  Informationen und in diesem Zusammenhang stehende Infrastruktur dürfen nur den berechtigten Personen zur Verfügung stehen.
- Integrität:
  Informationen dürfen nur von befugten Personen verändert werden und nur in der Weise, die für diese Person vorgesehen sind. Die Integrität bezieht sich auf die Unversehrtheit von Informationen mit dem Ziel, dies vor unerlaubten Veränderungen zu schützen.
- Verfügbarkeit / Belastbarkeit / Wiederherstellbarkeit:
  Informationen müssen den berechtigten Personen im benötigten Zeitraum und mit der erforderlichen Güte zugänglich gemacht werden sowie nutzbar sein.
- Belastbarkeit:
  Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst widerstandsfähig ausgestaltet sind.

Vertraulichkeit

Unter Vertraulichkeit im Sinne von Art. 32 Abs. 1 lit. b DSGVO fallen technische und organisatorische Maßnahmen, die sicherstellen, dass personenbezogene Daten ausschließlich einem bestimmten Empfängerkreis zugänglich sind. Dazu gehören Zutritts-, Zugangs, Zugriffs und Trennungskontrolle sowie weitere Maßnahmen wie Anonymisierung, Pseudonymisierung.

1. Zutrittskontrolle

Die INTREXX GmbH hat an ihrem Unternehmenssitz technische und organisatorische Maßnahmen zur Sicherung der Zutrittskontrolle getroffen. Zutrittsberechtigt zu den Datenverarbeitungsanlagen sind nur solche Personen, deren Anwesenheit zur Durchführung oder Sicherstellung des Betriebes oder zur Wahrnehmung von Kontrollaufgaben erforderlich ist.
Am Standort Freiburg finden aktive Kontrollen der Zutrittsberechtigung für alle Mitarbeiter statt, zudem sind eine Vielzahl von Maßnahmen realisiert worden.

1.1 Gelände und Objektsicherheit

- Das Gebäude ist videoüberwacht, eine Alarmanlage ist installiert;
- Der Haupteingang ist verschlossen und verfügt über einen – in Kernzeiten - besetzen Empfang;
- Weitere Objektzugänge, als auch Stockwerkszugangstüren sind mit einem Schließsystem gesichert;
- Die Ausgabe von Schlüsseln und Token erfolgt dokumentiert durch eine zentrale Stelle;
- Sicherheitszonen mit restriktiven Zutrittsberechtigungen sind definiert;
- Kontrollgänge nach Ende der offiziellen Arbeitszeit / Bürozeit;
- Maßnahmen zur Prophylaxe vor und Detektierung von unbefugten Zutritten und Zutrittsversuchen durch regelmäßige Überprüfung der Einbruchssicherheit der Türen, Tore und Fenster vor allem auf Einbruchspuren.

1.2 Regelung der Zutrittsberechtigungen

- Dokumentierte Zutrittsregelungen, in Abhängigkeit der definierten Sicherheitszonen, für bestimmte Personengruppen (Mitarbeiter, Führungskräfte, Firmenfremde, Besucher, Wartungs-, Reinigungspersonal, Lieferanten, Boten usw.);
- Besucher müssen sich am Empfang anmelden, es erfolgt eine Protokollierung über ein Empfangsbuch; sie werden abgeholt und begleitet; zum Betreten restriktiver Sicherheitszonen kann zudem eine Legitimation notwendig sein;
- Regelungen zum Unternehmenseintritt und Ausscheiden von Mitarbeitern sowie zu internen Stellen- bzw. Berechtigungswechsel;
- Regelungen und Folgemaßnahmen bei Verlust von Ausweisen, Schlüsseln usw.;
- Revisionsfähigkeit von Vergabe und Entzug der Zutrittsberechtigungen.

1.3 Rechenzentrum

- Das Rechenzentrum liegt in einem eigenen abgesicherten Bereich, in einem externen ISO/IEC27001 zertifizierten Rechenzentrum (Cage Colocation);
- Server befinden sich dort in separat verschlossenen Schränken;
- Sicherheitszonen und restriktive Zutrittsberechtigungen; der Personenkreis von (System-) Administratoren ist auf das erforderliche Mindestmaß beschränkt und dokumentiert;
- Techniker und Besucher müssen sich legitimieren und sind durch einen Mitarbeiter zu begleiten;
- Aufsicht von Wartungs- und Reparaturpersonal.

2. Zugangskontrolle

Bei der Zugangskontrolle werden alle technischen und organisatorischen Maßnahmen dokumentiert, die geeignet sind, die Nutzung der Datenverarbeitungssysteme, klassischerweise der Computer, durch Unbefugte zu verhindern.

2.1 Allgemeine Regelungen der Zugangsberechtigungen

- Zugang zu den IT-Systemen der INTREXX GmbH ist grundsätzlich nur nach einer Authentifizierung mithilfe von Benutzernamen und Kennwort möglich;
- Dokumentierte Vergabe von Benutzeraccounts;
- Administratoren-Konten werden ausschließlich für eng begrenzte Tätigkeiten genutzt;
- Protokollierte, nachweisbare Benutzung der Zugänge zu Datenverarbeitungssystemen;
- Kennwörter unterliegen einer Passwort-Richtlinie, in der Anforderungen hinterlegt sind wie z. B. Länge, Komplexität, Aufbewahrungszeit, Wiederverwendung zuvor verwendeter Kennwörter usw.
- Passwörter von Administratoren unterliegen höheren Anforderungen;
- Trennung oder Sperrung der Verbindung bei wiederholten Fehlversuchen oder Zeitüberschreitungen wo möglich;
- Regelungen für Fälle von Verlust oder Kompromittierung der Passwörter etabliert;
- Kritische Systeme werden mit einer 2-Faktor Authentifizierung ausgestattet;
- Verpflichtung und Sensibilisierung der Mitarbeiter, damit diese beim Verlassen des Arbeitsplatzes den Computer sperren, so dass zur Entsperrung eine Kennworteingabe erforderlich ist. Ergänzend ist eine automatische Bildschirmsperrung konfiguriert;
- Getrennte Infrastruktur für Besucher, Mitarbeiter und Dienstleister;
- Regelungen zum Deaktivieren nicht genutzter Accounts;
- Netzwerkzugänge sind gesperrt; generell werden keine fremden Systeme im internen Netzwerk der INTREXX GmbH zugelassen;
- Sicherung der Netzwerk-Infrastruktur durch Netzwerk-Port-Security nach IEEE 802.1X, Intrusion Detection Systeme, Nutzung von 2-Faktor-Authentisierung wo möglich, Trennung von Netzen, Content-Filter, verschlüsselte Netzwerkprotokolle;
- Regelmäßige Überprüfung der Protokolle auf sicherheitsrelevante Aktionen oder Vorgänge.

2.2 Zusätzliche Maßnahmen bei Fernzugängen

- Dokumentierte Regelungen für die Benutzung von Fernzugängen, insbesondere bei Benutzung durch Dritte, z. B. für Fernadministration und Fernwartung;
- Dokumentation von Personen, die zur Anmeldung von außerhalb berechtigt sind;
- Netzzugangssicherung durch Hard- und Softwaremaßnahmen;
- Unberechtigter Zugriff aus dem Internet wird durch den Einsatz von Firewalls verhindert;
- Starke Authentifikation durch z. B. Token und PIN;
- Protokollierung von Remotezugängen am (SSL) VPN-Gateway.

3. Zugriffskontrolle

Es ist zu 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.

3.1 Berechtigungskonzept

- Dokumentierte und nachvollziehbare Prozesse zur Erlangung, Veränderung, Verwaltung und Rücknahme von Zugriffsberechtigungen;
- Verwaltung der Zugriffsberechtigungen und Benutzergruppen erfolgt in einem zentralen Verzeichnisdienst soweit möglich;
- Die Vergabe individueller Zugriffsrechte erfolgt auf Personen- oder Gruppenebene;
- Berechtigungen bedürfen eines vorgelagerten Genehmigungsprozess.

3.2 Zugriffsschutz

- Einsatz von Verschlüsselungsroutinen, sowie die Möglichkeit zur Dateiverschlüsselung;
- Regelungen zur Verschlüsselung mobiler Endgeräte;
- Maßnahmen zur Sicherung des Netzzugriffs eingerichtet;
- Verwendung nur freigegebener Hard- und Software;
- Netzkomponenten sind gesichert;

- Standard-User und -Passwörter an Netzwerkkomponenten müssen geändert werden;
- Netzwerk segmentiert;
- Trennung von Test und Produktivumgebung;
- Beschränkung der freien Abfragemöglichkeiten (SQL-Query) von Datenbanken;
- Zeitliche Begrenzung der Zugriffsmöglichkeiten von extern;
- Maßnahmen zum Schutz von Endgeräten, Servern und anderen Infrastruktur-Elementen vor unbefugtem Zugriff: mehrstufiges Virenschutz-Konzept, Content-Filter, Application Firewall, Intrusion Detection System, Desktop-Firewall, System-Hardening, Content-Verschlüsselung.

3.3 Aufbewahrung und Verwendung von Datenträgern

- Datenträger-Verschlüsselung mit - nach aktuellem Stand der Technik - als sicher einzustufenden Algorithmen zum Schutz von mobilen Geräten (Notebooks, Tablet-PCs, Smartphones usw.) und Datenträgern (Externe Festplatten, USB-Sticks, Speicherkarten, usw.) erfolgt mittels Einsatzes einer entsprechenden Verschlüsselungssoftware;
- Regelungen zur in- und externen Aufbewahrung von Datenträgern inklusive Festlegung der zur Datenträgerentnahme befugten Personen (Schlüsselverwaltung, Quittierung, Rückgabe);
- nicht-reversible Löschung von Datenträgern bzw. datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger durch zertifizierte Entsorger.

3.4 Protokollierung von Zugriffen

- Protokollierung von Netzwerkzugriffen;
- Protokollierung von Lesezugriffen auf Datensicherungen;
- Protokollierung der autorisierten Weitergabe von Datenträgern (Externe Festplatten, USB-Sticks, Speicherkarten, usw.).

4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass die zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten getrennt verarbeitet werden:

- Die INTREXX GmbH gewährleistet durch den Einsatz von Zugriffsberechtigungen, dass nur berechtigte Nutzer auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können;
- Die Trennung der unterschiedlichen Datensätze erfolgt durch Speicherung in logisch getrennten Datenbanken bzw. Verzeichnissen;
- Trennung von Test-, Entwicklungs- und Produktivsystemen; Produktivdaten werden nicht für Tests verwendet;
- Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet;
- Gegebenenfalls vorhandene Kopien bzw. Auszüge aus Kundendatenbanken befinden sich auf eigenen Servern in jeweils pro Kunde getrennten Datenbanken, so dass ein Berechtigungsvergabe auf Personen- oder Gruppenebene pro Datenbank erfolgen kann.

5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne weitere Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

- Pseudonymisierungen werden durch die INTREXX GmbH auf Wunsch und Weisung des Auftraggebers im Einzelfall realisiert;
- Wo möglich: Ersetzen von personenbezogenen Daten (insbes. Name) durch Pseudonym, Speichern der Verknüpfungsinformationen zwischen ID und Namen in einer separaten Zuordnungsdatei und Aufbewahrung auf einem getrennten, abgesicherten IT-System;
- Regelmäßige Prüfung, welche Daten anonymisiert bzw. gelöscht werden können.

6. Verschlüsselung

- Für die Übermittlung von Datenbankkopien des Auftraggebers an die INTREXX GmbH steht ein verschlüsselter Kommunikationsweg zur Verfügung (SFTP);
- Mobile Endgeräte werden vollschlüsselt und sind mit einer Pre-Boot-Authentifizierung ausgestattet;
- Externe Datenträger, die das Firmengelände verlassen sind in der Regel verschlüsselt;
- Die Übertragung von E-Mails vom/zum Provider erfolgt transport-verschlüsselt;
- Beim Versuch unsere Webseiten unverschlüsselt aufzurufen, erfolgt eine automatische Umleitung auf verschlüsselten Zugriff („HTTPS“).

7. Weitere Maßnahmen

- Vertretungsregelungen definiert und berechtigungskonform ausgestaltet;
- Regelmäßiges Review der Zutritts-, Zugangs- und Zugriffsberechtigungen;
- Installation von kritischen/ oder wichtigen Sicherheits-Updates/Patches zur Gewährleistung der Vertraulichkeit.

Integrität

Integrität im Sinne von Art. 32 Abs. 1 lit. b DSGVO dokumentiert, wie man zu verhindern versucht, dass Daten und die darin enthaltenen Information verfälscht werden können. Die zwei wesentlichen Punkte hierzu sind die Weitergabekontrolle und die Eingabekontrolle.

1. Weitergabekontrolle

Bei der Weitergabekontrolle listet das Unternehmen alle Maßnahmen auf, die gewährleisten sollen, dass personenbezogene Daten während des Transports von unbefugten Dritten nicht gelesen, kopiert, verändert oder gelöscht werden können. Zur Sicherstellung sind folgende Maßnahmen implementiert:

1.1 Regelung der elektronischen Übertragung

- Dokumentierte Festlegung der Stellen (Dritte), an die Daten übermittelt werden dürfen sowie der Personen, die zur Übermittlung befugt sind (Berechtigungskonzept);
- Möglichkeiten zum verschlüsselten Versand bzw. zur Übertragung von Daten stehen bereit (VPN, https, etc.);
- Authentisierung bei E-Mails (digitale Signatur);
- Datenübermittlungen sowie Empfänger der Daten werden protokolliert.

1.2 Regelungen des Transports von Datenträgern

- Transport von Datenträgern ausschließlich durch betriebszugehörige Boten, gesicherte Transportverhältnisse oder sorgfältig ausgesuchte Dienstleister;
- Datenträger sind vorab stets zu verschlüsseln.

2. Eingabe-, Speicher- und Datenträgerkontrolle

Die Eingabekontrolle soll festhalten, von wem die Daten in ein Datenverarbeitungssystem aufgenommen, verändert oder entfernt worden sind. Die Protokollierung soll gewährleisten, dass man überprüfen kann, dass Daten nicht von Unberechtigten verfälscht worden sind.

- Jeder Beschäftigte hat einen personenbezogenen Zugang zu den IT-Systemen, basierend auf seinen Benutzernamen und Kennwort, gekoppelt an den für seine Zwecke erforderlichen Berechtigungen auf diese Daten („Erfassen/Bearbeiten“, „Nur Lesen“, „Keine Berechtigung“);
- Log-Daten bei der Änderung von personenbezogenen Daten;
- Nachvollziehbarkeit der Änderung, Löschung und Eingabe;
- Keine Nutzung von Gruppen-Accounts (auch Administratoren oder root) bzw. eines Accounts durch mehrere Mitarbeiter.

Verfügbarkeit / Belastbarkeit / Wiederherstellbarkeit

Folgende Maßnahmen wurden getroffen, um im Sinne von Art. 32 Abs. 1 lit. b DSGVO sicherzustellen, dass personenbezogene Daten nicht einfach „abhandenkommen" oder zufällig zerstört werden.

1. Rechenzentrum

1.1. Stromversorgung

- Gesonderter Stromkreis für Rechenzentrum;
- Die kritischsten Systeme im sind durch eine unterbrechungsfreie Stromversorgung („USV") sowie Überspannungsschutz geschützt.

1.2. Brandschutz

- Brand- und Rauchmeldeanlagen in Serverräumen, Rechenzentren und wichtigen Infrastrukturräumen;
- Brandschutzordnung für das gesamte Gebäude;
- CO2-Handlöscher für das Rechenzentrum;
- Richtlinien zur Brandlastreduzierung.

1.3. Klimatisierung

- Der Serverraum verfügt über mehrere Klimamodule zur optimalen Temperatursteuerung;
- Leckage Warnung mit Weiterleitung per E-Mail und SMS durch das Monitoring;
- Benachrichtigung der verantwortlichen Mitarbeiter durch das Monitoring per E-Mail und SMS;
- Temperaturüberwachung an mehreren Messpunkten mit Einbindung in das Operating- und Störungsmanagement.

1.4. Internet

- Redundante Internetanbindung gekoppelt mit entsprechenden Verfügbarkeits-SLAs.

1.5. Hard- und Software Komponenten

- Redundant ausgelegt Server-Komponenten;
- Redundante virtuelle Umgebung;
- Die Server- bzw. Speichersysteme sind mindestens mit einem RAID-1 ausgestattet, so dass die darauf gespeicherten Daten auf mindestens zwei Festplatten vorhanden sind;
- Zeitnaher Austausch defekter Server-Komponenten im Rahmen entsprechender Service Verträge (24x7x4);
- Strategisch wichtige Server-Komponenten werden z. T. zusätzlich vor Ort gelagert / bei IT-Dienstleister auf Abruf gelagert.

1.6. Kumulierte Maßnahmen

- USV, Brand- und Rauchmeldeanlage, Handlöscher sowie Klimatechnik unterliegen Wartungs- und Serviceverträgen. Zudem werden regelmäßig, dokumentierte Funktionstests durchgeführt, um die ordnungsgemäße Verfügbarkeit sicherzustellen;
- Monitoring der Hard-, Software- und Infrastrukturkomponenten.

2. Sicherung und Wiederherstellung von Informationen

- Dokumentiertes Datensicherungskonzept inkl. organisatorischer Regelungen zur Datenträgeraufbewahrung (Kennzeichnung, Aufbewahrungsfristen);
- Automatisierte, kontrollierte, protokollierte und regelmäßig vollständige Sicherung der Dateien, Datenbanken und Systemen, laut Datensicherungskonzept;
- Schreibschutz für Datensicherungsträger;
- Datensicherungen inkl. der Sicherungssysteme sind geschützt vor unberechtigten Zutritt, Zugang und Zugriff;
- Datensicherungsträger werden gesondert von den Sicherungssystemen an einen sicheren, besonders geschützten (externen) Orten, gelagert;
- Recoverykonzept zur schnellen Wiederherstellung von Dateien, Datenbanken und Systemen;
- Regelmäßige Test zur Wiederherstellung von Dateien, Datenbanken und Systemen;
- Desaster-Recoverykonzept mit Regelungen wie Zuständigkeiten, Wiederanlaufkonzepte, Rufbereitschaften, Notfallorganisation, etc. für den Katastrophenfall;
- Notfallübungen werden durchgeführt und dokumentiert.

3. Organisatorische Maßnahmen

- Ticketsystem zur Erfassung von Störungen an IT-Systemen des Auftraggebers;
- Vorgaben für Verfahrens- und Programmdokumentation;
- Eingesetzte Hard- und Software wird regelmäßig überprüft und ggf. an den Stand der Technik angepasst;
- Vorhandensein ausreichender Personalressourcen;
- Anwender werden regelmäßig geschult.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Datenschutz-Managementsystem

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist. Alle Elemente, die für die Sicherstellung des Datenschutzes erforderlich sind, unterliegen der systematischen Koordination des Datenschutz- Managementsystem.

- Die INTREXX GmbH hat eine Datenschutzorganisation installiert;
- Ein externer Datenschutzbeauftragter (DSB) ist schriftlich bestellt und Teil des Datenschutz-Teams. Fachkundenachweis und regelmäßige Weiterbildungsnachweise liegen vor. Aufgrund seiner gesetzlichen Verschwiegenheitsverpflichtung gegenüber Kunden, Beschäftigten, etc. muss er immer unmittelbar, auch für Aufsichtsbehörden, erreichbar sein. Sie erreichen unseren DSB unter der folgenden E-Mail-Adresse, die nur er abrufen und einsehen kann: Datenschutzbeauftragter@intrexx.com;
- Eine Datenschutz-Leitlinie wurde durch den Verantwortlichen erlassen und wird unterstützt durch diverse Richtlinien aus den Bereichen Datenschutz und Informationssicherheit;
- Die Beschäftigten der INTREXX GmbH werden regelmäßig in den Bereichen Datenschutz und Informationssicherheit durch den DSB geschult und sensibilisiert;
  - Beschäftigte werden mit Eintritt ins Unternehmen auf die Wahrung der Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet;
- Ein Verzeichnis von Verarbeitungstätigkeiten ist vorhanden und wird fortlaufend aktualisiert und durch den DSB auditiert;
- Die technischen und organisatorische Maßnahmen (TOM) sind ausgearbeitet und dienen u. a. als Basis für dieses Dokument;
- Es erfolgt eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitungen;
- Subunternehmen werden sorgfältig ausgewählt und regelmäßig überprüft;
- Betroffenen werden hinreichend Informationen bezüglich der Verarbeitung ihrer personenbezogenen Daten bereitgestellt. Das Informieren erfolgt bei Aufnahme der personenbezogenen Daten oder so zeitnah wie möglich;
- Im Rahmen der Betroffenen-Informationen wird auf die Intervenierbarkeit im Rahmen der Betroffenenrechte hingewiesen.

2. Incident-Response-Management

Um im Bedarfsfall zu gewährleisten, dass auf einen Datenschutzvorfall mit entsprechenden Maßnahmen reagiert wird, wurden folgende Schritte installiert:

- Festlegung von Meldeprozessen für:
  - Datenschutzverletzungen lt. Art. 4 Nr. 12 DSGVO ggü. den Aufsichtsbehörden (Art. 33 DSGVO);
  - Datenschutzverletzungen lt. Art. 4 Nr. 12 DSGVO ggü. den Betroffenen (Art. 34 DSGVO).
- Sensibilisierung der Mitarbeiter bezüglich Datenschutzverletzungen;
- Dokumentation von Datenschutzvorfällen;
- Kontinuierliche Weiterentwicklung der Meldeprozesse auf Basis der gewonnenen Erfahrungswerte.

3. Datenschutzfreundliche Voreinstellungen

Durch Voreinstellungen ist sicherzustellen, dass personenbezogene Daten nur nach dem jeweiligen bestimmten Verarbeitungszweck verarbeitet werden. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit.

- Neue Hard- und Softwareprodukte werden hinsichtlich datenschutzfreundlicher Voreinstellungen geprüft.

4. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers.

- Interner Prozess und Sensibilisierung der Mitarbeiter stellt sicher, dass notwendige Verträge zur Auftragsdatenverarbeitung abgeschlossen werden;
- Vereinbarungen zur Auftragsverarbeitung werden schriftlich oder digital zwischen Auftraggeber und Auftragnehmer abgeschlossen. Bestandteil der Vereinbarungen ist, dass Weisungen vom Auftraggeber schriftlich an den Auftragnehmer erteilt werden;
- Erstkontrolle im Sinne von Art. 28 Abs. 1 DSGVO;
- Bei Veränderungen bestehender bzw. Einführung neuer Verfahren zur Verarbeitung personenbezogenen Daten, wird der Datenschutzbeauftragte involviert;
- Benachrichtigung im Falle einer unrechtmäßigen Kenntniserlangung personenbezogener Daten;
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten;
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer;
- Verpflichtung zur Vertraulichkeit im Umgang mit personenbezogenen Daten der Mitarbeiter des Auftragnehmers (Artt. 5, 28, 29, 32 DSGVO);
- Sicherstellung der Vertrautheit der mit der Datenverarbeitung betrauten Personen mit den relevanten datenschutzrechtlichen und auftraggeberspezifischen Regelungen;
- Gewährleistung der unverzüglichen Berichtigung, Sperrung und Löschung von Auftragsdaten auf Weisung des Auftraggebers bzw. nach Beendigung des Auftrags;