# Vereinbarung zur Auftragsverarbeitung

**Nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO).**

Version 3.0

zur Kundennummer [10153204]
zwischen

Stefan, Oehl / Oehl Interaktive Medien
Berrenrather Strasse 188c
50937 Köln

als Auftraggeber
– nachfolgend Auftraggeber –

und

STRATO AG
Pascalstraße 10
10587 Berlin

als Auftragnehmer
- nachfolgend Auftragnehmer –

**1. Gegenstand und Dauer der Verarbeitung**
1.1. Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.
1.2. Die Dauer der Verarbeitung entspricht der im Auftrag vereinbarten Laufzeit.

**2. Art und Zweck der Verarbeitung**
2.1. Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.
2.2. Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung im Bereich Cloud-Dienstleistungen, Hosting, Software as a Service (SaaS) und IT-Support erforderlichen Zwecke.

**3. Art der personenbezogenen Daten und Kategorien von Betroffenen**
3.1. Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.
3.2. Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

**4. Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen**
4.1. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

4.2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.
4.3. Die vertraglich vereinbarte Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, soweit nicht etwas anderes vereinbart ist, z.B. über die Produktbeschreibung der beauftragten Leistung .
4.4. Ist Vertragsbestandteil die Registrierung von Domains bei Registrierungsstellen, die ihren Sitz in einem Drittland haben (außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums), ist auch vereinbart, dass der Auftragnehmer personenbezogene Daten - unter Beachtung der zwingend anwendbaren Vorschriften – an diese Registrierungsstellen übermittelt.
4.5. Die Parteien vereinbaren außerdem, dass der Auftragnehmer berechtigt ist, personenbezogene Daten - unter Beachtung der zwingend anwendbaren Vorschriften zur Leistungserbringung in einem Drittland zu übermitteln. Dies ist insbesondere der Fall, wenn Auftragsgegenstand der Dienst eines Drittanbieters ist, der diesen Dienst ganz oder teilweise in einem Drittland erbringt.

**5. Rechte des Auftraggebers, Pflichten des Auftragnehmers**
5.1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor (Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaates). Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
5.2. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung nach Möglichkeit den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche der betroffenen Personen nach Kapitel III der DSGVO. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.
5.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.
5.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Gleiches gilt für das Fernmeldegeheimnis nach § 88 TKG und – in Kenntnis der Strafbarkeit – für die Wahrung von Geheimnissen der Berufsgeheimnisträger nach § 203 StGB. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5.5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.
5.6. Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine

Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Eine Kontaktmöglichkeit wird auf der Webseite des Auftragnehmers veröffentlicht.
5.7. Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen.
5.8. Machen betroffene Person Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützt der Auftragnehmer den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

**6. Pflichten des Auftraggebers**
6.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
6.2. Im Falle der Beendigung verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in den Diensten gespeichert hat.
6.3. Auf Anforderung des Auftragnehmers benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

**7. Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO**
7.1. Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicher zu stellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftragnehmer ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.
7.2. Die aktuellen technischen und organisatorischen Maßnahmen sind im Anhang 2 aufgeführt.
7.3. Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.
7.4. Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen beim Stand der Technik und die Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird.

**8. Nachweis und Überprüfung**
8.1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen - einschließlich Inspektionen -, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt dazu bei. Der Auftragnehmer ist berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber und von dessen beauftragten Prüfer zu verlangen. Der Auftragnehmer stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftraggeber zu, sofern der Auftraggeber dem Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt. Wettbewerber des Auftraggebers oder Personen, die für Wettbewerber des Auftraggebers tätig sind, kann der Auftragnehmer als Prüfer ablehnen.
8.2. Als Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten reicht dem Auftraggeber die vorliegende Zertifizierung nach ISO 27001 aus. Das jeweils aktuelle Zertifikat stellt der Auftragnehmer auf seiner Webseite zur Verfügung.
8.3. Das Inspektionsrecht des Auftraggebers hat das Ziel, die Einhaltung der einem Auftragsverarbeiter obliegenden Pflichten gemäß der DSGVO und dieses Vertrages zu überprüfen. Der Nachweis der Einhaltung

dieser Pflichten wird durch die Zertifizierung nach vorstehendem Absatz erbracht. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel daran geltend macht, dass diese Zertifizierungen zureichend oder zutreffend sind, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung für den Auftraggeber dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen. Diese können zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt werden.
8.4. Für Informationen und Unterstützungshandlungen kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Aufwand für den Auftragnehmer durch eine Inspektion ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
8.5. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige staatliche oder kirchliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gelten die vorstehenden Regeln entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

**9. Subunternehmer (weitere Auftragsverarbeiter)**
9.1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.
9.2. Die aktuell eingesetzten weiteren Auftragsverarbeiter sind im Anhang 1 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.
9.3. Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.
9.4. Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrechtlichen Grund innerhalb einer angemessenen Frist nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist nach Zugang des Einspruchs einstellen.
9.5. Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.
9.6. Als weitere Auftragsverarbeiter im Sinne dieser Regelung sind nur solche Subunternehmer zu verstehen, die Dienstleistungen erbringen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören solche Nebenleistungen, die sich auf Telekommunikationsleistungen, Druck-/Post-/Transportdienstleistungen, Wartung und Pflege, Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der personenbezogenen Daten, Netze, Dienste, Datenverarbeitungsanlagen und sonstiger IT-Systeme, beziehen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit in Bezug auf die Daten des Auftraggebers auch bei solchen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

**10. Haftung und Schadensersatz**
10.1. Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.
10.2. Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.

**11. Vertragslaufzeit, Sonstiges**

11.1. Die Vereinbarung beginnt mit dem Abschluss durch den Kunden. Sie endet mit Ende des letzten Vertrages unter der o.g. Kundennummer. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächlichen Ende der Verarbeitung.
11.2. STRATO kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Es gilt Ziffer 1.4 AGB.
11.3. Ergänzend gelten die AGB des Auftragnehmers, abrufbar unter https://www.strato.de/agb/. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.
11.4. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Berlin. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland.
11.5. 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 und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der DSGVO liegen.

## Anhang 1 zur Vereinbarung zur Auftragsverarbeitung - Genehmigte Subunternehmer / weitere Auftragsverarbeiter

Stand 20180321

| Subunternehmer | Land | Adresse | Kurzbeschreibung der Leistung |
|---|---|---|---|
| Content Management AG | Deutschland | Im Medienpark 6, 50670 Köln | Entwicklung, Wartung und Pflege des Hompagebaukastens |
| ePages GmbH | Deutschland | Pilatuspool 2, 20355 Hamburg | Entwicklung, Wartung und Pflege der Webshops |
| Open-Xchange GmbH | Deutschland | Martinstraße 41, 57462 Olpe | Entwicklung, Wartung und Pflege des Communicators |
| 1&1 Internet SE | Deutschland | Elgendorfer Straße 7, 56410 Montabaur | Entwicklung und Betrieb der STRATO Online Buchhaltung |
| Seven IT GmbH | Deutschland | SevenIT, Hauptstraße 40, 77652 Offenburg | Betrieb und Support der STRATO Online Buchhaltung |

## Anhang 2 zur Vereinbarung zur Auftragsverarbeitung - Technische und Organisatorische Sicherheitsmaßnahmen gemäß Art 32 DSGVO

Version 1.0

**1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

1.1 Zutrittskontrolle

*Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht*

*sind.*
*Festlegung von Sicherheitsbereichen*
• Realisierung eines wirksamen Zutrittsschutzes
• Protokollierung des Zutritts
• Festlegung Zutrittsberechtigter Personen
• Verwaltung von personengebundenen Zutrittsberechtigungen
• Begleitung von Fremdpersonal
• Überwachung der Räume

1.2 Zugangskontrolle
*Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.*
• Festlegung des Schutzbedarfs
• Zugangsschutz
• Umsetzung sicherer Zugangsverfahren, starke Authentisierung
• Umsetzung einfacher Authentisierung per Username Passwort
• Protokollierung des Zugangs
• Monitoring bei kritischen IT-Systemen
• Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
• Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
• Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
• Festlegung befugter Personen
• Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
• Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle
*Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.*
• Erstellen eines Berechtigungskonzepts
• Umsetzung von Zugriffsbeschränkungen
• Vergabe minimaler Berechtigungen
• Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
• Vermeidung der Konzentration von Funktionen

1.4 Verwendungszweckkontrolle
*Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*
• Datensparsamkeit im Umgang mit personenbezogenen Daten
• Getrennte Verarbeitung verschiedener Datensätze
• Regelmäßige Verwendungszweckkontrolle und Löschung
• Trennung von Test- und Entwicklungsumgebung

1.5 datenschutzfreundliche Voreinstellungen
• Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

**2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
2.1 Weitergabekontrolle
*Ziel der Weitergabekontrolle ist es, zu 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.*

• Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
• Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
• Protokollierung von Übermittlungen gemäß Protokollierungskonzept
• Sichere Datenübertragung zwischen Server und Client
• Sicherung der Übertragung im Backend
• Sichere Übertragung zu externen Systemen
• Risikominimierung durch Netzseparierung
• Implementation von Sicherheitsgateways an den Netzübergabepunkten
• Härtung der Backendsysteme
• Beschreibung der Schnittstellen
• Umsetzung einer Maschine-Maschine-Authentisierung
• Sichere Ablage von Daten, inkl. Backups
• Gesicherte Speicherung auf mobilen Datenträgern
• Einführung eines Prozesses zur Datenträgerverwaltungen
• Prozess zur Sammlung und Entsorgung
• Datenschutzgerechter Lösch- und Zerstörungsverfahren
• Führung von Löschprotokollen

2.2 Eingabekontrolle

*Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

• Protokollierung der Eingaben
• Dokumentation der Eingabeberechtigungen

**3. Verfügbarkeit, Belastbarkeit, Desaster Recovery**

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

• Brandschutz
• Redundanz der Primärtechnik
• Redundanz der Stromversorgung
• Redundanz der Kommunikationsverbindungen
• Monitoring
• Resourcenplanung und Bereitstellung
• Abwehr von systembelastendem Missbrauch
• Datensicherungskonzepte und Umsetzung
• Regelmäßige Prüfung der Notfalleinrichtungen

3.2 Desaster Recovery – Rasche Wiederherstellung nach Zwischenfall Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

• Notfallplan
• Datensicherungskonzepte und Umsetzung

**4. Datenschutzorganisation**

• Festlegung von Verantwortlichkeiten
• Umsetzung und Kontrolle geeigneter Prozesse
• Melde- und Freigabeprozess
• Umsetzung von Schulungsmaßnahmen
• Verpflichtung auf Vertraulichkeit
• Regelungen zur internen Aufgabenverteilung
• Beachtung von Funktionstrennung und –zuordnung

• Einführung einer geeigneten Vertreterregelung

**5. Auftragskontrolle**

*Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

• Auswahl weiterer Auftragnehmer nach geeigneten Garantien
• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit STRATO

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

• Informationssicherheitsmanagement nach ISO 27001
• Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen
• Prozess Sicherheitsvorfall-Management
• Durchführung von technischen Überprüfungen

**Sie haben am 16.05.2018 erfolgreich eine Vereinbarung zur Auftragsverarbeitung mit STRATO abgeschlossen.**