Auftragsverarbeitungsvertrag

Der nachfolgende Auftragsverarbeitungsvertrag i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (nachfolgend „**AUFTRAGSVERARBEITUNGSVERTRAG**“) konkretisiert die Verpflichtungen zum Datenschutz der Taxy.io GmbH Jülicher Straße 72a 52070 Aachen (nachfolgend „**AUFTRAGNEHMER**“) als Auftragnehmer, die sich aus der Auftragsverarbeitung gegenüber dem Kunden, der als Steuerberater/Kanzlei das unter www.SmartGrundsteuer.de vorgehaltene Angebot nutzt, (nachfolgend „**AUFTRAGGEBER**“) ergeben. Der Auftragsverarbeitungsvertrag findet Anwendung auf alle Tätigkeiten, die mit dem zwischen den Parteien geschlossenen Hauptvertrag über die unter www.SmartGrundsteuer.de vorgehaltenen Leistungen (nachfolgend „**VERTRAG**“) in Zusammenhang stehen und bei denen Beschäftigte des AUFTRAGNEHMERS oder durch den AUFTRAGNEHMER Beauftragte personenbezogene Daten (nachfolgend „**DATEN**“) des AUFTRAGGEBERS verarbeiten.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem VERTRAG sowie der Aufstellung in **Anlage 1** ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Die Laufzeit dieses AUFTRAGSVERARBEITUNGSVERTRAGES richtet sich nach der Laufzeit des VERTRAGES, sofern sich aus den Bestimmungen dieses AUFTRAGSVERARBEITUNGSVERTRAGES nicht darüber hinausgehende Verpflichtungen ergeben.

2. Anwendungsbereich und Verantwortlichkeit

2.1. Der AUFTRAGNEHMER verarbeitet DATEN im Auftrag des AUFTRAGGEBERS. Dies umfasst Tätigkeiten, die im VERTRAG und in der obigen Beschreibung unter Ziffer 1 konkretisiert sind. Der AUFTRAGGEBER ist im Rahmen des 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).

2.2. Die Weisungen werden anfänglich durch den VERTRAG festgelegt und können vom AUFTRAGGEBER danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom AUFTRAGNEHMER bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (nachfolgend „**EINZELWEISUNG**“). EINZELWEISUNGEN, die im VERTRAG nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche EINZELWEISUNGEN sind unverzüglich schriftlich oder in Textform zu bestätigen.

3. Pflichten des Auftragnehmers

3.1. Der AUFTRAGNEHMER darf DATEN nur im Rahmen des Auftrages und der Weisungen des AUFTRAGGEBERS verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a) DSGVO vor. 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.

3.2. Der AUFTRAGNEHMER wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der DATEN des AUFTRAGGEBERS treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der AUFTRAGNEHMER hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem AUFTRAGGEBER sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden DATEN ein angemessenes Schutzniveau bieten.

Diese technischen und organisatorischen Maßnahmen sind in der beigefügten **Anlage 2** aufgelistet.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem AUFTRAGNEHMER vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.3. Der AUFTRAGNEHMER unterstützt soweit vereinbart den AUFTRAGGEBER im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

3.4. Der AUFTRAGNEHMER gewährleistet, dass es den mit der Verarbeitung der DATEN befassten Mitarbeitern und andere für den AUFTRAGNEHMER tätigen Personen untersagt ist, die DATEN außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der AUFTRAGNEHMER, dass sich die zur Verarbeitung der DATEN befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.5. Der AUFTRAGNEHMER unterrichtet den AUFTRAGGEBER unverzüglich, wenn ihm Verletzungen des Schutzes der DATEN des AUFTRAGGEBERS bekannt werden.

3.6. Der AUFTRAGNEHMER trifft die erforderlichen Maßnahmen zur Sicherung der DATEN und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem AUFTRAGGEBER ab.

3.7. Der AUFTRAGNEHMER nennt dem AUFTRAGGEBER den Ansprechpartner für im Rahmen des VERTRAGES anfallende Datenschutzfragen.

3.8. Der AUFTRAGNEHMER berichtigt oder löscht die DATEN, wenn der AUFTRAGGEBER dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der AUFTRAGNEHMER die datenschutzkonforme Vernichtung von

Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den AUFTRAGGEBER oder gibt diese Datenträger an den AUFTRAGGEBER zurück, sofern nicht im VERTRAG bereits vereinbart. In besonderen, vom AUFTRAGGEBER zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren.

3.9. DATEN, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des AUFTRAGGEBERS entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der DATEN, so trägt diese der AUFTRAGGEBER.

3.10. Im Falle einer Inanspruchnahme des AUFTRAGGEBERS durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der AUFTRAGNEHMER den AUFTRAGGEBER bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4. Pflichten des Auftraggebers

4.1. Der AUFTRAGGEBER hat den AUFTRAGNEHMER unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2. Im Falle einer Inanspruchnahme des AUFTRAGGEBERS durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt Ziffer 3.10 entsprechend.

4.3. Der AUFTRAGGEBER nennt dem AUFTRAGNEHMER den Ansprechpartner für im Rahmen des VERTRAGES anfallende Datenschutzfragen.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den AUFTRAGNEHMER, wird der AUFTRAGNEHMER die betroffene Person an den AUFTRAGGEBER verweisen, sofern eine Zuordnung an den AUFTRAGGEBER nach Angaben der betroffenen Person möglich ist. Der AUFTRAGNEHMER leitet den Antrag der betroffenen Person unverzüglich an den AUFTRAGGEBER weiter. Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der AUFTRAGNEHMER haftet nicht, wenn das Ersuchen der betroffenen Person vom AUFTRAGGEBER nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten

6.1. Der AUFTRAGNEHMER weist dem AUFTRAGGEBER die Einhaltung der in diesem AUFTRAGSVERARBEITUNGSVERTRAG niedergelegten Pflichten mit geeigneten Mitteln nach.

6.2. Sollten im Einzelfall Inspektionen durch den AUFTRAGGEBER oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der AUFTRAGNEHMER darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer

Verschwiegenheitserklärung hinsichtlich der DATEN anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den AUFTRAGGEBER beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem AUFTRAGNEHMER stehen, hat der AUFTRAGNEHMER gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der AUFTRAGNEHMER seine übliche Vergütung verlangen. Der Aufwand einer Inspektion ist für den AUFTRAGNEHMER grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

6.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des AUFTRAGGEBERS eine Inspektion vornehmen, gilt grundsätzlich Ziffer 6.2 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.

7. Sonderregelungen für Daten, die einem Berufsgeheimnis gemäß § 203 StGB unterliegen

7.1. Im Rahmen der Auftragsverarbeitung werden auch DATEN verarbeitet, die unter ein Berufsgeheimnis im Sinne von § 203 StGB fallen. Der AUFTRAGNEHMER verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen DATEN zu verschaffen, wie dies zur Erfüllung der dem AUFTRAGNEHMER zugewiesenen Aufgaben erforderlich ist. Der AUFTRAGGEBER weist den AUFTRAGNEHMER darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen gemäß § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

7.2. Der AUFTRAGNEHMER stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des AUFTRAGGEBERS befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der AUFTRAGNEHMER wird etwaige Subunternehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer vorgesehenen Tätigkeit Kenntnis von Daten erhalten, die einem Berufsgeheimnis unterliegen, zur Geheimhaltung verpflichten und auf die Folgen der Verletzung der Geheimhaltung hinweisen.

7.3. Der AUFTRAGNEHMER wird darauf hingewiesen, dass DATEN, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a Strafprozessordnung (StPO)).

Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der AUFTRAGNEHMER unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den AUFTRAGGEBER informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

7.4. Der AUFTRAGNEHMER wird darauf hingewiesen, dass die in seinem Gewahrsam befindlichen Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des AUFTRAGGEBERS (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der AUFTRAGNEHMER dieser widersprechen und unverzüglich den AUFTRAGGEBER informieren.

8. Subunternehmer

8.1. Der Einsatz von Subunternehmern als weiteren AUFTRAGSVERARBEITER ist nur zulässig, wenn der AUFTRAGGEBER vorher zugestimmt hat.

8.2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der AUFTRAGNEHMER weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im VERTRAG vereinbarten Leistung beauftragt. Der AUFTRAGNEHMER wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt. Der AUFTRAGGEBER stimmt dem Einsatz der nachfolgend aufgeführten Subunternehmer zu:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 USA Serverstandort: EU	Cloudspeicher und Cloudinfrastrukturdienste
Fortinet, Inc. Global Headquarters 899 Kifer Road Sunnyvale, CA 94086 USA Serverstandort: EU	Web Application Firewall
Auth0, Inc, 10800 NE 8th Street, Suite 700, Bellevue, WA 98004, USA Serverstandort: EU	Authentifizierungsdienst
DATEV eG Paumgartnerstr. 6 - 14 90429 Nürnberg	Single Sign On & Bereitstellung von Mandantenstammdaten

Mailjet SAS,13-13 bis, rue de l'Aubrac, 75012 Paris, Frankreich Serverstandort: EU	E-Mail-Versand von Benachrichtigungen über neue Ereignisse
Bayerisches Landesamt für Steuern - Dienststelle München Sophienstraße 6, 80333 München	Übermittlung der Steuerdaten an das Finanzamt
Stripe Payments Europe Limited 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland Serverstandort: EU	Zahlungsdienstleister
HubSpot, Inc., 25 First St., 2nd floor, Cambridge, Massachusetts 02141, USA Serverstandort: EU	Kundenverwaltung, Prozess- und Vertriebsunterstützung
Zendesk, Inc., 989 Market Street #300, San Francisco, CA 94102, USA Serverstandort: EWR	Management von Kontaktanfragen und Kommunikation

8.3. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der AUFTRAGNEHMER die Zustimmung des AUFTRAGGEBERS ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

8.4. Erteilt der AUFTRAGNEHMER Aufträge an Subunternehmer, so obliegt es dem AUFTRAGNEHMER, seine datenschutzrechtlichen Pflichten aus diesem AUFTRAGSVERARBEITUNGSVERTRAG dem Subunternehmer zu übertragen.

9. Informationspflichten, Textform, Rechtswahl

9.1. Sollten die DATEN 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.

9.2. Änderungen und Ergänzungen dieses AUFTRAGSVERARBEITUNGSVERTRAGES und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des AUFTRAGNEHMERS – bedürfen einer Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine

Änderung bzw. Ergänzung dieses AUFTRAGSVERARBEITUNGSVERTRAGES handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.3. Bei etwaigen Widersprüchen gehen Regelungen dieses AUFTRAGSVERARBEITUNGSVERTRAGES zum Datenschutz den Regelungen des VERTRAGES vor. Sollten einzelne Teile dieses AUFTRAGSVERARBEITUNGSVERTRAGES unwirksam sein, so berührt dies die Wirksamkeit des AUFTRAGSVERARBEITUNGSVERTRAGES im Übrigen nicht.

9.4. Es gilt deutsches Recht.

10. Haftung und Schadensersatz

Der AUFTRAGNEHMER haftet gemäß den im VERTRAG festgelegten Haftungsregelungen.

Anlage 1

Art und Zweck der Verarbeitung

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

Mandanten der Kanzlei, Mitarbeiter der Kanzlei

……

Kategorien von Daten

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):

Mandantenstammdaten, Mandantenkommunikation, Grundbesitzdaten, Mitarbeiterkontaktdaten

……

Kategorien von sensiblen Daten (falls zutreffend)

Die übermittelten personenbezogenen Daten umfassen folgende sensiblen Daten:

Keine

……

Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen

Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

Nutzung der Daten zur Klassifizierung der Grundstücksdaten in Grundstücksarten und Ermittlung nach Maßgabe des Bewertungsgesetzes der Einheitswerte

……

Verarbeitungszwecke

Die übermittelten personenbezogenen Daten werden zu folgenden Zwecken des Verantwortlichen verarbeitet:

Die Klassifizierung erfolgt mit dem Zweck der individualisierten Mandantenberatung sowie der Erstellung und Übermittlung der Feststellungserklärung.

……

Anlage 2

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

(vgl. Ziffer 3.2 des Auftragsverarbeitungsvertrages)

Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung eines erfolgreichen Angriffs

- Technische Maßnahmen
    - **Logische Zugriffskontrolle**: Die Vergabe von Zugriffsberechtigungen erfolgt nach dem „Need-to-Know"-Prinzip.
    - **Authentifizierung**: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
    - **Passwortsicherheit**: Soweit Passwörter zur Authentifizierung eingesetzt werden, sollten diese mindestens 8 Zeichen lang sein und aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter werden ausschließlich verschlüsselt gespeichert.
    - **Verschlüsselung auf dem Übertragungsweg**: Personenbezogener Daten werden auf dem Übertragungsweg über das Internet verschlüsselt, zumindest soweit es sich um Daten der Lohnverrechnung oder sensible Daten handelt.
    - **Verschlüsselung mobiler Geräte**: Mobile Endgeräte und mobile Datenträger werden verschlüsselt, zumindest soweit auf diesen Geräten Daten der Lohnverrechnung oder sensible Daten gespeichert werden.
    - **Netzwerksicherheit**: Es wird eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.
    - **Maßnahmen gegen Schadsoftware**: Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt. Alle eingehenden E-Mails werden automatisch auf Schadsoftware gescannt.
    - **Management von Sicherheitslücken**: Soweit möglich, wird auf allen Geräten die automatische Installation von Sicherheitsupdates aktiviert. Ansonsten erfolgt die Installation kritischer Sicherheitsupdates binnen 3 Arbeitstagen, die Installation von Sicherheitsupdates mittlerer Kritikalität binnen 25 Arbeitstagen und die Installation von Sicherheitsupdates geringer Kritikalität binnen 40 Arbeitstagen.
- Organisatorische Maßnahmen
    - **Klare Zuständigkeiten**: Interne Zuständigkeiten für Fragen der Datensicherheit werden definiert.

- **Verschwiegenheitspflicht der Dienstnehmer**: Die Dienstnehmer werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung eines Vorgesetzten an Dritte zu übermitteln.
- **Schulungen und Informationsmaßnahmen**: Die Dienstnehmer werden zu Fragen der Datensicherheit (intern oder extern) geschult und angemessen über Fragen der Datensicherheit informiert (z.B. Passwortsicherheit).
- **Geordnete Beendigung des Dienstverhältnisses**: Bei Beendigung des Dienstverhältnisses erfolgt eine unverzügliche Sperrung aller Konten des ausscheidenden Dienstnehmers sowie eine Abnahme aller Schlüssel des ausscheidenden Dienstnehmers.
- **Verwaltung von Computer-Hardware**: Es werden Aufzeichnungen darüber geführt, welchem Mitarbeiter welche Endgeräte (z.B. PC, Laptop, Mobiltelefon) zugewiesen wurden.
- **Eingabekontrolle**: Es bestehen Verfahren zur Kontrolle der Richtigkeit der eingegebenen personenbezogenen Daten.
- **Keine Doppelverwendung von Benutzer-Accounts**: Jede Person sollte ihren eigenen Benutzer-Account haben – das Teilen von Benutzer-Accounts ist untersagt.
- **Keine unnötige Verwendung administrativer Accounts**: Benutzer-Accounts mit administrativen Rechten werden nur in Ausnahmefällen verwendet – die reguläre Nutzung von IT-Systemen erfolgt ohne administrative Rechte.
- **Auswahl der Dienstleiser**: Bei der Auswahl von Dienstleistern wird das vom Dienstleister gebotene Datensicherheitsniveau berücksichtigt. Der Einsatz eines Dienstleisters, der als Auftragsverarbeiter einzustufen ist, erfolgt nur nach Abschluss einer Auftragsverarbeitervereinbarung.
- **Sichere Datenentsorgung**: Papier, welches personenbezogene Daten enthält, wird grundsätzlich geschreddert bzw. einem externen Dienstleister zur sicheren Vernichtung übergeben. Datenträger werden vor ihrer Entsorgung vollständig überschrieben oder physisch zerstört, sodass die darauf gespeicherten Daten nicht wieder hergestellt werden können.

- Physische Maßnahmen
  - **physische Zugangskontrolle**: Das Betreten der Betriebsräumlichkeiten ist für betriebsfremde Personen nur in Begleitung einer betriebsangehörigen Person zulässig.

- **Einbruchssicherheit**: Die Zugänge zu den Betriebsräumlichkeiten verfügen über einen angemessenen Einbruchsschutz (z.B. eine Sicherheitstüre höherer Widerstandsklasse).
- **Besonderer Schutz von Computer-Hardware**: Der Zugang zu Räumlichkeiten, in denen sich Computer-Server befinden ist durch besondere Maßnahmen gesichert (z.B. zusätzliches Schloss).
- **Schlüsselverwaltung**: Schlüssel, welchen den Zugang zu den Betriebsräumlichkeiten oder Teilen derselben ermöglichen, werden nur an besonders vertrauenswürdige Personen ausgehändigt und dies auch nur soweit und solange diese Personen tatsächlich einen eigenen Schlüssel benötigen.

Detektive Sicherheitsmaßnahmen – Maßnahmen zur Erkennung eines Angriffs

- Technische Maßnahmen
  - **Scans nach Schadsoftware**: Es werden regelmäßig Scans nach Schadsoftware (Anti-Viren-Scans) durchgeführt, um Schadsoftware zu identifizieren, welche ein IT-System bereits kompromittiert hat.
  - **Automatische Prüfung von Logfiles**: Soweit die Sicherheits-Logfiles mehrerer System auf einem System zentralisiert gesammelt werden, erfolgt eine automatisierte Auswertung der Logfiles, um mögliche Sicherheitsverletzungen zu erkennen.
  - **Sicherheits-Mailing-Listen**: Es wird sichergestellt, dass ein Mitarbeiter des Unternehmens oder ein externer Dienstleister einschlägige Mailing-Listen für die Bekanntgabe neuer IT-Sicherheits-Bedrohungen abonniert (z.B. Mailing-Listen der Hersteller der verwendeten Software), um über die aktuelle Bedrohungslage in Kenntnis zu sein.
- Organisatorische Maßnahmen
  - **Erkennung von Sicherheitsverletzungen durch Dienstnehmer**: Alle Dienstnehmer werden instruiert, wie sie Sicherheitsverletzung erkennen können (z.B. nicht mehr auffindbare Computer-Hardware, Meldungen von Anti-Viren-Software).
  - **Betriebsfremde Personen**: Alle Dienstnehmer werden instruiert, betriebsfremde Personen anzusprechen, sollten sie in den Betriebsräumlichkeiten angetroffen werden.
  - **Audits**: Es werden regelmäßige Audits durchgeführt (z.B. Prüfung, ob alle kritischen Sicherheits-Updates installiert wurden). Insbesondere erfolgt eine regelmäßige Prüfung der erteilten Zugriffs- und Zutrittsberechtigungen (welchem Mitarbeiter ist welcher Benutzer-Account mit welchen Zugriffsrechten zugewiesen; welche Personen verfügen über welche Schlüssel).

    - **Manuelle Prüfung von Logfiles**: Soweit Logfiles geführt werden (z.B. über erfolglose Authentifizierungsversuche), werden diese in regelmäßigen Abständen geprüft.

- Physische Maßnahmen
    - **Brandmelder**: Sofern dies aufgrund der Größe und Beschaffenheit der Betriebsräumlichkeiten angemessen ist, wird ein Brandmelder installiert, der durch Rauch automatisch ausgelöst wird.

Reaktive Sicherheitsmaßnahmen – Maßnahmen zur Reaktion auf einen Angriff

- Technische Maßnahmen
    - **Datensicherung**: Es werden regelmäßig Datensicherungen erstellt und sicher aufbewahrt.
    - **Datenwiederherstellungskonzept**: Es wird ein Konzept zur raschen Wiederherstellung von Datensicherungen entwickelt, um nach einer Sicherheitsverletzung zeitnah den regulären Betrieb wieder herstellen zu können.
    - **Automatische Entfernung von Schadsoftware**: Die eingesetzte Anti-Viren-Software verfügt über die Funktion, Schadsoftware automatische zu entfernen.
- Organisatorische Maßnahmen
    - **Meldepflicht für Dienstnehmer**: Alle Dienstnehmer werden angewiesen, Sicherheitsverletzungen unverzüglich an eine zuvor definierte interne Stelle bzw. Person zu melden.
    - **Meldepflicht für externe Dienstleister**: Allen Dienstleistern wurden Kontaktdaten für die Meldung von Sicherheitsverletzungen mitgeteilt.
    - **Prozess für die Reaktion auf Sicherheitsverletzungen**: Es wird durch einen geeigneten Prozess sichergestellt, dass Sicherheitsverletzungen innerhalb von 72 Stunden ab Kenntnis von der Sicherheitsverletzung an die Datenschutzbehörde gemeldet werden können. Insbesondere sind allen Dienstnehmern die Notfall-Telefonnummern der zu involvierenden Personen bekannt zu geben (z.B. Notfall-Telefonnummer für den IT-Support).
- Physische Maßnahmen
    - **Feuerlöscher**: In den Betriebsräumlichkeiten gibt es eine geeignete Anzahl an Feuerlöschern. Allen Dienstnehmern ist bekannt, wo sich die Feuerlöscher befinden.
    - **Feueralarm**: Soweit es keinen Brandmelder gibt, der über keine automatische Verbindung zur Feuerwehr verfügt, wird durch einen angemessenen Prozess sichergestellt, dass die Feuerwehr manuell verständigt werden kann.

Abschreckende Sicherheitsmaßnahmen – Maßnahmen zur Minderung der Angreifermotivation

- Technische Maßnahmen
    - **Automatische Warnmeldungen**: Nutzer erhalten automatische Warnmeldungen bei risikoträchtiger IT-Nutzung (z.B. durch den Webbrowser, wenn eine verschlüsselte Website kein korrektes SSL/TLS-Zertifikat verwendet).
- Organisatorische Maßnahmen

Sanktionen bei Angriffen durch eigene Dienstnehmer: Alle Dienstnehmer werden darüber informiert, dass Angriffe auf betriebseigene IT-Systeme nicht toleriert werden und schwerwiegende arbeitsrechtliche Konsequenzen, wie insbesondere eine Entlassung nach sich ziehen können.