

Auftragsverarbeitungsvertrag

der incaseof.law GmbH

zwischen

Kunde

- nachfolgend „Auftraggeber“ oder „Verantwortlicher“ -

und

incaseof.law GmbH, Rathausstraße 21/13, 1010 Wien, eingetragen im Firmenbuch des Handelsgericht Wien unter FN 505409 z

- nachfolgend „Auftragnehmer“ -

über Auftragsdatenverarbeitung iSd. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO, VO EU 2016/679).

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „Auftragsverarbeitungsvertrag“) konkretisiert die Verpflichtungen der Vertragsparteien zum Schutz personenbezogener Daten, die sich aus der Auftragsverarbeitung ergeben. Der Auftragsverarbeitungsvertrag findet Anwendung auf alle Tätigkeiten, die mit dem zwischen den Parteien am Tag der Registrierung des Auftraggebers bei incaseof.law GmbH geschlossenen Hauptvertrag (gemäß AGB) (nachfolgend „Vertrag“) in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Personen personenbezogene Daten (nachfolgend „Daten“) des Auftraggebers verarbeiten. Die in diesem Vertrag verwendeten Begriffe sind gemäß ihrer Definition in der DSGVO zu verstehen.

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 personenbezogene Daten im Auftrag des Auftraggebers iSd Art. 4 Nr. 8 und Art. 28 der DSGVO. Dies umfasst Tätigkeiten, die im Vertrag und in der 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. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

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 beigelegten 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 betroffener Personen gemäß 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 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 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 für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für datenschutzrechtliche Fragen im Rahmen des Vertrages.

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 Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien aufgrund 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 Anspruchs 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 hinsichtlich 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 datenschutzrechtliche Fragen im Rahmen des Vertrages.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen gemäß Kapitel III DSGVO (Auskunftserteilung, Berichtigung oder Löschung ihrer Daten) zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen und dessen Weisungen abwarten, sofern eine Zuordnung zum 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 bei der Erfüllung von dessen Pflichten gemäß Art. 12-22 DSGVO im Rahmen seiner Möglichkeiten. 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 zum 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. Subunternehmer und Unterauftragsverhältnisse

7.1. Der Auftragnehmer ist grundsätzlich berechtigt, Subauftragnehmer (weitere Auftragsverarbeiter) unter Beachtung der nachfolgenden Regelungen zu beauftragen. Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subauftragnehmers mitteilt.

7.2. 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. Der Auftragnehmer stellt sicher, dass der Subauftragnehmer die Pflichten erfüllt, denen der Auftragnehmer entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.

7.3. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt. Der Auftraggeber stimmt dem Einsatz der in Punkt 10. unserer Datenschutzerklärung genannten Subunternehmer zu.

7.4. 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. Der Auftraggeber hat das Recht, gegen die vorab schriftlich angekündigte Hinzuziehung weiterer Subauftragnehmer Einspruch zu erheben. Die Zustimmung durch den Auftraggeber gilt als erteilt, wenn der Auftraggeber nicht innerhalb von zwei Wochen nach Mitteilung Einspruch gegen die beabsichtigte Änderung von Subauftragnehmern erhebt.

7.5. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Auftragsverarbeitungsvertrag dem Subunternehmer zu übertragen.

7.6. Im Falle eines Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung entweder

- 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 innerhalb einer angemessenen Frist und vorheriger Information des Auftraggebers einstellen. Der Auftragnehmer wird den Auftraggeber unverzüglich über die beabsichtigte Einstellung und Frist informieren (Textform genügt). Beiden Parteien wird in diesem Fall das gesonderte Recht auf Kündigung innerhalb von 2 Wochen nach Bekanntgabe der Einstellung eingeräumt.

8. Informationspflichten, Textform, Rechtswahl

8.1. 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.

8.2. 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.

8.3. 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.

8.4. Es gilt österreichisches Recht.

9. Haftung und Schadenersatz

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: Kunden des Auftraggebers und ggf. Mitarbeiter dieser Kunden

Kategorien von Daten Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien: siehe Abschnitt 5.3 der Datenschutzerklärung

Kategorien von sensiblen Daten (falls zutreffend) Die übermittelten personenbezogenen Daten umfassen folgende sensiblen Daten: siehe Abschnitt 5.3 der Datenschutzerklärung

Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen: Technische Verarbeitung und Übernahme der Kundennamen und Adressen für Anschreiben / Mahnungen oder Mahnklagen im Rahmen des Forderungsmanagement-Prozesses und der Rechtsverfolgung

Verarbeitungszwecke Die übermittelten personenbezogenen Daten werden zu folgenden Zwecken des Verantwortlichen verarbeitet: Versand von Mahnungen, allgemeine außergerichtliche und gerichtliche Maßnahmen des Forderungsmanagements.

Standort der Datenverarbeitung Die vom Auftragnehmer ausgeführte Datenverarbeitung findet an folgenden Standorten statt: Geschäftsräume des Auftragnehmers: incaseof.law GmbH Rathausstraße 21/13 1010 Wien Die Datenverarbeitung findet darüber hinaus an den Verarbeitungsstandorten der Subauftragsverarbeiter statt.

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:** Personenbezogene Daten werden auf dem Übertragungsweg über das Internet verschlüsselt, zumindest soweit es sich um sensible Daten handelt.
- **Verschlüsselung mobiler Geräte:** Mobile Endgeräte und mobile Datenträger werden verschlüsselt, zumindest soweit auf diesen Geräten 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 des Auftragnehmers:** 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 nur in besonders begründeten Fällen erlaubt.
- **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 Dienstleister:** 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 wiederhergestellt 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, welche 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 Systeme 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 des Auftragnehmers:** Alle Dienstnehmer werden instruiert, wie sie Sicherheitsverletzungen 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 wiederherstellen zu können.
- **Automatische Entfernung von Schadsoftware:** Die eingesetzte Anti-Viren-Software verfügt über die Funktion, Schadsoftware automatisch 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 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.