Datenschutzhinweise
Webseiten (Loyalty-Aktion)

1. Datenschutz auf einen Blick

Allgemeine Hinweise

Die folgenden Hinweise geben in Ergänzung unserer auf unserer Website abrufbaren allgemeinen Datenschutzhinweise (https://schluetersche.de/datenschutz/datenschutz-gbt) einen einfachen Überblick über die spezifische Verarbeitung personenbezogener Daten, wenn Sie unsere Leistung Webseiten (Loyalty-Aktion), also die Gestaltung, Pflege und/oder Verwaltung von Internetseiten, (im Folgenden „Leistung“ genannt), nutzen.

Personenbezogene Daten sind alle Daten, mit denen Sie persönlich identifiziert werden können.

Datenerfassung

Wie erfassen wir Ihre Daten?

Ihre Daten werden zum einen dadurch erhoben, dass Sie uns diese mitteilen. Hierbei kann es sich z.B. um Daten handeln, die Sie in ein Kontakt-, Bestell-oder Anmeldeformular eingeben, oder solche, die Sie uns persönlich, telefonisch oder auf sonstige Weise mitteilen.

Andere Daten werden automatisch bei der Nutzung unserer Website oder Leistung durch unsere IT-Systeme oder solche beauftragter Dritter erfasst. Das sind vor allem technische Daten (z.B. Internetbrowser, Betriebssystem oder Uhrzeit des Seitenaufrufs). Die Erfassung dieser Daten erfolgt automatisch, sobald Sie oder andere Nutzer unsere Website oder die Leistung nutzen.

Wir weisen darauf hin, dass die Datenübertragung im Internet (z.B. bei der Kommunikation per E-Mail) Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich.

Wofür nutzen wir Ihre Daten?

Die Daten werden erhoben für die Erbringung der Leistung, die Kommunikation mit Ihnen und zur Verbesserung von beidem.

Welche Rechte haben Sie bezüglich Ihrer Daten?

Sie haben jederzeit das Recht unentgeltlich Auskunft über Herkunft, Empfänger und Zweck Ihrer gespeicherten personenbezogenen Daten zu erhalten. Sie haben außerdem ein Recht, die Berichtigung, Sperrung oder Löschung dieser Daten zu verlangen. Hierzu sowie zu weiteren Fragen zum Thema Datenschutz können Sie sich jederzeit unter der im Impressum angegebenen Adresse an uns wenden. Des Weiteren steht Ihnen ein Beschwerderecht bei der zuständigen Aufsichtsbehörde zu.

Widerruf Ihrer Einwilligung zur Datenverarbeitung

Viele Datenverarbeitungsvorgänge sind nur mit Ihrer ausdrücklichen Einwilligung möglich. Sie können eine bereits erteilte Einwilligung jederzeit widerrufen. Dazu reicht eine formlose

Mitteilung per E-Mail an uns. Die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.

Beachten Sie bitte, dass der Widerruf Ihrer Einwilligung in die Verarbeitung leistungsbezogener Daten unter Umständen dazu führen kann, dass wir die Leistung nicht mehr oder nicht mehr in der bisherigen Form erbringen können.

2. Verarbeitung Kunden- und Vertragsdaten

Allgemeines

Wir erheben, verarbeiten und nutzen personenbezogene Daten nur, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung des Rechtsverhältnisses über die Erbringung der Leistung sowie die Leistungserbringung selbst erforderlich sind (Bestandsdaten). In Einzelfällen kann die Verarbeitung (soweit angegeben) auch der Überprüfung dienen, ob Sie zur Begründung des Rechtsverhältnisses und/oder der Entgegenahme der gegenständlichen Leistungen berechtigt sind.

Die Verarbeitung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO, der die Verarbeitung von Daten zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen gestattet. Personenbezogene Daten über die Inanspruchnahme unserer Internetseiten (Nutzungsdaten) erheben, verarbeiten und nutzen wir nur, soweit dies erforderlich ist, um dem Nutzer die Inanspruchnahme des Dienstes zu ermöglichen oder abzurechnen.

Die erhobenen Kundendaten werden nach Abschluss des Auftrags oder Beendigung der Geschäftsbeziehung gelöscht. Gesetzliche Aufbewahrungsfristen bleiben unberührt.

Datenübermittlung

Wir übermitteln personenbezogene Daten an Dritte nur dann, wenn dies im Rahmen der Leistungserbringung oder der Kommunikation notwendig ist, etwa an mit der Lieferung von Waren oder der Erbringung von Teilleistungen betraute Unternehmen sowie mit der Zahlungsabwicklung beauftragte Kreditinstitute. Eine weitergehende Übermittlung der Daten erfolgt nicht bzw. nur dann, wenn Sie der Übermittlung ausdrücklich zugestimmt haben.

Grundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b DSGVO, der die Verarbeitung von Daten zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen gestattet.

3. Datenerfassung auf unserer Website

Informationen zur Datenverarbeitung bei Besuch unserer Webseite entnehmen Sie bitte den auf unserer Webseite abrufbaren Datenschutzhinweisen.

4. Auftragsverarbeitung

Soweit wir vereinbarungsgemäß in Ihrem Auftrag personenbezogene Daten verarbeiten („Auftragsverarbeitung“), finden unsere als Anlage beigefügten Regeln zur Auftragsverarbeitung Anwendung.

Stand: Februar 2020

Regelungen zur Auftragsverarbeitung – Webseiten

1. Geltungsbereich, Definitionen

1.1 Diese Regelungen zur Auftragsverarbeitung – Webseiten (im Folgenden „diese Regelungen“ genannt) konkretisieren die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag über die Erbringung der Leistung Webseiten einschließlich der einbezogenen Allgemeinen Geschäftsbedingungen (im Folgenden „Vertrag“ genannt) des Anbieters (im Folgenden „Auftragnehmer“ genannt) an seinen Kunden (im Folgenden „Auftragnehmer“ genannt) in ihren Einzelheiten beschriebenen Auftragsverarbeitung im Sinne des Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO) ergeben.

1.2 Auftragnehmer und Auftraggeber werden in diesen Regelungen auch „Vertragsparteien“ genannt.

1.3 Diese Regelungen finden Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (im Folgenden „Daten“ genannt) des Auftraggebers verarbeiten.

1.4 Die Inhalte dieser Regelungen gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf Daten nicht ausgeschlossen werden kann

1.5 Diese Regelungen in der vorliegenden Fassung ersetzen in ihrem Geltungsbereich gegebenen Falls alle bislang zwischen den Parteien bestehende Vereinbarungen über Auftragsdatenverarbeitung/Auftragsverarbeitung.

2. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

2.1 Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

2.2 Die Laufzeit dieser Regelungen richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Regelungen nicht darüber hinausgehende Verpflichtungen ergeben.

3. Anwendungsbereich und Verantwortlichkeit

3.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. 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).

3.2 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 (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

4. Pflichten des Auftragnehmers

4.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 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.

4.2 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.

4.3 Das im **Anhang 1** zu diesen Regelungen beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

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

4.5 Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO, sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer kann vom Auftraggeber für diese Unterstützung eine angemessene Vergütung verlangen.

4.6 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers 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 personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer

angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

4.7 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 der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

4.8 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

4.9 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

4.10 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen 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. Der Auftragnehmer kann vom Auftraggeber für diese Unterstützung eine angemessene Vergütung verlangen.

4.11 In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

4.12 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.

4.13 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. Der Auftragnehmer kann vom Auftraggeber für diese Unterstützung eine angemessene Vergütung verlangen.

5. Pflichten des Auftraggebers

5.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

5.2 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt Absatz 4.13 entsprechend.

5.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

6. 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.

7. Nachweismöglichkeiten

7.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesen Regelungen niedergelegten Pflichten mit geeigneten Mitteln nach.

7.2 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 kann der Auftragnehmer eine zu vereinbarende angemessene Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

7.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 7.2 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.

8. Subunternehmer (weitere Auftragsverarbeiter)

8.1 Eine Unterbeauftragung von Subunternehmen durch den Auftragnehmer mit im Rahmen des Vertrages geschuldeten Leistungspflichten ist grundsätzlich zulässig. Der Auftragnehmer muss jedoch den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines

Subunternehmers schriftlich oder im elektronischen Format (z.B. E-Mail) informieren. Lediglich in Notsituationen, die keine vorherige Information erlauben und ein sofortiges Handeln erfordern, um die weitere Datenverarbeitung garantieren zu können, kann von der vorherigen Information abgesehen werden. In diesen Fällen muss der Auftragnehmer den Auftraggeber unverzüglich nach der Beauftragung informieren.

8.2 Der Auftraggeber kann der Änderung – innerhalb einer Frist von 14 Tagen – aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als erteilt.

8.3 Eine Liste der jeweils aktuell durch den Auftraggeber genehmigten Subauftragnehmer ist diesen Regelungen als **Anhang 2** beigefügt.

8.4 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesen Regelungen dem Subunternehmer zu übertragen.

9. Informationspflichten, Schriftformklausel, Rechtswahl, Gerichtsstand

9.1 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.

9.2 Änderungen und Ergänzungen dieser Regelungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.3 Bei etwaigen Widersprüchen gehen diese Regelungen den Vereinbarungen im Vertrag vor. Sollten einzelne Teile dieser Regelungen unwirksam sein, so berührt dies die Wirksamkeit der Regelungen im Übrigen nicht.

9.4 Es gilt deutsches Recht.

9.5 Gerichtsstand für Streitigkeiten aus diesen Regelungen ist der Sitz des Auftragnehmers, wenn der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist. Das gilt auch, wenn der Auftraggeber im Inland keinen allgemeinen Gerichtsstand hat oder sein Wohnsitz unbekannt oder im Ausland ist.

10. Haftung und Schadensersatz

10.1 Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderer Vorschriften über den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich.

10.2 Im Falle einer rechts- oder pflichtwidrigen Datenverarbeitung, die in den Verantwortungsbereich des Auftragnehmers fällt, kommen die im Vertrag zwischen den Vertragsparteien getroffenen Haftungsvereinbarungen zur Anwendung.

Stand: Februar 2019

Anhang 1: Dokumentation der technischen und organisatorischen Maßnahmen

Folgende technische und organisatorische Maßnahmen (TOMs) werden zwischen dem Auftraggeber und dem Auftragnehmer umgesetzt. Auf Grundlage von Art. 32 Datenschutz-Grundverordnung (DSGVO) gibt der Auftragnehmer hier an, welche technischen und organisatorischen Maßnahmen er zur Gewährleistung des Datenschutzes und der Datensicherheit getroffen hat. Wenn anwendbar und vertretbar wird eine Maßnahme nach dem Stand der Technik durchgeführt.

Die Folgende Auflistung gibt eine Übersicht der TOMs nach Maßnahmenbereichen an. Der Auftraggeber hat die Möglichkeit, die umfassende und detaillierte Aufstellung aller datenschutz- und informationssicherheitsrelevanter TOMs aus den Maßnahmenbereichen anzufordern. In allen folgenden Maßnahmenbereichen wurden TOMs – soweit anwendbar – zur Gewährung eines angemessen Datenschutz- und Informationssicherheitsniveaus eingeführt.

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1 **Zutrittskontrolle**
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Betroffen sind Gebäude, Räume, Schränke in denen sich Datenverarbeitungsanlagen befinden bzw. durch die Zutritt zu diesen erlangt werden kann.

1.1.1. Bauliche Maßnahmen
- 1.1.1.1. Empfang, Pförtner
- 1.1.1.2. Türen
- 1.1.1.3. Fenster
- 1.1.1.4. Schließanlage
- 1.1.1.5. Manuelles Schließsystem
- 1.1.1.6. Sicherheitsschlösser
- 1.1.1.7. Absicherung der Gebäudeschächte

1.1.2. Technische Maßnahmen
- 1.1.2.1. Alarmanlage
- 1.1.2.2. Zugangserfassung mit NFC-Karte

1.1.3. Organisatorische Maßnahmen
- 1.1.3.1. Schlüsselregelung
- 1.1.3.2. Besucherbuch/Protokoll der Besucher
- 1.1.3.3. Sorgfalt bei Auswahl des Wachpersonals
- 1.1.3.4. Sorgfalt bei Auswahl Reinigungsdienste
- 1.1.3.5. Festlegung der zutrittsberechtigten Personen

1.2 **Zugangskontrolle**
Maßnahmen, die zu verhindern geeignet sind, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

1.2.1. Technische Maßnahmen
- 1.2.1.1. Login mit Benutzername und Passwort
- 1.2.1.2. Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- 1.2.1.3. Manuelle Zugangssperre
- 1.2.1.4. Automatische Bildschirm-Sperrung
- 1.2.1.5. Protokollierung der Zugänge (z.B. durch Event-Logs)
- 1.2.1.6. Sicherung der Arbeitsplätze bei Abwesenheit

1.2.2. Organisatorische Maßnahmen
- 1.2.2.1. Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- 1.2.2.2. Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- 1.2.2.3. Richtlinie "Clean desk"
- 1.2.2.4. Richtlinie "Sicheres Passwort"

1.3 **Zugriffskontrolle**
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben.

1.3.1. Technische Maßnahmen
- 1.3.1.1. Login mit Benutzername und Passwort
- 1.3.1.2. Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- 1.3.1.3. Manuelle Zugangssperre
- 1.3.1.4. Automatische Bildschirm-Sperrung
- 1.3.1.5. Protokollierung der Zugänge (z.B. durch Event-Logs)
- 1.3.1.6. Sicherung der Arbeitsplätze bei Abwesenheit

1.3.2. Organisatorische Maßnahmen
- 1.3.2.1. Berechtigungskonzept
- 1.3.2.2. Verwaltung und Kontrolle der Zugriffsberechtigungen

1.4 **Trennungskontrolle**
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
- 1.4.1.1. Funktionstrennung Produktion / Test
- 1.4.1.2. Aufteilung in Mandanten oder logische Trennung von Datenbeständen

2. Pseudonymisierung gemäß Art. 32 Abs. 1 lit. a, 25 Abs. 1 DSGVO
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

2.1.1. Technische Maßnahmen
Programme mit Pseudonymisierungsfunktion

2.1.2. Organisatorische Maßnahmen
Richtlinie über die Pseudonymisierung von personenbezogenen Daten

3. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

3.1 **Weitergabekontrolle**
Maßnahmen, die 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.

3.1.1. Technische Maßnahmen
- 3.1.1.1. Email-Verschlüsselung
- 3.1.1.2. Einsatz von VPN
- 3.1.1.3. Protokollierung der Zugriffe und Abrufe
- 3.1.1.4. Weitergabe von personenbezogenen Daten in anonymisierter oder pseudonymisierter Form
- 3.1.1.5. Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- 3.1.1.6. Sicherheitsgateways an den Netzübergabepunkten

3.1.2. Organisatorische Maßnahmen
- 3.1.2.1. Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- 3.1.2.2. Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- 3.1.2.3. Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- 3.1.2.4. Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder

3.2 **Eingabekontrolle**
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

3.2.1. Technische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten

3.2.2. Organisatorische Maßnahmen

3.2.2.1. Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
3.2.2.2. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
3.2.2.3. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

4. Verfügbarkeit und Belastbarkeit gemäß Art. 32 Abs. 1 lit. b DSGVO

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

4.1.1. Technische Maßnahmen

4.1.1.1. Feuer- und Rauchmeldeanlagen
4.1.1.2. Feuerlöscher Serverraum
4.1.1.3. Serverraumüberwachung Temperatur und Feuchtigkeit
4.1.1.4. Serverraum klimatisiert
4.1.1.5. Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
4.1.1.6. Unterbrechungsfreie Stromversorgung
4.1.1.7. Keine sanitären Anschlüsse im oder oberhalb des Serverraums
4.1.1.8. Schutzsteckdosenleisten Serverraum
4.1.1.9. Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)
4.1.1.10. Getrennte Partitionen für Betriebssysteme und Daten

4.1.2. Organisatorische Maßnahmen

4.1.2.1. Backup & Recovery-Konzept (ausformuliert)
4.1.2.2. Kontrolle des Sicherungsvorgangs
4.1.2.3. Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
4.1.2.4. Notfallplan (z.B. BSI IT-Grundschutz 100-4)

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gemäß Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)

5.1 **Datenschutz-Management**

Maßnahmen, die geeignet sind, eine Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

5.1.1. Technische Maßnahmen

Software-Lösungen für Datenschutzmanagement

5.1.2. Organisatorische Maßnahmen

5.1.2.1. Bestellung interne Datenschutzbeauftragte
5.1.2.2. Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
5.1.2.3. Schulung/Verpflichtung Mitarbeiter auf Vertraulichkeit/Datengeheimnis
5.1.2.4. Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)
5.1.2.5. Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen (mind. jährlich)
5.1.2.6. Durchführung Datenschutz-Folgenabschätzung (DSFA) bei Bedarf
5.1.2.7. Einhaltung der Informationspflichten nach Art. 13 und 14 DSGVO

5.2 **Incident-Response-Management**

Maßnahmen zur Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in Datenverarbeitungs-Bereichen.

5.2.1. Technische Maßnahmen

5.2.1.1. Einsatz von Firewall und regelmäßige Aktualisierung
5.2.1.2. Einsatz von Spamfilter und regelmäßige Aktualisierung
5.2.1.3. Einsatz von Virenscanner und regelmäßige Aktualisierung

5.2.2. Organisatorische Maßnahmen

5.2.2.1. Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
5.2.2.2. Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem

Anhang 2: Liste der Subunternehmer/Unterauftragnehmer

Gemäß Abschnitt 8 der Regelungen zur Auftragsverarbeitung meldet der Auftragnehmer hiermit folgende Subunternehmer, welche er – soweit das genannte Leistungsmerkmal Bestandteil der erbrachten Leistung ist – zur Erfüllung seiner sich aus dieser Auftragsverarbeitung ergebenden vertraglich vereinbarten Leistung unterbeauftragt:

1. **Content Management System (CMS) zum Erstellen von Webseiten:**
   Mono Solutions ApS, Hejrevej 28, 2400 København, Dänemark

2. **Kommunikationssystem für unsere Kommunikation mit dem Betreiber des CMS:**
   Jira, ein Kommunikationssystem der Atlassian Pty Ltd, c/o Atlassian, Inc., 1098 Harrison Street, San Francisco, CA, USA 94103, Vereinigte Staaten von Amerika,
   Server-Standorte: Vereinigte Staaten von Amerika und Irland.
   Slack, ein Kommunikationssystem der Slack Technologies Limited, 4th Floor, One Park Place, Hatch Street Upper, Dublin 2, Irland

3. **Webseiten-Tracking:**
   Google Analytics, ein Webanalysedienst der Google Inc., Amphitheatre Parkway, Mountain View, CA 94043, Vereinigte Staaten von Amerika

4. **Anrufauswertung:**
   matelso GmbH, Heilbronner Str. 150, 70191 Stuttgart, Deutschland

5. **Implementierung von Kartendaten:**
   Google Maps, ein Kartendatendienst der Google Inc., Amphitheatre Parkway, Mountain View, CA 94043, Vereinigte Staaten von Amerika.
   Openstreetmap Foundation, 132 Maney Hill Road, Sutton Coldfield, West Midlands, B72 1JU, Vereinigtes Königreich

6. **Domainregistrierung, Hosting von Webseiten (WebIndividuell):**
   ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland

7. **Hosting von Webseiten (sonstige):**
   Mono Solutions ApS, Hejrevej 28, 2400 København, Dänemark,
   Server-Standorte: Dänemark, Canada, Deutschland

8. **Domainregistrierung und –verwaltung (sonstige):**
   Tucows.com Co., 96 Mowat Avenue, Toronto, Ontario, M6K 3M1, Canada

9. **SSL-Zertifikate:**
   Let's Encrypt, eine Zertifizierungsstelle der gemeinnützigen Internet Security Research Group (ISRG), 1 Letterman Drive, Suite D4700, San Francisco, CA 94129, Vereinigte Staaten von Amerika

10. **Newsletterversand:**
    Inxmail GmbH, Wentzingerstr. 17, 79106 Freiburg, Deutschland
    MailChimp, ein Newsletter-Versand- und Analysedienst der Rocket Science Group LLC, 675 Ponce De Leon Ave NE, Suite 5000, Atlanta, GA 30308, Vereinigte Staaten von Amerika

11. **Facebook-Plugins:**
    Facebook Inc., 1 Hacker Way, Menlo Park, California 94025, Vereinigte Staaten von Amerika

12. **Twitter-Plugins:**
    Twitter Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, Vereinigte Staaten von Amerika

13. **Google+-Plugins:**
    Google Inc., Amphitheatre Parkway, Mountain View, CA 94043, Vereinigte Staaten von Amerika

14. **XING-Plugins:**
    XING AG, Dammtorstraße 29-32, 20354 Hamburg, Deutschland

15. **YouTube-Plugins und Hosting/Zugänglichmachung von Videos:**
    YouTube, LLC, 901 Cherry Ave., San Bruno, CA 94066, Vereinigte Staaten von Amerika

Stand: April 2019
Ältere Subunternehmer-Listen verlieren hiermit Ihre Gültigkeit.