Präambel

Führt ein Auftragsverarbeiter Leistungen im Auftrag seines Vertragspartners (Verantwortlicher) aus, müssen die Anforderungen der jeweils gültigen Datenschutzgesetze Berücksichtigung finden und insbesondere bei den Verarbeitungstätigkeiten ein angemessenes Datenschutzniveau garantiert sein. Die vorliegende Vereinbarung berücksichtigt die besonderen Anforderungen aus der EU-Datenschutzgrundverordnung[1].

1. Gegenstand des Auftrags

(1) Der Verantwortliche beauftragt den Auftragsverarbeiter mit der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten.

(2) Der Gegenstand des Auftrags und damit der Zweck, die Art und der Umfang der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten ist der Betrieb und die Wartung der SmartrOS-Server sowie der hierbei eingesetzten Software für den Verantwortlichen.

(3) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der einschlägigen Datenschutzgesetze erfüllt sind.

2. Dauer des Auftrags

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 3 Monat(en) zum Quartalsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

3. Art der Daten

Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten sind Daten aus den folgenden Datenartenkategorien:

Personenstammdaten, Authentifizierungsdaten, Zeiterfassungsdaten, IT-Nutzungsdaten, Protokolldaten, Verbrauchsdaten, Gebäude-/Objektdaten, Alarmanlagendaten, Videodaten

Weitere Datenkategorien: _____

_____

4. Kreis der Betroffenen

Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen, umfasst folgende Kategorien:

Beschäftigte, Besucher, Kunden, Dienstleister, Lieferanten, Geschäftspartner

Weitere Betroffenenkategorien: _____

_____

[1] Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, EU-DSGVO).

5. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben (**Anlage 1„Technisch-organisatorische Maßnahmen“**). Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die technisch-organisatorischen Maßnahmen sollen die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie die Systembelastbarkeit im Zuge der Datenverarbeitung sicherstellen. Aus den angegebenen Maßnahmen muss ein angemessenes Sicherheitsniveau ableitbar sein. Der Auftragsverarbeiter hat den Verantwortlichen bei der Ergreifung technisch-organisatorischer Maßnahmen bestmöglich zu unterstützen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. Berichtigung, Sperrung, Einschränkung und Löschung von Daten

Der Auftragsverarbeiter hat nur nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen, einzuschränken oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

7. Kontrollen und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.

b) Die Wahrung des Datengeheimnisses. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis und die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden. Dies umfasst auch die besonderen Bestimmungen zum Fernmeldegeheimnis nach § 3 TTDSG, Sozialgeheimnis nach § 35 SGB I und anderer Berufsgeheimnisse nach § 203 StGB, sofern sie im Rahmen dieser Auftragsverarbeitung relevant sind.

c) Der Auftragsverarbeiter stellt sicher, dass er die Verarbeitung personenbezogener Daten ausschließlich auf Grundlage dokumentierter Weisungen des Verantwortlichen vornimmt (vergl. § 11 dieses Vertrages). Sofern der Auftragsverarbeiter zu einer Verarbeitung gesetzlich verpflichtet ist, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

d) Der Auftragsverarbeiter hat den Verantwortlichen bei seiner Pflicht zur Wahrung der Betroffenenrechte zu unterstützen. Dies ist durch geeignete organisatorische Maßnahmen zu gewährleisten.

e) Sofern den Verantwortlichen aufgrund eines voraussichtlich hohen Risikos der Verarbeitung die Pflicht zur Datenschutz-Folgenabschätzung trifft, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Dies gilt ebenso für die Pflicht zur vorherigen Konsultation der Aufsichtsbehörde, sofern sich eine solche aus der vorangegangenen Folgenabschätzung ergibt.

f) Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde beim Auftragsverarbeiter ermittelt.

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen. Hierzu kann der Auftragsverarbeiter auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) oder andere hinreichende Garantien vorlegen.

8. Unterauftragsverhältnisse

(1) Soweit bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten des Verantwortlichen Unterauftragsverarbeiter für die vorliegende Verarbeitung von Daten im Auftrag einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

a) Der Auftragsverarbeiter hat den Verantwortlichen bei jeder Hinzuziehung oder Änderung von Unterauftragsverhältnissen rechtzeitig vorab zu informieren. Der Verantwortliche hat das Recht, einzelnen Unterauftragsvergaben oder Änderungen zu widersprechen.

b) Der Auftragsverarbeiter hat die vertraglichen Vereinbarungen mit dem/ den Unterauftragsverarbeiter(n) so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftragsverarbeiter und Verantwortlichem entsprechen. Es müssen hinreichende Garantien dafür geboten sein, dass die technischen und organisatorischen Maßnahmen den Anforderungen an die rechtmäßige Datenverarbeitung genügen.

c) Bei der Unterbeauftragung ist dem Verantwortlichen das Recht einzuräumen, vom Auftragsverarbeiter auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

(2) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer etc. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Der Auftragsverarbeiter setzt die in **Anlage 2 „Unterauftragsverarbeiter“** genannten Unterauftragsverarbeiter zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Sinne dieser Vereinbarung ein.

9. Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, eine Auftragskontrolle mit dem Auftragsverarbeiter durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter und dessen Pflichten nach Art. 28 EU-DSGVO in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Pflichten nach Art. 28 EU-DSGVO erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

(2) Im Hinblick auf die Kontrollverpflichtungen des Verantwortlichen vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragsverarbeiter sicher, dass sich der Verantwortliche von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragsverarbeiter dem Verantwortlichen auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) oder durch andere hinreichende Garantien erbracht werden.

10. Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter erstattet in allen Fällen dem Verantwortlichen eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

(2) Es ist dem Auftragsverarbeiter bekannt, dass Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Verantwortlichen mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Verantwortlichen. Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

(3) Soweit den Verantwortlichen Melde- und/oder Benachrichtigungspflichten treffen, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Dies gilt sowohl für die Meldung einer etwaigen Pflichtverletzung gegenüber der Aufsichtsbehörde als auch für die Benachrichtigung der von der Verletzung des Schutzes personenbezogenen Daten betroffenen Personen.

11. Weisungsbefugnis des Verantwortlichen

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Verantwortlichen. Der Verantwortliche behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustim-

men und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

(2) Mündliche Weisungen wird der Verantwortliche unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch eine beim Verantwortlichen befugte Person bestätigt oder geändert wird.

12. Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

13. Haftung

Für Schäden des Verantwortlichen durch schuldhafte Verstöße des Auftragsverarbeiters oder etwaiger Unterauftragsverarbeiter gegen diesen Vertrag sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen gelten die gesetzlichen Haftungsregelungen. Etwaige Haftungsbegrenzungen zwischen den Parteien (z.B. aus dem Hauptvertrag) finden auf diese Vereinbarung Anwendung.

14. Kostenregelung

(1) Dem Auftragsverarbeiter wird das Recht eingeräumt, etwaige Aufwände, die seinerseits durch diese Vereinbarung entstehen, dem Verantwortlichen in Rechnung zu stellen. Diese Regelung bezieht sich auf Aufwände im Zusammenhang mit

a) der Unterstützung des Verantwortlichen bei Datenschutz-Folgeabschätzungen gemäß §7 lit. e),

b) der Kontrolle im Geschäftsbetrieb des Auftragsverarbeiters gemäß §9 Abs. (1) und

c) der Löschung von Daten gemäß §12.

(2) Arbeiten auf Seiten des Auftragsverarbeiters werden mit 60 Euro/Stunde (zzgl. Umsatzsteuer) angesetzt. Etwaige Fremdkosten werden nach Nachweis berechnet.

15. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung 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.

(3) Es gilt deutsches Recht sowie das in Deutschland unmittelbar und zwingend anzuwendende Recht der Europäischen Union.

Technische und organisatorische Maßnahmen

der

Smartrplace GmbH
Ludwig-Erhard-Straße 8
34131 Kassel

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen. Die wesentlichen Datenverarbeitungen für unsere Kunden finden in externen Rechenzentren bei Unterauftragsverarbeitern statt. Diese haben eigenen Maßnahmen zum Schutz der Daten umgesetzt. Darüber hinaus haben wir auch eigene technische und organisatorische Maßnahmen umgesetzt:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

a) Zutrittskontrolle/Gebäudeabsicherung

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal

b) Zugangskontrolle/Absicherung Systemzugang

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

- Zuordnung von Benutzerrechten
- Einsatz von individuellen Benutzernamen
- Authentifikation mit Benutzername/Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie (Fernzugriff)
- Verschlüsselung von Datenträgern in Laptops

c) Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

d) Trennungskontrolle/Maßnahmen zur Zwecktrennung von Daten

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

- Für jeden Kunden wir eine eigene Instanz installiert
- Festlegung von Datenbank-Rechten
- Trennung von Produktiv- und Testsystem

2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

a) Weitergabekontrolle/Sicherheit beim Datentransfer

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- Einrichtung von Standleitungen bzw. VPN-Tunneln
- Auf Server wird mittels HTTPS zugegriffen
- E-Mail-Verschlüsselung auf dem Transportweg (TLS)

b) Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

- Protokollierung der Eingabe, Änderung und Löschung von Daten

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

a) Verfügbarkeitskontrolle/Schutz von Daten vor zufälliger Zerstörung und Verlust

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- und Recoverykonzepts

b) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c EU-DSGVO)

- Wiederherstellung nach Backup- und Recoverykonzept
- Teste von Datenwiederherstellung

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

a) Datenschutz-Management

- Die Grundsätze zum Datenschutz (Erhebung, Verarbeitung oder Nutzung personenbezogener Daten) sind in einer unternehmensinternen Richtlinie festgelegt
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit
- Schulung von Mitarbeitern
- Das Verzeichnis der Verarbeitungstätigkeiten ist vorhanden

b) Incident-Response-Management

- Einrichtung eines Incident Management-Plans
- Sicherheitsteam ist benannt und geschult

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)

- Beachtung privacy by design
- Beachtung privacy by default

d) Auftragskontrolle/Einbindung von Unter-Auftragsverarbeiter

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 EU-DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit
- Auftragsverarbeiter hat Datenschutzbeauftragten benannt (wenn erforderlich)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber Auftragsverarbeiter vereinbart

Unterauftragsverarbeiter

der

Smartrplace GmbH
Ludwig-Erhard-Straße 8
34131 Kassel

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
(Hosting der Server / primäres Rechenzentrum)

netcup GmbH
Daimlerstraße 25
D-76185 Karlsruhe
(Hosting der Server / sekundäres Rechenzentrum)