Anlage 1- Technische und organisatorische Maßnahmen

§ 1 Allgemeine Informationen

a) Geltungsbereich

Dieses Dokument ist Teil der Datenschutzdokumentation des Datenschutzmanagements von Outdooractive. Aufgrund der Vereinfachung der Darstellung wird im Folgenden für alle Rollen-, Stelle- und Funktionsbezeichnungen die männliche Form, stellvertretend für die weibliche und männliche Schreibweise, verwendet.
Dieses Dokument gilt für die informationsverarbeitenden Systeme und Netzwerke, Dokumente und Informationen von Outdooractive, mit denen personenbezogene Daten erhoben, verarbeitet genutzt und gespeichert werden.
Diese Version des Dokumentes ersetzt alle früheren Versionen und Ausgaben. Sollten vertragliche oder gesetzliche Festlegungen dieses Dokumentes oder Teile hiervon berühren, haben diese in jedem Fall Vorrang. Die Aktualisierung und Weiterentwicklung dieses Dokumentes obliegt dem Datenschutzbeauftragten von Outdooractive. Der Ausdruck dieses Dokumentes mit dem Vermerk „Original“ stellt eine gelenkte Kopie dar und unterliegt dem Änderungsdienst.
Die nachfolgende Auflistung dient nur der erläuternden Darstellung gesetzlicher Anforderungen in Bezug auf den Datenschutz. Die Rechte und Pflichten der Parteien ergeben sich allein aus den vertraglichen Vereinbarungen und den gesetzlichen Bestimmungen zum Datenschutz. Insofern können aus dieser Liste keine Ansprüche abgeleitet werden. Technische Änderungen und/oder Änderungen in der Organisation, die keinen Einfluss auf die Erfüllung der gesetzlichen Anforderungen der Datenschutzgrundverordnung in der jeweils aktuellen Fassung haben, bedürfen keiner gesonderten Information gegenüber dem Vertragspartner. Die angegebenen Punkte können je nach Vertrag variieren. Die Weitergabe an Dritte oder Veröffentlichung ist untersagt. Nur gültig für Vertragskunden.

b) geprüftes Rechenzentrum

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen

c) Unterauftragnehmer

Hetzner Finland Oy

§ 2 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

Outdooractive GmbH & Co. KG
Missener Str. 18
87509 Immenstadt

Maßnahmen:

Verantwortlich für die Zutrittskontrolle beim Auftragnehmer ist eine Abteilung beim Auftragnehmer, wobei der/die IS-/IT-Sicherheitsbeauftragte/r die zu sichernden Objekte und Bereiche beim Auftragnehmer festlegt. Es gibt ein dokumentiertes Verfahren für die Vergabe/Entzug von Zutrittsrechten.

Niemand, der nicht beim Auftragnehmer angestellt ist, verfügt über Zutrittsberechtigungen.
Die Eingangstüren und Nebentüren sind gesichert, so dass ein Schutz vor unbemerktem Betreten/Verlassen der Gebäude besteht.
Externe werden in den Gebäuden beaufsichtigt.
Besucher zum Besuchten werden begleitet bzw. von ihm abgeholt.
Fenster und nach außen gehende Türen werden verschlossen, wenn die Räume, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, nicht besetzt sind.
Nur IT-Systemtechniker und die Geschäftsführung dürfen die Serverräume betreten.
Die Haustechnik, das Infrastrukturteam und die IT-Systemtechniker dürfen das Rechenzentrum betreten. Die Serverräume und das Rechenzentrum sind vor dem Zutritt unberechtigter Personen, insbesondere auch außerhalb der Geschäftszeiten geschützt.
Der Zutritt zu DV-, TK-Systemen wird durch eine Schlüsselregelung für Unbefugte verwehrt.
Es werden schädigende Umgebungseinflüsse in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, bei der Installation und der Benutzung von IT-Komponenten beachtet.

§ 3 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Die Zugangskontrolle verhindert das Endringen Unbefugter in Datenverarbeitungs- (folgend: DV) Systeme. Insbesondere darf auch kein externer Zugang, z. B. über das Internet auf Datenverarbeitungsanlagen erfolgen (Hackerschutz).
Um die DV-Anlage vor Eindringlingen zu schützen, werden Verfahren der Identifikation und Authentifikation eingesetzt, welche den Zugang steuern:
Die Anmeldung erzwingt vor Zugriff auf Daten oder Programme die Eingabe eines persönlichen Passwortes verbunden mit einer Benutzerkennung (User – ID). Der Erstanmeldung folgt eine sofortige Passwortänderung. Die Mitarbeiter sind darauf hingewiesen worden, das Passwort regelmäßig zu wechseln.
Um die Entdeckung des Passwortes zu erschweren, ist eine minimale Länge von 8 Zeichen vorgegeben. Die Mitarbeiter/innen, die Daten des Auftraggebers verarbeiten/speichern sind aufgefordert, komplexe Passwörter einzusetzen. Für die Mitarbeiter/innen, die Daten des Auftraggebers verarbeiten und/oder speichern bzw. Systeme betreuen, bestehen Hinweise über den Umgang mit administrativen Passwörtern. Es besteht darüber hinaus eine Passwortrichtlinie, die die Struktur eines Passwortes, sowie Änderungsintervalle und die Nutzung beschreibt. Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort. Die Passwörter für die IT-Systeme /Nutzer werden nur verschlüsselt abgespeichert oder übertragen. Die Administrativpasswörter für die IT-Systeme und die Schlüssel für die Kryptographie-Verfahren werden gesichert aufbewahrt.
Protokolle hinsichtlich etwaiger Unregelmäßigkeiten werden manuell ausgewertet.

Die IT-Systeme werden gegen unbefugte Nutzer wie folgt abgesichert:

-Standleitung
-Teilnehmerkennung
-2-Faktor-Authentifizierunng
-funktionelle Zuordnung einzelner Datenendgeräte
-Protokollierung der Systemnutzung und Protokollauswertung.

Mobile PC’s, die Daten des Auftraggebers verarbeiten bzw. speichern werden außerhalb der Bürozeiten unter Verschluss gehalten. Die Identifizierung an IT-Systemen findet über die „Active

Directory Domäne“ und die Authentifizierung über den Benutzer und das dazugehörige Passwort statt.

Die Zugangsberechtigungen bei den IT-Systemen berechtigt das Rechenzentrum

Hetzner Online GmbH
Industriestr 25
91710 Gunzenhausen,

Die Einstellungen im BIOS-Setup werden vom IT-Administrator vorgenommen und der unbefugte Zugang zum BIOS-Setup ist nicht möglich.
Bei Arbeitsunterbrechungen wird ein passwortgeschützter Bildschirmschoner aktiviert.

§ 4 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Eine wirksame Zugriffskontrolle setzt eine geordnete Prüfung und Vergabe von Berechtigungen voraus. Die Zugriffskontrolle soll die unerlaubte Tätigkeit in DV – Systemen außerhalb eingeräumter Berechtigungen verhindern. Personenbezogene Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden.
Die Datenträger werden vor unbefugten Lesen, Kopieren, Verändern oder Entfernen durch eine Verschlüsselung geschützt und es gibt einen Verantwortlichen für die Datenträgerverwaltung. Die Datenträger werden außerhalb der Arbeitszeiten in verschließbaren Schränken und an der Datenträgerverarbeitungslage aufbewahrt. Die Datenträgerverwaltung wird durchgeführt, indem der Mitarbeiter den Datenträger bei seinem Abteilungsleiter holt und dieser den Vorgang überwacht.
Weiterhin wird durch eine Zugriffskontrolle sichergestellt, dass Mitarbeiter/innen nur auf Programme und Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen („Need-to-know-Prinzip“). Durch eine automatische Prüfung der Zugriffsberechtigung wird die Einschränkung der Zugriffsmöglichkeit der zur Benutzung eines IT-Systems Berechtigten auf ausschließlich die seiner Zugriffsberechtigung unterliegenden Daten gewährleistet.
Die differenzierte Zugriffsberechtigung ist dabei in Dateien, Datensätze, Datenfelder, Anwendungsprogramme, Betriebssystem und Server/IT-System aufgeteilt.
Die differenzierten Verarbeitungsmöglichkeiten sind in Lesen, Ändern und Löschen aufgeteilt.
Nutzer können nur auf getestete und freigegebene Anwendungssoftware zugreifen.
Die Zugriffsrechte für IT-Systeme werden nur auf Veranlassung der Geschäftsleitung vergeben. Die Geschäftsleitung genehmigt auch die Zugriffsberechtigung auf Daten und Applikationen.
Die Zugriffsberechtigungen im System vergibt der IT-Administrator, wobei Zugriffsrechte dokumentiert und alle drei Monate überprüft werden. Eine genehmigte Konfigurationsänderung darf nur der IT-Administrator vornehmen.

§ 5 Weitergabe Kontrolle/ Übermittlungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Die Weitergabe Kontrolle soll verhindern, dass personenbezogene Daten bei der elektronischen Übertragung unbefugt gelesen, kopiert, verändert oder entfernt werden.
Dies gilt auch für Dialogverarbeitung und Auftragsverarbeitung.
Es besteht ein Verbot der Mitnahme von Behältnissen in Räume mit DV-Anlagen oder in Datenträgerarchive und das Mitbringen privater Datenträger ist untersagt.
Unbenutzte Datenträger befinden sich in einem verschlossenen Behältnis.
Magnetische Datenträger werden durch mehrfaches Überschreiben durch ein sicheres Verfahren vernichtet. Optische Datenträger und defekte Festplatten werden durch physische Vernichtung und Papier/Mikrofilm durch einen bereitgestellten Aktenvernichter vernichtet.
Sowohl Datenträger als auch mobile Endgeräte und Datenübertragungsleitungen mit sensitivem Inhalt gem. Art. 32 DS-GVO, die zum Transport vorgesehen sind, werden verschlüsselt.
Das Internet wird zur Weitergabe von personenbezogenen Daten genutzt, wobei die Dienste, die dabei genutzt werden, E-Mail, WWW und elektronischer Geldverkehr sind. Sicherungsmechanismen, die dazu verwendet werden, sind beim WWW die Verschlüsselung mit „https“ oder „SSL/TLS“, alle Protokolle werden via VPN/IPsec und der elektronische Geldverkehr wird nach HBCI PIN TAN gesichert.
Als Sicherheitsmaßnahmen werden eine Firewall, ein Intrusion Detection System (IDS), ein Intrusion Prevention System (IPS) und ein Virtual Private Network (VPN) eingesetzt.
Durch eine Dokumentation der Übermittlungsstellen und –wege kann überprüft und festgestellt werden, an welche Stellen Datenübermittlung durch Einrichtung zur Datenübertragung vorgesehen ist.
Die IT-Systeme befinden sich in einem verschlossenen Raum und die Server-Konsolen sind gesperrt.
Weiterhin gibt es ein Berechtigungskonzept, in dem Netzwerkfreigaben und Zugriffsberechtigungen auf Ordner und Dateien für einzelne Benutzergruppen festgelegt sind. Dieses Konzept wird regelmäßig geprüft und aktualisiert.
Bei der Versetzung eines Mitarbeiters werden die nicht mehr benötigten Zugangsberechtigungen entzogen und bei Ausscheiden eines Mitarbeiters werden die Zugänge zu den IT-Systemen gesperrt.
Es wird die Möglichkeit zur Fernwartung fallbezogen durch den Netzwerkadministrator freigegeben.
Die Fernwartung erfolgt aufgrund einer vertraglichen Regelung und nur der Netzwerkadministrator baut die Fernwartungsverbindung zwischen den IT-Systemen und dem externen Dienstleistr auf. Bei der Fernwartung gibt es eine Schutzfunktion, welche kennwortgesteuert ist, gegen den Zugriff eines externen Dienstleisters auf Daten/Informationen der verantwortlichen Stelle.

§ 6 Eingabekontrolle/Plausibilitätskontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Die Eingabekontrolle soll Eingabe, Veränderung oder Entfernung personenbezogener Daten nachträglich überprüfbar machen und eine userbezogene Zuordnung von Aktivitäten gewährleisten.
Es gilt die Ursache einer Verfälschung zu ermitteln und die Integrität der Daten wiederherzustellen.
Durch eine Protokollierung eingegebener Daten und eine Verarbeitungskontrolle (Transaktionskontrolle) der Anwendung kann nachträglich überprüft und festgestellt werden, ob und von wem Daten in die IT-Systeme eingegeben, verändert oder entfernt worden sind. Es gibt einen Schadsoftwareschutz und mit diesem und einem Prüfsummenprogramm wird täglich die Integrität der Partitionstabelle, des Bootsektors, des Hauptverzeichnisses und aller Programmdateien geprüft.
Ein Update des Schadsoftwareschutzes erfolgt automatisch und täglich und sicherheitsrelevante Updates und Patches für die Betriebssysteme und Anwendungsprogramme erfolgt innerhalb von sieben Tagen nach der Veröffentlichung durch den Hersteller.

Die Daten und Programme werden in unterschiedlichen Verzeichnissen und unterschiedlichen Partitionen abgespeichert.
Es besteht eine vollständige und aktuelle Netzwerksdokumentation.
Die durchgeführten Wartungs-, Fernwartungs- oder Reparaturarbeiten werden dokumentiert und die Integrität von Datenträgern von externen Dienstleistern werden überprüft, bevor diese eingesetzt werden. Vor größeren Wartungs-, Fernwartungs- oder Reparaturarbeiten wird eine komplette Sicherung der betroffenen Systeme erstellt und der Fernwartungsvorgang wird durch einen Mitarbeiter der IT-Abteilung dauerhaft überprüft oder aufgezeichnet. Nach den durchgeführten Wartungs-, Fernwartungs- oder Reparaturarbeiten findet eine Integritätsprüfung statt.

§ 7 Auftragskontrolle/Vertragskonformitätskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Durch eine Protokollierung eingegebener Daten und einer Verarbeitungskontrolle (transaktionsbasiert) kann nachträglich überprüft und festgestellt werden, ob und von wem Daten in die IT-Systeme eingegeben, verändert oder entfernt worden sind.
Durch das Angebot und die Auftragsbestätigung wird gewährleistet, dass die Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers erfolgt. Sollten sich Änderungen im Verfahrensablauf/Programmänderungen durch den Auftragnehmer ergeben, werden diese im Verarbeitungsverzeichnis dokumentiert.
Zur Sicherung der Fernwartung/Fernadministration wird eine Ereignisauslösung vom Auftraggeber angewandt.

§ 8 Verfügbarkeitskontrolle

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

Die Verfügbarkeitskontrolle soll personenbezogene Daten gegen zufällige Zerstörung oder vor Verlust schützen. Mögliche Gefahren sind Wasserschäden, Blitzschlag, Brand, Sabotage oder Diebstahl.
Durch ein tägliches Backup, eine Festplattenspiegelung (RAID o.ä.), eine unterbrechungsfreie Stromversorgung (USV), einen Überspannungsfilter und eine vorliegenden Backup-Plan wird gewährleistet, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Es gibt ein Notfall und Krisenmanagement (BCM).
Zuständig für die Sicherung der Daten ist der Backup-Administrator und eine entsprechende Regelung ist vorhanden. Es existieren zwölf Generationen von Sicherungskopien und die Datensicherung wird täglich durchgeführt. Es wird auch eine regelmäßige Sicherung von datenverarbeitenden mobilen Endgeräten gewährleistet. Das allgemeine Backup-Verfahren wird regelmäßig kontrolliert und dokumentiert. Es werden Sicherungsprotokolle erstellt und geprüft. Als Backup-Methode wird die Totalsicherung, Selektivsicherung (nur Datenbestände) und die Sicherung veränderter Daten angewandt. Die Backup-Medien werden in einem Safe/Tresor, welches sich in einem anderen Gebäude befindet, aufbewahrt. Die gesetzlichen Aufbewahrungsfristen werden beachtet. Die gesetzlichen Vorgaben zur Löschung, Einschränkung und dem „Recht auf Vergessenwerden“ werden eingehalten.
Die E-Mails, die die Geschäftsbeziehung mit dem Auftraggeber betreffen bzw. Daten enthalten, die für die Vertragsabwicklung notwendig sind, werden regelmäßig archiviert. Die Archivierung der E-Mails erfolgt automatisch durch das Programm Mailstore. Das Archivsystem ist zertifiziert.
Als störende Einflüsse bestehen beim Auftragnehmer Hitze, Kälte und Feuchtigkeit und Stromausfall oder Stromschwankungen während des laufenden Betriebs in den Räumen bzw. Gebäuden, in denen

der Auftragnehmer Daten des Auftraggebers verarbeitet. Diese werden jedoch bei der Installation und der Benutzung der IT-Systeme beachtet. In den Serverräumen gibt es keine wasserführenden Leitungen oder leicht brennbare oder entzündliche Gegenstände. In den Serverräumen ist eine Klimaanlage installiert, was der technischen Spezifikation entspricht. Ein zuständiger Mitarbeiter wird per SMS bei einem Alarmsignal eines Sensors über den kritischen Zustand in den Serverräumen des Rechenzentrums informiert. Die Erreichbarkeit eines zuständigen Mitarbeiters im Katastrophenfall ist jederzeit durch eine Rufbereitschaft gewährleistet. Es bestehen Eskalationspläne und die Serverräume sind vor Einbruch ausreichend geschützt. Die Server stehen in 19‘‘-Racks und die Serverräume sind durch eine normale und eine feuersichere Tür ausgestattet. Verfahrensfremde Datenträger werden mit eindeutiger Zuordnung verwaltet. Es existiert ein eigener Archivraum zu dem nur ein beschränkter Zugang besteht und das Mitnehmen von Taschen und Mänteln, Telefonen, Fotoapparaten und anderen elektronischen Geräten in die Sicherheitszone (Archiv) untersagt ist. Die IT-Leitung und der IT-Administrator sind für die Einhaltung von Wartungsintervallen, der Auswahl und Beauftragung von Wartungsunternehmen verantwortlich.

§ 9 Datentrennungskontrolle/Mandantentrennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Die Datentrennung soll gewährleisten, dass personenbezogene Daten, welche zu unterschiedlichen Zwecken erhoben wurden, getrennt bearbeitet werden. Die Beachtung der Zweckbindung im Umgang mit personenbezogenen Daten erfordert technische und organisatorische Maßnahmen zur systematischen Trennung der Daten.
Durch einen softwareseitigen Ausschluss (Mandantentrennung), einem Datenbankprinzip (Trennung über Zugriffsregelungen) und eine eigene Datenbankinstanz wird gewährleistet, dass die zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Bei Test und Produktivsystemen ist aus Anforderungen an die Reproduzierbarkeit von Softwarefehlern in Zusammenhang mit bestimmten Datenständen es nicht möglich, Daten im vollen Rahmen zu trennen.

§ 10 Prüfung der Betriebsorganisation und Rechenschaftspflicht

Maßnahmen, die die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht werden:

Es ist ein Verfahrensregister beim Auftragnehmer vorhanden, welches vollständig und aktuell ist.
Es liegen Nachweise über durchgeführte Schulungen der Mitarbeiter zum Datenschutz vor.
Weiterhin liegen Nachwiese über die Einhaltung der datenschutzrechtlichen Verpflichtungen der verarbeitenden Mitarbeiter vor.
Es liegt eine Datenschutzordnung und ein Sicherheitskonzept vor. Das Sicherheitskonzept wird regelmäßig aktualisiert.
Es liegt ein Fachkundenachwies des Datenschutzbeauftragten vor.
Schriftliche Arbeitsanweisungen/Richtlinien/Merkblätter liegen vor. Die Programme/Verfahren werden ordnungsgemäß dokumentiert.
Die Aufbewahrung/Archivierung aller maschinell erzeugten Protokolle ist geregelt.
Es existiert eine Funktionstrennung im IT-Bereich. Abstimm- und Kontrollverfahren sind eingerichtet.
Es ist sichergestellt, dass bei der Übermittlung personenbezogener Daten außerhalb der EU in Drittstaaten ein angemessenes Datenschutzniveau nach Art. 44, 46, 49 DS-GVO eingehalten wird.
Einwilligungen nach Art. 6 Abs. 1 lit. a bis f DS-GVO liegen vor.
Benachrichtigungen, Auskunftsersuchen, Anliegen bezüglich Berichtigung, Löschung oder Sperrung wurden dokumentiert.