Allgemeine Beschreibung der technisch-organisatorische Maßnahmen „TOM“, die es ermöglich zu beurteilen, ob die Maßnahmen nach § 9 BDSG angemessen sind.

1. Technische und organisatorische Sicherheitsmaßnahmen

- Gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

2. Innerbehördliche oder innerbetriebliche Organisation des Auftragnehmers

- Der Auftragnehmer wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

3. Notwendige Kontrollen

- Die nachfolgend beschriebenen Kontrollen beziehen sich auf Dienste für deren Administration und Bereitstellung Convecto ausschließlich verantwortlich ist (bspw. Cloud-Dienste wie Hosted Exchange, SharePoint oder shared Webhosting). Sofern Convecto dem Kunden Dienste bereitstellt, die dem Kunden volle Administrationsrechte auf Serversysteme einräumen (bspw. virtuelle oder dedizierte Server) gelten diese Ausführungen nur eingeschränkt, da der Kunde in erster Linie selbst für die Absicherung, Wartung, Datenablage, -verwaltung und -sicherung verantwortlich ist, sofern keine andere vertragliche Vereinbarung geschlossen wurde. Allerdings wird Convecto, sofern der Kunde einen administrativen Zugang auf seine Systemen zu Wartungszwecken der Convecto eingerichtet hat, anfallende Arbeiten gemäß der folgend beschriebenen Maßgaben vornehmen.

4. Beschreibung der notwendigen Kontrollen

- Zutrittskontrolle
  Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
- Zugangskontrolle
  Es ist zu verhindern, dass Datenverarbeitungs-systeme von Unbefugten genutzt werden können.
- Zugriffskontrolle
  Es ist zu 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

cloudshift® | Convecto GmbH
http://cloudshift.io Ludwigstr. 180d | Heyne Fabrik | 63067 Offenbach | Germany
info@cloudshift.io Geschäftsführer: Julian M. Flockton | Markus Zebisch
t +49 69.1 75 37 34-60 Amtsgericht Offenbach | HRB 45375 | Ust.-ID: DE 212 131 139

nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Weitergabekontrolle
  Es ist zu gewährleisten, dass personen-bezogene 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.
- Eingabekontrolle
  Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind.
- Auftragskontrolle
  Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
- Verfügbarkeitskontrolle
  Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
- Trennungskontrolle
  Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

5. Konkretisierung der Einzelmaßnahmen

Zutrittskontrolle

- Der Betrieb sämtlicher Convecto IT-Infrastrukturen erfolgt in deutschen Hochsicherheitsrechenzentren, die nach der IT-Sicherheitsnorm ISO 27001 zertifiziert sind. Dies umfasst unter anderem folgende Zutrittssicherungsmaßnahmen:
- Sicherheitsdienst vor Ort überwacht das Gelände und die Gebäude (24x7 Überwachung)
- Videoüberwachung des Gelände
- Videoüberwachung der Gebäude im Innern
- Abgeschlossenes Gelände mit Zutritt nur für berechtigte Personen
- Nur explizit befugte Personen haben Zugang zu den Serverräumen; Zugänge sind auf ein Mindestmaß beschränkt
- Zutrittskontrollmaßnahmen zu den Gebäuden und Serverräumen:
  - Vereinzelungsanlage (Schleuse)
  - Schlüsselsystem basierend auf Magnetkarten
  - Biometrisches Kontrollsystem (Fingerabrücke)
- Zutrittskontrolle basiert auf einer dokumentierten Security-Policy

CloudShift® | Convecto GmbH
http://cloudshift.io Ludwigstr. 180d | Heyne Fabrik | 63067 Offenbach | Germany
info@cloudshift.io Geschäftsführer: Julian M. Flockton | Markus Zebisch
t +49 69.1 75 37 34-60 Amtsgericht Offenbach | HRB 45375 | Ust.-ID: DE 212 131 139

- Zutrittsberechtigungen werden innerhalb des Rechenzentrums nach unterschiedlichen Sicherheitszonen differenziert
- Erteilung von Zutrittsberechtigungen erfolgt revisionsfähig durch eine Stelle außerhalb des Rechenzentrums
- Ständige lückenlose Protokollierung aller Zu- und Abgänge
- Protokollierte Daten werden regelmäßig nach versuchten Sicherheitsverletzungen ausgewertet
- Zuständigkeit zur Auswertung der Log-Informationen ist eindeutig geregelt und die Informationen unterliegen einer strengen Zweckbindung
- Verwaltung und Wartung der Zutrittssysteme ist eindeutig geregelt
- Nach außen führenden Türen und Fenster der Gebäude sind auf die unbedingt nötigste Anzahl beschränkt; Fenster sind mit Splitterschutzfolie versehen und Serverräume verfügen über keine Fenster. Fenster und Türen sind mit Erschütterungs- und Öffnungsmeldern ausgestattet

Zugangskontrolle

- Passwortschutz von Serversystemen, Administrationssystemen und datenhaltenden Systemen
- Dokumentierte Passwort-Richtlinie über Anforderungen an sichere Passwörter
- Zugriff zur Administration erfolgt durch Convecto nur über verschlüsselte Verbindungen gemäß aktuellem Stand der Technik
- Begrenzung der Administrationszugänge ausgehend von definierten Netzwerksegmenten
- Reduktion der zugriffsberechtigten Personen auf ein Minimum
- Protokollierung von Logon-Vorgängen
- Systeme werden durch Firewalls geschützt

Zugriffskontrolle

- Zugriff auf datenhaltende Systeme erfolgt erst nach erfolgreicher Authentifizierung des Benutzers mittels Benutzerkennung und Passwort.
- Zugriff zur Administration erfolgt durch Convecto nur über verschlüsselte Verbindungen gemäß aktuellem Stand der Technik
- Reduktion der zugriffsberechtigten Personen auf ein Minimum
- Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.
- Protokollierung von Logon-Vorgängen
- Systeme werden durch Firewalls geschützt

CloudShift® | Convecto GmbH
http://cloudshift.io Ludwigstr. 180d | Heyne Fabrik | 63067 Offenbach | Germany
info@cloudshift.io Geschäftsführer: Julian M. Flockton | Markus Zebisch
t +49 69.1 75 37 34-60 Amtsgericht Offenbach | HRB 45375 | Ust.-ID: DE 212 131 139

_ Zugriff auf die Systeme, die personenbezogene Daten gespeichert haben können, erfolgt durch Administratoren. Ein differenziertes Benutzerberechtigungssystem, das den Administratoren keinen Zugriff auf die personenbezogenen Daten gibt, ist technisch leider nicht möglich. Eine Datenverschlüsselung der personenbezogenen Daten in diesem Bereich ist nicht möglich.

Weitergabekontrolle

_ Auf alle Systeme, die vertrauliche Daten gespeichert haben, wird ausschließlich über gesicherte Übertragungswege (bspw. VPN oder HTTPS) zugegriffen. Abgesehen von den Administratoren ist kein Benutzer der Convecto dazu in der Lage personenbezogene Daten über hierfür vorgesehene Prozeduren der Programme zu exportieren und damit weiterzugeben.
_ Die Löschung oder Entsorgung der Daten erfolgt nach Ablauf der gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen.

Eingabekontrolle

_ Convecto erhebt, verändert oder löscht personenbezogene primär im Rahmen der eigenen Kundenverwaltungssysteme. Eine Verarbeitung, der durch den Kunden bei Convecto im Rahmen der bereitgestellten Dienstleistung gespeicherten Daten durch Convecto Mitarbeiter erfolgt nicht.
_ Sofern personenbezogene Daten durch Convecto Mitarbeiter eingegeben, verändert oder gelöscht werden, erfolgt dies ausschließlich über personalisierte Zugänge der Mitarbeiter der Convecto. Durchgeführte Aktionen der Mitarbeiter werden mit der Mitarbeiterkennung, Zeitstempel und der durchgeführten Änderung protokolliert.

Auftragskontrolle

_ Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.
_ Die Löschung oder Entsorgung der Daten erfolgt nach Ablauf der gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen.
_ Sofern Dritte Dienste im Rahmen der durch Convecto bereitgestellten Leistungen erbringen, sind diese und deren Mitarbeiter auf die deutschen Datenschutzbestimmungen vertraglich verpflichtet gemäß BDSG, sind geeignete Geheimhaltungspflichten vertraglich vereinbart, die Dienste werden

CloudShift® | Convecto GmbH
http://cloudshift.io Ludwigstr. 180d | Heyne Fabrik | 63067 Offenbach | Germany
info@cloudshift.io Geschäftsführer: Julian M. Flockton | Markus Zebisch
t +49 69.1 75 37 34-60 Amtsgericht Offenbach | HRB 45375 | Ust.-ID: DE 212 131 139

ausschließlich in Deutschland erbracht gemäß deutschen Rechtsnormen und es werden regelmäßig materielle Überprüfungen über die Einhaltung dieser Bestimmungen durchgeführt.

Verfügbarkeitskontrolle

- Der Betrieb sämtlicher Convecto IT-Infrastrukturen erfolgt in deutschen Hochsicherheitsrechenzentren, die nach der IT-Sicherheitsnorm ISO 27001 zertifiziert sind.
- Räume sind an das Brand- und Raumüberwachungssystem angeschlossen
- DV-Räume sind als ein eigener, geschlossener Brandabschnitt (Wände F90, Türen T90, meist auch nur T30, Fenster B2) ausgestaltet
- Decken und Wände der DV-Räume wasserundurchlässig (Schutz gegen Löschwasser und Restfeuchte der Wände)
- Feuchtigkeitsfühler sind im Doppelboden der DV-Räume installiert und die Funktionsfähigkeit dieser Sensoren wird regelmäßig überprüft
- Wasserführende Leitungen sind durch Rückstau- und Lecksicherungsventile abgesichert
- Klimatisierung
    - Die Klimaanlagen sind in gesicherten Räumen untergebracht
    - Wasserfühler und Gassensoren sind in den Klimaanlagen installiert
    - Einrichtungen zur Überwachung der Temperatur und der relativen Luftfeuchtigkeit sind in den Rechnerräumen vorhanden
    - Für die Klimaanlagen sind Wartungsverträge abgeschlossen
- Stromversorgung
    - Ständige Überwachung der Stromversorgung
    - Absicherung der Stromverfügbarkeit über zwei verschiedene Stromschienen (A und B Stromversorgung)
    - USV und Diesel-Generatoren sowie Kraftstoff zur Sicherstellung der Notstromversorgung vorhanden
    - Räume der USV und Dieselgeneratoren sind ausreichend gesichert
    - USV-Anlagen und Diesel-Generatoren werden regelmäßig gewartet
- Brandfrüherkennung und -bekämpfung
    - Rauchmelder
    - Frühwarnsystem mit automatischen Brandmeldern (Ionisations- oder Rauchmelder) im Doppelboden, in der Decke sowie in den Zu- und Rücklaufkanälen der Klimaanlage installiert
    - Es wird ein sog. Zwei-Schleifen-Detektionssystem zur Vermeidung von Fehlalarmen eingesetzt

CloudShift® | Convecto GmbH
http://cloudshift.io Ludwigstr. 180d | Heyne Fabrik | 63067 Offenbach | Germany
info@cloudshift.io Geschäftsführer: Julian M. Flockton | Markus Zebisch
t +49 69.1 75 37 34-60 Amtsgericht Offenbach | HRB 45375 | Ust.-ID: DE 212 131 139

- Es werden ausschließlich Löschmittel in den Flutungsanlagen eingesetzt, die für IT-Systeme unschädlich sind
- Alarmmeldungen der Brandmeldeanlage werden an eine ständig besetzte Stelle weitergegeben
- Umfeld des DV-Bereichs ist in das Brandfrüherkennungs- und -bekämpfungssystem mit einbezogen
- Brandmeldeanlage regelmäßig gewartet

- Sicherheit
  - Die Räume, in denen sich die Klima- und USV-Anlagen befinden, sind in den Brand- und Einbruchsschutz mit einbezogen
  - durchgängige Außenhautsicherung des Rechenzentrums vorhanden
  - mehrstufige Sicherheitsbarrieren, damit ein Eindringling mehrere Hürden zu überwinden hat
    - Abgesperrtes Gelände
    - Gegensprechanlagen
    - Vereinzelungsanlagen
    - Elektrische Türöffnung
    - Biometrische Zugangssysteme
    - Videoüberwachung
- Datensicherung
  - Sofern je nach bereitgestellter Leistung Convecto für eine Datensicherung verantwortlich ist, wird diese im Einklang mit der jeweiligen Leistungsbeschreibung der Dienstleistung erbracht. Hierbei variieren die Sicherheitsbestimmungen je nach Dienstleistung. Es wird hierbei unterschiedenen, ob die gesicherten Daten im gleichen Brandabschnitt wie die Produktivsysteme gespeichert werden oder in einem baulich getrenntem Rechenzentrum. Die Datensicherung erfolgt mindestens täglich und die Aufbewahrung der Daten erfolgt im Minimum für 7 Kalendertage. Es erfolgen regelmäßige Stichprobentests, ob erfolgte Datensicherungen eine Rücksicherung der Daten erlauben.
  - Datensicherung nach Dienstleistungsart:
    - Webhosting: gleicher Brandabschnitt
    - Virtuelle Server: gleicher Brandabschnitt
    - Hosted Exchange, Hosted Sharepoint, E-Mail Archivierung: getrenntes RZ
    - Dedizierte Server, Co-Location / Housing, individuelle Projekt: Durchführung der Datensicherung und die damit verbundenen Sicherheitsanforderungen werden individuell vereinbart

CloudShift® | Convecto GmbH
http://cloudshift.io Ludwigstr. 180d | Heyne Fabrik | 63067 Offenbach | Germany
info@cloudshift.io Geschäftsführer: Julian M. Flockton | Markus Zebisch
t +49 69.1 75 37 34-60 Amtsgericht Offenbach | HRB 45375 | Ust.-ID: DE 212 131 139

Trennungskontrolle

- Personenbezogene Daten können ausschließlich im Rahmen der Ablage durch den Kunden auf dem zur Verfügung gestellten Speicherplatz/ Systemen, für die Nutzung der Dienste durch den Kunden oder in Ausnahmefällen in dem ERP System / Kundenverwaltungsportal bei Convecto gespeichert werden. In den ersten beiden Fällen werden die Daten zwar separat gespeichert, jedoch haben zugriffs-berechtigte Personen (Administratoren) auf beide Datenspeicher Zugriff. Eine getrennte Erhebung oder Auswertung der Daten ist möglich. Im letzteren Fall haben nur Personen Zugriff auf die Daten, die über entsprechende Berechtigungsstufen im ERP System der Convecto verfügen.

CloudShift® | Convecto GmbH
http://cloudshift.io Ludwigstr. 180d | Heyne Fabrik | 63067 Offenbach | Germany
info@cloudshift.io Geschäftsführer: Julian M. Flockton | Markus Zebisch
t +49 69.1 75 37 34-60 Amtsgericht Offenbach | HRB 45375 | Ust.-ID: DE 212 131 139