Anlage 1: Technische und Organisatorische Maßnahmen

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
1. Zutrittskontrolle (Räume und Gebäude) *Zielbeschreibung:* Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.	**Maßnahmen im Rechenzentrum:** - Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen. Es bestehen Sichtkontrollen und ein Besucherprotokoll am Empfang, sowie Berechtigtenausweise für die Dauer des Besuchs. - Neben einer Alarmanlage am Eingangsbereich, werden das gesamte Rechenzentrum und die einzelnen Server Videoüberwacht. Im Alarmfall werden die für das Gebäude verantwortlichen Mitarbeiter automatisch alarmiert. - Zusätzlich ist das Gebäude 24/7 durch eigenes Personal besetzt. Diesem Personal werden die Alarmmeldungen angezeigt. Es besteht eine restriktive Zutrittsregelung. **Maßnahmen am Firmensitz:** - Der Eingangsbereich wird Videoüberwacht und die Besucher sowie die Dauer des Besuchs werden protokolliert. - Nur Zugriffsberechtigte besitzen einen Schlüssel für den Serverraum. Die Schlüsselvergabe wurde dokumentiert und sowohl von der Firma als auch vom Besitzer unterzeichnet. - Das Reinigungspersonal wurde sorgfältig ausgewählt und wurde über die Datenschutzregelung informiert. Zudem wurde ein Auftragsverarbeitungsvertrag mit der Reinigungskraft abgeschlossen.

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
2. Zugangskontrolle (IT-Systeme, Anwendungen) *Zielbeschreibung:* Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	An jedem IT-System, das bei Intersolute GmbH im Einsatz ist, muss eine vorherige Authentifizierung erfolgen. Dies erfolgt auf Basis eines Benutzernamens und eines Passworts. Eine Berechtigung zur Nutzung eines IT-Systems oder einer Applikation muss vom jeweiligen Vorgesetzten für einen Mitarbeiter bei der IT-Administration beantragt werden. Es werden nur die Berechtigungen beantragt, die für den Mitarbeiter zwingend erforderlich sind, um seine zugewiesenen Aufgaben zu erfüllen, d. h. die Berechtigungen sind dabei auf das Minimale beschränkt. Technisch erfolgt die Genehmigung für das Erteilen und Löschen von Zugriffsrechten über Ticketsysteme, in denen der Vorgang dokumentiert wird. Bei Aufgabenwechsel des Mitarbeiters wird eine entsprechende Korrektur der Berechtigungen vorgenommen. Sobald ein Mitarbeiter das Unternehmen verlässt, wird die IT-Administration darüber informiert und der Entzug der Berechtigungen erfolgt innerhalb von 24 Stunden nach Ausscheiden des Mitarbeiters.
3. Zugriffskontrolle (auf Daten) *Zielbeschreibung:* Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und das personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Für die Erteilung von Benutzerrechten gilt bei der Intersolute ein Berechtigungskonzept. Dies beinhaltet, dass jeder Mitarbeiter nur die Berechtigungen erhält, die er unmittelbar benötigt, um seine Aufgaben im Unternehmen erfüllen zu können. Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein. Die Vergabe und der Entzug von Berechtigungen werden protokolliert. Eine quartalsweise Überprüfung erfolgt durch die IT-Administration in Zusammenarbeit mit den jeweiligen Vorgesetzten der Mitarbeitet.
4. Eingabekontrolle (in Datenverarbeitungssysteme) *Zielbeschreibung:* Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von	Jede Eingabe von Daten, die im Auftrag des Auftraggebers von der Intersolute GmbH verarbeitet werden, wird systemseitig unter Zuordnung der jeweiligen Benutzerkennung protokolliert. Gleiches gilt für die Änderung und Löschung von Daten. Im Falle einer Änderung von Daten ist aus der Protokollierung erkenntlich, welche Änderungen vorgenommen wurden.

wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.	Die Protokolle werden für die Dauer der Vertragslaufzeit von der Intersolute GmbH gespeichert. Eine vorherige Löschung kann zwischen den Parteien vereinbart werden. Durch die Protokollierung ist jederzeit nachvollziehbar, welche Benutzer Daten eingegeben, geändert oder gelöscht hat.

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
5. Weitergabekontrolle (von Daten) *Zielbeschreibung:* Es ist zu 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.	Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten haben, die im Auftrag verarbeitet werden, beschränkt ist. Ein Kopieren von Daten auf externe Datenträger ist systemseitig unterbunden. Ein Export von Daten wird auf Applikationsebene protokolliert und für einen Zeitraum von 12 Monaten unter Angabe der jeweiligen Benutzerkennung gespeichert. Jeder Zugriff auf und der Abruf von Daten der Applikation erfolgt verschlüsselt (TLS). Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch die Intersolute GmbH übergeben werden soll, werden die Parteien im Vorwege eine Verschlüsselungsmethode bzw. einen Weg der sicheren Übertragung vereinbaren.
6. Verfügbarkeitskontrolle (von Daten) *Zielbeschreibung:* Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	**Rechenzentrum:** *Keine Lagehinweise* Um die Sicherheit des Standorts der Rechenzentren zu gewährleisten, befinden sich am Gebäude keine Hinweise zum Rechenzentrum. *Protokolliertes Zugangssystem* Jeder Zutritt einer Person ins Rechenzentrum wird durch das Zugangssystem mit Kartenleser protokolliert. Somit ist schriftlich nachweisbar, ob und welche Personen sich im Rechenzentrum befinden. *Cages und Racks mit Zahlencode* Die Cages und Racks der Rechenzentren sind zusätzlich durch Zahlenschlösser gesichert. Dadurch sind die einzelnen Racks auch vor Zugriff durch Zutrittsberechtigte Personen des Rechenzentrums gesichert. *Auslegung der Räume als Brandabschnitt* Die Räume des Rechenzentrums sind in Brandabschnitte gegliedert, sodass diese separaten Serverräume zusätzlich vor Brandfällen geschützt sind.

	Argon-Gaslöschanlagen im Data Center Das innere des Rechenzentrums wird von Argon-Gaslöschanlagen geschützt. *Feuersichere Raumzellenbauweise nach F120 und F90* Gemäß der Brandschutzverordnung für Gebäude sind die Räume und Wände gemäß Feuerwiderstandsklasse F120 und F90 erstellt worden. *Überwachung durch Brandmeldeanlage im Gebäude* Die Brandmeldeanlage überwacht das komplette Gebäude und löst im Brandfall einen direkten Alarm aus. *Kühlleistung im Datacenter* Die Räume des Rechenzentrums werden mit Kühlsysteme effizient gekühlt. Die Klimatisierungssysteme leisten bis zu 2 W pro m² im Rechenzentrum. Die Klimaschränke und Rückkühlwerke sind redundant mit den Rechenzentren verbunden, sodass eine 24/7 Versorgung gewährleistet werden kann. *Ringförmige Anbindung an das 10kV-Netz* Eine ringförmige Anbindung an das Mittelspannungs-Netz der Stadtwerke Düsseldorf versorgt die eigenen Transformator-Anlagen des Rechenzentrums. Die Rechenzentrumsflächen erhalten bis zu 10 kW Anschlussleitung pro Quadratmeter. Die Leitungen der Stromversorgung sind doppelt ausgeführt. *USV- und Netzersatz-Anlagen* Wenn es beim Stromversorger eine Störung geben sollte, setzen USV- und Netzersatzanlagen ein, sie versorgen das Rechenzentrum weiter mit Strom. Die USV- und Netzersatzanlagen haben einen ausreichenden Vorrat an Diesel-Treibstoff, um bei größeren Ausfällen des Energieversorgers weiterhin Strom liefern zu können. *24/7 Betriebsüberwachung der Infrastruktur & Klimatechnik, Objektüberwachung & Videoüberwachung* Sowohl die Rechenzentren als auch das komplette Gelände werden rund um die Uhr durch Videokameras, Rechenzentrums eigenem Personal und zusätzlich von einem externen Sicherheitsdienst, überwacht. Die komplette Stromversorgung und die Klimageräte sowie auch die Rohrleitungen der Anlagen werden rund um die Uhr überwacht um eventuellen Problemen besser entgegentreten zu können.

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
7. Datentrennungskontrolle (zweckbezogen) *Zielbeschreibung:* Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten physikalisch und logisch getrennt voneinander verarbeitet werden.
8. Auftragskontrolle *Zielbeschreibung:* Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der Intersolute GmbH eine hohe Priorität. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet. Es gibt einen betrieblichen Datenschutzbeauftragten, der auch die regelmäßige Schulung der Mitarbeiter plant und durchführt. Alle Mitarbeiter erhalten mindestens eine jährliche Datenschutzschulung bzw. eine „Auffrischung". Mitarbeiter, die an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, sind im Hinblick auf die Verarbeitung der Daten instruiert. Sofern der Auftraggeber ergänzende Weisungen erteilt, wird die Intersolute GmbH alle betroffenen Mitarbeiter unverzüglich über die jeweilige Weisung informieren und Handlungsanweisungen zur Umsetzung geben. Die Datenschutzvorkehrungen der Intersolute GmbH beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Die Intersolute GmbH gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.