Technische und organisatorische Maßnahmen der KONTENT GmbH

Stand: 18.05.2018

1. Allgemeines

Der Auftraggeber und der Auftragnehmer (die KONTENT GmbH) haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten.
Der Auftragnehmer nutzt im eigenen Rechnenzentrum ausschließlich eigene Hardware und richtet sich in jedweder Hinsicht an die einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik. Die KONTENT GmbH hat die nachfolgenden Maßnahmen getroffen.

2. Technisch organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragnehmer hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.
Die Maßnahmen stehen in Übereinstimmung mit dem IT-Sicherheitskonzept und werden regelmäßig vom IT-Sicherheitsbeauftragten überprüft.

2.1 Zutrittskontrolle:

Maßnahmen des Auftragnehmers zur Verwehrung des Zutritts für Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird:

- jedwede Außentüren sind mit einem manuellen und technischen Schließsystem (Sicherheitsschlösser) versehen und grundsätzlich verschlossen
- alle Räumlichkeiten werden überwacht und im Alarmfall der Wachdienst informiert
- die den Mitarbeitern zur Verfügung gestellten Schlüssel sind personengebunden registriert und die Schlüsselausgabe wird quittiert
- der Zutritt ist durch materielle (RFID-Chips und Schlüssel) und geistige (PINs) Identifikationsmerkmale gesichert
- das Zutrittskontrollsystem sowie die Alarmanlage sind über USV gegen Stromausfall gesichert
- der Wachdienst überwacht die Zutritte und meldet unbefugte im 24/7-System
- der Zutritt zu der kundeneigenen Hardware ist ausschließlich durch den Kunden selbst und durch das zuständige Personal möglich
- Besucher können sich nur in Begleitung eines Mitarbeiters in den Räumlichkeiten bewegen
- Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben wird sorgfältig ausgewählt

2.2 Zugriffskontrolle

Maßnahmen des Auftragnehmers zur Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben und Maßnahmen wie

die unerlaubte Tätigkeit in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindert wird:
• die vergebenen Zugriffsrechte orientieren sich an dem aufgabenbedingten und datenschutzrechtlichen Erfordernissen (need-to-know Prinzip)
• die Vorgabe von Passwortrichtlinien inkl. Passwortlänge und Passwortwechsel erfolgt nach den Empfehlungen das BSI
• die Zugriffe auf Anwendungen, Dateien und sonstige Daten (Eingabe, Veränderung und Löschung) werden für mögliche Auswertungen protokolliert
• die Hard- und Software aller technischen Systeme ist durch eine Firewall geschützt
• es bestehen dedizierte Aufbewahrungspflichten
• VPN-Technologie (SSL/TLS) wird eingesetzt
• die Datenträger werden (soweit möglich) verschlüsselt

2.3 Zugangskontrolle
Maßnahmen des Auftragnehmers zur Verhinderung der Nutzung der Datenverarbeitungssysteme durch Unbefugte:
• Mitarbeiter arbeiten ausschließlich mit den personalisiert angelegten Benutzerprofilen, welche die Eingabe eines Passwort erfordern.
• Vorgabe von Passwortrichtlinien inkl. Passwortlänge und Passwortwechsel erfolgt nach den Empfehlungen das BSI
• eine klare Trennung von Produktiv- und Testinfrastruktur
• die Zugriffe auf Anwendungen, Dateien und sonstige Daten (Eingabe, Veränderung und Löschung) werden für mögliche Auswertungen protokolliert
• die Hard- und Software aller technischen Systeme ist durch eine Firewall geschützt
• der Virenschutz (Anti-Virensoftware) wird regelmäßig aktualisiert
• VPN-Technologie (SSL/TLS) wird zur Datenkommunikation und -übertragung eingesetzt

2.4 Trennungskontrolle
Maßnahmen des Auftragnehmers zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können:
• eine klare Trennung von Kundenzugriffen (logische Trennung durch individuelle Benutzerprofile mit Passwortschutz)
• eine klare Trennung von Produktiv- und Testinfrastruktur
• getrennte Verarbeitung zweckgebundener Daten

2.5 Datenintegrität
Maßnahmen des Auftragnehmers zur Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können:
• bei den Betriebssystemen und anderer eingesetzter Software werden alle notwendigen Updates durchgeführt
• bei der Einführung neuer Soft- oder Hardware werden Test- und Freigabeverfahren vor dem Produktiveinsatz durchlaufen
• alle relevanten Systeme sind mit Raid-Controller ausgestattet
• die Störfälle werden prozessual gemeldet und zeitnah behoben
• es bestehen dezidierte Backup- & Recoverykonzepte

2.6 Eingabekontrolle
Maßnahmen zur Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind:

• die Zugriffe auf Anwendungen, Dateien und sonstige Daten (Eingabe, Veränderung und Löschung) werden für mögliche Auswertungen protokolliert

2.7 Verfügbarkeitskontrolle

Maßnahmen des Auftragnehmers zur Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind

• es bestehen dezidierte Backup- & Recoverykonzepte
• die Datenwiederherstellbarkeit wird regelmäßig getestet
• alle relevanten Systeme sind mit Raid-Controller ausgestattet
• es besteht eine unterbrechungsfreie Stromversorgung (USV)
• die Räumlichkeiten sind in Brandabschnitten eingeteilt und jeweils mit Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen, Feuerlöscher) versehen
• die Klimaanlagen sind redundant ausgelegt
• Störfälle werden prozessual gemeldet und zeitnah behoben
• 24/7 Bereitschaft von Mitarbeitern zur Behebung von Störungen
• es werden externe und interne technische Sicherheitsanalysen durchgeführt
• die Stromversorgung wird durch Redundanzen sichergestellt (Notstromaggregate sowie USV Anlagen)
• die Hochwasser- und Erdbebenkritikalität wurde DIN-gerecht geprüft

2.8 Datenträgerkontrolle

Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern:

• die Datenträger (soweit möglich) werden restriktiv eingesetzt und verschlüsselt
• die ausgesonderten Datenträger werden in zutrittskontrollierten Räumen gelagert. Diese werden dann datenschutzkonform gelöscht und entsorgt.
• die Zugriffe auf Anwendungen, Dateien und sonstige Daten (Eingabe, Veränderung und Löschung) werden für mögliche Auswertungen protokolliert

2.9 Speicherkontrolle

Maßnahmen des Auftragnehmers zur Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten:

• die vergebenen Zugriffsrechte orientieren sich an dem aufgabenbedingten und datenschutzrechtlichen Erfordernissen (need-to-know Prinzip)
• die Zugriffe auf Anwendungen, Dateien und sonstige Daten (Eingabe, Veränderung und Löschung) werden für mögliche Auswertungen protokolliert
• die Datenverarbeitungssysteme sind passwortgeschützt
• die Vorgabe von Passwortrichtlinien inkl. Passwortlänge und Passwortwechsel erfolgt nach den Empfehlungen das BSI

2.10 Benutzerkontrolle

Maßnahmen des Auftragnehmers zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

• die Remote Zugriffe auf die Systeme sind durch verschlüsselte, Passphrase- und Zertifikat-gesichert
• die vergebenen Zugriffsrechte orientieren sich an dem aufgabenbedingten und datenschutzrechtlichen Erfordernissen (need-to-know Prinzip)
• die Zugriffe auf Anwendungen, Dateien und sonstige Daten (Eingabe, Veränderung und Löschung) werden für mögliche Auswertungen protokolliert

• die Hard- und Software aller technischen Systeme ist durch eine Firewall geschützt
• der Virenschutz (Anti-Virensoftware) wird regelmäßig aktualisiert

2.11 Übertragungskontrolle
Maßnahmen des Auftragnehmers zur Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:
• VPN-Technologie (SSL/TLS) wird zur Datenkommunikation und -übertragung eingesetzt
• bei der Übertragung von E-Mail-Nachrichten und sonstigen Informationen wird (wenn möglich) verschlüsselt und pseudonymisiert
• die Hard- und Software aller technischen Systeme ist durch eine Firewall geschützt
• der Virenschutz (Anti-Virensoftware) wird regelmäßig aktualisiert

2.12 Transportkontrolle
Maßnahmen des Auftragnehmers zur Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird:
• die Auswahl von Dritten erfolgt sorgfältig
• es exitieren detaillierte vertragliche Regelungen zum Auftragsverhältnis
• im Vertrag mit Dritten werden wirksame Kontroll- und oder Zugriffs- bzw. Löschungsrechte vereinbart
• es erfolgt eine regelmäßige Kontrolle durch den Datenschutzbeauftragten
• VPN-Technologie (SSL/TLS) wird zur Datenkommunikation eingesetzt
• bei der Übertragung von E-Mail-Nachrichten und sonstigen Informationen wird (wenn möglich) verschlüsselt und pseudonymisiert
• beim physischen Transport werden die Transportpersonen und -fahrzeuge sorgfältig ausgewählt

2.13 Wiederherstellbarkeit
Maßnahmen des Auftragnehmers zur Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können:
• es bestehen dezidierte Backup- & Recoverykonzepte
• die Datenwiederherstellbarkeit wird regelmäßig getestet
• alle relevanten Systeme sind mit Raid-Controller ausgestattet

2.14 Zuverlässigkeit
Maßnahmen des Auftragnehmers zur Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:
• Störfälle werden prozessual gemeldet und zeitnah behoben
• 24/7 Bereitschaft von Mitarbeitern zur Behebung von Störungen
• es werden externe und interne technische Sicherheitsanalysen durchgeführt
• bei der Einführung neuer Soft- oder Hardware werden Test- und Freigabeverfahren vor dem Produktiveinsatz durchlaufen
• permanentes Monitoring alle Systeme mit automatischer Auslösung der Notfallprozeduren

2.15 Auftragskontrolle
Maßnahmen des Auftragnehmers zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

• die sorgfältige Auswahl von Dritten geschieht in Zusammenarbeit mit dem Datenschutzbeauftragten
• es existieren detaillierte vertragliche Regelungen zum Auftragsverhältnis
• im Vertrag mit Dritten werden wirksame Kontroll- und oder Zugriffs- bzw. Löschungsrechte vereinbart
• der Datenschutzbeauftragte kontrolliert regelmäßig alle Verarbeitungsprozesse

2.16 Anpassung der innerbetrieblichen Organisation an die besonderen Anforderungen des Datenschutzes

Der Auftragnehmer hat sich den folgenden datenschutzrechtlichen Standards unterworfen:
• Erarbeitung eines IT-Sicherheitskonzepts
• Fertigung von internen Datenschutz- und Sicherheitsrichtlinien (Policies) sowie Arbeitsanweisungen
• Regelmäßige Kontrolle durch den Datenschutzbeauftragten
• Regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern
• Gelegentliche unangekündigte Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen

Der Auftragnehmer gewährleistet, dass die Leistungserbringung grundsätzlich im hauseigenen Rechenzentrumder KONTENT GmbH und unter Beachtung des deutschen Datenschutzrechts erfolgt. Die Leistungen des Auftgagnehmers orientieren sich zudem soweit möglich an den Vorgaben der Normen der ISO27001 Zertifizierung. Zudem verfolgt der Auftragnehmer die Prozesse, um die Anforderungen der ISO 20000 zu erfüllen. Der Auftragnehmer hat zudem nach den allgemein anerkannten Regeln von Wissenschaft und Technik die operativen Leistungskomponenten redundant ausgelegt.