Technische und organisatorische Maßnahmen

Datenschutzinformation

Planon GmbH & Planon Conject GmbH

Version: 1.2

Datum: 23.05.2019

Autor: Frank Bögel

planonsoftware.com

1 Dokumentinformationen

1.1 Änderungshistorie

Name	Datum	Version	Status	Beschreibung
Frank Bögel	21.05.2019	1.1	Freigegeben	Freigabe nach Erarbeitung
Frank Bögel	23.05.2019	1.2	Freigegeben	Vereinfachung durch Nutzung der Sammelbegriffs “Planon”

Inhalt

2 Zielsetzung der technischen und organisatorischen Maßnahmen

Als datenverarbeitendes Unternehmen sind sich die Planon GmbH und die Planon Conject GmbH der Verantwortung für die ihnen übergebenen bzw. mit ihren Systemen verarbeiteten Daten bewusst. Datenschutz sowie Maßnahmen zur Wahrung desselben sind daher von großer Bedeutung und gehören zu den Kernaufgaben der Unternehmen.

Zudem fordert die EU-Datenschutz-Grundverordnung (DSGVO) von Unternehmen die Ergreifung und Prüfung technischer und organisatorischer Maßnahmen zur angemessenen Sicherung von Daten eines Auftraggebers gegen Missbrauch und Verlust.

Die Planon GmbH und die Planon Conject GmbH sichern in ihrem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen entsprechend dieser Anlage zu. Insbesondere werden die Planon GmbH und die Planon Conject GmbH ihre innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Die davon insbesondere betroffenen Maßnahmen werden im Folgenden beschrieben. Da sämtliche in diesem Dokument beschriebenen Maßnahmen gleichermaßen für die Planon GmbH sowie die Planon Conject GmbH Gültigkeit haben, wird der Einfachheit halber im Folgenden stellvertretend “Planon” verwendet.

3 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Zutrittskontrolle

Die Zutrittskontrolle hat zum Ziel, Unbefugten den Zutritts zu Datenverarbeitungsanlagen zu verwehren.

3.1.1 Zutritt zu Geschäftsräumen

Die Geschäftsräume von Planon sind an allen Standorten stets verschlossen und ohne einen Schlüssel bzw. eine Schließkarte nicht zugänglich. Außerhalb der Geschäftszeiten ist auch der Zutritt zum Gebäude nur mittels Schlüssel bzw. Schließkarte möglich. Technik- und Serverräume sind durch zusätzliche Komponenten vor unbefugtem Zutritt geschützt.

Besucher erlangen Zutritt zu den Büroräumen nur durch manuelles Öffnen der Türen. Sie werden von der Tür bis zur besuchten Person begleitet. Betriebsfremden Personen ist die weitere Begehung nur in Begleitung eines Mitarbeiters gestattet.

3.1.2 Zutritt zu Technikräumen

In den Bürogebäuden liegende Technikräume sind zusätzlich durch weitere Schlüssel, Chipkarte und/oder PIN-Schlösser gesichert.

3.1.3 Zutritt zum Rechenzentrum

Für den Betrieb von Cloud- und SaaS-Lösungen sowie für das Hosting intern genutzter Systeme arbeitet Planon mit entsprechenden IT-Dienstleistungspartnern zusammen. Zugang zu den Rechenzentren der Dienstleistungspartner ist nur ausgewählten Mitarbeitern von Planon im Zuge von Audits gestattet. Die Dienstleistungsparter haben ihrerseits technische und organisatorische Maßnahmen zugesichert, die den hohen Sicherheitsansprüchen der Planon mehr als genügen.

3.2 Zugangskontrolle

Die Zugangskontrolle verfolgt das Ziel, die Nutzung der Datenverarbeitungsanlagen durch Unbefugte zu verhindern.

In der gesamten Planon Gruppe ist der Zugang zu sämtlichen Systemen sowie das Ausführen sämtlicher Transaktionen nur mit einer gültigen Authentifizierung und Autorisierung möglich. Der Zugang zu den Systemen wird durch mehrere Sicherheitsmechanismen abgesichert.

Der Zugang zu Systemen erfolgt durch Eingabe von Benutzername und Passwort, wobei das Passwort Restriktionen bzgl. Länge, Sonderzeichen etc. unterliegt. Passwörter müssen in regelmäßigen Abständen geändert werden. Durch eine entsprechende Policy wird die Wiederholung vorheriger Passwörter unterbunden.

Zugang zu Systemen, in denen Daten mit höherem Schutzbedarf verarbeitet werden, muss explizit beim HelpDesk angefordet und durch einen Vorgesetzten genehmigt werden.

Die Zugangskontrolle zu Systemen der Dienstleistungspartner obliegt deren Verantwortung und wird durch Planon regelmäßig überprüft. Bei der Auswahl der Dienstleistungspartner ist eine Zertifizierung desselben mindestens nach DIN ISO 27001 eine Mindestanforderung, um entsprechenden Sicherheitsstandards gerecht zu werden.

Netzwerke und Datenverarbeitungsanlagen sind von externen Netzwerken durch mehrstufige Firewalls getrennt und vor unbefugtem Zugang geschützt.

3.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, die Zugriffsmöglichkeiten für Berechtigte zu beschränken und das unbefugte Lesen, Kopieren, Verändern oder Löschen von Daten zu unterbinden.

Allen Nutzern sind entsprechend Ihren Tätigkeiten und Berechtigungen bestimmte erforderliche Funktionen zugeordnet, die über den Benutzernamen gesteuert werden. Die Einrichtung von Nutzern wird durch den HelpDesk durchgeführt. Die Nutzer erhalten vom HelpDesk Passwörter für den Zugang zu den Anwendungen, mit denen Daten verarbeitet werden. Planon setzt ein Single Sign On Verfahren ein, um eine systemubergreifende Zugriffskontrolle zu gewährleisten.

Der Zugriff auf Kundensysteme in der Cloud/ SaaS ist ebenfalls durch Authentifizierung und Autorisierung geschützt und folgt den jeweils eingestellten Berechtigungen im System. Der Zugriff erfolgt grundsätzlich verschlüsselt via SSL. Datenverarbeitende Transaktionen werden protokolliert und sind zum Zweck der Nachvollziehbarkeit einsehbar.

Nach Ablauf der jeweils festgelegten Aufbewahrungsdauer werden Daten und Protokolle zur Vermeidung von späterem, unbefugtem Zugriff permanent gelöscht.

3.4 Trennungskontrolle

Die Trennungskontrolle verfolgt das Ziel, die Zweckgebundenheit der Datenverarbeitung sicherzustellen

Die jeweils erforderlichen Daten werden ausschließlich in den dafür vorgesehenen Anwendungen gespeichert und verarbeitet. Die Daten werden dabei physikalisch und logisch voneinander getrennt. Mittels der eingesetzten Berechtigungskonzepte ist der Zugriff auf die Anwendungen und damit die Daten nur in dem für die Verarbeitung erforderlichen Ausmaß möglich. Ein Zugriff auf Daten über die Anwendungsgrenzen hinweg ist nicht möglich.

Innerhalb der einzelnen Anwendungen werden alle Transaktionen protokolliert. Einzelne Datensätze sowie Bearbeiter derselben sind anhand der Protokollierung eindeutig identifizierbar.

Beim Betrieb der Planon Software als Cloud- oder SaaS- Lösungen für Kunden erfolgt eine logische und/ oder physikalische Trennung der Datenhaltung. Innerhalb der Anwendung erfolgt eine Trennung der Daten auf Basis einer Mandantensteuerung.

Der Zugriff auf Kundendaten wird über einen jeweils eigenen Account für jeden Kunden gesteuert. Innerhalb jedes Kunden-Accounts können unterschiedliche Berechtigungen zur Steuerung der Datenverarbeitung vergeben werden. Die Trennung der Daten zum jeweiligen Verarbeitungszweck sowie die Administration der dem Verarbeitungszweck entsprechenden Zugriffsrechte obliegt in diesem Fall dem Kunden.

4 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Weitergabekontrolle

Die Weitergabekontrolle hat zum Ziel, das unbefugte Lesen, Schreiben, Ändern oder Löschen von Daten zu verhindern sowie die Übertragung von Daten nachvollziehbar zu machen.

Jeglicher Zugriff auf Daten, der nicht aus dem intenen Netzwerkes von Planon getätigt wird, erfolgt über eine veschlüsselte Verbindung. Der Zugriff auf die Daten erfolgt in dem Fall mittels VPN oder über Webservices, welche über HTTPS abgesichert sind.

Zugriff auf Daten und Veränderungen werden grundsätzlich protokolliert. Eine Identifizierung der zugreifdenden Person ist aufgrund der eingesetzten Authentifizierungs- und Autorisierungsverfahren prinzipiell möglich.

Für den Fall des Austausches vollständiger Kundendatenbanken wird eine gesicherte Möglichkeit zum Up- und Download seitens Planon zur Verfügung gestellt. Die Daten werden hier nach Bereitstellung durch den Kunden nur einmalig heruntergeladen und dann automatisch gelöscht. Spätestens nach Ablauf der definierten Aufbewahrungsfrist wird ein etwaiger Upload automatisch gelöscht.

Vor der Weitergabe von Daten kann eine Anonymisierung der personenbezogenen Daten erfolgen. Die Anonymisierung ist ein unumkehrbarer Vorgang, nach dessen Durchführung kein Rückschluss auf die Personen ohne Zuhilfenahme weiterer Daten und Werkzeuge möglich ist.

Physikalische Hardware wird nach dem Gebrauch bzw. nach dem turnusmäßigen Tausch durch einen Fachbetrieb mit entsprechender Zertifizierung fachgerecht entsorgt. Die Sammlung sowie der Transport von ausrangierter Hardware erfolgt in dafür geeigneten und gesicherten Behältnissen.

Unterlagen in Papierform wie Protokolle, Ausdrucke oder Listen werden in dafür vorgesehenen, abgeschlossenen Behältern gesammelt und ebenfalls durch einen zertifizierten Fachbetrieb fachgerecht entsorgt.

4.2 Eingabekontrolle

Das Ziel der Eingabekontrolle ist die Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten.

Auf Basis eines Rollen- und Rechtekonzepts erfolgt abhänig von der Funktion eines Benutzers/ Mitarbeiters eine Zuweisung von differenzierten Rechten für die jeweils zu bearbeitenden Daten. Die Aufgabe, diese Berechtigungen verantwortungsvoll zuzuweisen, obliegt dem Kunden.

Jede Dateverarbeitung wird in Transaktionen durchgeführt und protokolliert. Veränderungen das Datenbestandes sind damit dokumentiert und nachvollziehbar.

Aufgrund des verwendeten Authentifizierungs- und Autorisierungsverfahrens ist eine Identifizierung des Bearbeiters möglich.

Die Protokolle können durchsucht und auf Auffälligkeiten überprüft werden. Zusätzlich können die Protokolle zu Nachweiszwecken exportiert und gespeichert bzw. übermittelt werden.

5 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

5.1 Verfügbarkeitskontrolle

Das Ziel der Verfügbarkeitskontrolle ist es, sicherzustellen, dass kein Datenverlust eintritt und bei einem Systemausfall die Datenwiederherstellung in angemessener Zeit erfolgt.

Die Verfügbarkeit der Produktivsysteme und -daten wird durch ein in jeder Hinsicht auf Hochverfügbarkeit ausgelegte Betriebstechniken gewährleistet. Sämtliche Netzwerkkomponenten, Verbindungen und Betriebshardware sind (mehrfach) redundant ausgeführt.

In den Büroräumen von Planon befindliche Server- und Technikräume sind durch separate Überwachungssysteme, Feuerlöscheinrichtungen, USV, RAID-Systeme und Festplattenspiegelungen geschützt.

Die Rechenzentren der Dienstleistungspartner sind DIN ISO 27001 zertifiziert und genügen den höchsten Ansprüchen an Sicherheit. Die Speicherung der Daten und der Betrieb der Systeme erfolgt auf räumlich hinreichend getrennten, redundanten Infrastrukturen.

Die Verfügbarkeit der Systeme wird automatisiert überwacht. Ein Benachrichtigungs- und Alarmsystem sowie ein nachgelagerter Prozess zur Behandlung auftretender Fehler, Systemausfälle oder Sicherheitsvorfällen sichert schnelle Reaktionszeiten.

Die Datensicherung erfolgt mithilhe verschiedener Sicherungsmechanismen und -zyklen. Sicherungen werden sowohl in den Rechenzentren und Büroräumen als auch ausgelagert aufbewahrt.

6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

6.1 Datenschutz-Management

Datenschutz ist kein statisches Thema und ist bei Planon integraler Bestandteil der geschäftlichen Aktivitäten. Ziel des Datenschutz-Managements ist es, den Status Quo des Datenschutzes zu gewährleisten und stetig zu verbessern.

Mittels eines dezidierten Datenschutz-Management-Teams, dem der Datenschutzbeauftragte angehört, werden alle Datenschutz-relevanten Prozesse dokumentiert und die Dokumentationen regelmäßig veröffentlicht und revidiert. In regelmäßigen Veranstaltungen werden Datenschutzvorfälle und Optimierungspotenziale analysiert, aggregiert und in das Datenschutz-Management-System eingeplant.

Die Aufgaben innerhalb des Datenschutz- Management-System sind klar zugewiesen. Um sicher zu stellen, dass erforderliche Verbesserungen des Datenschutzes realisiert werden können, ist der Global Security Officer der Panon Gruppe Bestandteil des Datenschutz- Management-Systems. Er berichtet direkt an das Security Board der Planon Gruppe.

Jeder Mitarbeiter von Planon wird zur Einhaltung der Datenschutzvorgaben verpflichtet und dokumentiert dies durch die Unterzeichnung einer entsprechenden Verpflichtungserklärung. Zusätzlich finden regelmäßig Datenschutzschulungen statt- Die Teilnahme ist für Mitarbeiter verpflichtend und wird dokumentiert.

Um im Bedarfsfall eine Datenschutzfolgeabschätzung (DSFA) durchführen zu können, liegt eine generische Prozessbeschreibung zur Durchführung einer solchen Abschätzung vor. Die Erfordernis einer DSFA wird im individuellen Einzelfall geprüft.

6.2 Incident-Response-Management

Ziel des Incident-Response-Managements ist es, etwaige Datenschutzvorfälle zu erkennen und geeignete Gegenmaßnahmen in angemessener Zeit und Weise ergreifen zu können.

Die Systeme von Planon sind mit mehrschichtigen Schutzsystemen versehen. Sämtliche Systeme stehen unter regelmäßiger Kontrolle durch das Global Security Team der Planon Gruppe und werden permanent auf dem aktuellen Stand der Technik gehalten.

Im Falle von Sicherheitsvorfällen werden je nach Fehlerort und -typ definierte Teams automatisch benachrichtigt. Durch einen umfassend beschriebenen Incident-Management-Prozess mit dezidierter Zuweisung von Aufgaben und Verantwortungen ist sichergestellt, dass auf mögliche, Sicherheits-relevante Vorfälle in angemessener Zeit reagiert werden kann.

6.3 Auftragskontrolle (Outsourcing an Dritte)

Planon arbeitet zur Sicherstellung eines hochverfügbaren und professionellen Leistungsgangebotes mit Dienstleistungspartnern zusammen.

Bei der Auswahl der Dienstleistungspartner wird darauf geachtet, dass diese mindestens die Qualität des Datenschutzes garantieren kann, wie Planon gegenüber den Kunden. Zur Sicherstellung der Einhaltung dieser Vorgaben bestehen entsprechende Vereinbarungen zur Auftragsdatenverarbeitung mit jedem Dienstleistungspartner.

Planon stellt sicher, dass jederzeit Audits bzw. Begehungen zur Überprüfung der Einhaltung der Vereinbarungen durchgeführt werden können. Es wird regelmäßig überprüft, ob der Dienstleistungspartner seinen Verpflichtungen zum Datenschutz nachkommt.

7 Sonstiges

7.1 Überwachung durch die Aufsichtsbehörde

Planon unterliegt der Überprüfung durch die zuständige Aufsichtsbehörde. Mit Sitz in Frankfurt am Main ist als Aufsichtsbehörde der Hessische Datenschutzbeauftragte zuständig.