Technische und organisatorische Maßnahmen (TOMs) für SAP Fioneer Services

In diesem Dokument werden die technischen und organisatorischen Maßnahmen beschrieben, die für die Produktionsinstanz von Cloud Services, SAP Fioneer Support von SAP Fioneer oder dessen Unterauftragsverarbeitern und Consulting Services gelten, die von SAP Fioneer Premisses und Systemen durchgeführt werden (jonly „SAP Fioneer Services“). SAP Fioneer kann diese technischen und organisatorischen Maßnahmen jederzeit ohne vorherige Ankündigung ändern, solange sie ein gleichwertiges oder besseres Sicherheitsniveau aufrechterhalten.

1. ZUTRITTSKONTROLLE

Nur berechtigte Personen können physisch auf Räumlichkeiten, Gebäude oder Räume zugreifen, in denen Daten gespeichert sind. SAP Fioneer schützt seine Anlagen und Einrichtungen mit folgenden Mitteln:

1.1 Rechenzentren und Infrastruktursysteme sollen die Auswirkungen von Umweltrisiken, einschließlich Schäden durch Naturkatastrophen, minimieren.

1.2 Als Mindestanforderung sind die physischen Eingangspunkte der Bürogebäude und der Rechenzentrumsanlagen mit einem Schlüsselsystem ausgestattet.

1.3 Je nach Sicherheitseinstufung werden Gebäude, bestimmte Flächen und umliegende Räumlichkeiten durch zusätzliche Sicherheitsmaßnahmen weiter geschützt. Dazu gehören spezifische Zugangsprofile, Videoüberwachung, Einbruchmeldeanlagen, Smartcard-Zutrittskontrolle, aktives Schlüsselmanagement und biometrische Zutrittskontrollsysteme.

1.4 Zugriffsrechte werden berechtigten Personen auf individueller Basis gemäß den Maßnahmen der Systemzugriffskontrolle und Datenzugriffskontrolle gewährt. Dies gilt auch für den Besucherzugang. Gäste und Besucher in SAP Fioneer Gebäuden müssen sich am Empfang anmelden und werden von autorisiertem SAP Fioneer Personal begleitet.

1.5 Nur autorisierte Personen haben Zugriff auf Systeme und Infrastruktur innerhalb der Rechenzentren.

1.6 Jeder Person muss seinen Ausweis an allen SAP Fioneer-Standorten tragen.

1.7 Zusätzliche Maßnahmen für von SAP Fioneer betriebene Rechenzentren:

(a) Alle Rechenzentren halten strenge Sicherheitsverfahren ein, die von Wachleuten, Überwachungskameras, Bewegungsmeldern, Zugangskontrollmechanismen und anderen Maßnahmen durchgesetzt werden, um eine Gefährdung von Geräten und Rechenzentren zu verhindern. Um die ordnungsgemäße Funktion sicherzustellen, werden physische Sicherheitsausrüstungen (z. B. Bewegungssensoren, Kameras) regelmäßig gewartet.

(b) SAP Fioneer protokolliert die Namen und Zeiten autorisierter Mitarbeiter, die die dedizierten Sicherheitsbereiche von SAP Fioneer innerhalb der Rechenzentren betreten und verlassen.

2. SYSTEMZUGRIFFSKONTROLLE

Auf Systeme, die Daten verarbeiten, kann nur mit der entsprechenden Berechtigung zugegriffen werden. SAP Fioneer schützt seine Systeme und kontrolliert den Zugriff mit folgenden Mitteln:

2.1 Beim Gewähren des Zugriffs auf Systeme, einschließlich der Verarbeitung von Daten, werden mehrere Berechtigungsstufen verwendet. Berechtigungen werden über definierte Prozesse verwaltet.

2.2 Alle Mitarbeiter greifen über ein personalisiertes Konto (Benutzer-ID) auf die Systeme von SAP Fioneer zu.

2.3 Die Mitarbeiter haben nur Zugriff auf die Systeme, auf die sie zugreifen müssen, um ihre Aufgaben zu erfüllen. SAP Fioneer verfügt über Verfahren zur Umsetzung des „Need-to-know"-Prinzips, um den Systemzugriff zu ermöglichen. Wenn Mitarbeiter ihre zugewiesene Rolle im Unternehmen ändern, werden ihre Zugriffsrechte rechtzeitig widerrufen oder angepasst. Sobald ein Mitarbeiter SAP Fioneer verlässt, wird dessen Zugriff innerhalb von 24 Stunden generell widerrufen. SAP Fioneer verwendet Berechtigungskonzepte, die Genehmigungsprozesse und zugeordnete Rollen pro personalisiertem Konto (Benutzer-ID) dokumentieren. Darüber hinaus werden Berechtigungen und Zugriffrechte regelmäßig überprüft.

2.4 SAP Fioneer hat eine Kennwortrichtlinie eingerichtet, die die Weitergabe personalisierter Kennwörter verbietet, die Antworten auf die Offenlegung von Kennwörtern regelt, dass Kennwörter regelmäßig geändert und Standardkennwörter geändert werden müssen. Personalisierte Konten (Benutzer-IDs) werden zur Authentifizierung zugeordnet und dürfen nicht freigegeben werden. Alle Kennwörter erfüllen definierte Mindestanforderungen, insbesondere hinsichtlich Komplexität und Speicherung. Jedes Endbenutzergerät verfügt über einen kennwortgeschützten Bildschirmschoner.

2.5 Das Unternehmensnetzwerk ist durch Firewalls vor dem öffentlichen Netzwerk geschützt. SAP Fioneer betreibt ein unternehmensweites Bedrohungserkennungssystem, um Systeme und Infrastruktur kontinuierlich und aktiv gegen Angriffe zu verteidigen, indem sie Audit-Protokolle nutzt und analysiert.

2.6 SAP Fioneer setzt auf aktuelle kommerziell verfügbare Antiviren-/Malware-Schutzsoftware, um bekannten Schadcode zu verhindern, zu erkennen und zu entfernen. Dazu gehören signaturbasierte Detektionen von Malware, Viren, Spyware und Trojanern, wie sie für Eingangs- und Ausgangspunkte wie E-Mail-Dienste und Dateiübertragungen gelten. Außerdem werden Sicherheitsrisiken für schädlichen Code auf Systemen, Endpunkten und Geräten gemindert.

2.7 Das Sicherheitspatch-Management wird implementiert, um ein geplantes und regelmäßiges Deployment relevanter Sicherheitsupdates bereitzustellen. Der vollständige Remote-Zugriff auf das Unternehmensnetzwerk und die kritische Infrastruktur von SAP Fioneer ist durch eine starke Authentifizierung geschützt.

3. DATENZUGRIFFSKONTROLLE

Personen können nur gemäß ihrer Berechtigung auf Daten zugreifen. Daten, die im Rahmen der Services verarbeitet werden, werden wie folgt als Vertrauliche Informationen klassifiziert:

3.1 Der Zugriff auf Daten wird nach dem „Need-to-know"-Prinzip gewährt. Die Mitarbeiter haben Zugriff auf die Informationen, auf die sie zugreifen müssen, um ihre Pflichten zu erfüllen. Wenn Mitarbeiter ihre zugewiesene Rolle im Unternehmen verlassen oder ändern, werden ihre Zugriffsrechte rechtzeitig widerrufen oder angepasst. Sobald ein Mitarbeiter SAP Fioneer verlässt, wird dessen Zugriff innerhalb von 24 Stunden generell widerrufen. SAP Fioneer verwendet Berechtigungskonzepte, die Genehmigungsprozesse und zugeordnete Rollen pro Konto (Benutzer-ID) dokumentieren. Darüber hinaus werden Berechtigungen und Zugrifsrechte regelmäßig überprüft.

3.2 Daten und Datenträger werden sicher gelöscht oder vernichtet, wenn sie nicht mehr benötigt werden. Wenn Hardware aus Rechenzentren entfernt wird, wird ein physischer Stilllegungsprozess angewendet.

3.3 Sicherheitsmaßnahmen, die Anwendungen zur Datenverarbeitung schützen, werden regelmäßig getestet. Zu diesem Zweck führt SAP Fioneer interne und externe Sicherheitsprüfungen und Penetrationstests auf seinen IT-Systemen durch.

3.4 SAP Fioneer hat Richtlinien eingeführt, um die Installation nicht genehmigter Software auf Workstations und Servern zu verhindern. Mobile Geräte und Arbeitsplätze müssen manuell gesperrt werden, wenn sie unbeaufsichtigt bleiben. Der Bildschirmschoner ist so konfiguriert, dass der Bildschirm innerhalb von maximal fünf Minuten nach Inaktivität automatisch gesperrt wird. Diese zeitabhängige Sperre von Geräten darf nicht deaktiviert werden.

3.5 Bildschirme aller Systeme, die Informationen offenlegen könnten, die den Zugriff auf ein anderes SAP Fioneer-Gerät oder -System ermöglichen, oder Bildschirme, auf denen vertrauliche Informationen behandelt werden, sollten so positioniert werden, dass unbefugte Personen sie nicht ohne Weiteres durch ein Fenster, über die Schulter oder auf ähnliche Weise einsehen können.

3.6 Mobile Geräte, die den Zugriff auf Geräte oder Systeme, in denen Daten gespeichert sind, ermöglichen können, müssen im Besitz von Personal aufbewahrt oder an einem sicheren Ort gesperrt werden, wenn sie nicht genutzt werden. Mobile Geräte dürfen auf Reisen nicht als Gepäck eingecheckt werden.

4. DATENVERSCHLÜSSELUNGSKONTROLLEN

SAP Fioneer wendet die folgenden Maßnahmen an, um zu verhindern, dass personenbezogene Daten während der Übertragung und in Ruhe ohne Autorisierung gelesen, kopiert, geändert oder entfernt werden:

4.1 Daten werden im Ruhezustand mit marktüblichen Standards verschlüsselt

4.2 Daten werden bei der Übertragung zwischen gesicherten Netzwerken unter Kontrolle von SAP Fioneer mit marktakzeptierten Standards verschlüsselt. Daten in der Übertragung über gesicherte Netzwerke unter Kontrolle von SAP Fioneer sind angemessen gesichert.

4.3 Mobile Geräte, die Zugriff auf Geräte oder Systeme bieten könnten, auf denen Daten gespeichert sind, verwenden bei der Remote-Verbindung zu SAP Fioneer-Netzwerken die von SAP Fioneer kontollierte Netzwerkverschlüsselung.

4.4 Für die Übertragung von Daten zwischen SAP Fioneer und seinen Kunden stellt SAP Fioneer angemessene Schutzmaßnahmen für die übermittelten Daten bereit. Die Maßnahmen sind in der Produktdokumentation oder anderweitig in der Vereinbarung definiert. Dies gilt sowohl für die physische als auch für die netzwerkbasierte Datenübertragung. Wenn die Datenübertragung vom Auftraggeber initiiert wird und/oder Verschlüsselungsmaßnahmen unter der Kontrolle des Auftraggebers liegen, ist der Auftraggeber für jede solche Datenübertragung verantwortlich (z. B. Daten, die außerhalb der Firewall des Fioneer-Rechenzentrums übertragen werden). Der Auftraggeber ist verantwortlich für den physischen Transport (z. B. auf beweglichen Medien) außerhalb von Fioneer Räumlichkeiten (z. B. bei Bereitstellung an den Vertreter des Auftraggebers).

5. DATENINTEGRITÄTSKONTROLLEN

Fioneer wendet die folgenden Maßnahmen an, um Daten während der Verarbeitungsaktivitäten intakt, vollständig und aktuell zu halten:

5.1 SAP Fioneer lässt nur autorisierte Mitarbeiter auf Daten zugreifen, die im Rahmen ihrer Pflicht erforderlich sind.

5.2 SAP Fioneer hat ein System zur Protokollierung und Aufbewahrung von SAP Fioneers Input, Modifikation und Löschung oder Sperrung von Daten innerhalb der Cloud-Service-Infrastruktur implementiert.

5.3 Cloud-Service-Anwendungen stellen Protokollierungssysteme für die Eingabe, Änderung und Löschung oder Sperrung von Daten bereit, wie in der Dokumentation beschrieben.

5.4 SAP Fioneer nutzt die technischen Möglichkeiten der implementierten Software (z. B. Mehrmandantenfähigkeit oder separate Systemlandschaften), um eine Datentrennung zwischen Daten zu erreichen, die von mehreren Kunden stammen.

5.5 Die Daten des Auftraggebers (einschließlich seiner Verantwortlichen) sind logisch von den Daten anderer Kunden getrennt. Zugriffskontrollen verhindern den Zugriff anderer Kunden auf die Daten des Auftraggebers.

5.6 Für den SAP Fioneer Support:

(a) SAP Fioneer Kunden haben jederzeit die Kontrolle über ihre Remote-Support-Verbindungen. SAP Fioneer kann ohne Kenntnis und Zustimmung des Auftraggebers nicht auf ein System des Auftraggebers zugreifen. Für SAP Fioneer Suppor stellt SAP Fioneer eine speziell ausgewiesene, sichere Support-Ticket-Einrichtung zur Verfügung, in der SAP Fioneer einen speziellen zugangsgesteuerten und überwachten Sicherheitsbereich für die Übertragung von Zugangsdaten und Passwörtern zur Verfügung stellt. SAP Fioneer Kunden haben jederzeit die Kontrolle über ihre Remote-Support-Verbindungen. SAP Fioneer Mitarbeiter können ohne das Wissen und die aktive Beteiligung des Auftraggebers nicht auf ein On-Premise-System des Auftraggebers zugreifen.

(b) Wenn zur Bearbeitung einer Supportmeldung des Auftraggebers Personenbezogene Daten erforderlich sind, werden die Daten diesem bestimmten Vorgang zugeordnet und nur zur Bearbeitung dieses Vorfall verwendet. Es wird nicht auf diese zugegriffen, um andere Vorgänge zu bearbeiten. Diese Daten werden in dedizierten Supportsystemen gespeichert.

6. VERFÜGBARKEITSKONTROLLEN

Daten sind wie folgt vor versehentlicher oder unberechtigter Vernichtung oder Verlust geschützt:

(a) SAP Fioneer nutzt bei Bedarf regelmäßige Backup-Prozesse, um die Wiederherstellung von Daten und, sofern ausdrücklich für den jeweiligen Cloud Service vereinbart, Disaster-Recovery-Services bereitzustellen.
(b) SAP Fioneer nutzt unterbrechungsfreie Stromversorgungen (z. B. Batterien, Generatoren) für die unterbrechungsfreie Stromversorgung der Rechenzentren.
(c) SAP Fioneer hat angemessene Netzwerkverbindungsbandbreiten und Denial-of-Service-Präventionsmaßnahmen (Denial-of-Service, DoS) für das Rechenzentrum implementiert, das den Cloud Service bereitstellt.
(d) SAP Fioneer hat Notfallpläne für seine eigenen geschäftskritischen Prozesse definiert.
(e) Notfallprozesse und -systeme, einschließlich Datenwiederherstellung, werden regelmäßig getestet.

7. GOVERNANCE-KONTROLLEN

Die Daten werden gemäß der Vereinbarung und den zugehörigen Anweisungen des Auftraggebers wie folgt verarbeitet:

(a) SAP Fioneer überwacht die Einhaltung von Verträgen zwischen SAP Fioneer und seinen Kunden, Unterauftragsverarbeitern oder anderen Dienstleistern mithilfe von Kontrollen und Prozessen.
(b) Zur Verarbeitung von Daten gewähren SAP Fioneer und seine Unterauftragsverarbeiter nur autorisiertem Personal Zugriff, das sich zur Vertraulichkeit verpflichtet hat. SAP Fioneer und seine Unterauftragsverarbeiter schulen das Personal, das Zugriff auf Daten hat, regelmäßig in Bezug auf geltende Datensicherheits- und Datenschutzmaßnahmen.