

Technische und organisatorische Maßnahmen für IONOS Cloud

1 Allgemeines

Der Verantwortliche und der Auftragsverarbeiter 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 Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

Sowohl der Auftragsverarbeiter als auch die einzelnen von diesen beauftragten Rechenzentren haben insbesondere die folgenden Maßnahmen getroffen. Grundsätzlich ist eine Nutzung der Datenverarbeitungssysteme durch den Rechenzentrumsbetreiber nicht vorgesehen. Der Auftragsverarbeiter nutzt insofern in den Sicherheitsbereichen befindliche eigene Hardware, so dass weder Zugriffsrechte, Zugänge, Weitergaben, Eingaben der Daten des Verantwortlichen durch die Rechenzentren stattfinden.

2 Technisch organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragsverarbeiter hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.

2.1 Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten

2.1.1 Bei den Produkten Compute Engine, Cloud Cubes, Managed Kubernetes, S3 Object Storage

- Die Pseudonymisierung und Verschlüsselung im Auftrag verarbeiteter personenbezogener Daten obliegt dem Verantwortlichen

2.1.2 Bei dem Produkt Backup

- Verschlüsselung der gespeicherten Daten kann mittels eines vom Verantwortlichen definierten Schlüssels erfolgen

2.2 Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

2.2.1 Zugangskontrolle

Ziel: Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte

2.2.1.1 Rechenzentren

- Alle Rechenzentren sind nach dem ISO 27001 Standard zertifiziert
- Elektronische Zutrittskontrollsysteme überwachen und gewährleisten den Zutritt zum jeweiligen Rechenzentrum nur für autorisierte Personen
- Zutritt zum Gebäude ist über Sicherheitsschleusen geregelt
- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes
- Definierte Sicherheitszonen
- Alarmmeldung bei unberechtigtem Zutritt zu Rechenzentren
- 24/7 personelle Besetzung der Rechenzentren
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude

2.2.1.2 Verwaltung

- Empfangs- und Sicherheitsdienst
- Individuelle, dokumentierte und rollenabhängige Zutrittsberechtigungen (Karten, Transponder und Schlüssel)
- Bürofläche ist außerhalb der Arbeitszeit verschlossen
- Besucherausweise
- Besucher dürfen sich grundsätzlich nur in Begleitung eines Mitarbeiter im Gebäude aufhalten
- Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben, wird sorgfältig ausgewählt
- Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr
- Formale Benutzer- und Berechtigungsverfahren
- Systemisch forcierte Passwortrichtlinien
- Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung
- VPN bei Remotezugriff und durch vom Verantwortlichen verwaltete Geräte
- Automatische Sperre von Desktops nach wenigen Minuten Inaktivität
- Clean Desk-Policy

2.2.2 Datenträgerkontrolle

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

2.2.2.1 Bei den Produkten Compute Engine, Cloud Cubes, Managed Kubernetes, S3 Object Storage, Backup

- Speicherblöcke werden bei Rückgabe nicht wiederherstellbar gelöscht
- Defekte und ausgesonderte Datenträger werden physikalisch vernichtet

2.2.2.2 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Datenträger werden (soweit möglich) restriktiv eingesetzt sowie verschlüsselt
- ausgesonderte Datenträger werden datenschutzkonform gelöscht oder physikalisch vernichtet

2.2.3 Speicherkontrolle

Ziel: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

2.2.3.1 Bei den Produkten Compute Engine, Cloud Cubes und S3 Object Storage

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Berechtigungskonzept nach dem Need-to-Know-Prinzip),
- der Zugriff auf Anwendungen und Dateibenutzungen (Eingabe, Veränderung und Löschung) wird protokolliert und kann ausgewertet werden,
- die vom Kunden zu administrierenden Systeme datenschutzfreundliche Voreinstellungen enthalten (z.B. ist eine jederzeitige transparente Löschung möglich),
- freigegebene Speicherbereiche werden vor Neuzuweisung überschrieben (genullt).

2.2.3.2 Bei dem Produkt Managed Kubernetes

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Berechtigungskonzept nach dem Need-to-Know-Prinzip),
- der Zugriff auf Anwendungen und Dateibenutzungen (Eingabe, Veränderung und Löschung) wird protokolliert und kann ausgewertet werden,

- freigegebene Speicherbereiche werden vor Neuzuweisung überschrieben (genullt).

2.2.3.3 Bei dem Produkt Backup

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Berechtigungskonzept nach dem Need-to-Know-Prinzip)
- der Zugriff auf Anwendungen und Dateibenutzungen (Eingabe, Veränderung und Löschung) wird protokolliert und kann ausgewertet werden
- für die vom Verantwortlichen administrierten Produkte werden soweit möglich datenschutzfreundliche Voreinstellungen vorgeschlagen

2.2.3.4 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles)
- Zugriffsrechte orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Berechtigungskonzept nach dem Need-to-Know-Prinzip)

2.2.4 Benutzerkontrolle

Ziel: Verhinderung, dass automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte benutzt werden

2.2.4.1 Bei den Produkten Compute Engine, Cloud Cubes, S3 Object Storage, Managed Kubernetes, Backup

- die Umsetzung von Maßnahmen zur Benutzerkontrolle obliegt dem Verantwortlichen
- der Auftragsverarbeiter unterstützt den Verantwortlichen durch die Bereitstellung von produktspezifischen Funktionen zur Steuerung von Berechtigungen seiner Benutzer sowie durch die Bereitstellung produktspezifischer Protokollierungsmechanismen

2.2.4.2 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Need-to-Know-Prinzip)
- Trennung von Anwendungs- und Administrationszugängen
- Regelmäßige Kontrolle der vergebenen Berechtigungen
- VPN-Technologie zur Datenkommunikation eingesetzt wird
- Pflege und Aktualisierung des vorhandenen Virenschutz (Anti-Virensoftware)

2.2.5 Zugriffskontrolle

Ziel: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben

2.2.5.1 Bei den Produkten Compute Engine, Cloud Cubes, S3 Object Storage, Managed Kubernetes, Backup

- die Umsetzung von Maßnahmen zur Zugriffskontrolle obliegt dem Verantwortlichen
- der Auftragsverarbeiter unterstützt den Verantwortlichen durch die Bereitstellung von produktspezifischen Funktionen zur Steuerung von Berechtigungen seiner Benutzer sowie durch die Bereitstellung produktspezifischer Protokollierungsmechanismen

2.2.5.2 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Need-to-Know-Prinzip)
- Trennung von Anwendungs- und Administrationszugängen
- Regelmäßige Kontrolle der vergebenen Berechtigungen
- Führen von Assetregistern und Ableitung von Maßnahmen anhand der Datenklassifikation

- Passwortrichtlinien inkl. Passwortlänge und Anforderungen an Passwortwechsel

2.2.6 Übertragungskontrolle

Ziel: Gewährleistung, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

2.2.6.1 Bei den Produkten Compute Engine, Cloud Cubes, Managed Kubernetes

- die Umsetzung von Maßnahmen zur Übertragungskontrolle obliegt dem Verantwortlichen

2.2.6.2 Bei dem Produkt S3 Object Storage

- die Umsetzung von Maßnahmen zur Steuerung von Zugriffsberechtigungen auf Datenbuckets und Objekte obliegt dem Verantwortlichen
- der Auftragsverarbeiter unterstützt den Verantwortlichen durch die Bereitstellung von produktspezifischen Funktionen zur Übertragungskontrolle, wie z. B.
 - Dedizierte über HTTPS abgesicherte Endpunkte, über die Datenbuckets und Objekte bereitgestellt werden
 - Protokollierung des Zugriffs (Eingabe, Veränderung und Löschung)
 - Definition von Löschfristen für Objekte

2.2.6.3 Bei den Produkten Backup

- Dedizierte über HTTPS abgesicherte Endpunkte
- Protokollierung des Zugriffs (Eingabe, Veränderung und Löschung)
- Registrierung von Datensicherungsagents über Autorisierungstoken

2.2.6.4 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Bereitstellung von Daten über verschlüsselte Verbindungen
- Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know- / Need-to-Do-Prinzips
- Personenbezogene Daten werde nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden dürfen
- Wo möglich wird E-Mailverschlüsselung eingesetzt
- Wo möglich werden personenbezogene Daten nur in pseudonymisierter oder anonymisierter Form übermittelt
- Dokumentation der Weitergabe von physischen Speichermedien wofür geeignete Transportpersonen sorgfältig ausgewählt werden
- Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag

2.2.7 Eingabekontrolle

Ziel: 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

2.2.7.1 Bei den Produkten Compute Engine, Cloud Cubes, Managed Kubernetes

- die Umsetzung von Maßnahmen zur Eingabekontrolle obliegt dem Verantwortlichen

2.2.7.2 Bei den Produkten S3 Object Storage, Backup

- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten

2.2.7.3 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Verwendung von personalisierten und eindeutigen Benutzerkennungen

- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten

2.2.8 Transportkontrolle

Ziel: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden

2.2.8.1 Bei den Produkten Compute Engine, Cloud Cubes, Managed Kubernetes, S3 Object Storage

- die Umsetzung von Maßnahmen zur Transportkontrolle bei der Übermittlung personenbezogener Daten obliegt dem Verantwortlichen
- keine Übermittlung von Kundeneigenen Daten zwischen Lokationen in der Standardkonfiguration
- bei physischen Transport werden geeignete Transportpersonen sorgfältig ausgewählt

2.2.8.2 Bei dem Produkt Backup

- Kommunikation über Netzwerksegmente, die nicht unter der Kontrolle der Organisation selbst stehen, erfolgt über einen sicheren Kanal.
- bei physischen Transport werden geeignete Transportpersonen sorgfältig ausgewählt

2.2.8.3 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Kommunikation über Netzwerksegmente, die nicht unter der Kontrolle der Organisation selbst stehen, erfolgt über einen sicheren Kanal
- Einsatz von VPN-Technologie (TLS) zur Datenkommunikation
- Wo möglich wird E-Mailverschlüsselung eingesetzt
- bei physischen Transport werden geeignete Transportpersonen sorgfältig ausgewählt

2.2.9 Zuverlässigkeit

Ziel: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

2.2.9.1 Bei den Produkten Compute Engine, Cloud Cubes, Managed Kubernetes

- die Umsetzung von Maßnahmen zur Gewährleistung der Zuverlässigkeit von Verarbeitungen, die durch den Verantwortlichen innerhalb der Produkte durchgeführt werden, obliegt dem Verantwortlichen
- Wo möglich wird eine resiliente Systemarchitektur eingesetzt
- Kontinuierliche Überwachung der Systemverfügbarkeit
- Automatische Identifikation von Fehlfunktionen
- Behandlung von Fehlfunktionen in Incident und Problem Management
- Festgelegte Eskalations- und Informationswege im Falle von Fehlfunktionen

2.2.9.2 Bei den Produkten S3 Object Storage, Backup

- Wo möglich wird eine resiliente Systemarchitektur eingesetzt
- Kontinuierliche Überwachung der Systemverfügbarkeit
- Automatische Identifikation von Fehlfunktionen
- Behandlung von Fehlfunktionen in Incident und Problem Management
- Festgelegte Eskalations- und Informationswege im Falle von Fehlfunktionen

2.2.9.3 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Kontinuierliche Überwachung der Verfügbarkeit von produktionsrelevanten Systemen
- Automatische Identifikation von Fehlfunktionen von produktionsrelevanten Systemen

- Behandlung von Fehlfunktionen in Incident und Problem Management
- Festgelegte Eskalations- und Informationswege im Falle von Fehlfunktionen

2.2.10 Datenintegrität

Ziel: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

2.2.10.1 Bei den Produkten Compute Engine, Managed Kubernetes

- die Umsetzung von Maßnahmen zur Gewährleistung der Datenintegrität obliegt dem Verantwortlichen
- Speicherung der kundeneigenen Daten auf resilienter Speicherarchitektur mit RAID-Technologie
- Sicherung der Konfigurationsinformationen zur Kundenumgebung

2.2.10.2 Bei dem Produkt Cloud Cloud Cubes

- die Umsetzung von Maßnahmen zur Gewährleistung der Datenintegrität obliegt dem Verantwortlichen
- Speicherung der kundeneigenen Daten in einem Speichersystem mit RAID-Technologie
- Kundenvolumen wird regelmäßig gesichert
- Sicherung der Konfigurationsinformationen zur Kundenumgebung

2.2.10.3 Bei dem Produkt S3 Object Storage

- die Umsetzung von Maßnahmen zur Gewährleistung der Datenintegrität obliegt dem Verantwortlichen
- Einsatz einer resilienten Speicherarchitektur

2.2.10.4 Bei dem Produkt Backup

- Speicherung der kundeneigenen Daten auf resilienter Speicherarchitektur mit RAID-Technologie

2.2.10.5 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Datensicherung von produktionsrelevanten Systemen und Informationen

2.2.11 Auftragskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

- Daten die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet
- Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt
- Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert
- Sofern erforderlich werden Auftragsverarbeitungsvereinbarungen bzw. geeignete Garantien zur Übermittlung von Daten an Drittländer geschlossen

2.2.12 Verfügbarkeitskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind

Die Verfügbarkeit von im Auftrag verarbeiteter Daten wird sichergestellt mittels

- Stromversorgung wird durch Redundanzen sichergestellt (Notstromaggregate sowie USV-Anlagen mit n+1 Redundanz)
- Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
- Klimaanlage in Rechenzentren
- Brandmeldeanlage und Brandfrühersterkennung in Rechenzentren
- Notfallhandbücher für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
- Externe Audits und Sicherheitstests

2.2.12.1 Bei den Produkten Compute Engine, Managed Kubernetes, S3 Object Storage

- die Umsetzung von Maßnahmen zum Schutz der Daten gegen Zerstörung oder Verlust obliegt dem Verantwortlichen
- Speicherung der kundeneigenen Daten auf resilienter Speicherarchitektur mit RAID-Technologie

2.2.12.2 Bei dem Produkt Cloud Cubes

- die Umsetzung von Maßnahmen zur Gewährleistung der Datenintegrität obliegt dem Verantwortlichen
- Speicherung der kundeneigenen Daten in einem Speichersystem mit RAID-Technologie
- Kundenvolumen wird regelmäßig gesichert

2.2.12.3 Bei dem Produkt Backup

- Speicherung der kundeneigenen Daten auf resilienter Speicherarchitektur mit RAID-Technologie

2.2.13 Trennbarkeit

Ziel: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

2.2.13.1 Bei den Produkten Compute Engine, Managed Kubernetes

- die Umsetzung von Maßnahmen zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können obliegt dem Verantwortlichen
- klare Trennung und Nachvollziehbarkeit von Kundenzugriffen (logische Trennung durch individuelle Benutzerprofile mit Passwortschutz/ Trennung von Produktiv- und Testinfrastruktur)
- getrennte Verarbeitung zweckgebundener Daten

2.2.13.2 Bei dem Produkt Cloud Cubes

- die Umsetzung von Maßnahmen zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können obliegt dem Verantwortlichen

- klare Trennung und Nachvollziehbarkeit von Kundenzugriffen (logische Trennung durch individuelle Benutzerprofile mit Passwortschutz/ Trennung von Produktiv- und Testinfrastruktur)

2.2.13.3 Bei den Produkten S3 Object Storage, Backup

- klare Trennung und Nachvollziehbarkeit von Kundenzugriffen (logische Trennung durch individuelle Benutzerprofile mit Passwortschutz/ Trennung von Produktiv- und Testinfrastruktur)

2.3 Maßnahmen zur Wiederherstellbarkeit und Verfügbarkeit personenbezogener Daten bei einem physischen oder technischen Zwischenfall

2.3.1 Wiederherstellbarkeit

Ziel: Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können

2.3.1.1 Bei den Produkten Compute Engine, Managed Kubernetes, S3 Object Storage, Backup

- die Umsetzung von Maßnahmen zur Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können obliegt dem Verantwortlichen

2.3.1.2 Bei den Produkten Cloud Cubes

- die Umsetzung von Maßnahmen zur Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können obliegt dem Verantwortlichen
- Kundenvolumen wird regelmäßig gesichert

2.3.1.3 Bei den internen Verwaltungssystemen des Auftragsverarbeiters

- Erstellung eines Backup- und Recoverykonzepts
- Wo notwendig Nutzung redundanter Systeme (z.B. RAID)

2.3.2 Incident-Management

- Dokumentierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten

- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen unter Einbindung des Informationssicherheitsbeauftragten
- Protokollierung und Auswertung von Störungsvorfällen

2.4 Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

- Datenschutzbeauftragte und ein Informationssicherheitsbeauftragter sind benannt
- Etablierung einer Datenschutz- und Informationssicherheitsorganisation
- Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und werden auf Vertraulichkeit der Kommunikation - Fernmeldegeheimnis hingewiesen
- Mitarbeiter sind im Umgang mit personenbezogenen Daten durch regelmäßige Online-Schulungen sensibilisiert
- Neue Mitarbeiter erhalten Informationsmaterial bezüglich dem Umgang mit personenbezogenen Daten
- Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt
- Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert
- Regelmäßige Kontrolle durch den Datenschutzbeauftragten