cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

Erklärung zur einseitigen Verpflichtung

betreffend die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen nach Datenschutzgesetz (DSG) und Artikel 28 Datenschutzgrundverordnung (DSGVO)

durch die

CloudXcelerate GmbH

Wienerbergstraße 53, 1120 Wien

(im Folgenden „Auftragsverarbeiter“)

zugunsten von

Verantwortlicher

(im Folgenden „Verantwortlicher“),

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

Gegenstand der Verpflichtung

1. Der Auftragsverarbeiter erbringt aufgrund eines gesondert abgeschlossenen Vertrages (in der Folge „Grundvertrag") Dienstleistungen für den Verantwortlichen, welche in der Verarbeitung personenbezogener Daten (in der Folge kurz „Daten") im Sinne des Art. 4 Z. 1 und 2 der EU-Datenschutz-Grundverordnung (DS-GVO) bestehen oder eine solche mit sich bringen. Diese ergänzende Erklärung zur einseitigen Verpflichtung (in der Folge kurz „Verpflichtungserklärung") bildet die spezifische rechtsgeschäftliche Grundlage für die Datenverarbeitung gem. Art. 28 Abs. 3 DS-GVO, wobei der Verantwortliche diesbezüglich als (einziger) „Verantwortlicher" und der Auftragsverarbeiter als „Auftragsverarbeiter" fungiert. Sofern in dieser Verpflichtungserklärung der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der Verarbeitung im Sinne des Art. 4 Z. 2 DS-GVO zugrunde gelegt.
2. Der Auftragsverarbeiter sichert mit dieser Verpflichtungserklärung dem Verantwortlichen zu und verpflichtet sich, sämtliche Anforderungen, die sich aus Art. 28 DSGVO für ihn als Auftragsverarbeiter ergeben, einzuhalten und sicherzustellen. Dabei wird der Auftragsverarbeiter vor allem für die nachstehend ausgeführten Pflichten Sorge tragen und diese im Zuge des Verarbeitungsverhältnisses entsprechend umsetzen.

Eignung als Auftragsverarbeiter

3. Der Auftragsverarbeiter stellt einen Auftragsverarbeiter im Sinne des Art. 28 Abs. 1 DS-GVO dar, die hinreichenden Garantien bietet, dass geeignete technische und organisatorische Maßnahmen (in der Folge kurz „TOMs") entsprechend durchgeführt und sichergestellt werden. Die vom Auftragsverarbeiter umgesetzten und zugesicherten TOMs werden im **Anhang** zu dieser Verpflichtungserklärung aufgelistet.
4. Der Auftragsverarbeiter sichert zu und verpflichtet sich, dass diese TOMs für alle Datenverarbeitungen sichergestellt sind, die der Auftragsverarbeiter für den Verantwortlichen durchführt. Dies jedoch nur

insoweit, als sich die davon betroffenen Systeme und Zugriffe in der Sphäre des Auftragsverarbeiters befinden.

5. Sollten Systeme, die von der Datenverarbeitung betroffen sind, sich jedoch in der Sphäre des Verantwortlichen befinden, so werden die im Anhang gelisteten TOMs insoweit zugesichert, als sie sich im Einflussbereich des Auftragsverarbeiters befinden und die jeweilige TOM darauf anwendbar ist (erklärendes Beispiel: Befindet sich ein Server z. B. in den Räumlichkeiten des Verantwortlichen, so kommen die TOMs hinsichtlich Zutrittskontrolle zu diesem Server nicht zur Anwendung, da diese nicht im Sphärenbereich des Auftragsverarbeiters liegen.)
6. Soweit der Auftragsverarbeiter nicht gesetzlich zu bestimmten Verarbeitungen verpflichtet ist, verwendet er die Daten ausschließlich zur Erfüllung seiner Vertragspflichten gegenüber dem Verantwortlichen, also wie hier geregelt oder vom Verantwortlichen angewiesen. Von den weiteren gesetzlichen Verarbeitungspflichten setzt er den Verantwortlichen im zulässigen Ausmaß vorweg in Kenntnis.
7. Der Auftragsverarbeiter wird die Daten keinesfalls für eigene oder fremde Zwecke verwenden oder ohne schriftliche Weisung bzw. Genehmigung des Verantwortlichen an Dritte weitergeben. Kopien oder Duplikate von Daten werden ohne gesonderte Zustimmung des Verantwortlichen nur insoweit erstellt, als sie zur Gewährleistung der ordnungsgemäßen Verarbeitung (Sicherheitskopien) oder im Hinblick auf gesetzliche Aufbewahrungspflichten erforderlich sind.
8. Die Daten sind innerhalb des räumlichen Geltungsbereichs der DS-GVO zu verarbeiten, wenn nicht sowohl eine schriftliche Genehmigung des Verantwortlichen für eine Übermittlung in Drittstaaten als auch die spezifischen Voraussetzungen der Art. 44 ff. DS-GVO vorliegen.
9. Die Datenverarbeitung erfolgt insgesamt auf eine Weise, die den Verantwortlichen jederzeit bei der Erfüllung seiner datenschutzrechtlichen Pflichten gegenüber Betroffenen und Behörden unterstützt.
10. Nach Abschluss der vereinbarten Leistungserbringung (spätestens mit Vertragsbeendigung) oder bei vorheriger Aufforderung durch den Verantwortlichen wird der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Informationen, Unterlagen, die Verarbeitungs- und

Nutzungsergebnisse sowie die in Zusammenhang mit dem Auftragsverhältnis stehenden Datensätze (einschließlich Test- und Ausschussmaterial) in einem gängigen Dateiformat allein dem Verantwortlichen retournieren bzw. nach dessen vorheriger Zustimmung vernichten, sofern nicht eine rechtliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Rechte des Verantwortlichen

11. Dem Verantwortlichen steht gegenüber dem Auftragsverarbeiter ein umfassendes Weisungsrecht hinsichtlich Art und Umfang der Datenverarbeitung zu. Sofern eine solche Weisung nach Auffassung des Auftragsverarbeiters gegen geltendes Datenschutzrecht verstoßen könnte, hat er den Verantwortlichen unverzüglich zu warnen (Art. 28 Abs. 3 3. Satz DS-GVO).
12. Die Entscheidung über eine Auskunftserteilung, Einschränkung, Löschung oder Berichtigung vertragsgegenständlicher Daten steht ausschließlich dem Verantwortlichen zu. Der Auftragsverarbeiter hat dahingehend niemals eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen tätig zu werden. Wenden sich betroffene Personen diesbezüglich direkt an den Auftragsverarbeiter, bemüht sich dieser, solche Ersuchen dem Verantwortlichen weiterzuleiten.

Pflichten des Auftragsverarbeiters

13. Der Auftragsverarbeiter ist für die vertragsgemäße Auftragsdatenverarbeitung im Rahmen des geltenden Datenschutzrechts verantwortlich. Er bestätigt die Kenntnis aller einschlägigen Vorschriften und beachtet insbesondere die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art. 5 DS-GVO.
14. Der Auftragsverarbeiter verpflichtet sich, sämtliche personenbezogene Daten entsprechend den Vorgaben des Verantwortlichen gem. Art 4 Z 7 DS-GVO zu verarbeiten und ausschließlich diejenigen Mittel und Zwecke zu verfolgen, die durch den Verantwortlichen festgelegt wurden.

15. Konkrete Verpflichtungen bzw. detaillierte Verhaltensvorgaben, die sich weder direkt aus dem Grundvertrag noch aus objektivem Recht ergeben, sind als „Anweisungen zur Datenverarbeitung“ durch den Verantwortlichen dokumentiert festzulegen.
16. Der Auftragsverarbeiter garantiert, dass alle zur beauftragten Datenverarbeitung eingesetzten bzw. befugten Personen entsprechend geeignet sind und zur Vertraulichkeit verpflichtet wurden oder einer angemessenen – insbesondere gesetzlichen – Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DS-GVO). Die Verschwiegenheitspflicht ist auch nach Beendigung des Grundvertrags einzuhalten. Ausdrücklich erklärt der Auftragsverarbeiter, die betroffenen Mitarbeiter über Datenschutz/Informationssicherheit hinreichend zu instruieren, regelmäßig zu schulen bzw. zu sensibilisieren sowie konkret anzuleiten und zu überwachen.
17. Der Auftragsverarbeiter verpflichtet sich, im Sinne des Art. 32 DS-GVO alle für die Sicherheit der Datenverarbeitung erforderlichen Maßnahmen zu ergreifen (Art. 28 Abs. 3 lit. c DS-GVO). Er hat insbesondere alle organisatorischen und technischen Vorkehrungen ergriffen, sodass die Integrität der Verarbeitung gewährleistet, ein Verlust personenbezogener Daten verhütet und der unbefugte Zugriff Dritter darauf verhindert wird. Die vom Auftragsverarbeiter bereits umgesetzten Maßnahmen sind im Anhang angeführt und entsprechen dem Sicherheitskonzept nach ISO 27001. Das Zertifikat kann dem Verantwortlichen auf Verlangen vorgelegt werden. Der Auftragsverarbeiter wird seine Prozesse und Maßnahmeneffizienz regelmäßig kontrollieren und dokumentieren und gegebenenfalls notwendig gewordene oder technischen Fortschritte entsprechende Modifikationen vornehmen/veranlassen.
18. Der Auftragsverarbeiter wird den Verantwortlichen bei der Umsetzung seiner Informationspflichten und geltend gemachter Betroffenenrechte nach Möglichkeit unterstützen (Art. 28 Abs. 3 lit. e DS-GVO). Insbesondere schafft er die technischen und organisatorischen Voraussetzungen dafür, dass der Verantwortliche seinen Verpflichtungen gegenüber Betroffenen gem. Art. 15 ff. DS-GVO (Auskunftserteilung, Berichtigung, Löschung/Vergessenwerden, Datenportabilität,

Widerspruch) innerhalb der maßgeblichen Fristen nachkommen kann. Der Auftragsverarbeiter liefert dem Verantwortlichen jedenfalls die mit vertretbarem technischem und wirtschaftlichem Aufwand einholbaren Informationen.

19. Der Auftragsverarbeiter wird den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen auch bei der Erfüllung von dessen Verpflichtungen gemäß Art. 32–36 DS-GVO unterstützen (Art. 28 Abs. 3 lit. f DS-GVO).
20. Der Auftragsverarbeiter wird den Verantwortlichen (bzw. dessen namhaft gemachten Datenschutzbeauftragten) über relevante Verletzungen des Schutzes bzw. der Sicherheit vertragsgegenständlicher Daten in seinem Verantwortungsbereich unverzüglich ab Kenntnis vom relevanten Ereignis informieren. Dabei sind insbesondere die betroffenen Datensätze/Datenkategorien und Personen, die zu erwartenden Folgen der Datenschutzverletzung, die ergriffenen bzw. geplanten Gegenmaßnahmen und die Kontaktdaten einer verantwortlichen Person oder sonstigen Anlaufstelle des Auftragsverarbeiters für weitere Informationen/Abstimmungen anzugeben.
21. Der Auftragsverarbeiter wird dem Verantwortlichen in geeigneter Weise Informationen zum Nachweis der Einhaltung seiner Verpflichtungen zur Verfügung stellen und eine Überprüfung im Sinne des Art. 28 Abs. 3 lit. h DS-GVO ermöglichen.

Einsatz weiterer (Sub-)Auftragsverarbeiter

22. Das Hinzuziehen von Subauftragsverarbeitern durch den Auftragsverarbeiter bei der Erfüllung des Grundvertrags in Hinblick auf die Datenverarbeitung bedarf grundsätzlich der schriftlichen Genehmigung des Verantwortlichen, sofern die Erbringung der Hauptleistung(en) in Bezug auf die Datenverarbeitung selbst vertraglich verlagert bzw. delegiert werden soll. Nicht als in diesem Sinn relevante Sub-Auftragsverhältnisse gelten daher z. B. Hilfsdienstleistungen Dritter bei Telekommunikation, Versand/Transport, IT- Wartung (wie z.B. Herstellersupportleistungen und dgl.), Benutzerservices etc., wobei

allerdings auch insoweit für risikoangemessene und gesetzeskonforme Vertragsregelungen bzw. Kontrollmaßnahmen zu sorgen ist.

23. Der Auftragsverarbeiter wird jedoch – soweit für die Vertragserfüllung des Grundvertrages erforderlich – jene Unternehmen als Sub-Auftragsverarbeiter heranziehen, die für Leistungen aus dem Grundvertrag unbedingt notwendig sind. Diese Unternehmen werden bzw. wurden dem Verantwortlichen im Zuge der Beauftragung offengelegt und sind für die Leistungserbringung zwingend erforderlich. Der Verantwortliche hat jedenfalls das Recht, einer solchen Beauftragung zu widersprechen. In diesem Falle wird ausdrücklich erklärt, dass der Auftragsverarbeiter seine Leistungen aus dem Grundvertrag dann nicht mehr vereinbarungsgemäß erbringen kann. Der Auftragsverarbeiter wird jedoch nur solche Sub- Auftragsverarbeiter zuziehen, die zur konkreten vertragsgemäßen Tätigkeit objektiv geeignet sind, insbesondere hinreichende Garantien für die nötigen TOMs bieten und sich in belegbar abgeschlossenen Vereinbarungen gem. Art. 28 Abs. 3 DS-GVO zumindest zur Gewährleistung des vom gegenständlichen Vertrag vorgegebenen Datenschutzniveaus verpflichten. Erbringt der Sub-Auftragsverarbeiter die vereinbarte Leistung außerhalb der EU bzw. des EWR, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit sicher.
24. Über jede beabsichtigte Änderung (Ergänzung oder Ersetzung) beim Einsatz von Sub- Auftragsverarbeitern wird der Verantwortliche so rechtzeitig informiert, dass dieser noch vor der Umsetzung allfällige Einwände gegen bestimmte weitere Verarbeiter erheben kann.

Haftung

25. Der Auftragsverarbeiter haftet dem Verantwortlichen bei schuldhafter Verletzung dieser Verpflichtungserklärung ausschließlich nach den gesetzlichen Bestimmungen.

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

Vertragsdauer/Beendigung

26. Diese Verpflichtungserklärung gilt akzessorisch zum Grundvertrag, also jedenfalls solange der Auftragsverarbeiter, die darin bezeichneten, datenschutzrechtlich relevanten Dienstleistungen für den Verantwortlichen erbringt. Sie endet ohne Bedarf gesonderter Erklärungen mit vollständigem Wegfall des Grund-Rechtsverhältnisses (gleich aus welchem Grund) beziehungsweise durch Widerruf des Auftragsverarbeiters.

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

Schlussbestimmungen

27. Änderungen und Ergänzungen dieser Verpflichtungserklärung, einschließlich des einvernehmlichen Abgehens vom Erfordernis der Schriftlichkeit, bedürfen der Schriftform, wobei die Übermittlung elektronischer Nachrichten an die zuletzt angegebene (E-Mail-)-Kontaktadresse genügt.
28. Sollten einzelne Teile dieser Verpflichtungserklärung ungültig sein oder werden, so berührt dies nicht die Wirksamkeit der Übrigen. Eine weggefallene Bestimmung ist durch diejenige zulässige bzw. gültige zu ersetzen, die der Verpflichtung des Auftragsverarbeiters durch die DS-GVO am nächsten kommt. Gleichermaßen ist bei Regelungslücken vorzugehen.

Wien, 01.04.2024

Ort, Datum

Signiert von: Alexander Höllwart
Datum: 06.05.2024 07:20:28
TRUST
Dieses Dokument ist digital signiert!
Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.
Prüfinformation: Informationen zur Prüfung der elektronischen Signatur finden Sie unter: www.a-trust.at/pdf

Alexander Höllwart
Geschäftsführer
CloudXcelerate GmbH

Signiert von: Michael Wilhelm Obernberger
Datum: 30.04.2024 16:02:58
TRUST
Dieses Dokument ist digital signiert!
Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.
Prüfinformation: Informationen zur Prüfung der elektronischen Signatur finden Sie unter: www.a-trust.at/pdf

Michael Obernberger
Geschäftsführer
CloudXcelerate GmbH

CloudXcelerate GmbH, HG Wien FN 572310 h, UID ATU80296813, Raiffeisenlandesbank Oberösterreich: IBAN: AT82 3400 0000 0005 7380, BIC RZOOAT2LXXX

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

Anhang

Technisch-organisatorische Maßnahmen (Art. 32 Abs. 1 DSGVO)

Der Auftragsverarbeiter hat die Datensicherheit bzw. ein dem Verarbeitungsrisiko angemessenes, dem Stand der Technik entsprechendes Schutzniveau hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie hinsichtlich der Belastbarkeit von Systemen zu gewährleisten. Um stets ein Schutzniveau gemäß dem aktuellen Stand der Technik zu gewährleisten, ist der Auftragsverarbeiter nach ISO 9001 und ISO 27001 zertifiziert und strebt an, diese Zertifizierungen kontinuierlich aufrechtzuerhalten. Zudem verfügt der Auftragsverarbeiter über die Qualifikation, das Cyber Trust Austria Gold Label zu führen.

Es wird festgehalten, dass sämtliche genannten Maßnahmen lediglich in den Betriebsräumlichkeiten und in der Zugriffssphäre des Auftragsverarbeiters gelten und umgesetzt wurden. Der Auftragsverarbeiter übernimmt keine Verantwortung und Haftung für die im Macht- und Einflussbereich des Verantwortlichen notwendigen und/oder geltenden technischen oder organisatorischen Maßnahmen. Insbesondere ausgenommen sind im Verantwortungsbereich des Verantwortlichen befindliche(s) Einrichtungen, Personal, IT-Infrastruktur, Gegenstände und Daten.

Soweit für die Vertragserfüllung relevant, sind dahingehend bereits (oder werden noch rechtzeitig) folgende Maßnahmen durch den Auftragsverarbeiter in seiner Systemumgebung gesetzt:

Zutrittskontrolle

- ✓ Personenkontrolle durch Portier oder Sicherheits-/Wachdienst
- ✓ Bewachung an Wochenenden/Feiertagen
- ✓ Alarmanlage/Einbruchsmeldesystem
- ✓ Videoüberwachung der Zugänge
- ✓ Zugangsbeschränkung für Büro- und Geschäftsräume
- ✓ Sicherheitsschlösser
- ✓ Absicherung von Gebäudeschächten, Hintertüren, Nebeneingängen etc.
- ✓ Bewegungsmelder/Lichtschranken
- ✓ Chipkarten-/Transponderregelung
- ✓ Schlüsselregelung

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

- ✓ Manuelles Schließsystem
- ✓ Protokollierung von Schlüssel-/Chipkarten-/Transponderausgaben
- ✓ Generalschlüsselregelung
- ✓ Regelung des Besucherzutritts (Anmeldung, Protokollierung)
- ✓ Besucherberechtigungsausweis-Tragepflicht
- ✓ Spezielle Sicherung/Zutrittsbeschränkung für Serverräume und Archive

Zugangskontrolle

- ✓ Sichere Aufbewahrung von Datenträgern
- ✓ „clean desk“ (digitaler Arbeitsplatz, Reinigung des virtuellen Desktops)
- ✓ Absicherung interner Schnittstellen (WLAN, LAN etc.)
- ✓ Richtlinie zur Passwortsicherheit
- ✓ Berechtigungskonzept
- ✓ Erstellung von Benutzerprofilen
- ✓ Zuordnung von Rechten und Rollen zu Datenverarbeitungssystemen
- ✓ Authentifizierung über eindeutige User-ID
- ✓ Zwei-Faktor-Authentifizierung und MFA
- ✓ Authentifizierung über Benutzername und Passwort bzw. Möglichkeit zur biometrischen Anmeldung
- ✓ Gesicherte Verbindung bei Fernwartung
- ✓ Protokollierung der Zugänge (An- und Abmeldung) zu Datenverarbeitungssystemen inkl. SIEM
- ✓ Kontosperre bei fehlerhaften Zugangsversuchen
- ✓ Automatische Rechnersperre bei vorübergehender Abwesenheit
- ✓ Regelmäßiger erzwungener Passwortwechsel
- ✓ Unverzügliche Sperre der Berechtigung ausgeschiedener Benutzer
- ✓ Verwaltung der Rechte durch Systemadministrator
- ✓ Sichere Aufbewahrung des Administrator-Passworts
- ✓ Angriffserkennungssystem/Anti-Viren-Software sowie verhaltensbasierende Malware- / Ransomware-Erkennung und Sandboxing für Server und Arbeitsplatzrechner (SoC, EDR)
- ✓ Abschottung durch Firewall inkl. Intrusion Detection & Prevention System

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

- ✓ Daten-/Festplattenverschlüsselung von mobilen Endgeräten (Smartphone, Notebook, USB-Stick etc.)
- ✓ Einsatz von Schutzprogrammen und Administrationssoftware auf Smartphones und Tablet-PCs
- ✓ Verbot der nicht genehmigten Installation von Soft- und Hardware
- ✓ Regelmäßige Aktualisierung der Schutzprogramme (Updates etc.)

Zugriffskontrolle

- ✓ Zugriffsbeschränkung für Computersysteme und Netzlaufwerke auf berechtigte Benutzer
- ✓ Zugriffsbeschränkung für Backup-Datenträger auf Systemadministratoren
- ✓ Verschlüsselung der Back-Ups in einer isolierten Umgebung
- ✓ Berechtigungskonzept
- ✓ Prozess zur Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen
- ✓ Berechtigungsminimierung nach Zweckbindungsprinzip (the principle of least privilege)
- ✓ Differenzierte Berechtigungen
- ✓ Berechtigungsverwaltung durch Systemadministrator
- ✓ Meldung und Auswertung erfolgter/versuchter Sicherheitsverletzungen
- ✓ Überschreibung der Datenträger mit geeigneter Software vor Wiederverwendung
- ✓ Ordnungsgemäße Datenträgervernichtung
- ✓ Einsatz geeigneter Datenschutzbehälter zur Verhinderung unbefugter Entnahmen
- ✓ Protokollierung der Entsorgung von Daten
- ✓ Verschlüsselung von Datenträgern

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

Weitergabekontrolle

- ✓ Monitoring des Datenverkehrs
- ✓ Verschlüsselte programmgesteuerte Übermittlung von Daten
- ✓ Kryptografisches Verschlüsselungsverfahren (z. B. S/MIME)
- ✓ Datentransfer über gesicherte Verbindungen (z. B. https/SFTP)
- ✓ Protokollierung von Abruf- und Übermittlungsvorgängen
- ✓ Einrichtung von Standleitungen bzw. VPN-Verfahren (SD WAN)
- ✓ Einsatz von Passwörtern und Passwortsicherheit
- ✓ Getrennte Wege zur Passwortübermittlung
- ✓ Eingabekontrolle
- ✓ Nachvollziehbarkeit der Zugriffe anhand individueller Benutzernamen
- ✓ Nachvollziehbarkeit der Zugriffe anhand der Benutzergruppen
- ✓ Protokollierung von Eingabe, Änderung und Löschung von Daten
- ✓ Authentizität (jederzeitige Datenzuordenbarkeit zu ihrem Ursprung)
- ✓ Übersicht der Applikationen, mit denen Daten eingegeben/geändert/gelöscht werden
- ✓ Auftragskontrolle
- ✓ Auswahl weiterer (Sub-)Auftragsverarbeiter, z. B. Callcenter, nach Datensicherheitsgarantien
- ✓ Verpflichtung aller Auftragsverarbeiter gemäß Art. 28 Abs. 3 DSGVO
- ✓ Sorgfältige Auswahl von IT-, Wach-, Reinigungs-, Entsorgungs-, Transport- u. a. Dienstleistern
- ✓ Datenschutz-Audits beim Auftragsverarbeiter
- ✓ Sicherstellung der Rückgabe/ordnungsmäßen Vernichtung aller Daten bei Vertragsbeendigung
- ✓ Beachtung der Voraussetzungen der DSGVO bei Auftragsdatenverarbeitung in Drittstaaten
- ✓ Risikobasierende Prüfungen von Auftragsdatenverarbeitungen in Drittstaaten
- ✓ Verfügbarkeitskontrolle
- ✓ Datensicherungskonzept
- ✓ Führen von Backup-Verzeichnissen bzw. einer Backup-Verzeichnisstruktur
- ✓ Notfallplan/Recovery-Konzept

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

- ✓ Backup-Rechenzentrum
- ✓ Datenwiederherstellungstests
- ✓ Einsatz spezieller Monitoring-Programme zur Überwachung der Verfügbarkeit
- ✓ Unterbrechungsfreie Stromversorgung (USV)
- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Feuerlöschgeräte
- ✓ Besonderer Brand-/Wassereintrittsschutz für Serverräume und Archive
- ✓ Temperatur-/Feuchtigkeitsüberwachung/Klimaanlage in Serverräumen und Archiven
- ✓ Abgestimmte und umgesetzte Anforderungen für Datenverfügbarkeit und - verarbeitbarkeit
- ✓ Minimierung der Eintrittspunkte für Schadsoftware (Abschaltung verzichtbarer Dienste)

Trennungsprinzip

- ✓ Keine Mitbenutzung der Büroräume, Archive und Server durch Fremdfirmen
- ✓ Physisch getrennte Datenspeicherung auf gesonderten Systemen, Laufwerken und Datenträgern
- ✓ Logische Mandantentrennung
- ✓ Festlegung von Datenbankrechten (Zugriffsschranken für einzelne Ordner, Datensätze, Felder)
- ✓ Rollentrennung von Benutzern
- ✓ Berechtigungskonzept
- ✓ Verwaltung der Berechtigungen durch Systemadministrator
- ✓ Mittels Berechtigungskonzept getrennte Speicherung besonders sensibler Daten (z. B. Personalbereich)
- ✓ Trennung von Entwicklungs-, Test- und Produktivsystemen
- ✓ Informationelle Gewaltenteilung

cloudXcelerate
Wienerbergstraße 53,
A-1120 Wien

Organisation

- ✓ Bestellung eines Datenschutzbeauftragten
- ✓ Verpflichtung der Mitarbeiter zur Wahrung des Datengeheimnisses
- ✓ Verpflichtung des Fremdpersonals zur Wahrung des Datengeheimnisses
- ✓ Datenschutz-Schulungen für Mitarbeiter
- ✓ Informationssicherheitsrichtlinien
- ✓ Regelung privater Nutzung betrieblicher Kommunikationstechnik
- ✓ Direkt-/Adressmarketing nach datenschutzrechtlichen Vorgaben
- ✓ Einsatz von Cloud Computing nach datenschutzrechtlichen Vorgaben
- ✓ Regelmäßige Durchführung interner Audits
- ✓ Datenschutz-Richtlinie

CloudXcelerate GmbH, HG Wien FN 572310 h, UID ATU80296813, Raiffeisenlandesbank Oberösterreich: IBAN: AT82 3400 0000 0005 7380, BIC RZOOAT2LXXX