



VEREINBARUNG

über eine Auftragsverarbeitung nach § 28 DSGVO

zwischen

Firmenname

Anschrift

– (nachfolgend „Verantwortlicher“ oder „Kunde“) –

und

dox42 GmbH,

Linke Wienzeile 8/29

A-1060 Wien

– (nachfolgend „Auftragsverarbeiter“ oder „IT-Dienstleister“) –

– (gemeinsam bezeichnet als „Parteien“) –

Klassifizierung: INTERN

Version: 1.4

Status: FINAL

Gültig ab: 06.11.2024

Eigner: CISO

Geprüft durch: CEO

Freigabe durch: CEO



Änderungsverzeichnis

Datum	Version	Erstellt durch	Beschreibung der Änderung
12.03.2021	1.0	Christian Bauer	Final
25.10.2022	1.1	Julia Friedrich	ISMS-Layout wurde hinzugefügt
14.06.2023	1.2	Florian Parfuss	Adaptierung CI 2023
19.07.2023	1.3	Peter Wendlinger	Adaptierung Sonstiges
06.11.2024	1.4	Norina Aichholz	Unternehmensadresse geändert

Inhaltsverzeichnis

Änderungsverzeichnis	2
Präambel	3
1. Ziel und Dauer der Vereinbarung	3
2. Weisungsrecht	4
3. Vertraulichkeit	4
4. Datensicherheit	4
5. Sub-Auftragsverarbeitung	5
6. Unterstützung	6
7. Rückgabe von personenbezogenen Daten	6
8. Überprüfung	7
9. Haftung	7
10. Sonstiges	8

Präambel

Der Kunde nutzt nach dem Hauptvertragsverhältnis (Lizenzkauf) den vom Auftragsverarbeiter betriebenen internetbasierten Dienst („dox42 online“). In diesem Zusammenhang ist es nicht ausgeschlossen, dass der Auftragsverarbeiter personenbezogene Daten verarbeitet. Nach Art 28 DSGVO ist hierfür der Abschluss eines Auftragsdatenverarbeitungsvertrags erforderlich.

Voraussetzung für die Zulässigkeit einer solchen Auftragsverarbeitung iSd Art 28 DSGVO ist, dass der Kunde den Auftrag an den IT-Dienstleister zur Verarbeitung erteilt. Dieser Vertrag enthält diesen Auftrag des Kunden an den IT-Dienstleister und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit dieser Datenverarbeitung sowie die sich daraus ergebenden besonderen Pflichten in Bezug auf Datenschutz und Datensicherheit.

Grundsätzlich ist der Kunde für die Einhaltung der Vorschriften der DSGVO und anderer Vorschriften über den Datenschutz verantwortlich und behält insofern die Herrschaft und Kontrolle (Bestimmung über Mittel und Zweck) über die zu verarbeitenden Daten. Der IT-Dienstleister wird den Kunden hierbei in geeigneter Weise unterstützen.

1. Ziel und Dauer der Vereinbarung

- 1.1. Der Auftragsverarbeiter hat sich verpflichtet, die in Anhang 1 beschriebenen Datenverarbeitungen gegenüber dem Verantwortlichen zu erbringen. Für die Zwecke dieser Vereinbarung gelten die Begriffsdefinitionen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, nachfolgend kurz „DSGVO“).
- 1.2. Der Vertrag beginnt mit Abschluss des Hauptvertrages (Gegenstand ergibt sich aus der Leistungsvereinbarung oder Lizenzkaufvertrag) und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen durch den Kunden.
- 1.3. Wenn der Kunde eine Vertragsverlängerung vornimmt, gelten die zu diesem Zeitpunkt aktuellen Bestimmungen der Auftragsverarbeitung des IT-Dienstleisters. Ebenso sind Aktualisierungen oder Erweiterungen des angebotenen Dienstes von diesen Bestimmungen mitumfasst.
- 1.4. Der Kunde kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des IT-Dienstleisters gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der IT-Dienstleister eine Weisung des Kunden nicht ausführen kann oder will oder der IT-Dienstleister den Zutritt des Kunden oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

2. Weisungsrecht

- 2.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation –, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist.
- 2.2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er ohne Durchführung einer rechtlichen Prüfung durch einen Juristen der Auffassung ist, dass eine Weisung offensichtlich gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist nicht verpflichtet, sich in Zusammenhang mit der Erfüllung dieser Vereinbarung rechtlich beraten zu lassen und erbringt in Erfüllung dieser Vereinbarung auch keine Rechtsberatungsleistungen.
- 2.3. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er nach dem Recht der Union oder der Mitgliedstaaten dazu verpflichtet ist, entgegen den Weisungen des Verantwortlichen oder ohne Weisung des Verantwortlichen eine Datenverarbeitung vorzunehmen (sofern eine solche Mitteilung zulässig ist).
- 2.4. Weisungen des Verantwortlichen stehen im Einklang mit dem Regelungsgegenstand dieser Vereinbarung. Sollte dem Auftragsverarbeiter aus der Befolgung der Weisung ein Aufwand im Umfang von mehr als einer Arbeitsstunde entstehen, so ist der Aufwand vom Verantwortlichen zu vergüten.
- 2.5. Der Auftragsverarbeiter kann Informationen und Mitteilungen im Zusammenhang mit der Erfüllung seiner Pflichten elektronisch, auch per E-Mail oder über den Onlinedienst (Plattform) zur Verfügung stellen. Eine Benachrichtigung gilt ab jenem Datum als erteilt, an dem diese dem Kunden zur Verfügung gestellt wurde. Möchte der Kunde eine weisungsberechtigte Person bestimmen, so sind deren Kontaktdaten dem Auftragsverarbeiter bekannt zu geben.

3. Vertraulichkeit

- 3.1. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen bleibt auch nach Beendigung ihrer Tätigkeit und nach Ausscheiden beim Auftragsverarbeiter aufrecht.

4. Datensicherheit

- 4.1. Der Auftragsverarbeiter ergreift alle gemäß Artikel 32 DSGVO zwingend erforderlichen Maßnahmen.
- 4.2. Das Sicherheitsniveau der Auftragsverarbeitung muss so konzipiert sein, dass der Umstand und der Zweck der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos berücksichtigt werden. Die ergriffenen technischen und organisatorischen Maßnahmen sollen dem Risiko entsprechend ein angemessenes Schutzniveau gewährleisten.
- 4.3. Der Auftragsverarbeiter hat insbesondere die in Anhang 2 angeführten Maßnahmen zu implementieren. Über wesentliche Änderungen von Sicherheitsmaßnahmen wird der Verantwortliche zeitgerecht in Kenntnis gesetzt.

- 4.4. Der Auftragsverarbeiter wird den Verantwortlichen von jeder Verletzung des Schutzes personenbezogener Daten informieren („Data Breach“), sofern dies Daten betrifft, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet, und durch die Verletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen entsteht. Diese Information hat unverzüglich zu erfolgen, sobald der Auftragsverarbeiter von einer solchen Verletzung Kenntnis erlangt und ist an jene Kontaktstelle zu richten, die der Verantwortliche schriftlich bekannt gegeben hat.
- 4.5. Die unter Punkt 4.3 genannte Information des Verantwortlichen soll, soweit unter Berücksichtigung der Umstände möglich, Folgendes beinhalten:
- a) die Art der Verletzung des Schutzes personenbezogener Daten, wenn möglich einschließlich der Kategorien und der ungefähren Zahl der betroffenen Personen und der Kategorien und der ungefähren Zahl der betroffenen Datensätze;
 - b) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten; und
 - c) die vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten.

5. Sub-Auftragsverarbeitung

- 5.1. Der Auftragsverarbeiter informiert den Verantwortlichen zeitgerecht über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter oder Sub-Auftragsverarbeiter (im Folgenden zusammen „Sub-Auftragsverarbeiter“), wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen, der in Anhang 3 angeführten Sub-Auftragsverarbeiter, Einspruch zu erheben und die Hinzuziehung oder die Ersetzung zu untersagen. Erhebt der Verantwortliche innerhalb von zwei Wochen keinen Einspruch, so gilt die Hinzuziehung oder Ersetzung als genehmigt. Allfällige Ablehnungsgründe sind dem Auftragsverarbeiter schriftlich darzulegen. Im Falle eines Einspruchs stimmen sich beide Parteien in Bezug auf das weitere Vorgehen unverzüglich miteinander ab.
- 5.2. Nimmt der Auftragsverarbeiter einen anderen Sub-Auftragsverarbeiter in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Sub-Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des anwendbaren Datenschutzrechts erfolgt.
- 5.3. Ein Sub-Auftragsverarbeiterverhältnis im Sinne dieses Vertrags liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind (beispielsweise: Post-, Transport-, Versand-, Reinigungs-, Telekommunikationsleistungen ohne konkreten Bezug zur Leistungserfüllung). Wartungs- und Prüfleistungen stellen eine Subauftragsverarbeitung dar, soweit diese für jene IT-Systeme erbracht werden, die im Zusammenhang mit der Vertragsverfüllung für den Kunden stehen.

6. Unterstützung

- 6.1. Soweit dies möglich ist, unterstützt der Auftragsverarbeiter den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten des Verantwortlichen bei Anträgen auf Wahrnehmung der Betroffenenrechte gemäß dem anwendbaren Datenschutzrecht, einschließlich Kapitel III der DSGVO.
- 6.2. Der Auftragsverarbeiter erfüllt seine Pflicht nach Punkt 6.1 grundsätzlich dadurch, dass er dem Verantwortlichen eingelangte Anträge von Betroffenen weiterleitet. Soweit der Verantwortliche eine zusätzliche Unterstützung des Auftragsverarbeiters für notwendig erachtet und sich der Auftragsverarbeiter dazu bereit erklärt, eine solche Unterstützungsleistung zu erbringen, ist der Auftragsverarbeiter berechtigt, hierfür eine zusätzliche angemessene Vergütung zu fordern. Der Verantwortliche ist für die Beantwortung von Anfragen verantwortlich, einschließlich, falls erforderlich, zur Nutzung und Funktionalität des angebotenen Dienstes.
- 6.3. Darüber hinaus unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß dem anwendbaren Datenschutzrecht, einschließlich Artikel 32–36 DSGVO. Dies erfüllt der Auftragsverarbeiter durch (i) Ergreifen der Maßnahmen unter Punkt 3 („Vertraulichkeit“) und 4 („Datensicherheit“) dieser Vereinbarung, (ii) die Meldung an den Verantwortlichen über eine Verletzung des Schutzes personenbezogener Daten nach Punkt 4.3 sowie (iii) durch die Zurverfügungstellung der Informationen in Anhang 1 dieser Vereinbarung.

7. Rückgabe von personenbezogenen Daten

- 7.1. Nach Wahl des Verantwortlichen löscht der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten oder gibt diese in angemessenem Zeitraum zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
- 7.2. Wenn der Verantwortliche wählt, die Daten zurück zu erhalten, so hat der Auftragsverarbeiter die Daten an den Verantwortlichen in einem wiederverwendbaren und gängigen elektronischen Datenformat zu übermitteln, das in Abstimmung mit dem Verantwortlichen gewählt werden kann.

8. Überprüfung

- 8.1. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung.
- 8.2. Der Auftragsverarbeiter ermöglicht vorangemeldete Überprüfungen (sog. Audits) zu Geschäftszeiten durch einen unabhängigen Dritten, der einer Verschwiegenheitspflicht unterliegt. Solche Überprüfungen werden in angemessenen zeitlichen Abständen und in einer Art durchgeführt, die den Geschäftsbetrieb des Auftragsverarbeiters nicht stören. Kosten, welche durch solche Überprüfungen anfallen, sind vom Verantwortlichen zu tragen. Dem Auftragsverarbeiter steht für alle Leistungen in Zusammenhang mit der Unterstützung von Überprüfungen ein angemessenes Entgelt zu.
- 8.3. Der Auftragsverarbeiter kann seine Pflichten nach Punkt 8.2 auch dadurch erfüllen, dass er zumindest alle drei Jahre eine Überprüfung durch einen unabhängigen Dritten vornehmen lässt und die zusammengefassten Prüfungsergebnisse dem Verantwortlichen zukommen lässt. Ebenso kann der Auftragsverarbeiter seine Pflichten nach Punkt 8.2 dadurch erfüllen, wenn er eine anerkannte Zertifizierung nachweist, die ein dem Stand der Technik entsprechendes Datenschutzniveau bestätigt.
- 8.4. Wird der Auftragsverarbeiter durch eine Aufsichtsbehörde oder einer anderen behördlichen Stelle betreffend die Verarbeitung im Auftrag geprüft, verpflichtet sich der Verantwortliche die Unterstützungsleistung mit einem angemessenen Entgelt zu entschädigen.

9. Haftung

- 9.1. Es wird auf die Regelungen des Art 82 DSGVO verwiesen.
- 9.2. Der Auftragsverarbeiter haftet nach den Grundsätzen des österreichischen Zivilrechts.
- 9.3. Die Haftung beider Parteien ist auf grobes Verschulden beschränkt. Eine Haftung für bloße Vermögensschäden ist ausgeschlossen.
- 9.4. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter für einen durch eine datenschutzwidrige Verarbeitungstätigkeit entstandenen Schaden verantwortlich, so haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung.
- 9.5. Dessen ungeachtet haftet der Verantwortliche dem Auftragsverarbeiter für die Rechtmäßigkeit aller erteilten Weisungen und stellt ihn hinsichtlich aller aus der Befolgung einer Weisung resultierenden Schäden und Nachteile klag- und schadlos.
- 9.6. Im Falle einer Inanspruchnahme des Auftragsverarbeiter durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO, verpflichtet sich der Verantwortliche den Auftragsverarbeiter bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

10. Sonstiges

10.1. Es gilt österreichisches Recht.

10.2. Änderungen dieser Vereinbarung sind ausschließlich in schriftlicher Form vorzunehmen. Dies gilt auch für dieses Schriftlichkeitsgebot.

10.3. Sollte eine Bestimmung dieser Vereinbarung ungültig oder unwirksam sein, wird sie, soweit gesetzlich zulässig, durch jene Bestimmung ersetzt, die wirtschaftlich der ungültigen oder unwirksamen Bestimmung am nächsten kommt.

Im Namen des Verantwortlichen:

Im Namen des Auftragsverarbeiters:

DocuSigned by:
Christian Bauer
E159E8CE2CA249C...

Ort und Datum:

Ort und Datum: 11/8/2024

Anhang 1: Details zur Datenverarbeitung

Anhang 2: Technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten

Anhang 3: Eingesetzte Sub-Auftragsverarbeiter

Anhang 1: Details zur Datenverarbeitung

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

Vom Verantwortlichen durch Inanspruchnahme der vom Auftragsverarbeiter angebotenen IT-Services gespeicherte Daten von Interessenten (Test-User), Plattformnutzer, Endkunden (Lizenznehmer), Geschäftspartner oder Mitarbeiter.

Kategorien von Daten

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien:

Vom Verantwortlichen durch Inanspruchnahme der vom Auftragsverarbeiter angebotenen IT-Services gespeicherte Daten nämlich bspw. Name, Anschrift, E-Mail-Adresse, Rufnummer, Zahlungen etc. werden in folgende Kategorien zusammengefasst:

- ▶ Personenstammdaten
- ▶ Kommunikationsdaten (Mail Korrespondenz)
- ▶ Vertragsstammdaten
- ▶ Kundenhistorie (Bestellungen)
- ▶ Buchhaltung (Zahlungsdaten und Abrechnung)
- ▶ Firmen- und Bonitätsdaten (Auskunfteien, Firmenbuchauszug)
- ▶ Nutzerdaten (Protokolldaten, Daten im Zusammenhang mit Inanspruchnahme der Produkte und Dienstleistungen)
- ▶ Kundenservice

Kategorien von sensiblen Daten (falls zutreffend)

Werden Inhaltsdaten von Dokumenten verarbeitet, kann nicht ausgeschlossen werden, dass Daten der Kunden oder von Dritten ohne direkten geschäftlichen Bezug zum Auftragsverarbeiter oder Verantwortlichen betroffen sind. Nach Mitteilung des Verantwortlichen oder aufgrund des absehbaren Geschäftsmodells (Anwalt, Gesundheitsberufe, etc.) wird davon ausgegangen, dass die zu verarbeitenden personenbezogenen Daten teilweise als besonderen Kategorien personenbezogener Daten iSd Art 9 DSGVO einzuordnen sind.

Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen

Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

Gegenstand der Vereinbarung sind ausschließlich jene Datenverarbeitungen, welche für die Erfüllung des jeweiligen Verarbeitungsauftrages erforderlich oder zweckdienlich sind. Es werden außer diesen Daten keine weiteren Daten verarbeitet.

Im Einzelnen sind zur Durchführung des Verarbeitungsauftrages die teilweise oder gänzliche Durchführung einer oder mehrerer der folgenden Aufgaben Gegenstand dieser Vereinbarung

- ▶ Betrieb der Software;

- ▶ Wartung der Software (Updates), Unterstützung bei der Installation, Konfiguration und Anwendung von Software inklusive Dokumentation der jeweiligen Tätigkeit;
- ▶ Technischer Support, Untersuchung und Behebung von Störfällen inklusive Dokumentation

Verarbeitungszwecke

Die übermittelten personenbezogenen Daten werden zu folgenden Zwecken des Verantwortlichen verarbeitet:

Je nach Gegenstand der Verarbeitung des Verarbeitungsauftrages werden Daten zu folgenden Zwecken verarbeitet

- ▶ Betrieb einer Cloud-basierten Plattform zur Generierung und Versendung von Dokumenten
- ▶ Abwicklung des Kundenkontaktes

Anhang 2: Technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten (gem. Art. 32 DSGVO). Insbesondere um folgende aufgeführte Maßnahmen zur Sicherung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme sowie der zu verarbeitenden Daten zu gewährleisten:

- ▶ Zutrittskontrolle
- ▶ Zugangskontrolle
- ▶ Zugriffskontrolle
- ▶ Weitergabekontrolle
- ▶ Eingabekontrolle
- ▶ Auftragskontrolle
- ▶ Verfügbarkeitskontrolle
- ▶ Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er berücksichtigt, dass das gesetzlich notwendige Schutzniveau (siehe Punkt 4 des Vertrages) nicht unterschritten wird.

a. Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung einer Datenschutzverletzung

Technische Maßnahmen

- ▶ Authentifizierung: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
- ▶ Passwortsicherheit: Soweit Passwörter zur Authentifizierung eingesetzt werden, sollten diese mindestens acht Zeichen lang sein und aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter werden ausschließlich verschlüsselt gespeichert.
- ▶ Verschlüsselung auf dem Übertragungsweg: Personenbezogene Daten werden auf dem Übertragungsweg über das Internet verschlüsselt, zumindest, soweit es sich um sensible Daten handelt.
- ▶ Verschlüsselung mobiler Geräte: Mobile Endgeräte und mobile Datenträger werden verschlüsselt, zumindest, soweit auf diesen Geräten sensible Daten gespeichert werden.
- ▶ Netzwerksicherheit: Es wird eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.
- ▶ Maßnahmen gegen Schadsoftware: Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt. Alle eingehenden E-Mails werden automatisch auf Schadsoftware gescannt.

- ▶ Management von Sicherheitslücken: Soweit möglich, wird auf allen Geräten die automatische Installation von Sicherheitsupdates aktiviert. Die Installation von Updates an Servern findet organisiert durch den IT-Zuständigen zeitgerecht und je nach Kritikalität statt.

Organisatorische Maßnahmen

- ▶ Eindeutige Zuständigkeiten: Interne Zuständigkeiten für Fragen der Datensicherheit werden definiert.
- ▶ Verschwiegenheitspflicht der Dienstnehmer: Die Dienstnehmer werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung eines Vorgesetzten an Dritte zu über-mitteln.
- ▶ Schulungen und Informationsmaßnahmen: Die Dienstnehmer werden zu Fragen der Datensicherheit (intern oder extern) geschult und angemessen über Fragen der Datensicherheit informiert (zB Passwortsicherheit).
- ▶ Geordnete Beendigung des Dienstverhältnisses: Bei Beendigung des Dienstverhältnisses erfolgt eine unverzügliche Sperrung aller Konten des ausscheidenden Dienstnehmers sowie eine Abnahme aller Schlüssel des ausscheidenden Dienstnehmers.
- ▶ Eingabekontrolle: Es bestehen Verfahren zur Kontrolle der Richtigkeit der eingegebenen personenbezogenen Daten (zb Abgleich von Kundeninformationen, 2-Augenprinzip).
- ▶ Auswahl der Dienstleister: Bei der Auswahl von Dienstleistern wird das vom Dienstleister gebotene Datensicherheitsniveau berücksichtigt. Der Einsatz eines Dienstleisters, der als Auftragsverarbeiter einzustufen ist, erfolgt nur nach Abschluss einer Auftragsverarbeitervereinbarung.

Physische Maßnahmen

- ▶ Physische Zugangskontrolle: Das Betreten der Betriebsräumlichkeiten ist für betriebsfremde Personen nur in Begleitung einer betriebsangehörigen Person zulässig.
- ▶ Einbruchssicherheit: Die Zugänge zu den Betriebsräumlichkeiten verfügen über einen angemessenen Einbruchsschutz (zB eine Sicherheitstüre höherer Widerstandsklasse).

b. Maßnahmen zur Erkennung eines Angriffs

Technische Maßnahmen

- ▶ Scans nach Schadsoftware: Es werden regelmäßig Scans nach Schadsoftware (Anti-Viren-Scans) durchgeführt, um Schadsoftware zu identifizieren, welche ein IT-System bereits kompromittiert hat.

Organisatorische Maßnahmen

- ▶ Erkennung von Sicherheitsverletzungen durch Dienstnehmer: Alle Dienstnehmer werden instruiert, wie sie Sicherheitsverletzungen erkennen und berichten können (zB nicht mehr auffindbare Computer-Hardware, Meldungen von Anti-Viren-Software).
- ▶ Reporting-Systeme: Es bestehen Verfahren, die es Mitarbeitern ermöglichen, Auffälligkeiten und Anomalien bei technischen Systemen an die zuständigen Personen zu melden.
- ▶ Betriebsfremde Personen: Alle Dienstnehmer werden instruiert, betriebsfremde Personen anzusprechen, sollten sie in den Betriebsräumlichkeiten angetroffen werden.

- ▶ Audits: Es werden regelmäßige Audits durchgeführt (zB Prüfung, ob alle kritischen Sicherheits-Updates installiert wurden). Insbesondere erfolgt eine regelmäßige Prüfung der erteilten Zugriffs- und Zutrittsberechtigungen (welchem Mitarbeiter ist welcher Benutzer-Account mit welchen Zugriffsrechten zugewiesen; welche Personen verfügen über welche Schlüssel).
- ▶ Manuelle Prüfung von Logfiles: Soweit Logfiles geführt werden (zB über erfolglose Authentifizierungsversuche), werden diese in regelmäßigen Abständen geprüft.

c. Maßnahmen zur Reaktion auf eine Datenschutzverletzung

Technische Maßnahmen

- ▶ Datensicherung: Es werden regelmäßig Datensicherungen erstellt und sicher aufbewahrt.
- ▶ Datenwiederherstellungskonzept: Es wird ein Konzept zur raschen Wiederherstellung von Datensicherungen entwickelt, um nach einer Sicherheitsverletzung zeitnah den regulären Betrieb wiederherstellen zu können.
- ▶ Automatische Entfernung von Schadsoftware: Die eingesetzte Anti-Viren-Software verfügt über die Funktion, Schadsoftware automatisch zu entfernen.

Organisatorische Maßnahmen

- ▶ Meldepflicht für Dienstnehmer: Alle Dienstnehmer werden angewiesen, Sicherheitsverletzungen unverzüglich an eine zuvor definierte interne Stelle bzw Person zu melden.
- ▶ Prozess für die Reaktion auf Sicherheitsverletzungen: Es wird durch einen geeigneten Prozess sichergestellt, dass Sicherheitsverletzungen innerhalb von 72 Stunden ab Kenntnis an die Datenschutz-behörde gemeldet werden können. Insbesondere sind allen Dienstnehmern die Notfall-Telefonnummern der zu involvierenden Personen bekannt zu geben (zB Notfall-Telefonnummer für den IT-Support).

d. Maßnahmen zur Minderung einer Angreifer Motivation

Organisatorische Maßnahmen

- ▶ Protokollierung von Zugriffen: Zugriffe auf Anwendungen, insb Eingabe, Löschung und Änderung von Daten, werden protokolliert.

e. Standortbezogene Maßnahmen

Technische Maßnahmen

- ▶ Einrichtung von Schutzzonen: Soweit die Auftragstätigkeit für den Verantwortlichen eine Verarbeitung in einer besonderen Schutzzone erfordert, ist sichergestellt, dass für die zugehörigen Räume dieser Schutzzone besondere Zutrittsmittel nötig sind, die dazu beitragen, dass nur Befugte Zutritt zu diesen Schutzzonen erhalten. Soweit für die besonderen Schutzzonen darüber hinaus spezifische Vorkehrungen (wie z.B. Einbau einer Alarmanlage, Videoüberwachung, Einbruchssicherung) zu treffen sind, sind diese umgesetzt.

Organisatorische Maßnahmen

- ▶ Datenverarbeitung im Inland/EWR: Alle Standorte, an denen personenbezogene Daten des Verantwortlichen gespeichert werden, befinden sich in der EU bzw. in Österreich. Alle Standorte, von denen aus auf personenbezogene Daten des Verantwortlichen zugegriffen werden, befinden sich entweder in der EU, in einem Drittstaat mit ausreichendem Datenschutzniveau oder sind in einem EU-Standardvertrag bzw. in genehmigten Verhaltensregeln eingebunden.
- ▶ Protokollierung von Besuchern und Hilfspersonal: Besucher, die Zutritt zum Gebäude erhalten, in dem personenbezogene Daten des Verantwortlichen verarbeitet werden, werden begleitet oder auf Vertraulichkeit verpflichtet. Wartungstätigkeiten durch Fremdpersonal erfolgen im Serverraum nur unter Beaufsichtigung.

f. Maßnahmen für einen ordnungsgemäßen Betrieb

Technische Maßnahmen

- ▶ Datensicherheit und -sicherung: Zur Datensicherung eingesetzte Medien werden im Rahmen der Archivierung getrennt von produktiven Servern, mit denen personenbezogene Daten des Verantwortlichen verarbeitet werden, aufbewahrt. Die Wirksamkeit von Datensicherungen wird regelmäßig durch Wiedereinspieltests überprüft.
- ▶ Stromversorgung: Server, auf denen personenbezogene Daten des Verantwortlichen gespeichert werden, verfügen über eine ausreichend dimensionierte unterbrechungsfreie Stromversorgung.
- ▶ Löschung: Die beim Auftragsverarbeiter gespeicherten personenbezogenen Daten des Verantwortlichen werden nach Ablauf der festgelegten Speicherdauer gelöscht. Wenn Datenträger entsorgt werden sollen, die Daten des Verantwortlichen enthalten, welche mittels des eingesetzten Serversystems gespeichert, übertragen oder ausgewertet werden, werden diese Datenträger entweder physisch zerstört oder mittels einer Löschungssoftware so überschrieben, dass eine Rekonstruktion der Daten mit vertretbarem Aufwand nicht mehr möglich ist.

Organisatorische Maßnahmen

- ▶ Behandlung von Datenpannen: Im laufenden Betrieb festgestellte Sicherheitsvorfälle, die personenbezogene Daten des Verantwortlichen betreffen, werden dem Verantwortlichen unverzüglich gemeldet.
- ▶ Berechtigungen: Zugangsberechtigungen werden mit Ende der Gültigkeit der Berechtigungen unverzüglich gesperrt.

Anhang 3: Eingesetzte Sub-Auftragsverarbeiter

Der Auftragsverarbeiter setzt derzeit folgende Unterauftragnehmer ein:

Zweck: Bereitstellung der (Cloud-) Systeme [Windows Azure]

Microsoft Österreich GmbH

Am Euro Platz 3

1120 Wien

Austria – EU

Zweck: 7x24 Support

netgo GmbH

Weseler Str. 9

46325 Borken

Deutschland - EU

Zweck: DDOS Protection und DNS

Cloudflare Germany GmbH

Rosental 7,

80331 München

Deutschland - EU