Anlage Nutzungsbedingungen Finmas Portal

§ 1 Anwendungsbereich

(1) Finmas betreibt ein unter https://www.connect.finmas.de betriebenes Portal (nachfolgend das „Portal“). Mit Finmas vertraglich verbundene Unternehmen (nachfolgend „Partner“; zusammen nachfolgend „Parteien“) bekommen die Möglichkeit über das Portal ihren freigeschaltenen Zugang zu verwalten.
(2) Auf dem Portal können Partner Produkte und Leistungen einsehen, verwalten, steuern und managen, Zugänge für weitere Nutzer administrieren, Zugriffsbeschränkungen einrichten sowie enthaltene weiterführende Links zu Produkten nutzen.

§ 2 Allgemeines

(1) Diese Nutzungsbedingungen (einschließlich der Auftragsverarbeitungsvereinbarung) regeln die Rechte und Pflichten der Parteien in Bezug auf die Nutzung des Portals.
(2) Diese Nutzungsbedingen sind Teil der zwischen den Parteien vereinbarten „Finmas Konditionen“.
(3) Nur Unternehmen (Unternehmer nach § 14 BGB) dürfen sich als Portalnutzer auf dem Portal registrieren. Verbrauchern (nach § 13 BGB), ist die Nutzung nicht gestattet.

§ 3 Leistungsumfang

(1) Finmas stellt unter der URL connect.finmas.de (nachfolgend „Plattform-Website") das Portal zur Verfügung. Dem Partner wird die Möglichkeit gegeben verschiedene Vertriebskanäle zu steuern und auszuwerten.
(2) Finmas ist berechtigt, die auf dem Portal abgebildeten Produkte und Leistungen unter Berücksichtigung der berechtigten Interessen des Partners anzupassen.
(3) Finmas stellt dem Partner drei verschiedene Zugangsarten zur Verfügung. Unterschieden wird zwischen folgenden Zugängen:
    - Adminuser: Der vom Partner ausgewählte Adminuser kann über die Nutzerverwaltung eigenständig weitere Zugänge anlegen und auswählen welche Berechtigungen diese Zugänge erhalten. Der Adminuser hat Zugriff auf sämtliche Dashboards.
    - Systemuser: Der Systemuser kann weitere Zugänge anlegen und auswählen welche Berechtigungen diese Zugänge erhalten. Der Systemuser hat keinen Zugriff auf die Dashboards.

- User (Standardzugang): Der Standardzugang kann keine Nutzverwaltung durchführen oder über die Zugriffsverwaltung der Dashboards verfügen.

(4) Auf allen Zugängen zum Portal können eigene personen- und dienstbezogene Angaben (bspw. berufliche Stellung beim Partner, Kontaktdaten) eingegeben, geändert oder gelöscht werden.
(5) Auf allen Zugängen besteht die Möglichkeit Änderungen zum Newsletter Versand vorzunehmen, Supportanfragen zu stellen sowie auf einen FAQ-Bereich zuzugreifen.
(6) Hat der Partner einzelne Produkte innerhalb des Portals nicht gebucht, werden ihm diese Produkte zwar angezeigt, ein Abruf ist aber nichtmöglich.

§ 4 Registrierung

(1) Die Nutzung des Portals und der angeschlossenen Produkte und Folgefunktionen (bspw. Anbindung Dashboard) von Finmas setzt eine Registrierung durch den jeweiligen Partner voraus. Dabei werden sowohl die relevanten gewerblichen Daten des Partners als auch die dienstlichen Kontaktdaten der natürlichen Personen (Admin, einfache Nutzer) erfasst, welche die Registrierung für den Partner durchführen (nachfolgend „Nutzer"). Der Partner ist verpflichtet, alle relevanten geschäftlichen Daten vollständig und wahrheitsgemäß anzugeben. Der jeweilige Nutzer teilt zu seiner Registrierung seine geschäftliche E-Mail-Adresse mit und wählt ein Passwort aus.
(2) Als Nutzer ist jeder natürlichen Person die Durchführung einer Registrierung erlaubt, die vom jeweiligen Partner hierzu berechtigt ist. Finmas darf Partner Nachweise über die Berechtigung von Portalnutzern verlangen. Eine diesbezügliche Prüfungspflicht von Finmas besteht jedoch nicht. Weiter darf Finmas im Zusammenhang mit dem Betrieb des Portals jederzeit Kontakt mit einem Portalnutzer aufnehmen. Eine Kontaktaufnahme erfolgt per E-Mail, telefonisch oder postalisch. Es ist unzulässig, mehrere Registrierungen für denselben Portalnutzer anzulegen.
(3) Ein Anspruch auf Registrierung besteht nicht. Finmas ist berechtigt, eine Registrierung ohne Angabe von Gründen abzulehnen. Finmas ist berechtigt, das Konto eines Nutzers oder die Anmeldung eines Nutzers nicht freizuschalten oder nachträglich zu sperren, wenn Gefahr im Verzug droht. Wenn Anhaltspunkte für eine Nutzung der Plattform, die den berechtigten Interessen der übrigen Nutzer und Partner zuwiderläuft oder deren Rechte verletzt, bestehen oder Nutzer und Partner wissentlich falsche Angaben tätigten, hat Finmas das Recht, den betreffenden Nutzer und Partner von der Nutzung des Portals dauerhaft auszuschließen, wenn eine vorherige Abmahnung mit angemessener Fristsetzung keine Abhilfe geschaffen hat.

§ 5 Nutzung der Plattform

(1) Die Nutzung der Plattform ist für die Nutzer unentgeltlich.
(2) Ein gesonderter Nutzungsvertrag wird mit Finmas nicht geschlossen.
(3) Für vom Nutzer eingestellte Informationen und hochgeladene Daten übernimmt Finmas keine Haftung. Im Übrigen ergibt sich die Haftung aus den Konditionen.

§ 6 Sicherheit/ Kommunikation / Plattform-Website

(1) Finmas stellt mit angemessener Sorgfalt i.S.v. Art. 32 Abs. 2 DSGVO sicher, dass sämtliche Daten auf dem Portal und die Kommunikation über das Portal vor unberechtigten Zugriffen Dritter geschützt werden.
(2) Finmas verpflichtet sich, alle betreffenden datenschutzrechtlichen Anforderungen in ihrer jeweils geltenden Fassung zu einzuhalten. Auf die entsprechenden datenschutzrechtlichen Erklärungen in den Konditionen wird verwiesen.
(3) Finmas verarbeitet vom Nutzer zur Verfügung gestellte personenbezogene Daten als Auftragsverarbeiter i.S.v. Art. 28 DSGVO. Die Nutzer sind verpflichtet, die von ihnen jeweils zur Verfügung gestellten Daten außerhalb des Portals angemessen zu sichern.
(4) Der Partner verpflichtet sich zur Einsetzung von geeigneten IT-Sicherheitsmaßnahmen wie bspw. einer Festplattenverschlüsselung zum Schutz vor dem einfachen Auslesen von Zugangs- und Sitzungsdaten. Des Weiteren verwendet der Partner einen Malwareschutz (Virenscanner) auf denen von ihm eingesetzten Geräten.
(5) Das Portal bietet technische Möglichkeiten, Dokumente und andere geschäftliche Inhalte durch den Nutzer herunterzuladen. Der Partner sichert zu, die über die Download-Funktion erlangten Dokumente ausschließlich für seine geschäftliche Tätigkeit zu nutzen. Mit erfolgtem Download der bereitgestellten Inhalte ist ausschließlich der Nutzer für die weitere Verwendung verantwortlich.

§ 7 Änderung von Nutzungsbedingungen

(1) Änderungen dieser Nutzungsbedingungen können dadurch vereinbart werden, dass Finmas dem Partner die geänderten Nutzungsbedingungen spätestens vier Wochen vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform anbietet. Änderungen dieser Bedingungen können auch durch ein Angebot von Finmas über das Portal und die Annahme des Partners durch Aktivierung einer entsprechenden Schaltfläche oder Ankreuzoption auf dem Portal beim Login erfolgen.
(2) Die Zustimmung eines Partners gilt – bei Änderungen, die für ihn keine rechtlichen und wirtschaftlichen Nachteile enthalten – als erteilt, wenn er seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen gegenüber Finmas mitgeteilt hat.

(3) Änderungen – die rechtliche oder wirtschaftlichen Nachteile mit sich bringen – bietet Finmas dem Partner mit der Aufforderung zur aktiven Zustimmung an. Nimmt der Partner das Angebot nicht innerhalb der von Finmas gesetzten, mindestens sechs Wochen ab Zugang des Angebots beim Partner betragenden Frist an, ist Finmas zur Kündigung der Nutzung der Portals mit einer Frist von einem Monat zum Monatsende berechtigt.

(4) Finmas behält sich vor, das Portal in Bezug auf das Design oder vergleichbare Effekte zu ändern. Hierbei wird Finmas die berechtigten Belange der Nutzer berücksichtigen und diese mit einer Vorlauffrist von mindestens 2 Wochen von einer bevorstehenden Änderung informieren, wenn und soweit die Änderung nicht unerhebliche Nachteile (z.B. Umstellungsaufwand) für die Nutzer haben kann.

§ 8 Verfügbarkeit der Plattform, Ruhezeiten

(1) Zeitliche Begriffe

a. Zeitzone

Alle Zeitangaben beziehen sich auf die lokale Zeit in Deutschland.

(2) Bundeseinheitliche Feiertage mit Ruhezeiten

Name bundeseinheitlicher Feiertag	Datum
Neujahr	1. Januar
Internationaler Frauentag (Berlin)	8. März
Karfreitag	Variabel
Ostermontag	Variabel
Tag der Arbeit	1. Mai
Christi Himmelfahrt	Variabel
Pfingstmontag	Variabel
Tag der Deutschen Einheit	3. Oktober
1. Weihnachtsfeiertag	25. Dezember
2. Weihnachtsfeiertag	26. Dezember

Zuzüglich gelten Ruhezeiten an weiteren Feiertagen, die künftig zeitweise oder dauerhaft in allen deutschen Bundesländern gelten.

(3) Betriebszeit

Die Betriebszeit ist die Zeit, in der ein Serviceelement betriebsbereit ist und dem Auftraggeber zur grundsätzlichen Nutzung bereitsteht.

Betriebszeit	Montag bis Sonntag 00:00 bis 24:00 Uhr (24x7)

(4) Servicezeit

Die Servicezeit ist die Zeit innerhalb der Betriebszeit, in der im Falle von Störungen (Incidents) notwendige Maßnahmen eingeleitet werden, um die Störungen im Rahmen der vereinbarten Service Level zu beheben.

Servicezeit	Montag bis Freitag jeweils 08:00 bis 17:00 Uhr

(5) Wartungsfenster

Finmas führt geplante Wartungsarbeiten in Absprache mit den Nutzern innerhalb des Wartungsfensters durch. Wartungsarbeiten sind geplante Tätigkeiten, die die Finmas zur Aufrechterhaltung des Betriebes durchführen muss. Diese werden von der Finmas initiiert.

Wartungsfenster werden von der Finmas als Changes dokumentiert und durchgeführt. Darüber hinaus werden Wartungsarbeiten, die die Leistungserbringung der Finmas nicht beeinträchtigen, als unkritischer Change auch während der Servicezeit durchgeführt. Dies wird von der Finmas im Change entsprechend dokumentiert.

Notfallchanges aufgrund von sicherheitskritischen Vorfällen und Wartungsbedarfen werden von der Finmas auch außerhalb der definierten Wartungsfenster durchgeführt. Der Nutzer wird darüber unverzüglich informiert.

Wartungsfenster	Montag bis Freitag jeweils 22:00 bis 06:00 Uhr Samstag 15:00 Uhr bis Sonntag 20:00 Uhr

Finmas Kernwartungsfenster	Sonntag 01:00 bis 06:00 Uhr Das Finmas Kernwartungsfenster ist für auftragsübergreifende Wartungen an der Infrastruktur vorgesehen.

(6) Service Level

a. Verfügbarkeit der Systeme

Zur Bewertung der Verfügbarkeit wird die kumulierte Ausfalldauer herangezogen. Diese wird je Kalendermonat innerhalb der vereinbarten Servicezeit ermittelt.

Bei der Ermittlung der Ausfalldauer werden folgende Ausfallzeiten nicht zu Lasten der Finmas gewertet:

- Ausfallzeiten, die aufgrund angekündigter Wartungen innerhalb der Servicezeit entstehen
- Ausfallzeiten aufgrund höherer Gewalt/ Dritte
- Ausfallzeiten, die ursächlich im Verantwortungsbereich der Nutzer liegen

Service	Maximale Ausfalldauer (kumuliert je Kalendermonat)
Basissystem (Funktionalitäten laut Hauptvertrag)	480 Minuten* * Ausfälle des Basissystems werden nicht auf die Ausfallzeit der weiteren Services angerechnet
Immobilien-Services (Funktionalitäten laut Anlage 1.1)	480 Minuten
Baufinanzierungs-Services (Funktionalitäten laut Anlage 2.1)	720 Minuten (an Bankarbeitstagen in der Zeit von 08:00 bis 19:00 Uhr)

b. Verfügbarkeit des Support-Teams

Finmas wird alle Störungsmeldungen und Fragen des Nutzers durch ihr Support-Team per E-Mail innerhalb der im § 8 Abs.4 definierten Servicezeiten aufnehmen und die gemeldete Störung beseitigen. Finmas wird das Support-Team nur mit Personal besetzen, das zur Erfassung und ersten Klärung der Störungsmeldung qualifiziert ist. Die Kontaktdaten des Support-Teams werden dem Nutzer gesondert mitgeteilt.

Das Support-Team ist gemäß der unter § 8 Abs. 4 Verfügbarkeitszeiten - ausgenommen sind die unter § 8 Abs. 2 definierten bundeseinheitlichen Feiertage, gesetzliche Feiertage am Sitz von Finmas und des Nutzers, sowie 24.12. und 31.12. – erreichbar.

Die eingehenden Anliegen werden grundsätzlich in der Reihenfolge ihres Eingangs bearbeitet, Störungsmeldungen in der Reihenfolge ihrer Dringlichkeit. Um zu vermeiden, dass zeitkritische Anliegen verzögert bearbeitet werden, soll der Nutzer daher darauf hinwirken, dass Fragen und Probleme von Mitarbeitenden zunächst intern versucht werden zu klären (z.B. durch Benennung des für die Administration der Kundenplattform zuständigen Mitarbeitenden als erste Anlaufstelle), bevor der Support-Service von Finmas

in Anspruch genommen wird. Unabhängig davon sind jedoch alle Mitarbeitenden des Nutzers zur Inanspruchnahme des Support-Service berechtigt.

(7) Reaktionszeiten

Es werden folgende Reaktionszeiten (Zeit zwischen Erhalt der Störungsmeldung und Beginn der Störungsbeseitigung) vereinbart:

Innerhalb der Servicezeit:

Priorität	Beschreibung	Reaktionszeit
1 (Hoch)	Die gesamte Anwendung steht nicht zur Verfügung.	60 Minuten
2 (Mittel)	Ein Bestandteil der Anwendung steht nicht zur Verfügung	120 Minuten

Außerhalb der Servicezeit:

Priorität	Beschreibung	Reaktionszeit
1 (Hoch)	Die gesamte Anwendung steht nicht zur Verfügung.	180 Minuten
2 (Mittel)	Ein Bestandteil der Anwendung steht nicht zur Verfügung	320 Minuten
3 (Normal)	Die Anwendung funktioniert, weist jedoch erhöhte Reaktionszeiten auf.	3 Werktage

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung zum Vermittler-CRM

In diesem Dokument werden die technischen und organisatorischen Maßnahmen den Büro-Standort (**B**) und die Rechenzentren (**RZ**) beschrieben. Die Maßnahmen unterliegen einer ständigen Weiterentwicklung im Rahmen des Informationssicherheitsmanagements, daher ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen und stellt sicher, dass das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird.
Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

Maßnahme	**B**	**RZ**
Verschlüsselung des Übertragungsweges durch STARTTLS für E-Mail	x	x
Verschlüsselung des Übertragungsweges durch PGP oder S/MIME für E-Mail für konfigurierte E-Mail-Domains	x	x
Verschlüsselung der Übertragung durch HTTPS für externe Webanwendungen	x	x
Verschlüsselung der Übertragung durch HTTPS auch für interne Webanwendungen	x	x
Verschlüsselung der Speichermedien mobiler Geräte (Festplattenverschlüsselung)	x	n/a
Einsatz von Krypto-Containern für besonders sensible Daten (HR)	x	n/a

B. Vertraulichkeit

1. Zutrittskontrolle
Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.
Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Zutrittskontrollsystem

Maßnahme	**B**	**RZ**
Türsicherungen mit elektronischen Türöffnern	x	x
Ausweisleser für Magnetkarten an Außen- und Flurtüren	x	x
Prozesse zur Vergabe- und Entzug der Zugangskarten	x	x
Wachschutz 24/7	-	x
Empfang mit Gästeanmeldung	x	x
Protokollierung von Zutritten	x	x
Alarmanlagen für Server-Räume	n/a	x
Festlegung berechtigter Personen	x	x
Vorlage eines Lichtbildausweises	-	x

Verpflichtung auf das Datengeheimnis	x	x

Schlüssel / Schlüsselvergabe

Neben den Magnetkarten existieren für die Bürostandorte auch Schlüssel, die für den Notfall im Safe bereitliegen. Die Hausmeister und der Leiter IT haben eigene Schlüssel.

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

	B	**RZ**
Netzwerkzugriffskontrolle mit Richtlinienmanagement mit Authentifizierung und Autorisierung	x	x
Anmeldung von Nutzern an den Datenverarbeitungsanlagen	x	x
Sperre oder Pausieren des Zugangs nach fehlerhaften Anmeldungen	x	x
Passwort Richtlinien	x	x
Zwei- bzw, Mehrfaktor Authentifizierung (für sensible Anwendungen und MS Online Services)	x	x
Softwareverteilung / Software Inventory	x	x
Beschaffungsprozesse	x	x
Trennung von Netzwerken	x	x
Ausfallsichere, verteilte, mehrstufige Next-Generation Firewalls	x	x
Advanced Malware Protection und Virenschutz auf den Endgeräten	x	x
Programmprüfungs- und Freigabeverfahren	x	x
Thread Intelligence Systeme	x	x
Secure Internet Gateway	x	x
Private Leitungen und VPN zwischen den Standorten	x	x
MFA bei Anmeldung am Intranet und verschiedenen Diensten	x	x

C. Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Maßnahme	**B**	**RZ**
Pseudonyme bei Auswertungen für Management Information Systeme	n/a	x
Kommunikation zwischen internen Systemen und Datenbanken möglichst anhand interne Pseudonyme (z.B. interne EndkundenID), statt unmittelbar identifizierende Angaben (z.B. Name, E-Mail-Adresse)	n/a	x
Kommunikation mit externen Stellen (z.B. externe Dienstleister) möglichst anhand geeigneter Pseudonyme (z.B. Vorgangsnummer), statt unmittelbar identifizierende Angaben (z.B. Name, E-Mail-Adresse)	n/a	x

Die internen Pseudonyme können nur unter Zuhilfenahme interner Datenbanken aufgeschlüsselt werden. Diese Datenbanken sind Gegenstand der Rechte- und Rollenkonzepte. Die Verwendung interner Pseudonyme senkt daher das Risiko einer missbräuchlichen Verwendung personenbezogener Daten durch Dritte oder nicht autorisierte Personen.

D. Integrität

1. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Maßnahme	**B**	**RZ**
Prozesse zum Berechtigungsmanagement mit Protokollierung (Ticketsystem)	x	x
Berechtigungsmanagement über Active Directory oder Keymanager	x	x
Protokollierung von Zugriffen bei sensiblen Anwendungen	x	x
Network Security Analytics	x	x
Rollen und Rechtekonzepte bei mandantenfähigen Anwendungen	x	x
Release- und Patchmanagement	x	x
Prokollierung von Eingaben, Änderungen und Löschungen	-	x

2. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle ....

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Maßnahme	**B**	**RZ**
Nutzung von VPN vom Homeoffice	x	n/a
Private Netzwerke zwischen den Standorten	x	x
Verwendung von firmeneigenen mobilen Speichermedien	x	n/a
Verschlüsselung der Speichermedien mobiler Geräte (Festplattenverschlüsselung)	x	n/a
Hauspost	x	n/a
Hosting auf eigener Hardware	x	x
Dateschschutzkonforme Enstorgung von Datenträgern	x	x

3. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Maßnahme	**B**	**RZ**
Protokollierung der Änderungen von Daten	x	x
Einsatz von Protokollauswertesysteme	-	x

4. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Maßnahme	**B**	**RZ**
Formalisiertes Auftragsmanagement unter Einbeziehung des Informationssicherheits- und Datenschutzmanagements	x	x
Abgrenzung der Kompetenzen und Pflichten von Auftraggeber und Auftragnehmer	x	x

Kontrolle des Auftragnehmers bezüglich Einhaltung des Vertrages	x	x
Weisungen des Auftraggebers werden dokumentiert	x	x
Dienstleistermanagement und -Verzeichnis	x	x

E. Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

Maßnahme	**B**	**RZ**
Backup der Server	x	x
Backup der Daten	x	x
Getrennte Aufbewahrung der Backups	x	x
Unterbrechungsfreie Stromversorgung (USV)	x	x
Firewall	x	x
Virenschutz	x	x
Notfallpläne	x	x
Server-Virtualisierung	x	x
Hochverfügbare Storage Systeme	x	x
Brandmeldeanlagen	x	x
Automatische Löschanlagen für Serverräume	x	x
Monitoring mit Alarmierung	x	x
Incident Management	x	x

2. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Maßnahme	**B**	**RZ**
Mandantentrennung	x	x
Rechte- und Rollenkonzepte	x	x
Funktionstrennung nach Test und Produktionsumgebung	x	x

3. Wiederherstellung

a. Datensicherung

Die Sicherung der Daten und der virtuellen Server erfolgt durch die Hypoport Systems über Snapshots. Datenbanken werden über eigene Tools gesichert, wobei die Sicherungen wiederum per Snapshot gesichert werden können. Es werden Tages- und Wochen- und Monatssicherungen aufgehoben - abhängig von der Kritikalität der Daten. Zusätzlich wird noch die Sicherung über mehrere Standorte angeboten.

b. Wiederherstellung

Dank der einheitlichen Sicherungsstrategie über Snapshots ist die Wiederherstellung der Daten innerhalb von Minuten bis zu wenigen Stunden möglich. Die tatsächliche Wiederherstellungszeit ist von der Menge der Daten abhängig.

F. Regelmäßige Überprüfung der Sicherheit der Datenverarbeitung

Maßnahmen, die die Wirksamkeit der technischen und organisatorischen Maßnahmen sicherstellen.

Maßnahme	**B**	**RZ**
Bestellung eines Datenschutzbeauftragten	x	x
Bestellung eines Informationssicherheitsbeauftragten	x	x
Formalisierte Prozesse für Datenschutzvorfälle	x	x
Regelmäßige Überprüfung der Berechtigungen	x	x
Formalisiertes Auftragsmanagement	x	x
Schulung von Mitarbeitern zu Datenschutz und IT-Sicherheit	x	x
Verabschiedung von Richtlinien zu Datenschutz und IT-Sicherheit	x	x
Regelmäßige Berichte zum Informationssicherheitsmanagement an die Geschäftsführung	x	x
Regelmäßige Überprüfung des Schutzbedarfs und der technischen und organisatorischen Maßnahmen	x	x

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung (Portal)

Domäne	Praktiken
Organisation der IT-Sicherheit	**Verantwortung für die Sicherheit.** Microsoft hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordination und Überwachung der Sicherheitsregeln und -verfahren verantwortlich sind. **Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit.** Microsoft-Mitarbeiter, die Zugang zu Kundendaten oder Professional Services-Daten haben, sind zur Vertraulichkeit verpflichtet. **Risikomanagementprogramm.** Microsoft hat vor der Verarbeitung der Kundendaten oder dem Start des Onlinedienstes und vor der Verarbeitung von Professional Services-Daten oder dem Start der Professional Services eine Risikobewertung durchgeführt. Microsoft archiviert Sicherheitsunterlagen im Rahmen der Aufbewahrungspflichten, nachdem sie nicht mehr in Kraft sind.
Asset-Management	**Anlagenbestand.** Microsoft führt einen Bestand aller Medien, auf denen Kundendaten oder Professional Services-Daten gespeichert sind. Der Zugriff auf die Bestände solcher Medien ist auf Microsoft-Mitarbeiter beschränkt, die schriftlich dazu berechtigt sind. **Asset-Handling** - Microsoft klassifiziert Kundendaten Professional Services-Daten, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs darauf zu ermöglichen. - Microsoft legt Einschränkungen für das Drucken von Kundendaten und Professional Services-Daten fest und verfügt über Verfahren für die Entsorgung gedruckter Materialien, die solche Daten enthalten. o Mitarbeiter von Microsoft müssen eine Genehmigung von Microsoft einholen, bevor sie Kundendaten oder Professional Services-Daten auf tragbaren Geräten speichern, remote auf solche Daten zugreifen oder solche Daten außerhalb der Einrichtungen von Microsoft verarbeiten.
Personalsicherheit	**Sicherheitsschulungen.** Microsoft informiert seine Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Rollen. Microsoft informiert seine Mitarbeiter auch über mögliche Folgen einer Verletzung der Sicherheitsregeln und -verfahren. Microsoft verwendet in der Schulung nur anonyme Daten.
Physische und umgebungsbezogene Sicherheit	**Physischer Zugang zu Einrichtungen.** Microsoft beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten, auf identifizierte, autorisierte Personen.

	Physischer Zugriff auf Komponenten. Microsoft führt Aufzeichnungen über die ein- und ausgehenden Medien, die Kundendaten oder Professional Services-Daten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Arten von solchen Daten. **Schutz vor Unterbrechungen.** Microsoft nutzt eine Vielzahl von branchenüblichen Systemen, um den Verlust von Daten durch Stromausfall oder Leitungsstörungen zu verhindern. **Entsorgung von Komponenten.** Microsoft nutzt branchenübliche Prozesse, um Kundendaten und Professional Services-Daten zu löschen, wenn sie nicht mehr benötigt werden.
Kommunikations- und Betriebsmanagement	**Betriebsrichtlinie.** Microsoft führt Sicherheitsunterlagen, in denen die Sicherheitsmaßnahmen sowie die entsprechenden Verfahren und Verantwortlichkeiten der Mitarbeiter beschrieben sind, die Zugang zu Kundendaten oder Professional Services-Daten haben. **Datenwiederherstellungsverfahren** - Microsoft erstellt kontinuierlich, mindestens jedoch einmal pro Woche (es sei denn, es haben im betreffenden Zeitraum keine Aktualisierungen stattgefunden) mehrere Kopien von Kundendaten und Professional Services-Daten, aus denen solche Daten wiederhergestellt werden können. - -Microsoft bewahrt Kopien von Kundendaten und Professional Services-Daten und Datenwiederherstellungsverfahren an einem anderen Ort als dem auf, an dem sich die primären Computergeräte befinden, von denen die die Kundendaten und Professional Services-Datenverarbeitet werden. - -Microsoft verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten und Professional Services-Daten regeln. - -Microsoft prüft die Datenwiederherstellungsverfahren mindestens einmal alle sechs Monate. Ausgenommen hiervon sind Verfahren für Professional Services und für Azure Government Services, die alle zwölf Monate geprüft werden. - -Microsoft protokolliert Datenwiederherstellungsmaßnahmen. Dabei werden Informationen zur verantwortlichen Person, die Beschreibung der wiederhergestellten Daten sowie gegebenenfalls Angaben zu den Daten, die bei der Datenwiederherstellung manuell eingegeben werden mussten, aufgezeichnet. **Malware.** Microsoft nimmt Anti-Malware-Kontrollen vor, um zu verhindern, dass bösartige Software unbefugten Zugriff auf Kundendaten und Professional Services-Daten erhält, einschließlich bösartiger Software aus öffentlichen Netzwerken. **Daten außerhalb von Landesgrenzen** - -Microsoft verschlüsselt Kundendaten und Professional Services-Daten, die über öffentliche Netzwerke übermittelt werden, oder ermöglicht dem Kunden eine solche Verschlüsselung.

	- -Microsoft schränkt den Zugriff auf Kundendaten und Professional Services-Daten in Medien ein, die die Einrichtungen von Microsoft verlassen. **Ereignisprotokollierung.** Microsoft protokolliert den Zugriff und die Nutzung von Informationssystemen, die Kundendaten oder Professional Services-Daten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung.
Zugriffskontrolle	**Zugriffsrichtlinie.** Microsoft führt eine Aufzeichnung der Sicherheitsberechtigungen von Einzelpersonen, die Zugang zu Kundendaten oder Professional Services-Daten haben. **Zugriffsberechtigung** - Microsoft führt und aktualisiert Aufzeichnungen zu den Mitarbeitern, die zum Zugriff auf Microsoft-Systeme autorisiert sind, die Kundendaten oder Professional Services-Daten enthalten. - Microsoft deaktiviert Anmeldedaten, die über einen bestimmten Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden. - Microsoft benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen. - Wenn mehrere Personen Zugriff auf die Systeme haben, in denen Kundendaten oder Professional Services-Daten enthalten sind, stellt Microsoft sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen. **Geringste Rechte** - Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten und Professional Services-Daten nur gestattet, wenn dies erforderlich ist. - Microsoft schränkt den Zugriff auf Kundendaten und Professional Services-Daten auf solche Personen ein, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen. **Integrität und Vertraulichkeit** - Microsoft weist Mitarbeiter an, Administrationssitzungen zu deaktivieren, wenn sie Einrichtungen, die sich unter der Kontrolle von Microsoft befinden, verlassen oder wenn Computer anderweitig unbeaufsichtigt sind. - Microsoft speichert Kennwörter so, dass sie während des Gültigkeitszeitraums nicht erkennbar sind. **Authentifizierung** - Microsoft verwendet Verfahren nach Branchenstandard, um Benutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen. - Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass die Kennwörter regelmäßig erneuert werden müssen.

	- Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass das Kennwort mindestens acht Zeichen umfassen muss. - Microsoft stellt sicher, dass deaktivierte oder abgelaufene Kennungen an keine andere Person vergeben werden. - Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf Informationssysteme zu verschaffen, oder ermöglicht dem Kunden eine solche Überwachung. - Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die manipuliert oder versehentlich offengelegt wurden. - Microsoft verwendet Verfahren nach Branchenstandard zum Schutz von Kennwörtern, einschließlich Verfahren, die die Vertraulichkeit und Integrität von Kennwörtern während der Zuweisung und Verteilung sowie während der Speicherung wahren sollen. **Netzwerkdesign.** Microsoft führt Kontrollen durch, um zu verhindern, dass Personen Zugriffsrechte erhalten, die ihnen nicht zugewiesen wurden, um Zugang zu Kundendaten oder Professional Services-Daten zu erhalten, auf die sie nicht zugreifen dürfen.
Handhabung eines Informationssicherheitsvorfalls	**Vorfallreaktionsablauf** - Microsoft führt Unterlagen über Sicherheitsverletzungen unter Angabe einer Beschreibung der Verletzung, des Zeitraums, der Konsequenzen der Verletzung, des Namens der Person, die den Zwischenfall gemeldet hat, und der Person, der der Zwischenfall gemeldet wurde, sowie des Verfahrens für die Wiederherstellung von Daten. - Für jede Sicherheitsverletzung, bei der es sich um einen Sicherheitsvorfall handelt, erfolgt (wie im Abschnitt „Meldung von Sicherheitsvorfällen“ weiter oben beschrieben) unverzüglich und auf jeden Fall innerhalb von 72 Stunden eine Benachrichtigung seitens Microsoft. - Microsoft untersucht Offenlegungen von Kundendaten und Professional Services-Daten einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage. **Dienstüberwachung.** Das Microsoft-Sicherheitspersonal überprüft die Protokolle mindestens alle sechs Monate, um gegebenenfalls Abhilfemaßnahmen vorzuschlagen.
Geschäftsfortführungsmanagement	- Microsoft unterhält Notfall- und Alternativpläne für die Einrichtungen, in denen sich Microsoft-Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten. - Bei Microsoft sind redundante Speicherung und ihre Verfahren zur Datenwiederherstellung so konzipiert, dass versucht wird, Kundendaten und Professional Services-Daten in ihrem ursprünglichen oder zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren.