

## **Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO**

### **Präambel**

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Auftragsverhältnis im Sinne des Art. 28 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, „**DSGVO**“).

Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als „**Vereinbarung**“ bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus den zugrundeliegenden Nutzungsbedingungen der debtify-Plattform einschließlich aller Anlagen (nachfolgend gemeinsam als „**Hauptvertrag**“ bezeichnet).

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen zur Erfüllung des Hauptvertrages und dieser Vereinbarung nach Maßgabe der folgenden Bestimmungen:

### **§ 1 Anwendungsbereich und Begriffsbestimmungen**

- (1) Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 DSGVO, die der Auftragsverarbeiter auf Grundlage des Hauptvertrages gegenüber dem Verantwortlichen erbringt.
- (2) Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ von Daten benutzt wird, ist darunter allgemein die Verwendung von personenbezogenen Daten zu verstehen. Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
- (3) Auf die weiteren Begriffsbestimmungen in Art. 4 DSGVO wird verwiesen.

### **§ 2 Gegenstand und Dauer der Datenverarbeitung**

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.
- (2) Gegenstand des Auftrags ist die Beauftragung des Auftragsverarbeiters zur Bereitstellung einer Plattform über das Internet, die eine sichere Vernetzung und Kommunikation zwischen Kreditoren und Servicern im Bereich von Non-Performing-Loans ermöglicht, entweder durch

Nutzung einer auf der Plattform bereitgestellten Schnittstelle und/oder durch die Nutzung von durch App-Anbieter bereitgestellte Applikationen. Der spezifische Umfang der Bereitstellungsleistung ergibt sich aus dem Hauptvertrag.

(3) Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

### **§ 3 Art und Zweck der Datenverarbeitung**

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Dieser umfasst folgende Tätigkeit(en) und Zweck(e):

Ziel der Datenverarbeitung im Rahmen der für den Auftraggeber bereitgestellten Plattform ist es, die Vernetzung und Kommunikation zwischen Kreditoren und Dienstleistern im Bereich des „Non-Performing-Loans Real Estate“ („NPL“) zu ermöglichen. Die unter § 4 des hiesigen Auftragsverarbeitungsvertrags aufgeführten Daten werden im Zusammenhang mit den Korrespondenzen und den im Registrierungsprozess ausgefüllten Formularen verarbeitet.

### **§ 4 Kategorien betroffener Personen**

Im Rahmen dieser Vereinbarung werden personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet:

- Immobilieneigentümer
- Makler
- Beschäftigte der Auftraggeber
- Kreditnehmer
- Kaufinteressenten
- Insolvenzverwalter
- Zwangsverwalter
- Betreuer

### **§ 5 Art der personenbezogenen Daten**

Von der Auftragsverarbeitung sind folgende Datenarten betroffen:

- Personenstammdaten (Name, Anrede, Titel/akademischer Grad, Geburtsdatum)
- Kontaktdaten (E-Mail-Adresse, Telefonnummer, Anschrift)
- Vertragsdaten (Zahlungs- und Bestelldaten))
- Adressen und Wert der Immobilien

### **§ 6 Rechte und Pflichten des Verantwortlichen**

- (1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig und somit für die Verarbeitung Verantwortlicher im Sinne des Art. 4 Nr.7 DSGVO.
- (2) Der Verantwortliche ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragsverarbeiters unverzüglich vom Verantwortlichen schriftlich oder in Textform (z.B. per E-Mail) zu bestätigen.
- (3) Soweit es der Verantwortliche für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Verantwortliche dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Verantwortlichen ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.
- (4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter festgestellt werden.

## **§ 7 Pflichten des Auftragsverarbeiters**

### (1) Datenverarbeitung

Der Auftragsverarbeiter wird personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden Hauptvertrages sowie nach den Weisungen des Verantwortlichen verarbeiten.

### (2) Betroffenenrechte

- a. Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Sollte der Auftragsverarbeiter die in § 5 dieser Vereinbarung genannten personenbezogenen Daten im Auftrag des Verantwortlichen verarbeiten und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität gem. Art. 20 DSGVO, wird der Auftragsverarbeiter dem Verantwortlichen den betreffenden Datensatz innerhalb einer angemessen gesetzten Frist, im Übrigen innerhalb von sieben Arbeitstagen, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.
- b. Der Auftragsverarbeiter hat auf Weisung des Verantwortlichen die in § 5 dieser Vereinbarung genannten personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Das Gleiche gilt, wenn diese Vereinbarung eine Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten vorsieht.
- c. Soweit sich eine betroffene Person unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung der in § 5 dieser Vereinbarung

genannten personenbezogenen Daten wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich nach Erhalt an den Verantwortlichen weiterleiten.

(3) Kontrollpflichten

- a. Der Auftragsverarbeiter stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden.
- b. Der Auftragsverarbeiter wird sein Unternehmen und seine Betriebsabläufe so gestalten, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.
- c. Der Auftragsverarbeiter bestätigt, dass er gem. Art. 37 DSGVO und, sofern anwendbar, gemäß § 38 BDSG einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht. Datenschutzbeauftragter des Auftragsverarbeiters ist derzeit:

Johannes Nicol  
ISiCO Datenschutz GmbH  
Am Hamburger Bahnhof 4  
10557 Berlin

(4) Informationspflichten

- a. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine von dem Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.
- b. Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen.
- c. Soweit der Auftragsverarbeiter feststellt, dass es in seinem Verantwortungsbereich zu einer Verletzung des Schutzes personenbezogener Daten des Verantwortlichen gekommen ist, wird er den Verantwortlichen unverzüglich informieren.

(5) Ort der Datenverarbeitung

Die Verarbeitung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(6) Löschung der personenbezogenen Daten nach Auftragsbeendigung

Nach Beendigung des Hauptvertrages wird der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern der Löschung dieser Daten keine gesetzlichen Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen. Die datenschutzgerechte Löschung ist zu dokumentieren und gegenüber dem Verantwortlichen auf Anforderung zu bestätigen.

**§ 8 Kontrollrechte des Verantwortlichen**

- (1) Der Verantwortliche ist berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters oder Gefährdung der Sicherheitsmaßnahmen für andere Verantwortliche und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Auftragsverarbeiters aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte durchgeführt werden. Der Auftragsverarbeiter wird die notwendige Unterstützung zur Durchführung der Kontrollen anbieten.
- (2) Der Auftragsverarbeiter wird den Verantwortlichen über die Durchführung von Kontrollmaßnahmen der Aufsichtsbehörde informieren, soweit die Maßnahmen oder Datenverarbeitungen betreffen können, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

**§ 9 Unterauftragsverhältnisse**

- (1) Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Auftragsverarbeiter gemäß den nachfolgenden Absätzen in § 9 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. Art. 28 Abs. 2 DSGVO dar.
- (2) Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den in der **Anlage 2** benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.
- (3) Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragsverarbeiter wird den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Änderung Einspruch erheben.

- (4) Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragsverarbeiter zu erheben. Im Fall des Einspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragsverarbeiter nicht zumutbar ist – etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für den Auftragsverarbeiter – oder die Abstimmung eines weiteren Auftragsverarbeiters fehlschlägt, können der Verantwortliche und der Auftragsverarbeiter diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.
- (5) Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich.

## **§ 10 Vertraulichkeit**

- (1) Der Auftragsverarbeiter ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit verpflichtet.
- (2) Der Auftragsverarbeiter verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Die Vornahme der Verpflichtungen wird der Auftragsverarbeiter dem Verantwortlichen auf Nachfrage nachweisen.
- (3) Sofern der Verantwortliche anderweitigen Geheimnisschutzregeln unterliegt, wird er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird seine Mitarbeiter entsprechend den Anforderungen des Verantwortlichen auf diese Geheimnisschutzregeln verpflichten.

## **§ 11 Technische und organisatorische Maßnahmen**

- (1) Die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Der Auftragsverarbeiter kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.
- (2) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art. 32 i.V.m Art. 5 Abs. 1 DSGVO. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen

insbesondere Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird der Auftragsverarbeiter die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

## **§ 12 Haftung/ Freistellung**

- (1) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Eine Ersatzpflicht des Auftragsverarbeiters besteht nicht, sofern der Auftragsverarbeiter nachweist, dass er die ihm überlassenen Daten des Verantwortlichen ausschließlich nach den Weisungen des Verantwortlichen verarbeitet und seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nachgekommen ist.
- (2) Der Verantwortliche stellt den Auftragsverarbeiter von allen Ansprüchen Dritter frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus dieser Vereinbarung oder geltenden datenschutzrechtlichen Vorschriften durch den Verantwortlichen gegen den Auftragsverarbeiter geltend gemacht werden.

## **§ 13 Sonstiges**

- (1) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.
- (2) Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung. Mündliche Nebenabreden bestehen nicht und sich auch für künftige Änderungen dieser Vereinbarung ausgeschlossen.
- (3) Diese Vereinbarung unterliegt deutschem Recht.
- (4) Sofern der Zugriff auf die Daten, die der Verantwortliche dem Auftragsverarbeiter zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich hierüber zu benachrichtigen.

## **Anlagenverzeichnis**

- Anlage 1** Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

**Anlage 1**

**Technische und organisatorische Maßnahmen  
zur Gewährleistung der Sicherheit der Datenverarbeitung**

Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

**A. Maßnahmen zur 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.

Beschreibung der Maßnahmen zur Pseudonymisierung:

- Es werden verschiedene komplexe Methoden genutzt, um Daten zu pseudonymisieren insbesondere Data Masking, Data Salting und Hashing.
- Masking-Vorgaben, Salting-Parameter und Hashing-Algorithmus, die pseudonymisierten Daten sowie die Bezugsdaten werden jeweils getrennt voneinander aufbewahrt.
- Dynamisches Data Masking ermöglicht es den Kunden selbst zu bestimmen, inwieweit Daten mit minimaler Auswirkung auf die Anwendungsschicht offengelegt werden sollen.
- Es ist sichergestellt, dass personenbezogene Daten nur insoweit entpseudonymisiert und eingesehen werden können, wie es für die konkrete Verarbeitung nötig ist. Daten können sicher und umgehend anonymisiert werden. Pseudonymisieren, Anonymisieren und Überschreiben personenbezogener Daten kann vollständig und umgehend umgesetzt werden.

**B. Maßnahmen zur 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:

Beschreibung der Verschlüsselungsmaßnahmen:

- Alle sensiblen Daten werden per 256-bit AES verschlüsselt.
- Ende-zu-Ende-Verschlüsselung mit vom Kunden verwalteten Schlüssel.
- Ver- und Entschlüsselung der Datenbank, der zugehörigen Backups und der Transaktionsprotokolldateien im Ruhezustand in Echtzeit.
- Jegliche Kommunikation mit TLS-Verschlüsselung über das jeweils aktuelle TLS-Protokoll.



## **C. Maßnahmen zur Sicherung der Vertraulichkeit**

### **1. Zutrittskontrolle**

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Beschreibung des Zutrittskontrollsystems:

Bürostandort:

- Gebäudezutritt gesichert über Chipkarte/Schlüssel.
- Mieterbezogene Chipkartenverwaltung/Schlüsselverwaltung.
- Organisationsanweisung für Chipkartenausgabe/Schlüsselausgabe.
- Geräte werden nach Dienstschluss in verschlossenen Schränken verwahrt.

Serverstandort (Subdienstleister):

- Wachpersonal 24/7.
- Gesichertes Gelände (Zaun, Kameras).
- Gesicherte Gebäude mit zweistufiger Authentifizierung.
- Zutritt zur Rechenzentrumsetage nur nach vorheriger Personenkontrolle mit Metalldetektor. Beides wird beim Verlassen wiederholt.
- Dokumentiertes Zutritts- und Identifizierungssystem.
- Zutritt nur nach vorheriger Anmeldung unter Angabe eines triftigen Grundes (z. B. Compliance-Maßnahmen).

### **2. Zugangskontrolle**

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- Personalisierte Nutzerkonten.
- Kennwortverfahren, d.h. persönlicher und individueller User Log-In bei Anmeldung am System (u.a. Sonderzeichen, Mindestlänge von 16 Zeichen, regelmäßiger Wechsel des Kennwortes).
- Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs nach individueller Zahl von erfolglosen Versuchen. Smart Lockout: wird immer wieder das gleiche falsche Passwort versucht (Indiz für Berechtigte, die ihr Passwort verwechselt oder vergessen haben) wird langsamer gesperrt, als wenn verschiedene Passwörter ausprobiert werden (Indiz für Eindringling). Dies geschieht selbstverständlich über Hash-Werte, so dass die Vertraulichkeit der Passwörter jederzeit gewahrt ist.
- Vollständige Trennung der verschiedenen Umgebungen (Test-, Produktiv-, Entwicklungssystem) in Virtual Sub-Networks.
- Vollständige Trennung der verschiedenen Kunden in Virtual Sub-Networks.
- Access Management.
- Protokollierung der internen Nutzeraktivitäten.

- Keinerlei Nutzung externer Speichermedien (z. B. USB-Sticks).
- Multi-Faktor-Authentifizierung bei Zugang zu sensiblen Daten.
- Automatische Rechnersperre bei Inaktivität.
- Verbindliche Vorgaben zur Berechtigungsvergabe und Passwortrücksetzung.
- Begrenzung der Anzahl berechtigter Mitarbeiter.
- Automatische und regelmäßige Überprüfung der Antiviren- und Spyware-Filter.

### 3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

- Rollenbasiertes, granulares Berechtigungskonzept.
- Dokumentation der Berechtigungsvergabe.
- Trennung des Berechtigungsbezug von technischer Berechtigungsvergabe.
- Datenbankzugriff streng reglementiert.
- Protokollierung der internen Nutzeraktivitäten.
- Protokollierung von Zugriffen und Missbrauchsversuchen.
- Blockieren von Ein- und Ausgabeschnittstellen (z.B. USB-Sticks).

### 4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Rollenbasiertes, granulares Berechtigungskonzept, das die getrennte Verarbeitung von Daten verschiedener Kunden gewährleistet.
- Dokumentation der Berechtigungsvergabe.
- Verschlüsselte Speicherung sensibler Daten (256-bit AES).
- Vollständige Trennung der verschiedenen Umgebungen (Test-, Produktiv-, Entwicklungssystem) in Virtual Sub-Networks.

## D. Maßnahmen zur Sicherung der Integrität

### 1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität:

- Einspielen neuer Releases und Patches unter strengem mehrstufigem Management: Proofing, Aprooving, Testing (funktionales und nicht-funktionales Testing, Ergebniskontrolle) vor dem Release.

- Logging des Release- und Patch-Management sowie der Geschäftsprozesse.
- Redundante Speichersysteme und Datenbanken.
- Tägliche Backups.

## 2. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

Beschreibung der Übertragungskontrolle:

- Logging der Geschäftsprozesse sowie der Datenübertragungen.
- Überwachung und Kontrolle unbefugter Datenübertragungen.
- Es ist sicherheitsarchitektonisch sichergestellt, dass Daten nur verschlüsselt und gemäß des rollenbasierten, granularen Berechtigungskonzepts übertragen werden.

## 3. Transportkontrolle

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

Beschreibung der Transportkontrolle:

- Übermittlung von Daten nur verschlüsselt (256-bit EAS, TLS 1.3).
- Transportprozesse mit individueller Verantwortlichkeit
- Verschlüsselungsverfahren, die Datenveränderungen während des Transports aufdecken.
- Keinerlei Nutzung externer Datenträger (USB-Sticks, externe Festplatten).
- Umfassende Protokollierungsverfahren.
- Regelmäßiges Patching der Verschlüsselungsverfahren.
- Automatische Rotation der Zugriffsschlüssel.

## 4. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Beschreibung des Eingabekontrollvorgangs:

- Protokollierung aller Systemaktivitäten und Aufbewahrung der Protokolle für sechs Monate.
- Protokollierung der Administration (Anlegen und Ändern von Nutzern und Berechtigungen).
- Protokollauswertungssysteme.
- Digitale Signaturen.

## **E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit**

### **1. Verfügbarkeitskontrolle**

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems:

- Datensicherungsverfahren.
- Unterbrechungsfreie Stromversorgung am Serverstandort.
- Archivierungskonzept.
- Feueralarmsystem (Büro- und Serverstandort).
- Feuerlöschsystem (Serverstandort).
- Klimaanlage (Serverstandort).
- Vollständiges Backup- und Recovery-Konzept (RPO: 5 Sekunden, TRO: 30 Sekunden) und katastrophensicherer Aufbewahrung der Datenträger.
- Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung.
- Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).

### **2. Rasche Wiederherstellbarkeit**

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Wiederherstellbarkeit:

- Redundante Auslegung aller Systeme.
- Regelmäßige Tests der Datenwiederherstellung.
- Notfallpläne.

### **3. Zuverlässigkeit**

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

- Automatisches Monitoring mit E-Mail-Benachrichtigung.
- Notfallpläne mit Verantwortlichkeiten.
- IT-Notdienst 24/7.
- regelmäßige Tests der Datenwiederherstellung.

## **F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung**

### **1. Überprüfungsverfahren**

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Verpflichtung der Mitarbeiter auf die Vertraulichkeit/ datenschutzrechtliche Schulung der Mitarbeiter.
- Regelmäßige Re-Zertifizierung.
- Formalisierte Prozesse für Datenschutzvorfälle.
- Weisungen der Auftraggeber werden dokumentiert.
- Formalisiertes Auftragsmanagement.

## **2. Auftragskontrolle**

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

Beschreibung der Maßnahmen zur Auftragskontrolle:

- Weisungen der Auftraggeber werden dokumentiert.
- Formalisiertes Auftragsmanagement.

## **Anlage 2**

### **Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung**

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

#### **1. [Subunternehmer A]**

Name/Firma: Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland

Funktion/Tätigkeit: Bereitstellung der Server-Infrastruktur sowie technische Entwicklung und Wartung des Portals

Sitz: Dublin, Irland

Serverstandort: Deutschland

Verarbeitungsort: weltweit