Technische und organisatorische Maßnahmen (TOM)

Stand 18.10.2023

Inhaltsverzeichnis

Inhaltsverzeichnis 2

Präambel 3

I. Vertraulichkeit 4

1. Zutrittskontrolle 4

2. Zugangskontrolle 6

3. Zugriffskontrolle 9

4. Trennungskontrolle 11

5. Pseudonymisierung 12

II. Integrität 13

1. Weitergabekontrolle 13

2. Eingabekontrolle 15

III. Verfügbarkeit und Belastbarkeit 17

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 19

1. Datenschutzmanagement 19

2. Auftragskontrolle 20

3. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) 21

luckycloud GmbH

Solmsstraße 26
10961 Berlin
Germany

CEO & Founder

Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt

www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

Änderungshistorie:

Version	Datum	Autor	Genehmigt von	Change Control
1.0	17.05.2018	DSK Nicole Smuga	CEO Luc Mader	Freigabe 1. Version TOM-Beschreibung
1.1	06.02.2019	DSK Nicole Smuga	CEO Luc Mader	Überprüfung und Anpassung TOM-Beschreibung
1.2	02.12.2019	DSK Nicole Smuga	CEO Luc Mader	Überprüfung und Anpassung TOM-Beschreibung
1.3	15.01.2022	DSB Loan Truong	CEO Luc Mader	Überprüfung und Anpassung TOM-Beschreibung
2.0	09.02.2023	DSB Loan Truong	CEO Luc Mader	Freigabe 2. Version TOM-Beschreibung

Präambel

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat die luckycloud GmbH (nachfolgend „wir“) sowohl als Verantwortliche als auch als Auftragsverarbeiterin geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen werden nachfolgend näher beschrieben.

Weitere Informationen zur Datensicherheit bei luckycloud findest du auf unserer Hilfeseite:

https://docs.luckycloud.de/de/data-protection-and-security

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

I. Vertraulichkeit

Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen darf.

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (standortbezogene Maßnahmen).

Allgemein

Technische Maßnahmen
Schlüssel
Elektrische Türöffner
Alarmanlage
Videoüberwachung

Organisatorische Maßnahmen
Schlüsselverwaltung, insbesondere Dokumentation, Vergabe und Entzug von Zutrittsmitteln
Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung (HR) entsprechend angefordert wurde.
Besucherliste/Besucherausweis/Verpflichtung der Besucher auf Vertraulichkeit
Zutrittskonzept (insbesondere bzgl. HR)

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

Schutz unserer Server

Unsere IT-Infrastruktur liegt in ISO-27001, BSI zertifizierten und hochverfügbaren Rechenzentren. Der Zutritt wird in den Rechenzentren insbesondere durch folgende Maßnahmen streng kontrolliert:

Zusätzliche Maßnahmen im Rechenzentrum
Zutritt zum Rechenzentrum nur mit vorheriger Anmeldung über 2FA Portal möglich (durch autorisierte Person beim Auftragnehmer gemäß Zutrittskonzept)
Zutritt zum Rechenzentrum nur mit einer speziellen Zutrittskarte möglich
Zutritt nur für befugte Systemadministratoren und nur in Anwesenheit des RZ Personals
Besonderer Schutz der Server, insbesondere Standort in einem mehrfach abgeschlossenen Bereich

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen
Maßnahmen in Bezug auf Benutzer-IDs und Passwörter: • Individuelle Benutzer-IDs und Passwörter (Mitarbeiter erhält einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss.) • Technische Erzwingung von geeigneten Passwörtern (mind. 8 Zeichen, Groß- und Kleinschreibung, ein Sonderzeichen) • Passwörter werden verschlüsselt gespeichert. • Hinterlegung einer technischen Passwortrichtlinie, um insbesondere die wiederholte Nutzung von gleichen Passwörtern zu verhindern. • Implementierung von Sicherheitsmaßnahmen für den Fall, dass fehlerhafte Passwörter mehrmals eingegeben werden (wie Sperre des jeweiligen Benutzer-Accounts bei mehrmaliger Fehleingabe). • Fehlerhafte Anmeldeversuche werden protokolliert.
Nutzung verschiedener Authentifizierungsmechanismen, z. B. Single Sign-on (SSO), Zwei-Faktor-Authentifizierung
Maßnahmen in Bezug auf Admins: • Verschlüsselung der Admin PCs • Personalisierte Admin-Accounts (insbesondere für den Betrieb von Server) • Bei funktionalen Admin-Accounts: Kennwörter werden neu gesetzt, sobald ein zugangsbefugter Admin aus dem Team ausgeschieden ist. • Besonderer Schutz des administrativen Zugangs zum Server (z. B. durchgehendes Monitoring der Zugänge)
Automatische Sperrmechanismen (wie Bildschirmsperre nach längerer Inaktivität)
Unberechtigte Zugriffe von Dritten auf IT-Systeme werden technisch erkannt und unterbunden (insbesondere Intrusion-Prevention-System).

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet sind ebenfalls durch Firewalls gesichert. Nur die für die jeweilige Kommunikation erforderlichen Ports sind nutzbar. Alle anderen Ports sind entsprechend gesperrt.
Verschlüsselung von (mobilen) IT-Systemen (entsprechende Datenträgerverschlüsselung)

Organisatorische Maßnahmen
Passwortrichtlinie (insbesondere Mindestpasswortlänge, Passwortkomplexität)
Richtlinie für die Nutzung von IT-Systemen durch Mitarbeiter, insbesondere im Homeoffice („IT-Richtlinie“), z. B. • Bildschirmsperre beim Verlassen des Arbeitsplatzes • Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.
• Dokumentierter Prozess bzgl. Vergabe von Benutzerberechtigungen (Antrag über Vorgesetzten oder HR erforderlich) • Protokollierung Erteilung und Entzug von Berechtigungen • Regelmäßige Überprüfung der eingeräumten Berechtigungen
Wartungstätigkeiten durch Fremdpersonal nur unter Beaufsichtigung und mit entsprechender vertraglicher Regelung (NDA)

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

Maßnahmen für Kunden
Ermöglichung folgender Maßnahmen bzgl. Zugangskontrolle für Kunden: • Individuelle Benutzer-IDs und Passwörter • Technische Erzwingung von geeigneten Passwörtern (mind. 8 Zeichen, Groß- und Kleinschreibung, ein Sonderzeichen) • Passwörter werden verschlüsselt gespeichert. • Hinterlegung einer technischen Passwortrichtlinie, um insbesondere die wiederholte Nutzung von gleichen Passwörtern zu verhindern. • Implementierung von Sicherheitsmaßnahmen für den Fall, dass fehlerhafte Passwörter mehrmals eingegeben werden (wie Sperre des jeweiligen Benutzer-Accounts bei 3-maliger Fehleingabe). • Fehlerhafte Anmeldeversuche werden protokolliert. • Verschiedene Authentifizierungsmechanismen, z. B. Single Sign-on (SSO), optional: Zwei-Faktor-Authentifizierung

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems).

Technische Maßnahmen
Technische Berechtigungskonzepte/rollenbasierte Zugriffskontrolle
Clientseitige Verschlüsselung der Datenbanken bzw. Bibliotheken durch ein Passwort
Protokollierung von Zugriffen auf Anwendungen und/oder Daten (File Access Logs)
Individuelle Konten für einzelne Benutzer (grundsätzlich keine Teilung von Konten)
Zugriff auf die Systeme erfolgt nach dem Need-to-know-Prinzip (vorheriger Antrag durch Vorgesetzte/HR erforderlich).
Nicht mehr verwendete Datenträger und Papierunterlagen werden sicher gelöscht bzw. vernichtet (insbesondere Schredder; Datenträgervernichtung durch Dienstleister nach DIN 66399).
Datenträger nach Möglichkeit immer verschlüsselt

Organisatorische Maßnahmen
Regelmäßige Kontrolle der Zugriffsberechtigungen: • Übersicht der erteilten Freigaben (mit verschiedenen Optionen wie Entfernen von Freigaben) • Organisationsmanager: Kontrolle aller Zugriffe mithilfe von File Access Logs • Geräteübersicht: Auflistung aller Geräte, die auf ein bestimmtes Nutzerkonto zugegriffen haben.

Dokumentiertes Berechtigungskonzept, insbesondere • Vergabe minimaler Berechtigungen • Vermeidung der Konzentration von Funktionen
Richtlinie für die Nutzung von IT-Systemen durch Mitarbeiter, insbesondere im Homeoffice („IT-Richtlinie“)

Maßnahmen für Kunden
Ermöglichung folgender Maßnahmen bzgl. Zugangskontrolle für Kunden: • Freigabe einzelner Bibliotheken an befugte Personen mithilfe von individuell einstellbaren Berechtigungs- und Gruppenrichtlinien • Optional: clientseitige Verschlüsselung der Bibliotheken durch ein Passwort • Protokollierung von Zugriffen auf Anwendungen und/oder Daten (File Access Logs) • Regelmäßige Kontrolle der Zugriffsberechtigungen möglich: Übersicht der erteilten Freigaben/Organisationsmanager • Geräteübersicht

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

4. Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen
Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern (insbesondere bei Auftragsverarbeitung)
Logische Mandantentrennung (softwareseitig)
Sandboxing
Instanziierung in Datenbanken
Trennung von Test- und Entwicklungsumgebung

Organisatorische Maßnahmen
Dokumentierte Rechteverwaltung (inklusive regelmäßiger Kontrolle)
Festlegung von Datenbankrechten

Maßnahmen für Kunden
Ermöglichung folgender Maßnahme bzgl. Trennungskontrolle für Kunden: • Erstellung von verschiedenen Bibliotheken (bei Bedarf auch verschlüsselt)

5. Pseudonymisierung

Die personenbezogenen Daten werden so verarbeitet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen (Zuordnungsdatei) nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen
Personalnummer
Gesonderte Aufbewahrung der Zuordnungsdatei

Organisatorische Maßnahmen
Dokumentierter Prozess in Bezug auf die Pseudonymisierung von Daten

Maßnahmen für Kunden
Ermöglichung folgender Maßnahme bzgl. Pseudonymisierung für Kunden: • individuelle Benutzer-ID / E-Mail-Adresse nach Wahl des Nutzers

II. Integrität

Integrität bezeichnet insbesondere die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig, richtig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein, damit sie berücksichtigt und korrigiert werden können.

1. Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder beim Transport).

Technische Maßnahmen
Verschlüsselung von (mobilen) Datenträgern und Datenbanken bzw. Bibliotheken
SSL-Verschlüsselung und End-to-End-Verschlüsselung für die digitale Kommunikation
Virtual Private Networks (VPN)/jede Remote-Verbindung muss einen unternehmensintern zugelassenen verschlüsselten Kanal verwenden.
Einsatz geeigneter Firewall- und Verschlüsselungstechnologien zum Schutz von Daten-Knotenpunkten und -Pipelines
Implementation von Sicherheitsgateways an den Netzübergabepunkten
Risikominimierung durch Netzseparierung
Digitale Signatur
Alle PC- und Serverdatenträger-Ports werden standardmäßig deaktiviert.
Das Kopieren von Daten auf Wechseldatenträger wird technisch eingeschränkt.
Soweit möglich, werden Daten nur verschlüsselt an Empfänger übertragen.

Organisatorische Maßnahmen
Regelmäßige Überprüfung der erteilten Freigaben: • Freigaben-Übersicht • Remote-Wipe-Funktion: Mithilfe dieser Funktion können Daten von bestimmten Geräten entfernt werden. • Organisationsmanager: Kontrolle aller Zugriffe mithilfe von File Access Logs
Dokumentierte Regelung von Ausgabe- und Empfängerkreis
Protokollierung von Weitergaben
Prozess zu Datenträgerverwaltungen (inklusive Entsorgung)
Versiegelte Behälter
Dokumentation der Schnittstellen
Fernwartungskonzept

Maßnahmen für Kunden
Ermöglichung folgender Maßnahme bzgl. Weitergabekontrolle für Kunden: • Überprüfung der erteilten Freigaben: Freigaben-Übersicht/Remote-Wipe-Funktion /Organisationsmanager • Verschlüsselung der Bibliotheken: TLS-Verschlüsselung obligatorisch; End-to-End-Verschlüsselung optional

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

2. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen
Dokumentation/Protokollierung von wesentlichen Änderungen in Datenbanken, Kontendaten, Einstellungen und auf dem Server
Nachvollziehbarkeit der Nutzereingaben durch Zeitstempel
Individuelle Benutzer-IDs und Passwörter
Obligatorische Eingabe von vorgegebenen Identifikationsdaten für bestimmte Datenoperationen
Time-outs nach Ablauf von Sitzungen.

Organisatorische Maßnahmen
Dokumentenmanagement, insbesondere Dokumentation der Eingabeberechtigungen
Richtlinien, z. B. für Dateneingabe (Speichern) und für Lesen, Ändern oder Löschen von gespeicherten Daten
Mitarbeiter sind grundsätzlich verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

Maßnahmen für Kunden
Ermöglichung folgender Maßnahmen bzgl. Eingabekontrolle für Kunden: • Protokollierung bzw. Archivierung bei Änderung/Entfernung von Dokumenten (individuell einstellbarer Zeitraum): Wer hat wann Änderung/Entfernung durchgeführt? • Ältere oder gelöschte Versionen können im Nachhinein bei Bedarf angesehen und wiederhergestellt werden.

luckycloud GmbH
Solmsstraße 26
10961 Berlin
Germany

CEO & Founder
Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt
www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

III. Verfügbarkeit und Belastbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind. Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen müssen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Es ist zu gewährleisten, dass die zur Verarbeitung verwendeten Systeme und Dienste auch unter widrigen Einflüssen, die insbesondere von Dritten herrühren können, die Eigenschaften aufrechterhalten können, die eine rechtmäßige Verarbeitung gewährleisten.

Technische Maßnahmen
Sicherheitsmaßnahmen (insbesondere Virenschutz/Firewall; regelmäßige Updates)
Überwachung der Systemstabilität und -verfügbarkeit: Alle Serversysteme unterliegen einem Monitoring (24/7), das im Falle von Störungen unverzüglich einen Administrator benachrichtigt.
Regelmäßige Überprüfung und Minimierung von Schwachstellen
Abwehr von systembelastendem Missbrauch
Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht.
Überprüfung der Wirksamkeit von Datensicherungen (z. B. durch Einspieltests)
Klimatisierte Serverräume
Schutzmaßnahmen gegen Feuer, Überschwemmungen und sonstige Gefährdungen im Serverraum (insbesondere Brandmeldeanlage, Löschanlage)
Unterbrechungsfreie Stromversorgung (USV)
Redundanz der Primärtechnik/Kommunikationsverbindungen
Gehärtete Server und Netzwerkkomponente, die für die Datenverarbeitung genutzt werden
Netzwerksegmentierung/Netzwerksegregation
Vollwertige Disaster-Recovery-Methoden
Regelmäßige Backup-/Recovery-Verfahren

Für den Server besteht eine sichere und ausreichend robuste Default-Einstellung, um einen abgesicherten Wiederanlauf des Serversystems in der vorgesehenen Zeit durchführen zu können.
Festplattenspiegelung

Organisatorische Maßnahmen
Ressourcenplanung und Bereitstellung
Serverraum: Wartungstätigkeiten durch Fremdpersonal nur unter Beaufsichtigung
Dokumentierte Backup- und Recovery-Strategie
Incident Response Management (Notfallpläne mit Wiederanlaufplan/Tests für Anwendung und Infrastruktur)
Verfügbarkeit eines Notfallrechenzentrums

luckycloud GmbH

Solmsstraße 26
10961 Berlin
Germany

CEO & Founder

Luc Mader
legal@luckycloud.de
+49 (0) 30 814 570 920

Kontakt

www.luckycloud.de
legal@luckycloud.de
+49 (0) 30 814 570 920

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Datenschutzmanagement

Dem Datenschutzmanagement unterfallen Maßnahmen, die den datenschutzkonformen Umgang mit personenbezogenen Daten durch Prozesse gewährleisten sollen. Diese Maßnahmen sollen einerseits mithilfe von innerbetrieblichen Strukturen Datenschutzverletzungen vorbeugen, andererseits aber auch helfen, diese nachträglich zu beheben. Es ist demnach ein System von Richtlinien und Prozessen erforderlich, das regelmäßig intern evaluiert und angepasst werden muss.

Technische Maßnahmen
Automatische Wiedervorlagen zwecks Überprüfung von Datenverarbeitungsprozessen
Beachtung von Privacy by Design/Default (z. B. nach Möglichkeit Pseudonymisierung von Daten)

Organisatorische Maßnahmen
Verpflichtung der Mitarbeiter zur Vertraulichkeit
Richtlinie für die Nutzung von IT-Systemen durch Mitarbeiter, insbesondere im Homeoffice („IT-Richtlinie“)
Regelmäßige Schulung der Mitarbeiter
Datenschutz-Policy (mit verschiedenen Prozessbeschreibungen)
Regelungen zur Datenschutzorganisation (insbesondere organisatorische Festlegung von Rollen und Verantwortlichkeiten sowie von Melde- und Freigabeprozessen)
Benennung und dokumentierte Einbindung eines Datenschutzbeauftragten
Verzeichnisse
Incident Response Management (Notfallpläne und Tests für Anwendung und Infrastruktur)

Datenschutzrechtliche Regelungen bei der Einsetzung von Dienstleistern (z. B. in AV-Verträgen oder in NDA)
Fremdpersonal (Reinigung, Hausmeister, Sicherheitskräfte etc.) wird auf Vertraulichkeit verpflichtet.
Regelmäßige Evaluierung und bei Bedarf Anpassung der Dokumente und Prozesse
Prozess zur Evaluation der technischen und organisatorischen Maßnahmen (insbesondere regelmäßige Durchführung von technischen Überprüfungen)
In Rechenzentren zertifizierte Managementsysteme nach BSI-Grundschutz, ISO 9001, 27001 und 50001

2. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die gem. Art. 28 DS-GVO im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen
Automatische Wiedervorlagen zwecks Überprüfung von (weiteren) Auftragsverarbeitern

Organisatorische Maßnahmen
Abschluss Auftragsverarbeitungsvertrag nach zuvor durchgeführter Prüfung
Vertragliche Beschränkungen im AV-Vertrag zur Verhinderung unbefugter Verarbeitung
Regelmäßige Überwachung der Aktivitäten von Dienstleistern
Weisungsbefugte Personen und befugte Empfänger sind definiert; Dokumentation von Weisungen
Bei Auftragsverarbeitung seitens luckycloud: Zugriff auf die betreffenden Kundendaten nur nach Weisung

3. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)

Um die Einhaltung der DS-GVO nachweisen zu können, hat der Verantwortliche interne Strategien festzulegen und Maßnahmen zu ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (Privcay by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) Genüge tun (EG 78).

Privacy by Design
Pseudonymisierung (vgl. oben)
Daten werden nach Möglichkeit verschlüsselt gespeichert.

Privacy by Default
Mitarbeiter/Kunden müssen in den Verarbeitungssystemen nur Informationen mitteilen, die zur Zweckerfüllung absolut notwendig sind.
Datenschutzfreundliche Benutzer-Interfaces
Zero-Knowledge-Prinzip
Bei Löschung eines Accounts werden automatisch alle Daten gelöscht. (Aus Sicherheitsgründen werden gelöschte Daten grundsätzlich für 30 Tage archiviert.)

Maßnahmen für Kunden
Ermöglichung folgender Maßnahmen bzgl. Privacy by Design/Default für Kunden: • Individuelle Benutzer-ID/E-Mail-Adresse nach Wahl des Nutzers • Datenschutzfreundliche Benutzer-Interfaces • Bei Löschung eines Accounts werden automatisch alle Daten gelöscht. (Aus Sicherheitsgründen werden gelöschte Daten grundsätzlich für 30 Tage archiviert.)