luca

TOM culture4life GmbH und luca System

Technisch-Organisatorische Maßnahmen (TOM) der culture4life GmbH und des luca Systems

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BSI	Sicherheit in der Informationstechnik
BSI-C5	Sicherheit in der Informationstechnik (BSI) den Anforderungskatalog Cloud Computing (C5)
CPU	Central Processing Unit
CSM	Certificate Service Manager
DDoS	Distributed-Denial-of-Service
DSB	Datenschutzbeauftragte
DSGVO	Datenschutz-Grundverordnung
IAM	Identity- and Access Management
ISB	Informationssicherheitsbeauftragte
MFA	Multi-Faktor-Authentisierung
NIST	National Institute of Standards and Technology
OTC	Open Telekom Cloud
OWASP	Open Web Application Security Project
PGP	Pretty Good Privacy
SQL	Structured Query Language
TLS	Transport Layer Security
TOM	Technisch-Organisatorische Maßnahmen
VPN	Virtual Private Network

1 Einleitung

1.1 Gegenstand und Ziele

Das vorliegende Dokument beschreibt die Technisch-Organisatorischen Maßnahmen (TOM) der culture4life GmbH (nachfolgend culture4life) und des luca Systems zum Schutz von personenbezogenen Daten.

1.2 Geltungsbereich

Das Dokument gilt unmittelbar für den culture4life Standort Berlin sowie mittelbar über vertragliche Regelungen (Vertrag zur Auftragsverarbeitung) für alle Orte und Prozesse der Verarbeitung von personenbezogenen Daten von culture4life für das luca System. Die gesamte Entwicklung und der gesamte Betrieb von Frontend und Backend der luca-App wird durch die neXenio GmbH (nachfolgend neXenio) aus Berlin verantwortet, sodass die TOM durch neXenio zur Verfügung gestellt werden.

1.3 Verantwortlichkeiten

Für die Erstellung und Pflege des TOM-Dokumentes ist die Geschäftsführung der culture4life verantwortlich. Die Geschäftsführung kann diese Aufgaben an die benannte Datenschutzbeauftragte (DSB) und wenn benannt den Informationssicherheitsbeauftragten (ISB) der culture4life delegieren, bleibt aber für den gesetzeskonformen Umgang der culture4life mit personenbezogenen Daten verantwortlich. Der Betrieb des Frontends und des Backends von luca wird durch neXenio verantwortet, sodass diese von der Geschäftsführung der culture4life in den Erstellungs- und Pflegeprozess des TOM-Dokumentes einbezogen wird und die DSB von culture4life unterstützt. In jedem Fall bleibt die Geschäftsführung von culture4life weiterhin verantwortlich.

2 Ableitung Schutzziele, TOM und Einzelmaßnahmen

Gemäß Art. 32 DSGVO („Sicherheit der Verarbeitung“) müssen Verantwortliche und Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für

die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein den Risiken angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;
b) die Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit der Systeme und Dienste** im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den **Zugang** zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen;**
d) ein Verfahren zur regelmäßigen **Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Erläuterungen zu:

a) Pseudonymisierung und Verschlüsselung sind zwei Einzelmaßnahmen, welche zur Erreichung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit eingesetzt werden.

b) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sind weitere wichtige Schutzziele der DSGVO siehe Erläuterung zu a).

c) Verfügbarkeit ist ein Schutzziel, Zugang ist eine TOM gemäß § 64 BDSG.

d) Maßnahmen zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM müssen implementiert werden und im Rahmen eines Managementsystems auf ihre Wirksamkeit überprüft werden. In diesem regelmäßig zu wiederholendem Prozess ist beispielsweise zu prüfen, ob die eingesetzten Maßnahmen noch angemessen sind.

Zusammenfassend stehen auf der obersten Ebene die gemäß § 64 BDSG zu erreichenden **Schutzziele**, welche durch **Einzelmaßnahmen** erfüllt werden.

Die Zwecke der Schutzziele können Art. 32 DSGVO sowie § 64 BDSG entnommen werden und geben wertvolle Hinweise auf die umzusetzenden Maßnahmen zum Erreichen dieser Zwecke und damit der Schutzziele des BDSG und der DSGVO:

- **Zugangskontrolle**: Verwehrung des Zugangs für Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird.

  Schutzziel: Vertraulichkeit
- **Zugriffskontrolle**: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

  Schutzziel: Vertraulichkeit
- **Übertragungskontrolle**: Gewährleistung, 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.

  Schutzziel: Vertraulichkeit
- **Benutzerkontrolle**: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

  Schutzziel: Vertraulichkeit
- **Eingabekontrolle**: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

  Schutzziel: Integrität
- **Auftragskontrolle**: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

  Schutzziel: Integrität
- **Datenintegrität**: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

  Schutzziel: Integrität

- **Datenträgerkontrolle**: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

  Schutzziele: Vertraulichkeit, Integrität

- **Speicherkontrolle**: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

  Schutzziele: Vertraulichkeit, Integrität

- **Transportkontrolle**: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

  Schutzziele: Vertraulichkeit, Integrität

- **Trennbarkeit**: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

  Schutzziele: Vertraulichkeit, Integrität

- **Wiederherstellbarkeit**: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

  Schutzziele: Verfügbarkeit, Belastbarkeit

- **Zuverlässigkeit**: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

  Schutzziele: Verfügbarkeit, Belastbarkeit

- **Verfügbarkeitskontrolle**: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

  Schutzziele: Verfügbarkeit, Belastbarkeit

Schutzziele / TOM	Vertraulichkeit	Integrität	Verfügbarkeit & Belastbarkeit
Zugangskontrolle	X		
Zugriffskontrolle	X		
Übertragungskontrolle	X		
Benutzerkontrolle	X		
Eingabekontrolle		X	
Auftragskontrolle		X	
Datenintegrität		X	
Datenträgerkontrolle	X	X	
Speicherkontrolle	X	X	
Transportkontrolle	X	X	
Trennbarkeit	X	X	
Wiederherstellbarkeit			X
Zuverlässigkeit			X
Verfügbarkeitskontrolle			X

Abbildung 1: Abbildung der TOM hinsichtlich Schutzziele

3 TOM bei culture4life und des luca Systems

Hier werden die bei culture4life für die Organisation (die culture4life GmbH) und das luca System umgesetzten Technisch-Organisatorischen Maßnahmen dargestellt. Unter das luca System fallen die Frontends (luca-App (web und mobil) für Nutzer, luca Badge für Nutzer, luca Venue Owner Frontend für Betreiber, luca Scanner Frontend für Betreiber, luca Frontend Gesundheitsamt) und das luca Backend.

3.1 Zutrittskontrolle

Maßnahmen zur Zutrittskontrolle gewährleisten, dass der Zutritt zu den Datenverarbeitungsanlagen nur jenen Personen gewährt wird, welche dazu berechtig sind.

Die Büroräume von culture4life befinden sich in einem Bürokomplex in Berlin. Der Eingang des Gebäudekomplexes ist über eine Zutrittstür gesichert, die stets verschlossen und selbstschließend ist. Das Bürogebäude kann nur über einen Eingang im Erdgeschoss betreten werden. Der Zutritt zu dem Bürogebäude kann nur mit Hilfe eines per-

sonalisierten Transponders erfolgen. Für Besucher und Postboten gibt es die Möglichkeit, sich über eine Gegensprechanlage mit dem Empfang von culture4life in Verbindung zu setzen und nach erfolgreicher Authentifizierung die Eingangstüren zu entsperren.

Alle Aufzüge sind mit einem Transponder Lesegerät ausgestattet, um sicherzustellen, dass nur Personen in entsprechende Etagen fahren können, die auch eine Zutrittsberechtigung in Form eines personalisierten Transponders haben. Für den Zeitraum von 20:00 bis 6:00 Uhr des Folgetages ist die Verwendung eines personalisierten Transponders notwendig, um die Aufzüge zu nutzen. Zu Geschäftszeiten können auch Personen ohne personalisierten Transponder in die entsprechende Etage fahren. Alle aktiven Aufzüge gewähren lediglich Zugang zu den Fluren mit den Eingangstüren zu den Büroräumen.

Für die Türen zu den Geschäftsräumen von culture4life ist ein eigenes elektronisches Schließsystem im Einsatz. Die Ausgabe von Transpondern erfolgt auf Basis des 4-Augen-Prinzips und wird protokolliert („Transponderausgabe-Prozess“). Mitarbeiter sind verpflichtet, einen Transponderverlust unverzüglich zu melden. Im Falle eines Verlusts erfolgt eine sofortige elektronische Sperrung des jeweiligen Transponders. Ferner gibt es einen Prozess bei dem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Transpondern und sonstigem Eigentum der culture4life durch den ausscheidenden Mitarbeiter beinhaltet. Personen, die keine Mitarbeiter der culture4life sind, haben die Möglichkeit, sich an der Tür zu den Räumlichkeiten über eine Klingel anzumelden und vom Empfang persönlich abholen zu lassen. Jeder Zugang einer externen Person wird protokolliert. Jeder Besucher wird in den gesamten Büro-Räumlichkeiten von einem Mitarbeiter begleitet.

Neben den aktiven Aufzügen befinden sich zwei weitere inaktive Aufzugschächte, deren Türen sich direkt in den Räumlichkeiten der culture4life befinden. Die Etage der culture4life ist für diese Aufzüge nicht freigeschaltet und sie sind physikalisch verschlossen. Sollte sich eine Person außerhalb der Geschäftszeiten über die deaktivierten Aufzüge unbefugt Zutritt in die Räumlichkeiten der culture4life verschaffen, wird ein Alarm ausgelöst.

Es existieren drei separate Treppen als Rettungswege. Diese können nur verwendet werden, um das Gebäude auf direktem Weg nach unten zu verlassen. Die Türen zu den Treppen lassen sich von außen (in Richtung der Büroräume) nicht öffnen. Auch kann der Zugang zum Treppenhaus des Rettungswegs nicht ohne Weiteres von außen geöffnet werden. Bei aktivierter Alarmanlage (außerhalb der Geschäftszeiten) werden die Rettungswege ebenfalls über die Alarmanlage überwacht.

Die Geschäftsräume von culture4life sind durch eine Alarmanlage gesichert. Versteckte Bewegungsmelder im gesamten Büro registrieren jede Bewegung und lösen sofort einen Alarm aus, sofern keine Mitarbeiter der culture4life bzw. des Dienstleisters neXenio anwesend sind. Die Alarmanlage wird morgens vom ersten Mitarbeiter, der das Büro betritt, deaktiviert und vom letzten Mitarbeiter bei Verlassen der Büroräume aktiviert. Zudem gibt es eine automatische Aktivierung der Alarmanlage täglich um 22 Uhr, die verhindern soll, dass die Alarmanlage infolge des Vergessens der Mitarbeiter inaktiv bleibt. Aktivierung und Deaktivierung der Alarmanlage erfolgen durch einen Transponder, den Mitarbeiter erhalten. Auch hierfür gilt der Transponderausgabe-Prozess. Der Transponder ist mit einer Nummer versehen, die dem jeweiligen Mitarbeiter intern zugeordnet werden kann. In der Alarmanlage werden Aktivierungen und Deaktivierungen auf Basis der Transponder-Nummer protokolliert.

Alle Fenster und Balkone werden mit dem letzten Mitarbeiter, der das Büro verlässt, verschlossen. Fenster und Balkone, die nicht ordnungsmäßig verschlossen wurden, lösen nach Aktivieren der Alarmanlage den Alarm aus.

Nach Auslösen der Alarmanlage wird umgehend automatisch ein Sicherheitsdienstleister informiert und eine Benachrichtigung an berechtigte Personen versendet. Der Sicherheitsdienst überprüft die Situation in den Räumlichkeiten. Es gibt keine Möglichkeit, den persönlichen Besuch des Sicherheitsmitarbeiters zu verhindern.

Neben dem Überwachen des Büros existiert eine separate Alarmschaltung für den hauseigenen Serverraum. Dieser ist ebenfalls mit einem Transponderlesegerät ausgestattet. Nur Mitarbeiter, die Zugang zum Serverraum benötigen, besitzen einen gesonderten personalisierten Transponder, Alarmcode und Schlüssel. Die Alarmanlage zu

diesem aktiviert sich unabhängig vom gesamten Büro und ggf. noch anwesenden Mitarbeitern zu einer festgelegten Zeit.

Daten, die im Zusammenhang mit den Produkten und Diensten verarbeitet werden, werden ausschließlich bei den zwei IT-Dienstleistern, der Bundesdruckerei GmbH (CSM) und der Open Telekom Cloud (OTC), gespeichert und verarbeitet. Die Rechenzentren liegen innerhalb Deutschlands. Die Rechenzentren der Open Telekom Cloud (Backend des luca Dienstes) sind BSI-C5 zertifiziert. Die OTC zeichnet sich durch ihre (geographisch hinreichend voneinander getrennten) Standorte in Deutschland aus.

Die Rechenzentren von OTC und CSM sind in unscheinbaren Gebäuden untergebracht, die von außen nicht sofort als Rechenzentrum zu erkennen sind. Das Rechenzentrum selbst ist durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt sowohl weiträumig (z. B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern.

Der Zutritt zum Rechenzentrum wird durch elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde.

Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet. Der Zutritt zu sensiblen Bereichen wird durch Videoüberwachung geschützt. Ausgebildete Sicherheitskräfte bewachen das Rechenzentrum und dessen unmittelbare Umgebung 24 Stunden am Tag, 7 Tage die Woche.

3.2 Zugangskontrolle

Maßnahmen zur Zugangskontrolle gewährleisten, dass die Verwehrung des Zugangs durch Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, durch weitreichende Maßnahmen umfassend sichergestellt ist.

Die Büroräume der culture4life befinden sich im sechsten Stock. Die Fenster sind aufgrund der Entfernung nicht durch gegenüberliegende Büros auf gleicher Höhe einsehbar. Die Bildschirme der Mitarbeiter sind stets so ausgerichtet, dass eine Einsichtnahme von außen nicht erfolgen kann.

An jedem IT-System, das bei culture4life im Einsatz ist, muss eine vorherige Authentifizierung erfolgen. Dies erfolgt auf Basis eines Benutzernamens und eines Passworts oder des Fingerabdruckes.

Eine Berechtigung zur Nutzung eines IT-Systems oder einer Applikation wird nach dem 4-Augen-Prinzip erteilt. Eine Berechtigung muss daher zwingend vom jeweiligen Vorgesetzten für einen Mitarbeiter bei der IT-Administration beantragt werden. Der Vorgesetzte ist verpflichtet, hierbei nur die Berechtigungen zu beantragen, die für den jeweiligen Mitarbeiter unbedingt erforderlich sind, damit dieser die ihm zugewiesenen Aufgaben erfüllen kann. Berechtigungen sind dabei auf das Minimale zu beschränken.

Erteilte Berechtigungen (und der Entzug) werden von der IT-Administration und systemseitig protokolliert. Die IT-Administration prüft quartalsweise in Absprache mit den Vorgesetzten, ob die erteilten Berechtigungen noch erforderlich sind. Vorgesetzte sind darüber hinaus verpflichtet, im Falle von Aufgabenwechsel von Mitarbeitern eine entsprechende Korrektur von Berechtigungen bei der IT-Administration zu beantragen.

Im Falle des Ausscheidens von Mitarbeitern informieren die Personalverantwortlichen die IT-Administration unverzüglich über anstehende Veränderungen, damit die IT-Administration entsprechende Berechtigungen entziehen kann. Der Entzug aller Berechtigungen muss binnen 24 Stunden nach Ausscheiden eines Mitarbeiters durchgeführt worden sein.

Werden Initialpasswörter vergeben, ist bei culture4life stets vorgesehen, dass das Initialpasswort bei der ersten Anmeldung geändert wird. Dies wird technisch erzwungen.

Bei culture4life gibt es Richtlinien zur Passwortverwendung, die ebenfalls grundsätzlich technisch erzwungen werden. Die Mindestpasswortlänge beträgt 8 Zeichen. Passwörter sind komplex zu wählen. Dies beinhaltet die Verwendung von Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern. Die automatische Verrieglung aller IT-Systeme nach spätestens 15 Minuten ist aktiviert. Sollte sich der Stand der Technik bei der Verwendung von Passwörtern ändern, wird culture4life die Passwortrichtlinien entsprechend anpassen. Die Verwendung von Passwörtern ist ebenfalls geregelt und sieht die Verwendung von komplexen Passwörtern, einen Passwortwechsel nach spätestens 90 Tagen sowie eine Passworthistorie vor (die 5 letzten Passwörter).

Ein Zugriff auf die externen IT-Systeme findet ausschließlich über verschlüsselte Verbindungen statt. Die dabei verwendeten Verschlüsselungsalgorithmen und Schlüssellängen entsprechen dem Stand der Technik. Für den Fall einer zertifikatsbasierten Zugriffstechnologie ist gewährleistet, dass die Zertifikate durch Mitarbeiter der IT-Administration verwaltet werden.

Alle IT-Systeme, mit denen Daten (im Auftrag) verarbeitet werden, sind mit Antivirus-Software ausgestattet. Das Firmennetzwerk ist durch eine Firewall geschützt. Nur vertrauenswürdige und geprüfte Software kommt zum Einsatz auf den Servern. Übergänge zum Firmennetz, wie E-Mail-Accounts, werden stets von Antivirus-Software geprüft. Sicherheitsrelevante Softwareupdates werden regelmäßig und automatisiert in die vorhandene Software eingespielt.

Für die Rechenzentren der Bundesdruckerei GmbH und der Open Telecom Cloud gilt, dass auch dort alle Berechtigungen nach dem Prinzip der Minimalberechtigung erteilt und Berechtigungen regelmäßig überprüft werden. Vergabe und Entzug von Berechtigungen werden protokolliert. Die Verwendung von Passwörtern ist ebenfalls geregelt und sieht die Verwendung von komplexen Passwörtern, einen Passwortwechsel nach spätestens 90 Tagen sowie eine Passworthistorie vor.

3.3 Zugriffskontrolle

Maßnahmen zur Zugriffskontrolle gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

Für die Erteilung von Benutzerrechten gilt bei neXenio ein Berechtigungskonzept. Dies sieht vor, dass Berechtigungen ausschließlich auf Basis des 4-Augenprinzips und nach dem Minimalprinzip vergeben werden. Dies beinhaltet, dass jeder Mitarbeiter nur die Berechtigungen erhält, die er unmittelbar benötigt, um seine Aufgaben im Unter-nehmen erfüllen zu können. Das Berechtigungskonzept ist rollenbasiert. Jedem Mitar-beiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abwei-chende Berechtigungen müssen begründet sein. Die Vergabe und der Entzug von Berechtigungen werden protokolliert. Eine quartalsweise Überprüfung erfolgt durch die IT-Administration in Zusammenarbeit mit den jeweiligen Vorgesetzten.

Sofern möglich, werden alle Handlungen, die einer Autorisierung bedürfen, protokolliert. Dazu gehören insbesondere der Zugriff auf das geschützte Netzwerk via VPN, das Editieren von Dokumentationen und Auditlogs für Datenbanken.

Die neXenio verfügt über verschiedene Netzwerke. Dazu gehören ein komplett losgelöstes öffentliches Netzwerk, das über einen Zugangsschlüssel gesichert ist und nur Besuchern und Mitarbeitern der neXenio zur Verfügung steht. Für alle Mitarbeiter, die Zugang zu den Entwicklungssystemen der neXenio haben, gibt es ein gesichertes Netzwerk, auf das man nur mit einem personalisierten Zertifikat Zugriff hat. Die Zerti-fikate laufen nach einer vorgegebenen Zeit ab und müssen regelmäßig erneuert wer-den.

Jeder Mitarbeitercomputer wird mit einer Festplattenverschlüsselung betrieben und ist durch personalisierte Benutzerkonten und Passwörter (oder Fingerabdruck) ge-schützt. Um Fremdzugriff zu verhindern, werden alle Mitarbeiter angewiesen ihre Computer zu sperren sobald sie diese unbeaufsichtigt lassen. Eine automatische Desktopsperre ist aktiviert. Allen Mitarbeitern stehen abschließbare Rollcontainer zur Verfügung.

3.4 Übertragungskontrolle

Siehe Kapitel 3.11.

3.5 Benutzerkontrolle

Maßnahmen zur Benutzerkontrolle gewährleisten, dass die zu Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte erfolgt.

Folgende Maßnahmen dienen der Benutzerkontrolle:

- Kryptographie

Der Abschnitt gliedert sich in Maßnahmen zur Verschlüsselung während des Transports und bei Speicherung von Daten und Maßnahmen zur Gewährleistung einer Ende-zu-Ende-Verschlüsselung zwischen den am luca System beteiligten Entitäten. Für detaillierte Informationen zu kryptographischen Operationen wird an dieser Stelle auf das Kryptokonzept verwiesen. Die culture4life lässt sich bei der Planung des Einsatzes von kryptographischen Operationen durch Experten des Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC beraten.

- Identitäts- und Zugriffsmanagement

Für das Identitäts- und Zugriffsmanagement (IAM) stellt das luca System verschiedene Maßnahmen zur Verfügung:

  - Password Policy
  - 2-Way-TLS und MFA für Verbindungen zwischen einem Gesundheitsamt und dem luca Server
  - Risk-based Access Control
  - Rate-Limiting
  - Prüfung der Authentizität und Integrität verschlüsselter Informationen
  - Multi-Factor-Authentisierung bei Zugriffen auf Ressourcen
  - Least Privilege Principle
  - Single-Sign-On
  - Härtung verwalteter Passwörter gegen Offline-Angriffe
  - Session-Management

- Security Monitoring und Alerting

Automatische Überwachung sicherheitsrelevanter Logeinträge mit regelbasierter Alarmierung des IT-Sicherheitsteams.

3.6 Eingabekontrolle

Maßnahmen zur Eingabekontrolle gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Jede Eingabe von Daten wird systemseitig unter Zuordnung der jeweiligen Benutzerkennung protokolliert. Gleiches gilt für die Änderung und Löschung von Daten. Im Falle einer Änderung von Daten ist aus der Protokollierung erkenntlich, welche Änderungen vorgenommen wurden. Die Protokolle werden für die Dauer von 1 Woche von neXenio gespeichert.

Folgende Maßnahmen dienen der Eingabekontrolle:

- Identitäts- und Zugriffsmanagement (siehe Kapitel 3.5)

3.7 Auftragskontrolle

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

Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei neXenio eine höchste Priorität. Alle Mitarbeiter sind auf das Datengeheimnis und auf Vertraulichkeit verpflichtet.

Es gibt einen betrieblichen Datenschutzbeauftragten, der u.a. die regelmäßige Schulung der Mitarbeiter plant und durchführt. Alle Mitarbeiter erhalten eine jährliche Datenschutzschulung. Mitarbeiter, die bereits mehrfach geschult wurden, erhalten eine Auffrischung.

Die Datenschutzvorkehrungen neXenios beinhalten eine regelmäßige Überprüfung und Bewertung der getroffenen Technisch-Organisatorischer Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Auf diese Weise gewährleistet neXenio eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten. Mit Auftragnehmern bestehen Verträge zur Arbeitsverarbeitung im Sinne der DSGVO.

3.8 Datenintegrität

Maßnahmen zur Datenintegrität gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Folgende Maßnahmen dienen der Datenintegrität:

- Integrität (inkl. Authentizität)
  - Systemkonzept: luca nimmt für besonders schützenswerte Daten ausschließlich eine Vermittlerrolle ein, die keine Einsicht in Klardaten erhält. Dies wird über eine Ende-zu-Ende-Verschlüsselung erreicht.
  - Durchgängige Verschlüsselung: Die durchgängige Verschlüsselung (Transportweg und at Rest) der im luca Server verarbeiteten Daten wirkt sich positiv auf die Integrität aus, da Man-In-The-Middle-Angriffe hierdurch wirksam abgewehrt werden.

- Schutz vor Manipulation der im luca Server verarbeiteten Daten.
- Schutz vor Manipulation der Anwendungskomponenten.
- Penetrationstests und Audits.
- Verwendung der von Browsern bereitgestellten Schutzmaßnahmen zum Schutz der Web Frontends.
- Selbstgehostete Frontends.

3.9 Datenträgerkontrolle

Maßnahmen zur Datenträgerkontrolle gewährleisten, dass das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern verhindert wird.

Durch die Kontrolle von Zutritt (siehe Kapitel 3.1), Zugang (siehe Kapitel 3.2) und Zugriff (siehe Kapitel 3.3) wird eine hinreichende Datenträgerkontrolle erreicht.

Folgende Maßnahmen dienen über die Kontrolle von Zugang und Zugriff der Datenintegrität:

- Kryptographie (siehe Kapitel 3.5)
- Identitäts- und Zugriffsmanagement (siehe Kapitel 3.5)
- Security Monitoring und Alerting (siehe Kapitel 3.5)

3.10 Speicherkontrolle

Maßnahmen zur Speicherkontrolle gewährleisten, dass die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.

Durch die Kontrolle von Zutritt (siehe Kapitel 3.1), Zugang (siehe Kapitel 3.2) und Zugriff (siehe Kapitel 3.3) wird eine hinreichende Speicherkontrolle erreicht.

Folgende Maßnahmen dienen über die Kontrolle von Zugang und Zugriff der Speicherkontrolle:

- Identitäts- und Zugriffsmanagement (siehe Kapitel 3.5)
- Security Monitoring und Alerting (siehe Kapitel 3.5)

3.11 Transportkontrolle/Übertragungskontrolle

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

Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten haben, die verarbeitet werden, beschränkt ist. Die Verwendung von externen Datenträgern ist nicht vorgesehen. Zum Übermitteln von Daten muss ausschließlich Bdrive (von der neXenio für die Bundesdruckerei entwickelte hochsichere Cloud-Lösung) verwendet werden.

Generell wird versucht, Ausdrucke auf Papier so gering wie möglich zu halten. Vertrauliche Ausdrucke werden in abgeschlossenen Aktenschränken in getrennten Büroräumen aufbewahrt. Dokumente werden mit einem Aktenvernichter vernichtet.

Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch neXenio übergeben werden sollen, werden die Parteien in den Vorwegen eine Verschlüsselungsmethode bzw. einen Weg der sicheren Übertragung vereinbaren. Jeder Mitarbeiter, der eine E-Mail-Adresse erhält, muss einen Pretty Good Private (PGP) Key erstellen. Vertrauliche Dateien dürfen nicht via E-Mail verschickt werden, sondern müssen über Bdrive als Linkshare verschickt werden. Dabei kann ein zeitlich limitierter Link erstellt werden, der als Anhang der E-Mail angefügt werden kann. Neben einem möglichen Passwortschutz für diesen Linkshare lässt sich auch eine Autorisierung via SMS konfigurieren, die es ausschließlich dem Besitzer der Telefonnummer erlaubt, den Linkshare herunterzuladen und zu entschlüsseln. Jeder Zugriff auf und der Abruf von Daten der Applikation erfolgt verschlüsselt (TLS).

3.12 Trennbarkeit

Maßnahmen zur Trennbarkeit gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet (Speicherung, Veränderung, Löschung, Übermittlung) werden können.

Die IT-Systeme sind mandantenfähig. Es ist sichergestellt, dass Daten von luca getrennt von anderen Mandanten verarbeitet werden. Es besteht ein Berechtigungskonzept, das den Datenzugriff von Mitarbeitern ausschließt. Mitarbeiter der neXenio sind schriftlich verpflichtet, Informationen aus Datenbeständen von luca nicht für andere Mandanten oder für andere Zwecke mit einzubringen.

3.13 Wiederherstellbarkeit

Maßnahmen zur Wiederherstellbarkeit gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Folgende Maßnahmen dienen der Wiederherstellbarkeit:

- Automatische Skalierung des Systems: Dynamische Skalierung des Systems in Abhängigkeit von CPU-Auslastung und Speicherbedarf.
- Redundant ausgelegte Nameserver: luca verwendet vier Nameserver mit unterschiedlichen Top-Level-Domains.
- Georedundanz: Der luca Server wird in physikalisch getrennten Verfügbarkeitszonen der Open Telekom Cloud (OTC) betrieben. Der Ausfall eines Rechenzentrums führt nicht zum Ausfall des luca Systems.
- Backup- und Restore-Management: Maßnahmen zur Wiederherstellung des Betriebs im Falle von Datenverlusten:
    - Verwendung einer Managed PostgreSQL Datenbank Speicherung persistierter Daten in einer Managed PostgreSQL Datenbank der OTC mit Backup- und Restore-Funktionalitäten.
    - Nachhaltung sämtlicher Änderungen an Artefakten des luca Systems: Sämtliche Änderungen am Quellcode oder der Konfiguration von Komponenten des luca Systems werden nachgehalten. Zudem ist es möglich, das System auf jeden früheren Zustand zurückzusetzen.
- Health Monitoring: kontinuierliche Überwachung der eingesetzten Systemkomponenten (syslogs), Systemzustand über Monitoring-Dashboards, kritische Abweichungen von der Norm bewirken die Alarmierung des Operations-Teams.

3.14 Zuverlässigkeit

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

Folgende Maßnahmen dienen der Zuverlässigkeit:

- Schutz vor Denial-of-Service-Angriffen: Anti-DDoS-Service der OTC (150mbit/s).
- Redundant ausgelegte Nameserver: luca verwendet vier Nameserver mit unterschiedlichen Top-Level-Domains.
- Georedundanz: Der luca Server wird in physikalisch getrennten Verfügbarkeitszonen der OTC betrieben. Der Ausfall eines Rechenzentrums führt nicht zum Ausfall des luca Systems.
- Konfiguration von Komponenten gemäß Empfehlungen etablierter Quellen: Komponenten des luca Systems werden gemäß Empfehlungen etablierter Quellen konfiguriert wie z.B. OWASP Cheat Sheets/Testing Guides, BSI Technische Richtlinien, NIST Standards/Empfehlungen, Konfigurationsempfehlungen der Hersteller von Komponenten.
- Patch- und Vulnerability-Management: Maßnahmen zur Vermeidung von Sicherheitslücken durch unzureichend gepatchte Systeme bzw. durch Verwendung von Systemen mit bekannten Verwundbarkeiten:
    - Wartung und Pflege von Kubernetes durch OTC.
    - Wartung und Pflege der PostgreSQL Datenbank durch OTC.
    - Unterbindung der Übernahme von Änderungen bei möglichen Schwachstellen.
- Backup- und Restore-Management: Maßnahmen zur Wiederherstellung des Betriebs im Falle von Datenverlusten:
    - Verwendung einer Managed PostgreSQL Datenbank: Speicherung persistierter Daten in einer Managed PostgreSQL Datenbank der OTC mit Backup- und Restore-Funktionalitäten.

- Nachhaltung sämtlicher Änderungen an Artefakten des luca Systems: Sämtliche Änderungen am Quellcode oder der Konfiguration von Komponenten des luca Systems werden nachgehalten. Zudem ist es möglich, das System auf jeden früheren Zustand zurückzusetzen.

- Health Monitoring: kontinuierliche Überwachung der eingesetzten Systemkomponenten (syslogs), Systemzustand über Monitoring-Dashboards, kritische Abweichungen von der Norm bewirken die Alarmierung des Operations-Teams.

3.15 Verfügbarkeitskontrolle

Maßnahmen zur Verfügbarkeitskontrolle gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Alle Daten werden in einem Rechenzentrum verarbeitet. neXenio hat Maßnahmen getroffen, die eine Sicherung der Daten und Wiederherstellung von Daten gewährleistet. Es gibt ein Datensicherungs- und Wiederherstellungskonzept, dessen Wirksamkeit regelmäßig getestet wird. Für alle personenbezogenen Daten, die auf Systemen von Cloud-Anbietern verarbeitet werden, werden regelmäßig Full-Backups (mindestens 1x am Tag) erstellt und auf Cloud Speichern gesichert.

Im Rechenzentrum sind umfangreiche Maßnahmen zur Gewährleistung der Verfügbarkeit getroffen:

Im Rechenzentrum ist eine automatische Branderkennung und -bekämpfung installiert. Das Branderkennungssystem setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur, Kühlräumen und sowie in den Räumen, in denen die Generatoren untergebracht sind, ein.

Alle Stromversorgungssysteme sind redundant. Eine unterbrechungsfreie Stromversorgung (USV) sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Das Rechenzentrum verfügt darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können. Das Rechenzentrum verfügt über eine Klimatisierung und Temperaturkontrolle. Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

- Redundant ausgelegte Nameserver: luca verwendet vier Nameserver mit unterschiedlichen Top-Level-Domains.
- Georedundanz: Der luca Server wird in physikalisch getrennten Verfügbarkeitszonen der OTC betrieben. Der Ausfall eines Rechenzentrums führt nicht zum Ausfall des luca Systems.
- Backup- und Restore-Management: Maßnahmen zur Wiederherstellung des Betriebs im Falle von Datenverlusten:
    - Verwendung einer Managed PostgreSQL Datenbank: Speicherung persistierter Daten in einer Managed PostgreSQL Datenbank der OTC mit Backup- und Restore-Funktionalitäten.
    - Nachhaltung sämtlicher Änderungen an Artefakten des luca Systems: Sämtliche Änderungen am Quellcode oder der Konfiguration von Komponenten des luca Systems werden nachgehalten. Zudem ist es möglich, das System auf jeden früheren Zustand zurückzusetzen.
- Health Monitoring: Kontinuierliche Überwachung der eingesetzten Systemkomponenten (syslogs), Systemzustand über Monitoring-Dashboards, kritische Abweichungen von der Norm bewirken die Alarmierung des Operations-Teams:

3.16 Übergreifende Maßnahmen

Das luca System weist jenseits der aus Artikel 32 DSGVO und § 64 BDSG-neu abgeleiteten Schutzziele weitere Maßnahmen auf, die übergreifend zur Systemsicherheit beitragen.

Zu diesen Maßnahmen gehören:

- Security and Privacy by Design
    - Ende-zu-Ende-Ansatz
    - Schlüsselhoheit
    - Datensparsamkeit
    - Trennung von Rollen und Verantwortlichkeiten
    - Ad-Hoc Nutzbarkeit
    - Migrierbarkeit
    - Unabhängige externe Sicherheitsexpertise bereits in Planungsphasen

- Kryptoagilität
    - Aktualisierung des Hash-Verfahrens für Passwörter
    - Aktualisierung asymmetrischer Schlüssellängen und Verfahren
    - Aktualisierung asymmetrischer Schlüssellängen und Verfahren in QR-Codes
    - Aktualisierung symmetrischer Schlüssellängen und Verfahren
- Auditierung und Sicherheitstests
- Sicherer Softwareentwicklungszyklus
    - Vier-Augen-Prinzip im Release-Prozess
    - Verwendung von BitBucket zur Quellcode-Verwaltung
    - Sicherheitskritische und kryptographische Operationen in eigenen Modulen
    - Trennung der Entwicklungsumgebungen
    - Schulung der Mitarbeiter

4 Regelmäßige Überprüfung, Bewertung und Evaluierung der TOM

culture4life verfügt über ein Datenschutz-Managementsystem (DSMS) bestehend aus:

- Extern bestellte Datenschutzbeauftragte (DSB)
- Datenschutzerklärung(en)
- Datenschutzleitlinie
- Verarbeitungsverzeichnis
- Verzeichnis der Auftragsverarbeitungsverträge
- Löschkonzept
- TOM-Dokument
- Datenschutz-Folgenabschätzung
- Betroffenenrechtekonzept
- Management-Attention durch jährliches Review des DSMS

Sämtliche Komponenten vom luca System erfahren im Rahmen des sicheren Softwareentwicklungszyklus regelmäßige Audits und Sicherheitstests:

- Unabhängiges Code-Review durch das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)
- Penetrationstests
- Quelltext-Reviews bei jeder Änderung, die für den Produktivbetrieb vorgesehen ist
- Automatisierte Quelltext-Reviews

5 Anhang

5.1 Verweise

- Kryptokonzept luca

5.2 Anlagen

/