Vereinbarung zur Datenverarbeitung im Auftrag

zwischen

Unternehmen: Gemeinde Handewitt - Der Bürgermeister -
Adresse: Hauptstr. 9, 24983 Handewitt

– Verantwortlicher, nachstehend „**Auftraggeber**" –

und

culture4life GmbH
Charlottenstraße 59, D-10117 Berlin

– Auftragsverarbeiter, nachstehend „**culture4life**" –
– jeder eine „**Partei**", gemeinsam nachstehend die „**Parteien**" –

Präambel

(A) Die Parteien haben am Datum: 01.04.2021 einen Vertrag über die Nutzung des Betreiber-Portals für die Applikation „luca" geschlossen, welcher die Erbringung bestimmter Leistungen auf dem Gebiet der verschlüsselten Kontaktdatenübermittlung durch culture4life für den Auftraggeber zum Gegenstand hat. culture4life wird bei der Erfüllung seiner vertraglichen Pflichten unter dem vorgenannten Vertrag und weiterer in diesem Zusammenhang abgeschlossener Verträge (nachstehend insgesamt der „**Hauptvertrag**") voraussichtlich Zugriff auf personenbezogene Daten erhalten und diese nach Weisung des Auftraggebers im Rahmen der vertraglichen Zusammenarbeit verarbeiten.

(B) Zum Zwecke der Einhaltung geltender datenschutzrechtlicher Vorschriften und des Schutzes personenbezogener Daten beabsichtigen der Auftraggeber und culture4life den Abschluss einer Vereinbarung zur Datenverarbeitung im Auftrag.

Dies vorangestellt vereinbaren die Parteien was folgt:

1. Gegenstand dieser Vereinbarung

1.1 Diese Vereinbarung (nachstehend die „**Vereinbarung**") findet Anwendung auf die Verarbeitung personenbezogener Daten, die mit dem Hauptvertrag im Zusammenhang stehen, durch culture4life oder durch von culture4life beauftragte Dritte.

1.2 Gegenstand dieser Vereinbarung ist die Erbringung folgender Datenverarbeitungsleistungen durch culture4life für den Auftraggeber (nachstehend die „**Datenverarbeitung**"):

Erbringung elektronischer Datenverarbeitungsleistungen im Zusammenhang mit der Endnutzer-Applikation „luca" zur sicheren Kontaktnachverfolgung. Weitere Einzelheiten ergeben sich aus dem Hauptvertrag.

1.3 culture4life wird bei der Durchführung der Datenverarbeitung Zugriff voraussichtlich Zugriff auf folgende, näher beschriebene personenbezogene Daten erhalten, davon Kenntnis erlangen bzw. diese verarbeiten:

Art der personenbezogenen Daten	Kategorien betroffener Personen
Personenstammdaten, Kommunikationsdaten (Telefonnummer, E-Mail-Adresse), Daten zur Vertragsbeziehung	Ansprechpartner und Mitarbeiter des Auftraggebers
Personenstammdaten, Kommunikationsdaten (Telefonnummer, Emailadresse, Adresse), Aufenthaltsdaten (Zeitraum des Aufenthalts, Adresse Ihres Aufenthalts, Geo-Koordinaten (nur bei ausdrücklicher Einwilligung Art. 9 (2) a.), Platznummer, Tischnummer), funktionale Daten (Datenzuordnungs-IDs, Schlüsselfragmente, QR-Codes)	Gäste und Besucher des Auftraggebers

Weitere Einzelheiten ergeben sich aus dem Hauptvertrag.

2. Allgemeine Rechte und Pflichten der Parteien

2.1 Die Datenverarbeitung durch culture4life erfolgt im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung geltender Datenschutzvorschriften verantwortlich.

2.2 culture4life darf personenbezogene Daten nur im Rahmen dieser Vereinbarung und der Weisungen des Auftraggebers verarbeiten, es sei denn, culture4life ist durch das Recht der Europäischen Union oder ihrer Mitgliedstaaten zur Verarbeitung dieser Daten verpflichtet. Insbesondere wird culture4life personenbezogene Daten nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit sich eine betroffene Person diesbezüglich unmittelbar an culture4life wendet, wird culture4life ein solches Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2.3 Der Auftraggeber wird culture4life mündliche Weisungen nur in dringenden Fällen erteilen und diese im Anschluss unverzüglich mindestens in Textform bestätigen.

2.4 culture4life wird personenbezogene Daten ausschließlich innerhalb von Mitgliedstaaten der Europäischen Union oder von Vertragsstaaten des Europäischen Wirtschaftsraumes verarbeiten. Eine Verlagerung und Verarbeitung personenbezogener Daten in Drittländer bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. der Datenschutz-Grundverordnung der Europäischen Union (DSGVO) erfüllt sind.

2.5 culture4life wird seine internen Prozesse und datenschutzrechtlichen Sicherheitsmechanismen regelmäßig auf Übereinstimmung mit geltenden Datenschutzvorschriften kontrollieren.

2.6 culture4life hat schriftlich einen Datenschutzbeauftragten bestellt. culture4life wird dem Auftraggeber die Kontaktdaten dieses Datenschutzbeauftragten zum Zwecke der direkten Kontaktaufnahme mitteilen.

2.7 culture4life wird den Auftraggeber im Rahmen seiner Möglichkeiten bei der Einhaltung von dessen Pflichten gegenüber betroffenen Personen aus Art. 12 bis 22 DSGVO sowie dessen Pflichten aus Art. 32 bis 36 DSGVO unterstützen.

2.8 culture4life wird bei der Datenverarbeitung nur Beschäftigte einsetzen, die zur Vertraulichkeit verpflichtet worden sind bzw. einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die culture4life unterstellten Personen, die Zugang zu personenbezogenen Daten haben, welche Gegenstand der Datenverarbeitung sind, dürfen diese Daten ausschließlich nach den Weisungen des Auftraggebers verarbeiten, es sei denn, sie sind gesetzlich zur Verarbeitung dieser Daten verpflichtet.

2.9 Nach Abschluss der Datenverarbeitung und spätestens mit der vollständigen Beendigung des Hauptvertrages wird culture4life, nach Wahl des Auftraggebers, alle personenbezogenen Daten und alle im Zusammenhang mit dieser Vereinbarung in seinen Besitz gelangten Unterlagen, Datenbestände und Kopien, welche personenbezogene Daten beinhalten, an den Auftraggeber zurückgeben oder nach vorheriger schriftlicher Zustimmung des Auftraggebers löschen bzw. vernichten, soweit culture4life nicht gesetzlich zu deren Aufbewahrung verpflichtet ist.

3. Informationspflichten

3.1 culture4life wird den Auftraggeber unverzüglich darüber informieren, falls culture4life der Auffassung ist, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt. culture4life ist berechtigt, die Durchführung einer solchen Weisung solange auszusetzen, bis sie durch den Auftraggeber schriftlich bestätigt oder geändert wird.

3.2 culture4life wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen von Ermittlungs- und Aufsichtsbehörden informieren, soweit diese im Zusammenhang mit der Datenverarbeitung stehen.

3.3 culture4life wird den Auftraggeber unverzüglich darüber informieren, wenn culture4life eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die mit dieser Vereinbarung in Zusammenhang steht.

4. Technische und Organisatorische Maßnahmen

4.1 culture4life wird zum Schutz personenbezogener Daten angemessene technische und organisatorische Maßnahmen treffen, die den Anforderungen der DSGVO genügen, insbesondere Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der für die Datenverarbeitung eingesetzten Systeme und Dienste (jede solcher technischen und organisatorischen Maßnahmen nachstehend einzeln „**TOM**“ und gemeinsam „**TOMs**“).

4.2 Die von culture4life getroffenen TOMs werden in **Anlage 1** näher beschrieben. **Anlage 1** ist wesentlicher Bestandteil dieser Vereinbarung.

4.3 culture4life ist berechtigt, die getroffenen TOMs durch alternative Maßnahmen mit vergleichbarem Schutzniveau zu ersetzen.

5. Unterauftragnehmer

5.1 Die Beauftragung von Dritten mit der Durchführung der Datenverarbeitung durch culture4life (nachstehend „**Unterauftragnehmer**") ist nach vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftraggeber wird seine Zustimmung nicht ohne wichtigen datenschutzrechtlichen Grund verweigern.

5.2 Nicht als Unterauftragnehmer im Sinne dieser Regelung sind solche Dritte zu verstehen, die culture4life im Zusammenhang mit dem Hauptvertrag im Sinne einer Nebenleistung unterstützen und deren Tätigkeit keine Verarbeitung personenbezogener Daten für den Kunden beinhaltet.

5.3 Der Auftraggeber stimmt bereits jetzt der Beauftragung der nachfolgenden Unterauftragnehmer durch culture4life zu:

Firma des Unterauftragnehmers	Geschäftsanschrift	Beschreibung der Leistungen	Ort der Datenverarbeitung
neXenio GmbH	Charlottenstr. 59, 10117 Berlin Deutschland	Wartung und Betrieb	Deutschland
Telekom Deutschland GmbH	Landgrabenweg 151, 53227 Bonn Deutschland	Software-Hosting-Leistungen, SMS-Versandleistungen	Deutschland und Ungarn
Mailjet SAS	13-13 bis, rue de l'Aubrac, 75012 Paris Frankreich	E-Mail-Versand-Leistungen	Frankreich, Deutschland, Belgien, Vereinigtes Königreich
Message Mobile GmbH	Stresemannstraße 6, 21335 Lüneburg Deutschland	SMS-Versandleistungen	Deutschland

5.4 culture4life wird seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung auch den beauftragten Unterauftragnehmern auferlegen.

5.5 Ziffern 5.1 und 5.4 gelten entsprechend für den Austausch von Unterauftragnehmern durch culture4life sowie für die Beauftragung weiterer Unterauftragnehmer durch Unterauftragnehmer.

6. Nachweis der Einhaltung von Pflichten

6.1 culture4life wird dem Auftraggeber oder einem von diesem beauftragten externen Prüfer ermöglichen, sich von der Einhaltung dieser Vereinbarung (einschließlich der gemäß Ziffer 4 zu treffenden technischen und organisatorischen Maßnahmen) durch culture4life zu überzeugen.

6.2 culture4life ist berechtigt, die Einhaltung dieser Vereinbarung durch die Vorlage geeigneter Prüfberichte, Testate und Datenschutz-Zertifikate unabhängiger Stellen, Selbstaudits sowie Berichte über die Einhaltung genehmigter Verhaltensregeln nachzuweisen.

6.3 Sofern dies im Einzelfall für den unter Ziffer 6.1 beschriebenen Zweck notwendig ist, wird culture4life dem Auftraggeber ermöglichen, bei culture4life während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs Inspektionen vorzunehmen. Solche

Inspektionen sind vom Auftraggeber 14 Tage im Voraus schriftlich anzukündigen und dürfen höchstens einmal pro Kalenderjahr und nur durch unabhängige externe Prüfer erfolgen. Den Prüfern ist es dabei nicht gestattet, Zugriff auf Betriebs- und Geschäftsgeheimnisse und vertrauliche Informationen von culture4life sowie auf Daten, die nicht Gegenstand dieser Vereinbarung sind, zu nehmen. culture4life kann dem Einsatz externer Prüfer aus wichtigem Grund widersprechen, insbesondere, wenn und soweit ein Prüfer in einem Wettbewerbsverhältnis zu culture4life steht.

7. Laufzeit und Kündigung

Diese Vereinbarung tritt mit ihrer Unterzeichnung durch beide Parteien in Kraft. Die Regelungen des Hauptvertrages zu dessen Laufzeit und Beendigung gelten für diese Vereinbarung entsprechend. Sofern nicht anderweitig schriftlich vereinbart, endet diese Vereinbarung automatisch mit der vollständigen Beendigung des Hauptvertrages.

8. Haftung

Die Regelungen des Hauptvertrages zur Haftung der Parteien untereinander gelten für diese Vereinbarung entsprechend. Soweit ein Tun oder Unterlassen einer Partei zu einer Haftung sowohl unter dem Hauptvertrag als auch unter dieser Vereinbarung führt, kommt eine etwaige unter dem Hauptvertrag festgelegte Haftungshöchstgrenze zugunsten dieser Partei für dasselbe Tun oder Unterlassen insgesamt nur einmal zur Anwendung. Die Haftung der Parteien gegenüber Dritten gemäß Art. 82 DSGVO bleibt hiervon unberührt.

9. Schlussbestimmungen

9.1 Mündliche oder schriftliche Nebenabreden zu dieser Vereinbarung bestehen nicht.

9.2 Änderungen oder Ergänzungen dieser Vereinbarung bedürfen für ihre Wirksamkeit unter Ausschluss der Regelung des § 127 Abs. 2 BGB der Schriftform i. S. d. § 126 BGB sowie der ausdrücklichen Bezugnahme auf diese Vereinbarung. Das gilt auch für jegliche Vereinbarung, von diesem Formerfordernis abzuweichen oder es aufzuheben.

9.3 Diese Vereinbarung unterliegt ausschließlich deutschem Recht unter Ausschluss von Kollisionsrecht, das zur Anwendung des Rechts eines anderen Staates führt.

9.4 Gerichtsstand für sämtliche Streitigkeiten zwischen den Parteien aus oder im Zusammenhang mit dieser Vereinbarung ist Berlin, Deutschland.

9.5 Sollte eine Regelung dieser Vereinbarung ganz oder teilweise unwirksam oder nichtig sein oder werden, so wird davon die Wirksamkeit der übrigen Regelungen dieser Vereinbarung nicht berührt. An die Stelle der unwirksamen oder nichtigen Regelung tritt in diesem Fall eine Regelung, die dem am nächsten kommt, was die Parteien nach dem Sinn und Zweck der Regelung und dieser Vereinbarung in gesetzlich zulässiger Weise vereinbart hätten, wenn sie die Unwirksamkeit oder Nichtigkeit der ursprünglichen Regelung erkannt hätten. Beruht die Unwirksamkeit oder Nichtigkeit einer Regelung auf einem darin festgelegten Maß der Leistung oder der Zeit (Frist oder Termin), so tritt an deren Stelle eine Regelung mit einem

dem ursprünglichen Maß am nächsten kommenden rechtlich zulässigen Maß. Das Vorstehende gilt auch für eine von den Parteien nicht beabsichtigte etwaige Regelungslücke.

Ort, Datum	Berlin, 01.03.2021
Handewitt, 01.04.2021	
Rasmussen, Bürgermeister	
[Auftraggeber]	**culture4life GmbH**
[Person, Position]	Patrick Hennig, CEO

Anlage 1

Beschreibung der Technischen und Organisatorischen Maßnahmen (TOMs)

Der Auftragnehmer trifft folgende TOMs:

1. Maßnahmen zum Zwecke der Vertraulichkeit

1.1 Zutrittskontrolle

Physische Maßnahmen zur Verhinderung eines Zutritts unbefugter Personen zu Datenverarbeitungsanlagen.

Die Büroräume der culture4life GmbH 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 personalisierten Transponders geöffnet werden. Für Besucher und Postboten gibt es die Möglichkeit, sich über eine Gegensprechanlage mit dem Empfang 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 des Folgetages ist die Verwendung eines personalisierten Transponders notwendig, um die Fahrstühle zu verwenden. 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 ist ein eigenes elektronisches Schließsystem im Einsatz. Die Ausgabe von Transponder folgt auf Basis eines 4-Augen-Prinzips. Die Ausgabe von Transpondern 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 einem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Transpondern und sonstigem Eigentum der culture4life GmbH durch den ausscheidenden Mitarbeiter beinhaltet. Personen, die keine Mitarbeiter der culture4life GmbH sind, haben die Möglichkeit sich an der Tür zu den Räumlichkeiten über ein Klingen anzumelden und vom Empfang persönlich abholen zu lassen. Jeder Zugang einer externen Person wird protokolliert. Jeder Besucher wird in dem gesamten Büro von einem Mitarbeiter begleitet.

Neben den aktiven Aufzügen befinden sich zwei weitere inaktive Aufzugschächte, deren Türen sich direkt in den Räumlichkeiten der der culture4life GmbH liegen. Die Etage der culture4life GmbH ist für diese Aufzüge nicht freigeschaltet und physikalisch verschlossen. Sollte sich eine Person außerhalb der Geschäftszeiten über die deaktivierten Aufzüge unbefugt Zutritt in die Räumlichkeiten 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 Rettungsweg nicht ohne Weiteres von außen geöffnet werden. Bei aktivierter Alarmanlage (außerhalb der Geschäftszeiten) werden die Rettungswege ebenfalls über die Alarmanlage überwacht.

Die Geschäftsräume sind durch eine Alarmanlage gesichert. Versteckte Bewegungsmelder im gesamten Büro registrieren jede Bewegung und lösen sofort einen Alarm aus. 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 und 24 Uhr, die verhindern soll, dass eine Aktivierung der Alarmanlage durch einen Mitarbeiter vergessen wird. Aktivierung und Deaktivierung der Alarmanlage erfolgen durch einen Token, den Mitarbeiter erhalten. Auch hierfür gilt der Transponderausgabe-Prozess. Die Token sind mit einer Nummer versehen, die dem jeweiligen Mitarbeiter intern zugeordnet werden kann. In der Alarmanlage werden Aktivierungen und Deaktivierungen auf Basis der Token-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 es 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, gespeichert und verarbeitet. Die Rechenzentren liegen innerhalb Deutschlands. Dort sind folgende Maßnahmen zur Zutrittskontrolle getroffen:

Das Rechenzentrum und die dort verwendeten Systeme 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. Zutritt zu sensiblen Bereichen wird durch Videoüberwachung überwacht. Ausgebildete Sicherheitskräfte bewachen das Rechenzentrum und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

1.2 Zugangskontrolle

Maßnahmen zur Verhinderung der Nutzung von Datenverarbeitungsanlagen durch unbefugte Personen.

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

An jedem IT-System, das bei der culture4life GmbH 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 Mitarbeiter informieren die Personalverantwortlichen die IT-Administration unverzüglich über anstehende Veränderungen, damit die IT-Administration entsprechende Berechtigungen entziehen kann. Der Entzug von Berechtigungen muss binnen 24 Stunden nach Ausscheiden eines Mitarbeiters durchgeführt worden sein.

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

Es gibt 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. Ein Passwortwechsel ist spätestens nach 90 Tagen zwingend. Sollte sich der Stand der Technik bei der Verwendung von Passwörtern ändern, wird die culture4life GmbH die Passwortrichtlinien entsprechend anpassen.

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 Servern. Übergänge zum Firmennetz, wie E-Mail-Accounts, werden von Antivirus-Software geprüft. Sicherheitsrelevante Softwareupdates werden regelmäßig und automatisiert in die vorhandene Software eingespielt.

Für die Rechenzentren der Bundesdruckerei und der Open Telecom Cloud gilt, dass auch dort alle Berechtigungen nach dem Prinzip der Minimalberechtigung erteilt und Berechtigungen

regelmäßig überprüft werden. Die Vergabe und der 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.

1.3 Zugriffskontrolle

Maßnahmen, die sicherstellen, dass die zur Benutzung einer Datenverarbeitungsanlage befugten Personen nur auf Daten zugreifen können, die ihrer Zugriffsberechtigung unterliegen und dass personenbezogene Daten nicht während der Verarbeitung, Nutzung bzw. nach ihrer Speicherung gelesen, kopiert, verändert oder entfernt werden können.

Für die Erteilung von Benutzerrechten gilt bei der culture4life GmbH 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 Unternehmen erfüllen zu können. Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende 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, der mitarbeitet.

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 culture4life GmbH verfügt über verschiedene Netzwerke. Dazu gehören ein komplett losgelöstes öffentliches Netzwerk, das über einen Zugangsschlüssel gesichert ist und nur Besuchern und Mitarbeitern zur Verfügung steht. Für alle Mitarbeiter, die Zugang zu den Entwicklungssystemen haben gibt es ein gesichertes Netzwerk, auf das man nur mit einem personalisierten Zertifikat Zugriff hat. Die Zertifikate laufen nach einer vorgegebenen Zeit ab und müssen regelmäßig erneuert werden.

Jeder Mitarbeitercomputer wird mit einer Festplattenverschlüsselung betrieben und ist durch personalisierte Benutzerkonten und Passwörter (oder Fingerabdruck) geschützt. Lässt ein Mitarbeiter seinen Computer unbeaufsichtigt ist es zwingend erforderlich ihn zu sperren, um Fremdzugriff zu verhindern. Sollte sich der Computer nicht in den Geschäftsräumen der culture4life GmbH befinden oder wird der Computer unbeaufsichtigt gelassen, werden die IT-Systeme auszuschalten und die Festplattenverschlüsselung aktiviert. Allen Mitarbeitern stehen abschließbare Rollcontainer zur Verfügung.

Zur Entwicklung werden sog. Staging bzw. Testumgebungen genutzt, welche von Entwicklern zur Validierung von neu implementierten Funktionen genutzt werden. Dieses Testumgebungen sind virtuelle via Multitenant-Mechanismen sowohl von Cloud-Anbietern als auch in der physischen Infrastruktur strikt von den Produktivumgebungen getrennt. Lediglich Mitarbeiter mit expliziter Freigabe erhalten Zugriff auf Produktivumgebungen zur Wartung und Fehlerbehebung.

1.4 Trennungskontrolle

Maßnahmen, die sicherstellen, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten getrennt voneinander verarbeitet werden. Es besteht ein Berechtigungskonzept, das den Datenzugriff von Mitarbeitern ausschließt. Mitarbeiter der culture4life GmbH sind schriftlich verpflichtet, Informationen aus Datenbeständen des Auftragsgebers nicht in andere Projekte oder für andere Zwecke mit einzubringen.

2. Maßnahmen zum Zwecke der Integrität

2.1 Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten während einer elektronischen Übertragung, ihres Transports oder ihrer Speicherung auf Datenträger nicht gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Datenübertragungsanlagen vorgesehen ist.

Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten haben, die im Auftrag verarbeitet werden, beschränkt ist. Die Verwendung von externen Datenträgern ist nicht vorgesehen. Zum Übermitteln von Daten muss ausschließlich Bdrive (sichere Ablagelösung der Bundesdruckerei) verwendet werden. Um Daten temporär auf einem externen Datenträger zwischen zu speichern (zum Beispiel beim Erstellen eines Backups beim Wechsel des Arbeitsgerätes) stehen einzelne Datenträger zur Verfügung, die das Büro nicht verlassen dürfen. Vorzugsweise werden externe Datenträger vor der Verwendung verschlüsselt.

Generell wird versucht Ausdrucke auf Papier so gering wie möglich zu halten. Sollten sich Personenbezogene Daten auf Ausdrucken befinden werden diese in abgeschlossenen Aktenschränken in getrennten Büroräumen aufbewahrt. Bei Löschfristen werden die Dokumente mit einem Aktenvernichter vernichtet.

Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch der culture4life GmbH übergeben werden soll, 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 PGP Key erstellen. Alle Mitarbeiter sind dazu angehalten eine verschlüsselte Kommunikation via E-Mail zu verwende sofern möglich. Vertrauliche Dateien dürfen nicht via E-Mail verschickt werden, sondern müssen über das von der neXenio GmbH für die Bundesdruckerei entwickelte 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 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).

Fernzugriffe auf Infrastrukturen und IT-Systeme sind lediglich mit den Unternehmenslaptops gestattet, welche durch den zuständigen IT-Administrator mit nicht exportierbaren Zertifikaten ausgestattet werden. Diese Zertifikate in Kombination mit den Zugangsdaten der Mitarbeiter

können zum Aufbau eines sicheren VPN Tunnels genutzt werden, welcher neben anderen Zugangsdaten Voraussetzung für den Zugriff auf interne Systeme ist.

2.2 Eingabekontrolle

Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder entfernt worden sind.

Jede Eingabe von Daten, die im Auftrag des Auftraggebers von der culture4life GmbH verarbeitet werden, 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 der culture4life GmbH gespeichert. Eine vorherige Löschung kann zwischen den Parteien vereinbart werden.

3. Maßnahmen zum Zwecke von Verfügbarkeit und Belastbarkeit

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörungen bzw. Verlust geschützt werden und nach einem Zwischenfall rasch wiederhergestellt werden können.

Alle Daten, die für den Auftraggeber verarbeitet werden, befinden sich im Rechenzentrum. Die culture4life GmbH 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 vollständige 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.

Die Verfügbarkeit aller relevanten Dienste wird dauerhaft überwacht. Hierbei werden Monitoring-Services (Sicherstellung der Funktionalität), Metric-Services (Überwachung der Infrastruktur) und Log-Monitoring-Services (Überwachung der Applikations- und Server-Logs) genutzt. Ein Fehlverhalten der Dienste wird unmittelbar via Alerting-Funktionen an das culture4life Fast Response Team (nFRT) weitergeleitet.

Über die Betriebsüberwachung hinaus, werden regelmäßig automatisiert die Schwachstellen der verwendeten Applikation geprüft (CVE-Monitoring). Zusätzlich wird manuell die Veröffentlichung von CVEs für verwendete Bibliotheken und Module wöchentlich überprüft. Zur Sicherheit der Applikation selbst werden regelmäßige Lasttests, welche die Belastbarkeit sicherstellen, und

statische Code-Analyse, welche auf Unregelmäßigkeiten in der Programmierung prüfen, durchgeführt.

4. Verfahren zur Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Management

Maßnahmen zur Planung und Organisation der Anforderungen an den Datenschutz.

Die Datenschutzkoordination wird von dem Datenschutzteam verantwortet. Abstimmungen und Klärungen werden mit dem Datenschutzteam im 2-wöchentlichen Rhythmus mit den Produktverantwortlichen und der Geschäftsführung durchgeführt. Die regelmäßigen Datenschutzschulungen werden quartalweise für alle Mitarbeiter angeboten und eine jährliche Teilnahme aller Mitarbeiter wird hierbei sichergestellt. Ebenso sorgt das Datenschutzteam für die Prüfung von Auftragsdatenverarbeitern und deren AVVs und Verträgen, sowie der Einhaltungen der Datenschutzvorgaben.

Das Datenschutzteam ist in allen relevanten Prozessen involviert und sorgt für die Umsetzung der jeweiligen Betroffenenrechte.

4.2 Incident-Response-Management

Maßnahmen zur Reaktion auf erkannte oder vermutete Sicherheitsvorfälle im Bereich von genutzten Datenverarbeitungsanlagen.

Im Falle einer Meldung eines möglichen Sicherheitsvorfalls durch Monitoring-Services, Mitarbeiter oder externe Quellen, wird dieser dem nFRT gemeldet. Der Manager des nFRT-Teams nimmt die Kategorisierung basierend auf den betroffenen Daten und Systeme vor. Je nach Schwergrad des Sicherheitsvorfalls werden die Vorfälle an die Projekt- bzw. Unternehmensverantwortlichen eskaliert. Basierend auf der Analyse des Vorfalls werden die zu informierenden Stellen identifiziert. Hierbei werden min. die betroffenen Kunden, Stakeholder bzw. Nutzer informiert. Bei schweren Vorfällen wird nach Prüfung der Landesdatenschutz in Kenntnis gesetzt.

Zur Wiederherstellung der Daten wird basierend auf dem Backup-Konzept ein Recovery angestoßen. Sollten Systeme nicht automatisch wiederherstellbar sein, kann die Systemlandschaft nach dem Infrastructure-as-Code Prinzip neuaufgebaut und mit Backups bespielt werden.

4.3 Auftragskontrolle

Maßnahmen, die sicherstellen, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend den Weisungen von culture4life verarbeitet werden können.

Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der culture4life GmbH eine hohe Priorität. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.

Es gibt einen betrieblichen Datenschutzbeauftragten, der auch die regelmäßige Schulung der Mitarbeiter plant und durchführt. Alle Mitarbeiter erhalten mindestens eine jährliche Datenschutzschulung bzw. eine „Auffrischung".

Mitarbeiter, die an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, sind im Hinblick auf die Verarbeitung der Daten instruiert. Sofern der Auftraggeber ergänzende Weisungen erteilt, wird die culture4life GmbH alle betroffenen Mitarbeiter unverzüglich über die jeweilige Weisung informieren und Handlungsanweisungen zur Umsetzung geben.

Die Datenschutzvorkehrungen der culture4life GmbH beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Die culture4life GmbH gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten. Mit Unterauftragsnehmern, die Daten des Auftraggebers verarbeiten, bestehen Verträge zur Arbeitsverarbeitung im Sinne der DSGVO.