Anhang 1: Technisch-Organisatorische Maßnahmen

(Version 1.1 - STAND: 10.06.2020)

1 Inhalt

1.1.1 Dokumentation und Konzeption

1001 **Dokumentation**

Es müssen die folgenden Konzepte bereitgestellt werden:

Datenschutzkonzepte für

- Rahmendokument
- CWA Mobile Client
- CWA Backend
- Verifikation und Testergebnisse Backend
- Hotline

Berechtigungskonzepte für Komponenten

- CWA-Server
- Testresult-Server
- Portal Server
- Verification Server
- CDN

Die Erfüllung der Anforderung 1001 wird für diesen Vertrag verpflichtend vereinbart. ☒

1002 **Dokumentation**

Für die Server (CWA Server, Testresult Server, Portal Server, Verification Server und CDN) müssen außerdem

- Betriebskonzepte
- Architekturdokumentation

bereitgestellt werden.

Die Erfüllung der Anforderung 1002 wird für diesen Vertrag verpflichtend vereinbart. ☒

1003 **Dokumentation**

Es muss ein Verzeichnis der Verarbeitungstätigkeiten bereitgestellt werden

Die Erfüllung der Anforderung 1003 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2 Spezielle Technisch-Organisatorische Maßnahmen

1.2.1 Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zur Zuordenbarkeit erforderlichen zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, so dass der Verantwortliche/der Dienstleister keinen Zugriff auf diese Informationen hat.

1.2.1.1 Technische Maßnahmen

1004 **Pseudonymisierung**

Zur Pseudonymisierung müssen die Zuordnungsdaten in getrennten und abgesicherten Systemen aufbewahrt werden, auf welche die pseudonymen Daten verarbeitende Personen keinen Zugriff haben.

Die Erfüllung der Anforderung 1004 wird für diesen Vertrag verpflichtend vereinbart. ☒

1005 **Pseudonymisierung**

Die notwendigen zur Pseudonymisierung aufbewahrten Zuordnungsdaten müssen verschlüsselt abgelegt werden. Personen, die pseudonymen Daten verarbeiten, dürfen keinen Zugriff auf die Schlüssel haben.

Die Erfüllung der Anforderung 1005 wird für diesen Vertrag verpflichtend vereinbart. ☒

1006 **Pseudonymisierung**

Die Pseudonymisierung muss immer im jeweiligen Quellsystem erfolgen.

Die Erfüllung der Anforderung 1006 wird für diesen Vertrag verpflichtend vereinbart. ☒

1007 **Pseudonymisierung**

Der Quellcode der Erzeugungsfunktion muss einsehbar sein.

Die Erfüllung der Anforderung 1007 wird für diesen Vertrag verpflichtend vereinbart. ☒

1008 **Pseudonymisierung**

Eine Prüfung auf Inplausibilitäten und Dopplungen im Vorfeld einer Pseudonymisierung erfolgt grundsätzlich automatisiert.

Die Erfüllung der Anforderung 1008 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.1.2 Organisatorische Maßnahmen

1009 **Pseudonymisierung**

Es werden alle Daten frühestmöglich pseudonymisiert verarbeitet.

Die Erfüllung der Anforderung 1009 wird für diesen Vertrag verpflichtend vereinbart. ☒

1010 **Getrennte Verarbeitung**

Die Server werden von getrennten Teams betrieben, um Re-Identifikationsattacken durch Administratoren zu erschweren. Um sicherzustellen, dass kein Missbrauch der Administrationsrechte stattfindet werden die Logs in regelmäßigen Abständen geprüft und ausgewertet.

Die Erfüllung der Anforderung 1010 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.2 Verschlüsselung

1.2.2.1 Technische Maßnahmen

1011 **Datenminimierung**

Auf den Servern gespeicherte personenbezogene Daten (Pseudonyme) müssen verhasht werden. Gesundheitsdaten (Diagnoseschlüssel und TAN) müssen verschlüsselt gespeichert werden.

Die Erfüllung der Anforderung 1011 wird für diesen Vertrag verpflichtend vereinbart. ☒

1012 **Datenminimierung**

Für den Datenaustausch zwischen der CWA und den Servern und die Speicherung personenbezogener Daten (Pseudonyme) werden dem aktuellen Stand der Technik entsprechende kryptographische Verfahren eingesetzt. Hierfür werden folgende Techniken eingesetzt:

- Standardisierte Verfahren für symmetrische (AES) und asymmetrische (TLS) Verschlüsselung
- Hash-Funktionen der Familie Secure Hash Algorithm (SHA)
- Verschlüsselte Speicherung von gehashten Werten oder Public Domain Information (TEKs)

- Pseudonymisierung durch Hashing der Parameter für Datenbank Abfragen

Die Erfüllung der Anforderung 1012 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.2.2 Organisatorische Maßnahmen

1013 **Datenminimierung**

Bei dem Einsatz von Verschlüsselung wird sichergestellt, dass

- die Erzeugung des Schlüssels bzw. Schlüsselmaterials ein sicherer Prozess ist
- Salt (soweit eingesetzt) und/oder der Schlüssel bzw. das Schlüsselmaterial derart erzeugt werden, dass diese weder vorhersagbar sind noch erraten werden können
- der Erzeugung des Schlüssels bzw. Schlüsselmaterials eine qualitativ hochwertige Zufallszahlenquelle zugrunde liegt
- die Vertraulichkeit des Schlüssels bzw. des Schlüsselmaterials während des vollständigen Lebenszyklus der verarbeiteten personenbezogenen Daten gewährleistet ist
- der Zugriff auf den Salt und/oder den Schlüssel bzw. das Schlüsselmaterial auf ein absolutes Minimum vertrauenswürdiger Anwender beschränkt ist und geheim gehalten wird

Es liegt ein Konzept zum Schlüsselmanagement vor und dieses enthält Informationen sowohl zum Schlüsseltausch als auch zur Feststellung von Vorgehensweisen bei Kompromittierung.

Die Erfüllung der Anforderung 1013 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.3 Datenminimierung

1.2.3.1 Technische Maßnahmen

1014 **Datenminimierung**

Es werden nur die für die Erreichung des Zwecks der CWA erforderlichen Daten verarbeitet. Es werden nur die Diagnoseschlüssel der letzten 2 Wochen auf das CWA Backend geladen.

Die Erfüllung der Anforderung 1014 wird für diesen Vertrag verpflichtend vereinbart. ☒

1015 **Datenminimierung**

Die Server müssen mit großer Sorgfalt konfiguriert werden, so dass keine unnötigen Daten erhoben werden (es werden keine Kennungen in die Serverprotokolle aufgenommen). Anfragen der CWA an

die Server geben keine unnötigen Informationen über den Benutzer preis. Es werden keine Standortdaten verarbeitet, auch nicht, um die Interoperabilität mit Mitgliedsstaaten zu ermöglichen.

Die Erfüllung der Anforderung 1015 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.3.2 Organisatorische Maßnahmen

1.2.4 Vertraulichkeit

1.2.4.1 Zutrittskontrolle

Mit dem Begriff „Zutritt" ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT- Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netzverkabelungen befinden und verlegt sind, gehören hierzu. Die Datenverarbeitung erfolgt in Rechenzentren der OpenTelekomCloud (OTC).

1.2.4.1.1 Technische Maßnahmen

1016 **Festlegung von Sicherheitsbereichen**

Der Schutzbedarf eines Gebäudes bzw. Raumes ist festzustellen anhand der darin befindlichen DV-Anlagen sowie ggf. sonstiger Unterlagen auf denen personenbezogene Daten verarbeitet bzw. gespeichert werden.

Die Erfüllung der Anforderung 1016 wird für diesen Vertrag verpflichtend vereinbart. ☒

1017 **Realisierung eines wirksamen Zutrittsschutzes**

Sicherheitsbereiche sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete technische (z.B. Spezialverglasung, Einbruchmeldesystem, Drehkreuz mit Chipkarte, Vereinzelungsanlage, Schließanlage) Maßnahmen abgesichert werden.

Es erfolgen folgende Zutrittskontrolle für den Zutritt zu den Servern:

- Sicherheitstür(en)
- Transponderkarte
- Schlüssel / Manuelles Schließsystem
- Schließsystem mit Codesperre
- Einbruchmeldeanlage
- Brandmeldeanlage
- Videoüberwachung
- Elektronische Signatur

Der Zutritt zum Rechenzentrum ist wie folgt gesichert:

- Alarmanlagen
- Vergitterte Fenster/Sicherheitsfenster, -schlösser, -türen mit einer definierten Widerstandsklasse
- Bewegungsmelder
- Durchbrechschutz gegen Fahrzeuge

Zudem befinden sich die Server in abschließbaren Serverschränken. Gelagerte Notebooks befinden sich unter Verschluss in gesicherten Räumen. Die Aufbewahrung von Datensicherungen (z. B. Bänder, CDs) erfolgt in zutrittsgeschützten Safes oder Räumen.

Die Erfüllung der Anforderung 1017 wird für diesen Vertrag verpflichtend vereinbart. ☒

1018 Festlegung zutrittsberechtigter Personen

Die Voraussetzungen sowie der Kreis der allgemein zutrittsberechtigten Personen müssen festgelegt und die Zutrittsberechtigungen zu sicherheitsrelevanten Bereichen, auf das notwendige Minimum beschränkt werden ("Prinzip der minimalen Berechtigung"). Der Zutritt ist bei fehlender Berechtigung zu verwehren. Zutrittsmittel zu Gebäuden bzw. Räumlichkeiten sind grundsätzlich personengebunden zu vergeben und dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür zu sensibilisieren.

Die Erfüllung der Anforderung 1018 wird für diesen Vertrag verpflichtend vereinbart. ☒

1019 Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus

Ein Prozess zur Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. zum Entzug von Zutrittsrechten (einschl. Schlüssel-, Sichtausweise, Transponder, Chipkartenverwaltung etc.) ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Sperren von Zutrittsberechtigungen sind zu beschreiben. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zutrittsmittel und -rechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr erforderlichen Räumlichkeiten unverzüglich zu entziehen. Sämtliche mit Sicherheitsaufgaben betraute Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.

Die Erfüllung der Anforderung 1019 wird für diesen Vertrag verpflichtend vereinbart. ☒

1020 Begleitung von Besuchern und Fremdpersonal

Es existieren schriftlich fixierte Regelungen zum Zutritt für Firmenfremde, wie Gäste oder Lieferanten. Diese Regelungen beinhalten minimal die Anforderung, dass Firmenfremde Ihren berechtigten Aufenthalt innerhalb der Gebäude jederzeit nachweisen können, z.B. mittels Gästeausweis, Besucherausweis, oder Lieferantenausweis. Namen und Herkunft (Firmenzugehörigkeit, Geschäftsadresse oder Privatadresse) der Personen sind zu protokollieren. Die stichprobenartige Prüfung des berechtigten Aufenthaltes innerhalb der Gebäude ist obligatorisch. Besteht ein erhöhter Schutzbedarf, sind nicht autorisierte Personen zu begleiten bzw. während ihrer Tätigkeit zu beaufsichtigen.

Die Erfüllung der Anforderung 1020 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.1.2 Organisatorische Maßnahmen

1021 **Realisierung eines wirksamen Zutrittsschutzes**

Sicherheitsbereiche sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete organisatorische (z.B. Pförtner) Maßnahmen abgesichert werden. Hierzu existiert ein Zutrittskontrollsystem, in welchem die zutrittsberechtigten Mitarbeiter festgelegt sind. Es bestehen Regelungen für den Zutritt von Fremdpersonal, Reinigungspersonal und Besucher. Die Begleitung von Gästen im Gebäude ist in einer Richtlinie geregelt. Differenzierte Sicherheitsbereiche/-zonen (z. B. für Server, Großrechner, Archiv) sind festgelegt. Auch die Datenträger sind Bestandteil des Zutrittsschutzkonzepts und es liegt eine Anweisung zur Ausgabe von Schlüsseln vor. Es erfolgen folgende Zutrittskontrolle für den Zutritt zum Betriebsgelände/Gebäude:

- Empfang/Rezeption/Pförtner
- Besucherbuch/Protokoll der Besucher
- Verschließen von Türen und Fenstern, sobald Personal nicht im Raum
- Mitarbeiterausweise
- Besucherausweise
- Werkschutz/Wachpersonal

Die Erfüllung der Anforderung 1021 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.2 Zugangskontrolle

Maßnahmen zur Zugangskontrolle dienen der Verhinderung der unbefugten Nutzung von Anlagen/Systemen, mit welchen (personenbezogene) Daten verarbeitet werden. Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV- Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden.

1.2.4.2.1 Technische Maßnahmen

1022 **Zugangsschutz (Authentifizierung)**

Der Zugang zu DV-Anlagen, auf denen Daten verarbeitet werden, darf erst nach Identifikation und erfolgreicher Authentifizierung (z.B. durch Benutzername und Passwort oder Chipkarte/ PIN) der befugten Personen durch dem Stand der Technik entsprechende Sicherheitsmaßnahmen möglich sein. Der Zugang ist bei fehlender Berechtigung entsprechend zu verwehren.

Die Erfüllung der Anforderung 1022 wird für diesen Vertrag verpflichtend vereinbart. ☒

1023 Starke Authentisierung bei hohem bis höchstem Schutzniveau

Eine starke Authentisierung erfolgt immer auf Basis mehrerer (mindestens zweier) Merkmale wie z.B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer eigenen Eigenschaft. Dies sind beispielsweise:

- Chipkarte mit Zertifikaten und PIN
- OneTimePassworte (OTP Generator, SMS TAN, ChipTAN) und Nutzerpasswort

Im Rahmen der Zwei-Faktor-Authentifizierung werden als die zwei Faktoren verwandt:

- Hardware Token (Smart Card)
- PKI / zertifikatsbasierte Anmeldung
- Geräte-Identifikation
- Virtuelle Smartcards

Die Erfüllung der Anforderung 1023 wird für diesen Vertrag verpflichtend vereinbart. ☒

1024 Nutzung der Datenübertragung durch Dritte

Die Nutzung von IT-Systemen mithilfe von Einrichtungen der Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert oder zumindest nachvollziehbar gemacht:

- Standleitung
- Teilnehmerkennung
- Ausweisleser
- Protokollierung der Systemnutzung und Protokollauswertung
- Sonstige: gleiche Sicherungen wie bei Zwei-Faktor-Authentifizierung

Die Erfüllung der Anforderung 1024 wird für diesen Vertrag verpflichtend vereinbart. ☒

1025 Protokollierung des Zugangs

Über alle Aktivitäten in den IT-Systemen werden automatisch Protokolle erstellt. Alle erfolgreichen und abgewiesenen Zugangsversuche müssen protokolliert (verwendete Kennung, Rechner, IP-Adresse) und für mindestens 30 Tage revisionssicher archiviert werden. Zur Missbrauchserkennung sind regelmäßig stichprobenartige Auswertungen vorzunehmen.

Die Erfüllung der Anforderung 1025 wird für diesen Vertrag verpflichtend vereinbart. ☒

1026 Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk

Das Authentisierungsgeheimnis (z.B. Benutzerkennung und Passwort) darf nie ungeschützt über das Netzwerk übertragen werden.

Die Erfüllung der Anforderung 1026 wird für diesen Vertrag verpflichtend vereinbart. ☒

1027 **Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen**

Nach wiederholter fehlerhafter Authentisierung muss der Zugang gesperrt werden. Ein Prozess zur Rücksetzung bzw. Entsperrung von gesperrten Zugangskennungen ist einzurichten, zu beschreiben und anzuwenden. Benutzerkennungen, welche über einen längeren Zeitraum nicht genutzt werden, müssen automatisch gesperrt bzw. auf inaktiv gesetzt werden.

Die Erfüllung der Anforderung 1027 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.2.2 Organisatorische Maßnahmen

1028 **Einfache Authentisierung (per Benutzername/Passwort) bei niedrigem bis mittlerem Schutzniveau**

Es gibt eine Richtlinie zur Vergabe und Nutzung von Passwörtern. Jeder Berechtigte verfügt über ein eigenes nur ihm bekanntes Passwort. Passworte müssen angemessenen Mindestregeln entsprechen wie z.B. einer minimalen Passwortlänge und Komplexität. Passworte müssen in regelmäßigen Abständen geändert werden. Erstpassworte müssen umgehend geändert werden. Die Umsetzung der Anforderungen an Passwortlänge, Passwortkomplexität und Gültigkeit ist soweit möglich durch technische Einstellungen sicherzustellen.

- Ein Passwort besteht aus mindestens 8 Zeichen.
- Das Passwort setzt sich aus einem Zeichenmix zusammen. Die verfügbaren Zeichen werden in vier Kategorien unterteilt:
  - Kleine Buchstaben z.B. abcdefgh...
  - Große Buchstaben z.B. ABCDEFGH...
  - Ziffern z.B. 123456...
  - Sonderzeichen z.B. !“§$%...
  - Der Zeichenmix muss aus mindestens drei der oben genannten Kategorien bestehen.
- Für das Passwort dürfen keine leicht zu erratenden Begriffe und keine Trivialpasswörter verwendet werden.
- Ein Passwort ist in regelmäßigen Abständen, mindestens jedoch jährlich zu ändern
- Bei Änderung darf nicht eines der letzten 4 verwendeten Passworte wieder verwendet werden
- Das Passwort darf bei der Eingabe nicht im Klartext auf dem Bildschirm sichtbar wird.
- Das Erstpasswort muss auf sicherem Wege zum Nutzer kommen und/oder dieser mindestens sofort nach erstmaliger Anmeldung aufgefordert werden, dieses zu ändern

Passwörter werden ausschließlich verschlüsselt gespeichert.

Die Erfüllung der Anforderung 1028 wird für diesen Vertrag verpflichtend vereinbart. ☒

1029 **Festlegung befugter Personen**

Für die Server existiert eine Benutzerverwaltung, in welcher Benutzern Authentifizierungsmöglichkeiten zugewiesen werden. Der Kreis der Personen, die befugt Zugang zu

DV-Anlagen auf oder mit denen Daten verarbeitet und/oder gespeichert werden (können), ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum zu beschränken. Zugänge für temporär beschäftigte Personen (Berater, Praktikanten, Auszubildende) müssen individuell vergeben werden. Wieder verwendbare Kennungen (z.B. Berater1, Praktikant1, etc.) dürfen nicht vergeben werden.

Die Erfüllung der Anforderung 1029 wird für diesen Vertrag verpflichtend vereinbart. ☒

1030 Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen ist einzurichten, zu beschreiben und zwingend anzuwenden. Dieser beinhaltet mindestens einen Beantragungs- und Genehmigungsprozess sowie den Prozess zur Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen.

Die Vergabe von Zugangsberechtigungen darf immer nur für diejenigen DV- Anlagen(-typen) erfolgen, zu welchen der Zugang im Rahmen der Aufgabenwahrnehmung notwendig ist ("Prinzip der minimalen Berechtigung"). Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu DV-Anlagen sind grundsätzlich personengebunden zu vergeben und an ein persönliches Credential (z.B. Passwort, Token, Chipkarte) zu knüpfen (Benutzerkennung). Authentifizierungsmedien und/oder Benutzerkennung/Passwort-Kombination dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür zu sensibilisieren.

Regelungen und Verfahren zum Sperren und datenschutzgerechten Löschen von Zugangskennungen müssen beschrieben werden. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Authentifizierungsmedien und Zugangsberechtigungen zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV-Anlagen, unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration).

Die Erfüllung der Anforderung 1030 wird für diesen Vertrag verpflichtend vereinbart. ☒

1031 Persönliche Zuordnung von Authentifizierungsmedien und Zugangskennungen

Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu Anlagen und Systemen des Auftraggebers sind grundsätzlich personengebunden und an ein persönliches Passwort geknüpft (Benutzerkennung). Authentifizierungsmedien und/oder Zugangskennung/Passwort-Kombination dürfen nicht an Dritte weitergegeben werden.

Die Erfüllung der Anforderung 1031 wird für diesen Vertrag verpflichtend vereinbart. ☒

1032 Verhaltensweise

Der Mitarbeiter oder Erfüllungsgehilfe des Auftragnehmers/Dienstleisters ist verpflichtet, die Regelungen und Vorgaben der technischen und organisatorischen Zugangskontrolle zu befolgen und stellt zudem sicher, dass nicht durch falsches Verhalten Unberechtigten der Zugang zu DV-Anlagen des Auftraggebers ermöglicht wird.

Die Erfüllung der Anforderung 1032 wird für diesen Vertrag verpflichtend vereinbart. ☒

1033 **Sicherheitsmanagement**

Neue Schwachstellen in den IT-Systemen werden nach Bekanntwerden gemeldet, analysiert und ggf. behoben, um das Eindringen seitens unbefugter Dritter in die IT-Systeme zu verhindern. Es gibt definierte und erprobte/wirksame Verfahren im Fall eines (erfolgten) externen Angriffs auf relevante Daten und Systeme im Rahmen der OTC. Für die CWA existiert ein Life-Cyclemanagement. IT-Systeme werden auf die Wirksamkeit (Effektivität) eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter mindestens jährlich durch Penetrationstests getestet.

Die Erfüllung der Anforderung 1033 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.3 Zugriffskontrolle

Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können.

1.2.4.3.1 Technische Maßnahmen

1034 **Zugriffskontrolle technische Maßnahmen**

Zur Sicherstellung der Zugriffskontrolle werden eine oder mehrere der folgenden technischen Maßnahmen ergriffen:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
  - Type Enforcement (TE)
  - Multi-Level Security (MLS)
- Role Based Access Control (RBAC)
- Attribute-based access control (ABAC)
- Context-Based Access Control (CBAC)
- Media Access Control

Zudem liegt eine eindeutige Zuordnung zwischen jedem Datenträger (Laufwerk etc.) und Berechtigten vor (insb. bei Gruppenlaufwerken).

Die Erfüllung der Anforderung 1034 wird für diesen Vertrag verpflichtend vereinbart. ☒

1035 **Protokollierung und Auswertung der Programm- und Dateibenutzung**

Die Programm- und Dateibenutzung wird protokolliert und stichprobenartig ausgewertet. Für den Fall, dass sog. „Superuser“ Accounts eingesetzt werden, erfolgt ein Monitoring sowie eine regelmäßige Kontrolle von Aktivitäten, die mithilfe dieser Benutzerkonten durchgeführt werden.

Die Erfüllung der Anforderung 1035 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.3.2 Organisatorische Maßnahmen

1036 **Erstellen eines Berechtigungskonzepts**

Ein Berechtigungskonzept (Benutzer- und Administrationsberechtigungen) gewährleistet, dass der Zugriff auf Daten des Systems nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung gemäß interner Aufgabenverteilung und Funktionstrennung des Benutzers erforderlich ist. Es wird verbindlich geregelt, wie Berechtigungen beantragt, freigegeben, umgesetzt und wieder entzogen werden. Dazu werden die folgenden Maßnahmen ergriffen:

- Für jedes eingesetzte (Datenbank-)system sind im Berechtigungssystem die Rechte an Datenbanktransaktionen festgehalten.
- Im Rahmen dieses Berechtigungsmanagements ist manipulationssicher nachweisbar, wer wann welche Berechtigungen innehatte.
- Es bestehen differenzierte Berechtigungen (z. B. für Lesen, Löschen, Ändern).
- Es bestehen differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem.
- Es besteht eine funktionelle/personelle Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (techn.).
- Es existiert eine Benutzerverwaltung, über die Berechtigungen verwaltet werden.
- Es liegt ein Konzept der Laufwerksnutzung und -zuordnung vor.
- Die Wiederherstellung von Daten aus Backups ist in einem verbindlichen Verfahren geregelt (wer darf wann auf wessen Anforderung Backup-Daten einspielen?).

Die Erfüllung der Anforderung 1036 wird für diesen Vertrag verpflichtend vereinbart. ☒

1037 **Umsetzung von Zugriffsbeschränkungen**

Mit jeder Zugangsberechtigung muss eine Zugriffsberechtigung verknüpft sein, beispielsweise durch die Verknüpfung mit einer oder mehrere im Berechtigungskonzept definierten Rollen. Jeder Zugangsberechtigte darf nur mit den Anwendungen und innerhalb dieser Anwendungen nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind.

Soweit Datenbestände mehrerer Auftraggeber in einer Datenbank gespeichert oder mit einer Datenverarbeitungsanlage verarbeitet werden, sind logische Zugriffseinschränkungen vorzusehen, die ausschließlich auf die Datenverarbeitung für den jeweiligen Auftraggeber ausgerichtet sind (Mandantenfähigkeit). Zudem ist die Datenverarbeitung selbst soweit einzuschränken, dass ausschließlich die minimal erforderlichen Funktionen für die Verarbeitung der personenbezogenen Daten verwendet werden können.

Es werden in den Datenverarbeitungsanlagen eindeutige Merkmale eingebaut, die es der zugreifenden Person ermöglicht, zu erkennen, dass es sich um eine authentische Datenverarbeitungsanlage handelt. Zudem muss sich auch der Zugriffsberechtigte gegenüber der Datenverarbeitungsanlage anhand von

nachprüfbaren eindeutigen Merkmalen identifizieren und authentisieren lassen, z.B. mittels Ausweislesern an den Terminals.

Die Erfüllung der Anforderung 1037 wird für diesen Vertrag verpflichtend vereinbart. ☒

1038 Vergabe minimaler Berechtigungen

Der Umfang der Berechtigungen, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum zu beschränken. Soweit bestimmte Funktionen ohne Verlust der Qualität der Datenverarbeitung zeitlich beschränkbar sind, sind Zugriffe auf die personenbezogenen Daten und Berechtigungen zeitlich zu begrenzen.

Die Erfüllung der Anforderung 1038 wird für diesen Vertrag verpflichtend vereinbart. ☒

1039 Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen und deren Prüfung ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Erteilen/Entziehen von Berechtigungen bzw. der Zuweisung von Benutzerrollen sind zu beschreiben. Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account zu knüpfen. Dies schließt den Einsatz von mehreren Personen genutzten Gruppenkennungen/-passwörtern aus.

Bei der Vergabe der Berechtigungen bzw. Zuweisung von Benutzerrollen dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-know-Prinzip"). Dabei ist sicherzustellen, dass die im System abgebildete Funktionstrennung nicht durch kumulierte Berechtigungen aufgehoben wird.

Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zugriffsrechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV- Anlagen und Speicherbereichen unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration). Die Dokumentationen sind 3 Monate aufzubewahren.

Die Erfüllung der Anforderung 1039 wird für diesen Vertrag verpflichtend vereinbart. ☒

1040 Trennung zwischen Test- und Produktionsumgebung

Es erfolgt bei einer evtl. Programmentwicklung eine Funktionstrennung zwischen Test- und Produktionsumgebung.

Die Erfüllung der Anforderung 1040 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.4 Weitergabekontrolle

Hierbei handelt es sich um Maßnahmen, die verhindern, dass Daten unbefugt weitergegeben werden. Insbesondere soll verhindert werden, dass Daten bei einer elektronischen Übertragung bzw. Transport nicht unbefugt verarbeitet werden können.

1.2.4.4.1 Technische Maßnahmen

1041 **Legitimationsprüfung**

Es erfolgt eine Legitimationsprüfung der Berechtigten.

Die Erfüllung der Anforderung 1041 wird für diesen Vertrag verpflichtend vereinbart. ☒

1042 **Versendungsarten**

Folgende Versendungsarten stehen für die Versendung personenbezogener Daten zur Verfügung:

- Datenverschlüsselung
- SSH
- VPN (Verschlüsselung)
- Sicheres Web-Formular / -Portal
- Gesicherte/Verschlüsselte Datenleitung

Die Erfüllung der Anforderung 1042 wird für diesen Vertrag verpflichtend vereinbart. ☒

1043 **Ausschluss Datenträgertransport**

Der Datenträgertransport ist ausgeschlossen.

Die Erfüllung der Anforderung 1043 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.4.2 Organisatorische Maßnahmen

1044 **Festlegung empfangs-/weitergabeberechtigter Instanzen/Personen**

Es ist gemeinsam mit dem Auftraggeber festzulegen welche Stellen/Personen an wen, welche Daten übermitteln dürfen und auf welchem Übertragungsweg dies geschehen soll.

Die Erfüllung der Anforderung 1044 wird für diesen Vertrag verpflichtend vereinbart. ☒

1045 **Rechtmäßigkeit der Weitergabe ins Ausland**

Die Erhebung, bzw. die Verarbeitung von Daten im Ausland ist grundsätzlich nur mit vorheriger Genehmigung des Auftraggebers möglich.

Die Erfüllung der Anforderung 1045 wird für diesen Vertrag verpflichtend vereinbart. ☒

1046 Übertragung zu externen Systemen

Werden personenbezogene Daten zu externen Systemen übertragen, ist eine Verschlüsselung zwingend erforderlich.

Die Erfüllung der Anforderung 1046 wird für diesen Vertrag verpflichtend vereinbart. ☒

1047 Implementation von Sicherheitsgateways an den Netzübergabepunkten

Die IT-/NT-Systeme, auf denen personenbezogene Daten verarbeitet werden, sind durch dem aktuellen Stand der Technik entsprechende Maßnahmen (i.d.R. Firewalls) vor unerwünschten Zugriffen oder Datenströme sowohl aus dem eigenen wie auch aus anderen Netzen zu schützen. Unabhängig davon, ob es sich um Netzwerk-/Hardware-Firewalls oder ergänzend dazu um hostbasierte Firewalls handelt, müssen diese dauerhaft aktiviert sein. Jedwede Deaktivierung oder Umgehung der Funktionen durch den Anwender muss dabei wirksam ausgeschlossen werden. Das Regelwerk muss so aufgesetzt werden, dass alle Kommunikationsbeziehungen außer den notwendigen automatisch geblockt werden.

Die Erfüllung der Anforderung 1047 wird für diesen Vertrag verpflichtend vereinbart. ☒

1048 Härtung der Backendsysteme

Die Backendsysteme müssen nach dem Stand der Technik gehärtet werden, damit sich ein Angreifer nicht aufgrund von Schwachstellen unbefugt Zugriff auf die Systeme und Daten verschaffen kann.

Die Erfüllung der Anforderung 1048 wird für diesen Vertrag verpflichtend vereinbart. ☒

1049 Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder

Alle Schnittstellen zu anderen IV-Verfahren sind zu dokumentieren. Diese Dokumentation muss mindestens die folgenden Informationen beinhalten:

- alle personenbezogenen Datenfelder
- Richtung der Übermittlung (Import/ Export)
- der jeweilige Verwendungszweck für die Übermittlung
- das IV-Verfahren/ die Schnittstelle, an das die Daten exportiert werden
- Art der Authentisierung der Schnittstelle
- Schutz der Übertragung (z.B. Verschlüsselung)

Insbesondere sind auch Import- und Exportschnittstellen aus bzw. in Dateien zu beschreiben, und wie deren Verwendung technisch oder organisatorisch geschützt wird. Auch Datenmigrationen sind entsprechend als Schnittstelle zu beschreiben.

Die Erfüllung der Anforderung 1049 wird für diesen Vertrag verpflichtend vereinbart. ☒

1050 Gesicherte Speicherung auf mobilen Datenträgern

Die Speicherung auf mobilen Datenträgern ist aufgrund des hohen Verlustrisikos zu vermeiden. Sollte eine Speicherung dennoch unumgänglich sein, so ist die Nutzung zu regeln und die Verschlüsselung der Daten auf dem Medium muss technisch sichergestellt sein. Nicht mehr benötigte Daten sind umgehend datenschutzgerecht zu löschen.

Die verwendete Hardware ist zudem gegen Verlust/Diebstahl zu schützen.

Die Erfüllung der Anforderung 1050 wird für diesen Vertrag verpflichtend vereinbart. ☒

1051 Einführung eines Prozesses zur Datenträgerverwaltungen

Es muss eine qualifizierte Datenträgerverwaltung existieren. Die Verwaltung der Datenträger muss dokumentieren, wie viele Datenträger mit personenbezogenen Daten für welche Aufgaben und Verarbeitungen erstellt wurden und wo diese bis zur Vernichtung gelagert werden. Über den Bestand der Datenträger ist regelmäßig eine Bestandskontrolle durchzuführen. Eine Lagerung der erstellten Datenträger in einem kontrollierten Sicherheitsbereich ist bei personenbezogenen Daten obligatorisch. Darüber hinaus wird die Anfertigung von Kopien von Datenträgern dokumentiert und für einen Zeitraum von 3 Monaten ab Beendigung des Auftrages oder der Tätigkeit aufbewahrt.

Die Erfüllung der Anforderung 1051 wird für diesen Vertrag verpflichtend vereinbart. ☒

1052 Prozess zur Sammlung und Entsorgung

Ein Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern und Informationsträgern in Papierform ist einzurichten und zu beschreiben. Dabei werden Regelungen und Verfahren zur sicheren Sammlung und internen Weitergabe sowie zu Lagerung, Transport und Vernichtung unter Berücksichtigung medientypischer Eigenarten in einer Organisationsrichtlinie/Verfahrensanweisung beschrieben. Das datenschutzgerechte Vernichten bzw. Löschen ist arbeitsplatz- und zeitnah durchzuführen, um ein Zwischenlagern der Datenträger weitgehend zu vermeiden. Dadurch wird auch der Personenkreis, der mit den Datenträgern umgeht, eingeschränkt und die Sicherheit erhöht. Alternative Entsorgungswege sind organisatorisch auszuschließen. Die Mitarbeiter sind hierfür regelmäßig zu sensibilisieren.

Die Erfüllung der Anforderung 1052 wird für diesen Vertrag verpflichtend vereinbart. ☒

1053 Einführung datenschutzgerechter Lösch- und Zerstörungsverfahren

Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor deren internen Wiederverwendung (z.B. Wechsel des Hauptnutzers) oder Weitergabe an externe Stellen datenschutzgerecht gelöscht werden. Die Formatierung ist als sicheres Löschverfahren ungeeignet. Es müssen andere sichere Lösch-/ Zerstörungsverfahren gewählt werden, die eine Rekonstruktion der Daten nur mit hohem Aufwand erlauben.

Die Erfüllung der Anforderung 1053 wird für diesen Vertrag verpflichtend vereinbart. ☒

1054 Führung von Löschprotokollen

Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit personenbezogenen Daten ist zu protokollieren. Die Protokolle sind mindestens 12 Monate revisionssicher zu archivieren.

Die Erfüllung der Anforderung 1054 wird für diesen Vertrag verpflichtend vereinbart. ☒

1055 **Weitergabe von Datenträgern**

Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor der Weitergabe an externe Stellen stets datenschutzgerecht gelöscht werden.

Die Erfüllung der Anforderung 1055 wird für diesen Vertrag verpflichtend vereinbart. ☒

1056 **Verbot der Vervielfältigung**

Jegliche Art der Vervielfältigung (elektronisch und/oder analog) von Daten, Datenträgern oder Unterlagen des Auftraggebers ist unzulässig, sofern dies nicht explizit Bestandteil der Auftragsausführung ist. In diesem Fall dürfen Kopien ausschließlich für die vom Auftraggeber festgelegten Zwecke sowie in dem hierfür erforderlichen Umfang angefertigt werden. Als Vervielfältigen gilt auch der elektronische Versand z.B. via E-Mail.

Die Erfüllung der Anforderung 1056 wird für diesen Vertrag verpflichtend vereinbart. ☒

1057 **Wechseldatenträger**

Sowohl das Einbinden externer (Wechsel-)datenträger (USB, Speicherkarten, CD/DVD etc.) in DV-Anlagen des Auftraggebers als auch das Kopieren von Daten des Auftraggebers auf externe (Wechsel-)datenträger ist untersagt, sofern dies nicht explizit Bestandteil der Auftragsausführung ist und durch den Leiter der zuständigen Stelle des Auftraggebers genehmigt wurde.

Die Erfüllung der Anforderung 1057 wird für diesen Vertrag verpflichtend vereinbart. ☒

1058 **Festlegung empfangs-/weitergabeberechtigter Instanzen/Personen**

Die Server verbinden sich nicht mit Profilen sozialer Medien.

Die Erfüllung der Anforderung 1058 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.5 Trennungskontrolle

Hierbei handelt es sich um Maßnahmen, welche gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische oder physikalische Trennung der Daten erreicht werden.

1.2.4.5.1 Technische Maßnahmen

1059 **Sparsamkeit bei der Datenerhebung**

Es dürfen nur solche Daten erhoben, gespeichert oder verarbeitet werden, die unmittelbar dem eigentlichen Zweck dienen, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses zwingend notwendig sind. Dieser Zweck darf sich in keinem nachgelagerten Schritt der Verarbeitung, auch nicht nach einer Übermittlung ändern.

Die Erfüllung der Anforderung 1059 wird für diesen Vertrag verpflichtend vereinbart. ☒

1060 **Getrennte Verarbeitung**

Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit unterschiedlichen Vertragszwecken sind zu dokumentieren und anzuwenden.

Die Erfüllung der Anforderung 1060 wird für diesen Vertrag verpflichtend vereinbart. ☒

1061 **Getrennte Verarbeitung**

Die Testergebnisse werden nicht auf dem Verification Server, sondern nur auf dem Testresult Server gespeichert. Die Daten werden auf dem Verification Server, Testresult Server und Portal Server getrennt voneinander verarbeitet.

Die Erfüllung der Anforderung 1061 wird für diesen Vertrag verpflichtend vereinbart. ☒

1062 **Getrennte Verarbeitung**

OTC Infrastruktur sowie der Verification Server, Testresult Server und der CWA-Server, sowie die zugeordneten Datenbankinstanzen werden von unterschiedlichen Betriebsteams und in verschiedenen Cloud Subscriptions betrieben.

Die Erfüllung der Anforderung 1062 wird für diesen Vertrag verpflichtend vereinbart. ☒

1063 **Getrennte Verarbeitung**

Es existiert eine Trennung zwischen Test- und Produktivdaten.

Die Erfüllung der Anforderung 1063 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.4.5.2 Organisatorische Maßnahmen

1064 **Getrennte Verarbeitung**

Die Daten verschiedener Mandanten werden von unterschiedlichen Mitarbeitern beim Auftragnehmer verarbeitet, so dass die Gefahr der Weitergabe von personenbezogenen Daten unterbunden wird.

Die Erfüllung der Anforderung 1064 wird für diesen Vertrag verpflichtend vereinbart. ☒

1065 **Getrennte Verarbeitung**

Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung der Daten anderer Mandanten Rechnung trägt.

Die Erfüllung der Anforderung 1065 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.5 Integrität

1.2.5.1 Eingabekontrolle

Diese Maßnahmen sollen dafür sorgen, dass man nachträglich feststellen kann, ob und wenn ja von wem personenbezogene Daten in informationstechnischen Systemen eingegeben, verändert oder entfernt worden sind.

1.2.5.1.1 Technische Maßnahmen

1066 **Protokollierung Administratorentätigkeiten**

Es erfolgt eine Protokollierung der Administratorentätigkeiten insbesondere von Anlegen von Benutzern, sowie des Änderns von Benutzerrechten.

Die Erfüllung der Anforderung 1066 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.5.1.2 Organisatorische Maßnahmen

1067 **Übersicht IT-Systeme**

Es existiert eine Übersicht, welche IT-Systeme die Erfassung personenbezogener Daten ermöglichen.

Die Erfüllung der Anforderung 1067 wird für diesen Vertrag verpflichtend vereinbart. ☒

1068 **Benutzerberechtigungen**

Es sind Benutzerberechtigungen festgelegt und diese sind wie folgt differenziert:

- Lesen
- Ändern
- Löschen

Die Erfüllung der Anforderung 1068 wird für diesen Vertrag verpflichtend vereinbart. ☒

1069 **Löschkonzept**

Es existiert ein Löschkonzept. In welchem festgelegt ist, wer welche Daten zu welchen Zeitpunkten auf welche Weise löschen darf bzw. muss.

Die Erfüllung der Anforderung 1069 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.5.2 Auftragskontrolle

Hierunter fallen Maßnahmen, welche gewährleisten, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden.

Organisatorische Maßnahmen

1070 Auswahl des Auftragsverarbeiters

Auftragsverarbeiter werden ausschließlich nach einer Überprüfung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. Es werden nur Auftragsverarbeiter ausgewählt, die einen qualifizierten Datenschutzbeauftragten benannt haben und bei denen der Datenschutzbeauftragte über angemessene Ressourcen zur Wahrnehmung seiner Aufgabe verfügt.

Die Erfüllung der Anforderung 1070 wird für diesen Vertrag verpflichtend vereinbart. ☒

1071 Auftragsverarbeitungsvertrag

Es existiert ein Vertrag zur Auftragsverarbeitung, der den Anforderungen der DSGVO genügt.

Die Erfüllung der Anforderung 1071 wird für diesen Vertrag verpflichtend vereinbart. ☒

1072 Geheimhaltungsverpflichtungen

Im Vertrag zur Auftragsverarbeitung wird jeder Auftragsverarbeiter vertraglich verpflichtet, dass die Geheimhaltungsverpflichtungen auch an die Auftragsverarbeiter weitergegeben werden.

Die Erfüllung der Anforderung 1072 wird für diesen Vertrag verpflichtend vereinbart. ☒

1073 Verzeichnis der Verarbeitungstätigkeiten

Es wurde vereinbart, dass der Auftragsverarbeiter ein Verzeichnis der Auftrags-Verarbeitungstätigkeiten führt.

Die Erfüllung der Anforderung 1073 wird für diesen Vertrag verpflichtend vereinbart. ☒

1074 Aufgabenteilung

Die Aufgabenteilung zwischen Auftraggeber und Auftragnehmer einerseits, sowie Auftragnehmer und Subunternehmer anderseits, sind vor Aufnahme der Tätigkeit schriftlich festzulegen, soweit sich dies nicht bereits aus den abgeschlossenen Verträgen ergibt.

Die Erfüllung der Anforderung 1074 wird für diesen Vertrag verpflichtend vereinbart. ☒

1075 Weisungen

Die weisungsbefugten Personen auf Seite des Auftraggebers sind benannt und beim Auftragnehmer bekannt. Die zur Entgegennahme und Ausführung von Weisungen des Auftraggebers beim Auftragnehmer befugten Personen sind benannt. Alle Weisungen des Auftraggebers an den Auftragnehmer erfolgen schriftlich.

Die Erfüllung der Anforderung 1075 wird für diesen Vertrag verpflichtend vereinbart. ☒

1076 Regelungen/Beschränkungen der Auftragsausführung

Es dürfen nur die Arbeiten durchgeführt werden, die in der zu erstellenden Leistungsbeschreibung enthalten sind. Alle darüber hinaus gehenden Arbeitsschritte müssen vorher dezidiert mit der zuständigen Stelle auf Seiten des Auftraggebers abgesprochen und schriftlich freigegeben werden. Der Auftragnehmer stimmt den terminlichen Ablauf der Auftragsausführung vorab mit dem Auftraggeber ab.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. Der Auftragnehmer wird diese unverzüglich beheben. Die meldepflichtigen Vorfälle sind spezifiziert und sowohl den eigenen Beschäftigten als auch allen vom Auftragnehmer eingesetzten Personen bekannt, inkl. Mitarbeitern von ggf. existierenden Unterauftragnehmern.

Die Erfüllung der Anforderung 1076 wird für diesen Vertrag verpflichtend vereinbart. ☒

1077 Unterauftragnehmer

Soweit der Auftraggeber einem Einsatz von Unterauftragnehmern (Subunternehmer/Dienstleister - siehe Begriffsbestimmung) zugestimmt hat und soweit es sich nicht um Konzernunternehmen handelt, sind die Unterauftragnehmer sorgfältig auszuwählen, Art und Umfang der zu erbringenden Leistungen im Rahmen eines datenschutzrechtlichen Unterauftragsverhältnisses zu regeln und die Ausführung der Tätigkeiten und Leistungen im Sinne der vertraglichen Regelungen mit dem Auftraggeber zu überprüfen. Die Ergebnisse dieser Überprüfungen (beispielsweise im Rahmen der ISO 27001) sind schriftlich zu dokumentieren und dem Auftragnehmer auf Verlangen vorzulegen. Die unmittelbaren Kontrollrechte des Auftraggebers bleiben hiervon unberührt.

Wenn der Auftragnehmer einen Unterauftragnehmer zur Erfüllung der Auftragsverarbeitung einsetzt, ist gewährleistet, dass mit Unterauftragnehmern Auftragsverarbeitungsverträge abgeschlossen werden und die Verträge des Auftragnehmers mit dem Unterauftragnehmern die Anforderungen des Auftraggebers an den Auftragnehmer widerspiegeln. Mit Unterauftragnehmern werden Datenschutzvereinbarungen abgeschlossen, nach denen der Unterauftragnehmer seine Beschäftigten auf das Datengeheimnis zu verpflichten hat. .

Die Erfüllung der Anforderung 1077 wird für diesen Vertrag verpflichtend vereinbart. ☒

1078 Dokumentation

Es existiert eine Dokumentation, welche die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung erforderlichen Arbeitsschritte gewährleistet.

Die Erfüllung der Anforderung 1078 wird für diesen Vertrag verpflichtend vereinbart. ☒

1079 Übergabe bei Beendigung des Auftragsverhältnisses

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Daten, Unterlagen und Betriebsmittel erfolgen.

Die Erfüllung der Anforderung 1079 wird für diesen Vertrag verpflichtend vereinbart. ☒

1080 **Konfigurationsänderungen**

Konfigurationsänderungen an Anlagen oder Systemen des Auftraggebers sind unzulässig, wenn dies nicht explizit schriftlich als Bestandteil des Auftrags vereinbart wurde. In diesem Fall ist dies vorab mit der verantwortlichen Stelle abzustimmen und durch eine geeignete Dokumentation die Nachvollziehbarkeit der durchgeführten Änderungen zu gewährleisten.

Die Erfüllung der Anforderung 1080 wird für diesen Vertrag verpflichtend vereinbart. ☒

1081 **Audits**

Bei den Auftragsverarbeitern erfolgen jährlich Audits. Es werden automatisch Nachweise bzgl. der Sicherheit der Verarbeitung (Art. 32 DS-GVO) bei Dienstleistern angefordert.

Die Erfüllung der Anforderung 1081 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.6 Verfügbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten gegen zufällige Zerstörung oder zufälligen Verlust geschützt sind.

1.2.6.1 Technische Maßnahmen

1082 **Sicherung der Serverräume**

Folgende Maßnahmen werden zur Sicherung der Serverräume ergriffen:

- Es existiert ein Brandschutz, insbesondere Feuer- und Rauchmeldeanlagen.
- Im Serverraum ist ein Feuerlöscher verfügbar.
- Der Serverraum ist klimatisiert.
- Im Serverraum erfolgt eine Überwachung von Temperatur und Feuchtigkeit.
- Jeder Server ist mit einer unterbrechungsfreien Stromversorgung (USV) verbunden.
- Es werden Hardware-RAID-Systeme eingesetzt.
- Im Serverraum sind Schutzsteckdosenleisten im Einsatz.
- Es existiert eine Alarmanlage, welche ein unbefugtes Eindringen in den Serverraum meldet.

Die Erfüllung der Anforderung 1082 wird für diesen Vertrag verpflichtend vereinbart. ☒

1083 **Datenschutztresor**

Es ist ein Datenschutztresor (entsprechend S60DIS, S120DIS oder anderer geeigneter Normen mit Quelldichtung etc.) vorhanden.

Die Erfüllung der Anforderung 1083 wird für diesen Vertrag verpflichtend vereinbart. ☒

1084 **Vernichtung Datenträger**

Alte oder unbrauchbare Datenträger werden datenschutzrechtlich ordnungsgemäß vernichtet.

Die Erfüllung der Anforderung 1084 wird für diesen Vertrag verpflichtend vereinbart. ☒

1085 **Verfügbarkeit der IT Infrastruktur**

Einsatz von Distributed Denial of Service (DDoS) Gegenmaßnahmen zum Schutz der Backend Infrastruktur.

Die Corona-Warn-App Backend Infrastruktur wird auf drei verschiedene Verfügbarkeitszonen (Availability Zones) repliziert.

Die Erfüllung der Anforderung 1085 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.6.2 Organisatorische Maßnahmen

1086 **Backup-Konzept**

Es existiert ein angemessenes Backup- und Recovery-Konzept. Um die Verfügbarkeit der Daten auch im Notfall sicherzustellen, müssen die Daten regelmäßig gesichert werden. Zu diesem Zweck muss ein Backup-Konzept erstellt werden, dass einen befugten Mitarbeiter in die Lage versetzt, sämtliche Mittel für die Wiederherstellung der Daten so zu nutzen, dass die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung stehen. Hier wird unter anderem geregelt, dass Backups regelmäßig auf Datenvollständigkeit kontrolliert werden, regelmäßig überprüft wird, ob eine Rekonstruktion der gesicherten Daten tatsächlich möglich ist, welche Daten für welchen Zeitraum gesichert werden müssen, die anschließende Löschung der Daten, das „Haltbarkeitsdatum“ der Sicherungsbänder und die katastrophensichere Aufbewahrung der Datenträger.

Die Erfüllung der Anforderung 1086 wird für diesen Vertrag verpflichtend vereinbart. ☒

1087 **Notfallplan**

Es existiert ein Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (BCM-Konzept). Der Auftraggeber ist über jede Störung (z.B. vorsätzlicher Angriff intern/extern) und Außerbetriebnahme der Datenverarbeitung schnellstmöglich zu informieren. Liegen Anzeichen für eine Störung vor, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Notfallplan zu erstellen, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen, insb. auch auf Seite des Auftraggebers, über den Vorfall zu unterrichten sind.

Die Erfüllung der Anforderung 1087 wird für diesen Vertrag verpflichtend vereinbart. ☒

1088 **Notfallhandbuch**

Es existiert ein Notfallhandbuch mit Notfallplänen, Darstellung der Notfallorganisation – klare Regelung der Verantwortlichkeiten im Notfall.

Die Erfüllung der Anforderung 1088 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.7 Authentizität

1089 **Vortäuschen falscher Infektionsereignisse**

Um Vortäuschen falscher Infektionsereignisse zu begegnen, wird von der Anwendung unmittelbar nach dem Scannen des QR-Codes der QR-Code auf dem Verifikationsserver gegen eine Registration Token eingetauscht und der QR-Code auf dem Server als verbraucht gekennzeichnet.

Die Erfüllung der Anforderung 1089 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.8 Resilienz/ Belastbarkeit/ Ausfallsicherheit/Wiederherstellbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten bei Verlust oder Zerstörung schnell wiederhergestellt werden können.

1.2.8.1 Technische Maßnahmen

1090 **Netzwerk-Monitoring**

Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet.

Die Erfüllung der Anforderung 1090 wird für diesen Vertrag verpflichtend vereinbart. ☒

1091 **Server- und Client-Absicherung**

Es gibt eine unterbrechungsfreie Stromversorgung. Es werden Hardware-RAID-Systeme eingesetzt. Es gibt Reserve-Clients (PC, Laptop, Tablet, Smartphone, …), so dass bei einem Ausfall der Client ausgetauscht und die Arbeit schnellstmöglich wieder aufgenommen werden kann. Folgende Sicherheitssysteme schützen zudem Soft- und/oder Hardware vor Angriffen:

- Virenscanner
- Firewalls
- Spamfilter
- Verschlüsselungsprogramme
- Intrusion-Detection-System
- Intrusion-Prevention-System

Die Erfüllung der Anforderung 1091 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.8.2 Organisatorische Maßnahmen

1092 **Ansprechpartner**

Es wurde festgelegt, welche Person bei welcher Störung oder welchem Ausfall zu benachrichtigen ist.

Die Erfüllung der Anforderung 1092 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.9 Intervenierbarkeit

1093 **Betroffenenrechte**

Durch die verarbeiteten Daten können die Benutzer nicht identifiziert werden. Daher können Ersuchen nach Art. 15 bis 20 DSGVO nicht beantwortet werden. Die Bereitstellung von Informationen, die die Identifizierung der Benutzer ermöglichen würde, findet nicht statt. Dies würde dem Ziel zuwiderlaufen, den Gesamtprozess so datensparsam wie möglich durchzuführen. Die Art. 15 bis 20 DSGVO sind daher nicht anwendbar (Art. 11 Abs.2 DSGVO).

Die Erfüllung der Anforderung 1093 wird für diesen Vertrag verpflichtend vereinbart. ☒

1094 **Betroffenenrechte**

Eine Überprüfung der automatisierten Entscheidungsfindung (Überprüfung der Empfehlungen im Kontaktfall) nach Art. 22 Abs. 3 DSGVO ist nicht notwendig, da durch die CWA und die angebundene IT-Infrastruktur keine rechtsverbindlichen Entscheidungen getroffen werden, sondern nur Empfehlungen ausgesprochen werden.

Die Erfüllung der Anforderung 1094 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.10 Transparenz

1095 **Transparenz**

Durch die folgenden Maßnahmen wird eine größtmögliche Transparenz hergestellt:

- App und alle Komponenten sind quelloffen und auf Github dokumentiert
- öffentliche Diskussion unter anderem auf Github mit der technikinteressierten Öffentlichkeit und Beteiligung von Nichtregierungsorganisationen (NGO)
- Einbindung des in gesamten Entwicklungsprozess BfDI
- Datenschutzhinweise
- Erstellung des Verzeichnisses der Verarbeitungstätigkeiten für Auftragsverarbeiter
- Datenschutzkonzepte für alle Komponenten

- Datenschutzfolgenabschätzung

Die Erfüllung der Anforderung 1095 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.11 Zweckbindung / Nichtverkettung

1.2.11.1 Technische Maßnahmen

1096 **Keine zentrale Entität**

Das Vertrauen in die Server ist begrenzt. Die CWA wird auf der Grundlage einer Technologie mit einem dezentralisierten Ansatz entwickelt. Als Grundlage dienen die Protokolle DP-3T (Decentralized Privacy-Preserving Proximity Tracing) und TCN sowie die Spezifikationen für Privacy-Preserving Contact Tracing von Apple und Google. Die Begegnungsdaten der Benutzer verbleiben lokal auf dem Gerät und werden nicht geteilt.

Die Erfüllung der Anforderung 1096 wird für diesen Vertrag verpflichtend vereinbart. ☒

1097 **Kontrolle der Verarbeitungen**

Die Verwaltung des zentralen Servers folgt klar definierten Governance-Regeln und schließt alle erforderlichen Maßnahmen zur Gewährleistung seiner Sicherheit ein. Der Standort des zentralen Servers ist in Deutschland, so dass eine wirksame Aufsicht durch die zuständige Aufsichtsbehörde gewährleistet ist.

Die Erfüllung der Anforderung 1097 wird für diesen Vertrag verpflichtend vereinbart. ☒

1098 **Begegnungsdaten nur lokal**

Die Begegnungsdaten mit einer infizierten Person (exposures) verbleiben lokal auf dem Gerät und werden nicht geteilt (dezentrale Lösung). Auch Berechnungen, ob es durch den Kontakt zu einer infizierten Person zu einer Ansteckung gekommen sein kann, werden nur lokal auf dem Gerät durchgeführt.

Die Erfüllung der Anforderung 1098 wird für diesen Vertrag verpflichtend vereinbart. ☒

1099 **Löschung**

Alle personenbezogenen Daten werden sobald sie nicht mehr benötigt werden gelöscht.

Die Erfüllung der Anforderung 1099 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.2.11.2 Organisatorische Maßnahmen

1100 **Minimale Datenverarbeitung**

Es werden nur solche Daten verarbeitet, die unmittelbar dem eigentlichen Zweck dienen und die zur Erfüllung der Aufgabe oder Durchführung des Prozesses notwendig sind.

Die Erfüllung der Anforderung 1100 wird für diesen Vertrag verpflichtend vereinbart. ☒

1101 **Auftragsverarbeitungsverträge**

Durch die Auftragsverarbeitungsverträge wird sichergestellt, dass auch die eingesetzten Vertragspartner die datenschutzrechtlichen Bestimmungen beachten.

Die Erfüllung der Anforderung 1101 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1.3.1 Datenschutzmanagement

1.3.1.1 Technische Maßnahmen

1102 **Datenschutzmanagement**

Folgende Maßnahmen werden spezifisch ergriffen, um ein ordnungsgemäßes Datenschutzmanagement zu gewährleisten:

- Datenschutzmanagement-IT-System im Einsatz
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Beschäftigte und Externe nach Bedarf / Berechtigung
  - Intranet
  - Wiki
  - Github

Die Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird mindestens jährlich durchgeführt, sowie bei entsprechenden Anhaltspunkten auch in kürzeren Zyklen nach Bedarf.

Die Erfüllung der Anforderung 1102 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.3.1.2 Organisatorische Maßnahmen

1103 **Datenschutzmanagement**

Der Auftraggeber kommt seinen gesetzlichen Rechenschaftspflichten nach (Nachweis über Einhaltung datenschutzrechtlicher Vorgaben). Er hat einen internen Datenschutzbeauftragten benannt. Die

Beschäftigten werden regelmäßig geschult und auf die Vertraulichkeit/Geheimhaltung verpflichtet, sowie bei Bedarf nach § 203 StGB.

Die Erfüllung der Anforderung 1103 wird für diesen Vertrag verpflichtend vereinbart. ☒

1104 Privacy by Design und Privacy by Default

Datenschutz durch Technikgestaltung („Privacy by Design“) und Datenschutz durch datenschutzfreundliche Voreinstellungen („Privacy by Default“) werden bei allen Verarbeitungsprozessen umgesetzt.

Die Erfüllung der Anforderung 1104 wird für diesen Vertrag verpflichtend vereinbart. ☒

1105 Datenschutz-Folgenabschätzung

Bei Bedarf werden Datenschutz-Folgenabschätzungen durchgeführt.

Die Erfüllung der Anforderung 1105 wird für diesen Vertrag verpflichtend vereinbart. ☒

1106 Betroffenenrechte

Die Betroffenenrechte werden gewährleistet. Entsprechende Prozesse sind etabliert.

Die Erfüllung der Anforderung 1106 wird für diesen Vertrag verpflichtend vereinbart. ☒

1107 Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten wird ständig auf dem aktuellsten Stand gehalten.

Die Erfüllung der Anforderung 1107 wird für diesen Vertrag verpflichtend vereinbart. ☒

1108 Datenschutzvorfälle

Datenschutzvorfälle werden dokumentiert (Art. 33, 34 DSGVO).

Die Erfüllung der Anforderung 1108 wird für diesen Vertrag verpflichtend vereinbart. ☒

1.3.2 Organisationskontrolle

1109 Umsetzung von Schulungsmaßnahmen

Alle Personen, die mit personenbezogenen Daten umgehen oder sonst an der Auftragsdurchführung beteiligt sind (z.B. sofern vereinbart Wartungsunternehmen, Datenvernichter) sind nachweislich zu folgenden Themenkomplexen zu unterweisen:

- Grundsätze des Datenschutzes, einschließlich den technisch-organisatorischen Maßnahmen
- Pflicht zur Wahrung des Datengeheimnisses und Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse einschließlich Vorgängen des Auftraggebers

- Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Datenträgern und sonstigen Unterlagen
- Fernmeldegeheimnis (Verpflichtung nach §88 TKG)
- soweit erforderlich spezielle weitere Verschwiegenheitspflichten
- soweit erforderlich spezielle Hinweise, die sich aus der vertraglichen Vereinbarung und dem vorliegenden Katalog der Mindestvorgaben ergeben können.

Die Unterweisung hat durch geeignete und dem Auftrag angemessene Maßnahmen zu erfolgen und ist mindestens alle zwei Jahre, bei Bedarf (z.B. Änderung der Auftragsumstände oder gesetzlicher Bestimmungen) jedoch auch in kürzeren Abständen, zu wiederholen.

Die Erfüllung der Anforderung 1109 wird für diesen Vertrag verpflichtend vereinbart. ☒

1110 Funktionstrennung und -zuordnung

Im nächsten Schritt ist die Funktionstrennung festzulegen, zu dokumentieren und zu begründen, d.h. welche Funktionen nicht miteinander vereinbar sind, also nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür ergeben sich aus den Aufgaben selbst, den Anforderungen dieser Vereinbarung (insb. dem Katalog der Mindestvorgaben sowie ergänzender Standards) und aus gesetzlichen Bestimmungen. Grundsätzlich sind dabei operative Funktionen nicht mit kontrollierenden Funktionen vereinbar. Nach der Festlegung der einzuhaltenden Funktionstrennung erfolgt Zuordnung der Funktionen zu Personen.

Die Erfüllung der Anforderung 1110 wird für diesen Vertrag verpflichtend vereinbart. ☒

1111 Interne Audits

Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen müssen protokolliert (Benutzerkennung, Transaktionsdetails) werden.

Durch interne Auditierung beim Auftragnehmer wird sichergestellt, dass die Protokolle der Zugriffe auf die personenbezogenen Daten regelmäßig, spätestens jedoch alle zwei Monate, ausgewertet werden. Unregelmäßigkeiten werden dokumentiert, dem Auftraggeber unverzüglich schriftlich mitgeteilt und für einen Zeitraum von 3 Monaten ab Beendigung des Auftrages oder der Tätigkeit aufbewahrt.

Die Erfüllung der Anforderung 1111 wird für diesen Vertrag verpflichtend vereinbart. ☒