Zwischen

Auftraggeber (Verantwortlicher):

und

Auftragnehmer (Auftragsverarbeiter):

Makrolog AG, vertreten durch den Vorsitzenden Andreas Herberger,

Patrickstraße 43, 65191 Wiesbaden

wird die anliegende Vereinbarung zur Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO geschlossen.

Weisungsberechtigte beim Auftraggeber (gemäss Nr. 4 der Vereinbarung) sind:

Ort / Datum:

_____

Unterschrift Auftraggeber

Ort / Datum:

_____

Unterschrift Auftragnehmer

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Zur Verfügungstellung eines Tools zum Speichern der Daten für digitale Anwesenheitsnachweise (https://www.corona-presence.de), insbesondere unter dem Aspekt der Nachverfolgung potentieller Infektionsketten.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist ist vier Wochen zum Monatsende.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Speicherung der zur Rückverfolgung im Sinne der Corona-Verordnungen erforderlichen Daten wie z.B. Name, Vorname, Anschrift, E-Mail-Adresse, Datum des Besuchs der Lokalität, ggf. Dauer des Besuchs der Lokalität.

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO): Die Daten werden erhoben, erfasst, gespeichert.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO): Siehe oben.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO): siehe oben, personenbezogene Daten der Person und Daten des Aufenthaltes.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22

DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers - Siehe Deckblatt.

Weisungsempfänger beim Auftragnehmer sind:

(Jenny Berger oder Eva Kumar, jenny.berger@makrolog.de / e.kumar@makrolog.de)

Für Weisung zu nutzende Kommunikationskanäle:

Bevorzugt über das Makrolog-Ticket-Systems https://makrolog.freshdesk.com in dringenden Fällen auch per E-Mail oder Telefon.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Die Weisung, die Daten gemäß der gesetzlichen Vorgaben (z. B. Corona-Verordnungen) zu löschen, gilt als implizit erteilt.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO).

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden mindestens die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und Dienste, sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, wie datenschutzgerecht zu löschen bzw. zu vernichten.

Die Löschung bzw. Vernichtung sind dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Die Weisung, die Daten gemäß der gesetzlichen Vorgaben (z. B. Corona-Verordnungen) zu löschen, gilt als implizit erteilt.

10. Haftung

Auf Art. 82 DS-GVO wird verwiesen. Im Übrigen wird folgendes vereinbart:

11. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers bei Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 zum Vertrag über Auftragsverarbeitung für Corona-Presence

Darstellung der bei der Makrolog AG gemäß § 9 BDSG / Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen (Stand 20.07.2020):

Zutrittskontrolle

Anforderung:

Die Zutrittskontrolle verlangt, Unbefugten den körperlichen Zutritt zur Datenverarbeitungsanlage, mit der personenbezogene Daten verarbeitet werden, zu verwehren. Es soll verhindert werden, dass Personen, die dazu nicht befugt sind, unkontrolliert in die Nähe von Datenverarbeitungsanlagen kommen.

Realisierte Maßnahmen:

- Das Rechenzentrum des beauftragten Hosting-Providers (Amazon Web Services am Standort Frankfurt) ist nach dem Cloud Computing Compliance Controls Catalogue, C5 des BSI sowie nach ISO/IEC 27018:2019 zertifiziert und erfüllt damit die Anforderung.

Zugangskontrolle

Anforderung:

Im Gegensatz zur Zutrittskontrolle ist hiermit der Schutz vor einem Eindringen unbefugter Personen in das EDV System selbst, also dessen Benutzung, beabsichtigt. Es müssen daher Maßnahmen getroffen werden, die das unberechtigte Eindringen in die EDV-Systeme verhindern.

Realisierte Maßnahmen:

- Richtlinien zur sicheren Wahl und dem ordnungsgemäßen Umgang mit Passwörtern
- Zugriff auf Serversysteme mit persönlicher Schlüsseldatei über eine verschlüsselte Verbindung mittels SSH (Secure Shell) für alle Benutzer
- Zusätzliche Passwortverschlüsselung der persönlichen Schlüsseldatei
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern

Zugriffskontrolle

Anforderung:

Maßnahmen der Zugriffskontrolle müssen geeignet sein, zu gewährleisten, dass ausschließlich die zur Benutzung des Systems berechtigten Personen auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Realisierte Maßnahmen:

- Trennung von Berechtigungsbewilligung (organisatorisch) durch Geschäftsleitung von technischer Ausführung durch Administratoren
- Schlüssel sind eindeutig autorisierten Benutzern zugeordnet (siehe auch Zugangskontrolle SSH)
- Produktspezifische Steuerung mit welchen Schlüsseln auf die Serversysteme zugegriffen werden darf

- Nur der Besitzer einer Anwesenheitsliste kann auf die von ihm erfassten personenbezogenen Daten zugreifen. Die Authentifizierung erfolgt über die Telefonnummer mit einem per SMS zugesandten PIN-Code.

Weitergabekontrolle

Anforderung:

Maßnahmen zur Weitergabekontrolle müssen geeignet sein, um sicherzustellen, das personenbezogene Daten bei der Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Realisierte Maßnahmen:

- Genereller Einsatz von HTTPS oder sonstiger geeigneter Verschlüsselung bei Übertragung
- Der Zugriff auf personenbezogene Daten erfolgt nur nach Authentifizierung (siehe auch Zugriffskonstrolle)
- Der Zugriff auf das interne Netzwerk des Auftragnehmers erfolgt grundsätzlich über verschlüsselte VPN-Verbindungen

Eingabekontrolle:

Anforderung:

Die Maßnahmen zur Eingabekontrolle müssen gewährleisten, dass alle sicherheitsrelevanten Abläufe und alle Vorgänge, die personenbezogene Daten betreffen, durch das System protokolliert (geloggt) werden.

Realisierung:

- Die Datenerfassung erfolgt durch die Personen selbst, die die personenbezogenen Daten zur Verfügung stellen.
- Die Protokollierung erfolgt implizit durch Abspeichern in der jeweiligen Anwesenheitsliste, d.h. Speicherung und Protokollierung sind ein und derselbe Vorgang.

Auftragskonktrolle*:*

Anforderung:

Die Auftragskontrolle verpflichtet den Auftragsverarbeiter, den Auftrag, bei dem personenbezogenen Daten verarbeitet oder genutzt werden, gemäß den Vorschriften des Datenschutzes und den Vorgaben des Auftraggebers abzuwickeln und dem Auftraggeber als verantwortliche Stelle Kontrollen vor Ort zu ermöglichen. Maßnahmen zur Auftragskontrolle müssen sicherstellen, dass die überlassenen Daten nur im Rahmen des Auftrages verarbeitet werden können.

Realisierung:

- Verpflichtung aller Mitarbeiter auf die Einhaltung der Regeln in Bezug auf Daten-, Fernmelde- und Geschäftsgeheimnis
- Belehrung / Unterweisung der Mitarbeiter in Bezug auf die relevanten datenschutzrechtlichen Regelungen
- Prüfung und Sicherstellung der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit durch Einsatz von BSI/ISO-zertifizierten Hosting-Dienstleistern

Verfügbarkeitskontrolle:

Anforderung:

Maßnahmen zur Verfügbarkeitskontrolle müssen sicherstellen, dass personenbezogene Daten nicht unbeabsichtigt zerstört werden oder „verloren“ gehen.

Realisierung:

- Einsatz von virtuellen Plattformen
- Nutzung redundanter Infrastrukturen beim Hosting-Provider
- Monitoring aller Systeme zur Erkennung von Störungen
- Regelmäßige Backups (mindestens alle 24h)

Trennungskontrolle:

Anforderung:

Maßnahmen der Trennungskontrolle müssen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können. Eine Trennung darf nicht nur auf einem System oder nur auf dem Hauptsystem realisiert sein, sondern muss für die davon betroffenen Verfahren insgesamt durchgängig umgesetzt sein.

Realisierung:

- Trennung von Entwicklungs- und Produktivsystemen durch unterschiedliche virtuelle Maschinen.
- Speicherung der Corona-Presence-Daten in einer eigenen durch Zugriffsrechte abgesicherten Systembibliothek.