Accu-Chek Care - Ergänzung zur Datenverarbeitung

Verarbeitung gemäß Artikel 28 der Datenschutz-Grundverordnung (DSGVO)

Die vorliegende Datenverarbeitungsvereinbarung (im Folgenden: „Datenverarbeitungsvereinbarung" oder „DVV") wird zwischen der Gesundheitseinrichtung, die Sie als für die Datenverarbeitung Verantwortlicher vertreten (im Folgenden: „Sie"), und der Roche Diabetes Care GmbH, Sandhofer Straße 116, 68305 Mannheim, Deutschland (im Folgenden: „Roche") als Datenverarbeiter vereinbart, wenn die DSGVO für Ihre Nutzung der Plattformdienste zur Verarbeitung personenbezogener Daten von Patienten gilt.

1. GEGENSTAND UND LAUFZEIT

(1) Gegenstand

Diese Datenverarbeitungsvereinbarung bildet als Anhang einen festen Bestandteil des Plattformvertrages, der den Nutzungsbedingungen unterliegt (im Folgenden: „Vertrag"). Der Gegenstand dieser Datenverarbeitungsvereinbarung ergibt sich aus dem Vertrag und beschränkt sich auf die Verarbeitung der personenbezogenen Daten der Patienten in Ihrem Plattform-Konto.

(2) Laufzeit

Die Laufzeit der vorliegenden Datenverarbeitungsvereinbarung entspricht der Laufzeit des Vertrags.

2. LEISTUNGSBESCHREIBUNG

(1) Art und Zweck der Verarbeitung von personenbezogenen Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch Roche sind im Vertrag und insbesondere in der Leistungsbeschreibung genau definiert.

(2) Geografischer Geltungsbereich

Für die Datenverarbeitung und -speicherung setzen wir vertrauenswürdige Dienstleister ein, die Ihre Daten in unserem Auftrag verarbeiten (Art. 28 DSGVO).

Zur Erfüllung der oben genannten dieser Zwecke können Ihre Daten in Länder innerhalb und außerhalb der EU bzw. des Europäischen Wirtschaftsraums übermittelt werden, insbesondere in die Schweiz, USA und Indien. Für einige dieser Länder ist ein angemessenes Datenschutzniveau durch einen Angemessenheitsbeschluss der EU-Kommission festgestellt (derzeit etwa die Schweiz). Für Übermittlungen, die nicht auf einen Angemessenheitsbeschluss gestützt werden, wird die Einhaltung eines angemessenen Datenschutzniveaus durch geeignete Garantien, insbesondere EU-Standardvertragsklauseln, und bei Bedarf zusätzlichen

Maßnahmen, sichergestellt. Weitere Informationen zu den Garantien erhalten Sie über den Datenschutzbeauftragten.

(3) Art der personenbezogenen Daten

Folgende Arten von personenbezogenen Daten werden im Rahmen dieser Datenverarbeitungsvereinbarung verarbeitet:

- Stammdaten und demografische Daten der Patienten, die Sie in die Plattform eingeben, wenn Sie ein Patientenprofil anlegen (Name, Alter, Adresse, Telefon, E-Mail, Versicherungsnummern usw.)
- Gesundheitsdaten Ihrer Patienten, die Sie in die Plattform eingeben oder von Dritten erhalten, wie z. B. anderen medizinischen Fachkräften oder Patienten, einschließlich Daten von den Messgeräten Ihrer Patienten, anderen Geräten und/oder Apps (Blutzuckerzielbereiche, Blutzuckermesswerte, dokumentiertes Insulin, dokumentierte Nahrung, dokumentierter Sport und andere dokumentierte Notizen, Informationen zu den Geräten wie Geräte-ID, Daten zur Bluetooth-Verbindung usw.)

(4) Kategorien von Datensubjekten

Die Datensubjekte im Geltungsbereich dieser Datenverarbeitungsvereinbarung sind die Patienten, die Sie auf der Plattform eingeben.

3. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

(1) Die erforderlichen technischen und organisatorischen Maßnahmen sind in der **Anlage** („Technische und organisatorische Maßnahmen“) dokumentiert und werden hiermit von Ihnen bestätigt. Die dokumentierten Maßnahmen bilden die Grundlage der Datenverarbeitungsvereinbarung. Im Rahmen der genannten Maßnahmen können Sie über die in den Einstellungen Ihres Plattform-Kontos verfügbaren Optionen Weisungen erteilen, die sich auf die Verarbeitung auswirken.

(2) Auf der Grundlage der vereinbarten technischen und organisatorischen Maßnahmen wird Roche die Sicherheit gemäß Artikel 28 Absatz 3 lit. c und Artikel 32 DSGVO, insbesondere in Verbindung mit Artikel 5 Absatz 1 und 2 DSGVO, nach Ihren Weisungen herstellen. Bei den zu treffenden technischen und organisatorischen Maßnahmen handelt es sich um Maßnahmen der Datensicherheit und Maßnahmen, die ein dem Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gewährleisten. Dabei werden der Stand der Technik, die Implementierungskosten, die Art, der Umfang und der Zweck der Verarbeitung sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Artikel 32 Absatz 1 DSGVO berücksichtigt.

(3) Sie sind verpflichtet, die Weitergabe von Daten, die als Gegenstand der Leistungen von Roche beschrieben wurden, zu kennzeichnen und angemessen zu begrenzen.

(4) Roche informiert Sie, wenn eine Ihrer Weisungen nach unserer Auffassung gegen geltendes Datenschutzrecht verstößt, falls diese Anforderung für Roche keine Verpflichtung zu einer unabhängigen Untersuchung oder rechtlichen oder regulatorischen Beratung begründet.

(5) Wenn Sie verlangen, dass Roche eine Verarbeitungsanweisung trotz unseres Hinweises befolgt, dass eine solche Weisung gegen anwendbares Datenschutzrecht verstößt, sind Sie für jede Haftung verantwortlich und müssen Roche gegen alle Ansprüche und Schäden verteidigen, entschädigen und schadlos halten, die sich aus einer weiteren Verarbeitung in Übereinstimmung mit solchen Weisungen ergeben.

(6) Sie erkennen hiermit an und erklären, dass Sie die in der **Anlage** beschriebenen technischen und organisatorischen Maßnahmen unter Berücksichtigung des aktuellen Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und des Zwecks der Verarbeitung sowie der Wahrscheinlichkeit und Schwere des Risikos für die Datensubjekte für angemessen halten.

(7) Die technischen und organisatorischen Maßnahmen können sich im Zuge des technischen Fortschritts und der Weiterentwicklung ändern. Insofern ist es zulässig, dass Roche alternative angemessene Maßnahmen umsetzt. Dabei darf das Sicherheitsniveau der definierten Maßnahmen nicht herabgesetzt werden. Wesentliche Änderungen müssen von den Parteien vereinbart werden.

(8) Im Falle einer Änderung (einschließlich Änderungen oder weiterer Hinweise zur Auslegung) eines anwendbaren Datenschutzgesetzes, die eine Änderung aller oder eines Teils der technischen und organisatorischen Maßnahmen erfordert, welche unsere Kosten und Aufwendungen erhöht, wird gemeinsam eine Vereinbarung über den Ausgleich getroffen.

4. BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG PERSONENBEZOGENER DATEN

(1) Roche darf personenbezogene Daten, die in Ihrem Auftrag verarbeitet werden, nicht eigenmächtig berichtigen, löschen oder deren Verarbeitung einschränken, sondern nur nach dokumentierter Weisung Ihrerseits.

Wenn sich ein Datensubjekt bezüglich einer Berichtigung, Löschung oder Einschränkung der Verarbeitung direkt an uns wendet, werden wir den Antrag des Datensubjekts unverzüglich an Sie weiterleiten.

(2) Soweit im Leistungsumfang enthalten, werden die Löschung, das „Recht auf Vergessenwerden", die Berichtigung, die Datenübertragbarkeit und der Zugriff nach dokumentierten Weisungen von Ihnen unverzüglich von Roche sichergestellt.

5. QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN VON ROCHE

Neben der Einhaltung der in dieser Datenverarbeitungsvereinbarung festgelegten Regelungen hat Roche die in den Artikeln 28 bis 33 DSGVO genannten gesetzlichen Anforderungen zu erfüllen; dementsprechend stellt Roche insbesondere die Einhaltung der folgenden Anforderungen sicher:

a) Ernennung eines Datenschutzbeauftragten, der seine Aufgaben in Übereinstimmung mit den Artikeln 38 und 39 DSGVO wahrnimmt. Der Datenschutzbeauftragte kann unter Germany.privacy@roche.com kontaktiert werden.

b) Vertraulichkeit gemäß Artikel 28 Absatz 3 Satz 2 lit. b, Artikel 29 und 32 Absatz 4 DSGVO. Roche betraut nur solche Mitarbeiter mit der in dieser Datenverarbeitungsvereinbarung beschriebenen Datenverarbeitung, die sich zur Vertraulichkeit und Geheimhaltung verpflichtet haben und zuvor mit den für ihre Tätigkeit relevanten Bestimmungen vertraut gemacht wurden. Roche und alle im Auftrag von Roche handelnden Personen, die Zugang zu personenbezogenen Daten haben, dürfen diese personenbezogenen Daten nicht bearbeiten, wenn sie von Ihnen keine entsprechende Weisung erhalten, wozu auch die in dieser Datenverarbeitungsvereinbarung erteilten Befugnisse gehören, es sei denn, sie sind nach geltendem Recht dazu verpflichtet.

c) Umsetzung und Einhaltung aller für diese Datenverarbeitungsvereinbarung erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 28 Abs. 3 Satz 2 lit. c, Artikel 32 DSGVO und wie in Abschnitt 3 und in der **Anlage** dargelegt.

d) Die Parteien werden, falls gewünscht, bei der Erfüllung ihrer Aufgaben mit der Aufsichtsbehörde zusammenarbeiten.

e) Sie sind unverzüglich über Prüfungen und Maßnahmen der Aufsichtsbehörde zu unterrichten, soweit sie sich auf diese Datenverarbeitungsvereinbarung beziehen. Dies gilt auch, falls Roche im Zusammenhang mit Verstößen gegen zivil- oder strafrechtliche Vorschriften oder gegen Verwaltungsvorschriften über die Verarbeitung personenbezogener Daten im Zusammenhang mit dieser Datenverarbeitungsvereinbarung von einer Untersuchung durch eine zuständige Behörde betroffen oder an einer solchen Untersuchung beteiligt ist.

f) Wenn für Sie eine Prüfung durch die Aufsichtsbehörde, ein Ordnungswidrigkeits- oder Strafverfahren, ein Haftungsanspruch eines Datensubjekts oder eines Dritten oder ein sonstiger Anspruch im Zusammenhang mit der Datenverarbeitung nach dieser Datenverarbeitungsvereinbarung durch Roche vorliegt, werden wir uns nach Kräften bemühen, Sie zu unterstützen.

g) Roche überwacht in regelmäßigen Abständen die internen Prozesse und die technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung im Verantwortungsbereich von Roche mit den Anforderungen des geltenden Datenschutzrechts und dem Schutz der Rechte des Datensubjekts in Einklang steht.

6. UNTERAUFTRAGSVERGABE

(1) Als Unteraufträge im Sinne dieser Datenverarbeitungsvereinbarung sind Leistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, d. h. die Verarbeitung der personenbezogenen Daten Ihrer Patienten in Ihrem Auftrag. Davon ausgenommen sind Nebenleistungen, wie z. B. Telekommunikationsleistungen, Post-/Transportleistungen, Wartungs- und Kundendienstleistungen, die Ihnen oder einem Mitglied Ihrer Gesundheitseinrichtung zur Verfügung gestellt werden, oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Roche ist jedoch verpflichtet, angemessene und rechtsverbindliche vertragliche Vereinbarungen zu

treffen und geeignete Kontrollmaßnahmen zu ergreifen, um den Datenschutz und die Datensicherheit Ihrer Daten auch im Falle ausgelagerter Nebenleistungen zu gewährleisten.

(2) Sie erklären sich damit einverstanden, dass Roche zur Erfüllung seiner vertraglichen Pflichten nach dieser DVV Unterauftragnehmer einsetzt. Auf der Website der Plattform (derzeit unter https://care.rochediabetes.com/c2a im Bereich „Hilfe“) sind die Unterauftragnehmer aufgeführt, die derzeit von Roche mit der Durchführung von Verarbeitungstätigkeiten an personenbezogenen Daten von Patienten in Ihrem Auftrag beauftragt sind. Roche wird mindestens 30 Tage, bevor Roche einen neuen Unterauftragnehmer mit der Durchführung solcher Verarbeitungstätigkeiten beauftragt, die entsprechende Website aktualisieren und Ihnen eine Mitteilung über diese Aktualisierung zukommen lassen. Roche kann diese Datenverarbeitungsvereinbarung und den Vertrag mit einer Frist von 30 Tagen kündigen, wenn Sie der geplanten Verarbeitung durch den Unterauftragnehmer widersprechen. Mit Ausnahme der in diesem Abschnitt genannten oder von Ihnen anderweitig genehmigten Fälle wird Roche keinem Unterauftragnehmer gestatten, in Ihrem Auftrag Verarbeitungsaktivitäten an personenbezogenen Daten von Patienten durchzuführen.

(3) Wenn Roche einen Unterauftragnehmer autorisiert, gilt:

a) Roche schließt mit dem Unterauftragnehmer eine schriftliche Vereinbarung gemäß Artikel 28 DSGVO ab (weitere Auslagerungen durch den Unterauftragnehmer unterliegen denselben Regelungen);

b) Roche bleibt für die Einhaltung der Verpflichtungen aus dieser DVV und für alle Handlungen oder Unterlassungen der Unterauftragnehmer verantwortlich, die eine Verletzung der Verpflichtungen von Roche aus dieser DVV zur Folge haben.

7. KONTROLLBEFUGNISSE

(1) Sie haben das Recht, nach Rücksprache mit Roche Kontrollen durchzuführen oder durch einen im Einzelfall zu bestimmenden Prüfer durchführen zu lassen. Sie haben das Recht, sich durch stichprobenartige, in der Regel rechtzeitig anzukündigende Kontrollen von der Einhaltung dieser Datenverarbeitungsvereinbarung durch Roche im Geschäftsbetrieb zu überzeugen.

(2) Roche verpflichtet sich, Ihnen auf Anfrage die erforderlichen Auskünfte zu erteilen und insbesondere die Durchführung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen kann erbracht werden durch

- Einhaltung der genehmigten Verhaltenskodizes gemäß Artikel 40 DSGVO; und/oder
- Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO; und/oder
- aktuelle Prüfbescheinigungen, Berichte oder Auszüge aus Berichten unabhängiger Stellen (z. B. Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor); und/oder

- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzauditierung (z. B. nach BSI-Grundschutz oder ISO/IEC 27001).

(4) Roche kann einen Ausgleich für die Ermöglichung Ihrer Inspektionen verlangen, soweit Ihre Auditwünsche nicht mit den Standardinformationen erfüllt werden können, die uns gemäß Absatz (3) für alle medizinischen Fachkräfte zur Verfügung stehen und die nicht auf Versäumnisse auf Seiten von Roche zurückzuführen sind.

8. KOMMUNIKATION IM FALLE VON VERSTÖßEN

(1) Roche unterstützt Sie bei der Einhaltung der Pflichten zur Sicherheit personenbezogener Daten, der Meldepflichten bei Datenschutzverletzungen, der Datenschutz-Folgenabschätzungen und der vorherigen Konsultationen, die in den Artikeln 32 bis 36 der Datenschutz-Grundverordnung genannt sind. Dazu gehören:

a) Die Gewährleistung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die den Umständen und Zwecken der Verarbeitung sowie der voraussichtlichen Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung aufgrund von Sicherheitslücken Rechnung tragen und eine unverzügliche Erkennung von für die Verletzung relevanten Ereignissen ermöglichen.

b) Die Pflicht, Sie unverzüglich über eine Verletzung des Schutzes personenbezogener Daten in Kenntnis zu setzen.

c) Die Pflicht, Sie im Hinblick auf die Informationspflicht gegenüber dem Datensubjekt zu unterstützen und Ihnen diesbezüglich unverzüglich alle relevanten Informationen zur Verfügung zu stellen.

d) Die Unterstützung bei der jeweiligen Datenschutz-Folgenabschätzung.

e) Die Unterstützung im Hinblick auf die vorherige Konsultation der Aufsichtsbehörde.

(2) Für Kundendienstleistungen, die nicht in der Leistungsbeschreibung enthalten sind und die nicht auf Versäumnisse auf Seiten von Roche zurückzuführen sind, kann Roche einen Ausgleich verlangen.

9. BERECHTIGUNG ZUR ERTEILUNG VON WEISUNGEN

(1) Sie können Weisungen, die sich auf unsere Verarbeitung auswirken, in erster Linie über die Einstellungen in Ihrem Plattform-Konto erteilen. In Fällen, in denen dies nicht funktioniert, können Sie Weisungen auch über den Kundendienst entweder in elektronischer Form (Ticketsystem) oder mündlich (per Telefon) erteilen. Mündliche Weisungen haben Sie jedoch unverzüglich (mindestens in Textform) zu bestätigen.

(2) Roche wird Sie unverzüglich informieren, wenn wir der Ansicht sind, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt oder eine entsprechende Konfiguration der Plattform nicht praktikabel ist. Roche ist in diesem Fall berechtigt, die Ausführung der betreffenden Weisungen auszusetzen, bis Sie diese bestätigen oder ändern. Wenn nach

vernünftiger Einschätzung von Roche keine Einigung erzielt werden kann, so kann Roche die Datenverarbeitungsvereinbarung und den Vertrag mit einer Frist von 30 Tagen kündigen.

10. ANONYMISIERUNG DER PERSONENBEZOGENEN DATEN

Roche wird hiermit angewiesen, personenbezogene Patientendaten im Rahmen der Erbringung der Dienstleistung (z. B. Payer Dashboard), des Entwicklungszyklus und der Produktverbesserung zu anonymisieren. Diese Weisung unterliegt den folgenden Bedingungen:

- Die anonymisierten Daten können nicht wieder einzelnen Patienten zugeordnet werden und werden sicher von den von Roche verarbeiteten personenbezogenen Patientendaten getrennt.
- Anonyme Datensätze können auch zu Zwecken der Forschung und Statistik (stets unter Einhaltung der anerkannten ethischen wissenschaftlichen Standards) und für interne Analysen verwendet werden. Dies dient hauptsächlich dazu, die Wirksamkeit von Methoden zur Kontrolle und Behandlung von Diabetes zu ermitteln und zu verbessern.
- Wir verwenden nur einen kleinen Teil der demografischen Informationen im Rahmen der anonymen Daten, wie z. B. Geburtsjahr und Land des Wohnsitzes. Dieser kleine Teil der demografischen Daten wird mit den Daten des Plattform-Kontos (wie z. B. Kontoeinstellungen, Zielbereiche für Blutzuckerwerte, Mahlzeitenmuster, Nutzungstage, durchschnittliche Blutzuckerwerte usw.) zusammengeführt. Solche für Forschungszwecke verarbeiteten aggregierten Daten sind statistische Informationen, die aus mehreren Messungen kombiniert werden. Wir ergreifen Maßnahmen, um sicherzustellen, dass es mit angemessenen Mitteln nicht möglich ist, diese aggregierten Daten zur Identifizierung einer Person zu verwenden. Roche wird solche aggregierten Daten nicht mit anderen Informationen kombinieren, die zur Identifizierung von Patienten verwendet werden können.

11. LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

(1) Kopien oder Duplikate der Daten werden niemals ohne Ihr Wissen erstellt, mit Ausnahme von Sicherungskopien, soweit diese zur Sicherstellung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie von Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten benötigt werden.

(2) Nach Beendigung der beauftragten Arbeiten bzw. auf Ihren Wunsch auch früher, spätestens jedoch bei Beendigung des Dienstleistungsvertrages, löscht Roche alle in Ihrem Auftrag verarbeiteten personenbezogenen Daten durch Anonymisierung oder ein entsprechendes Verfahren. Das Protokoll der Löschung ist auf Verlangen vorzulegen.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung gemäß der Datenverarbeitungsvereinbarung dienen, werden von Roche über die Vertragslaufzeit hinaus entsprechend den jeweiligen Aufbewahrungsfristen aufbewahrt. Roche kann diese Dokumentation nach Ablauf der Vertragslaufzeit an Sie aushändigen, um von dieser vertraglichen Verpflichtung entbunden zu werden.

Anlage

Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Artikel 32 Absatz 1 lit. b DSGVO)

- Physische Zugangskontrolle

  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B. durch Magnet- oder Chipkarten, Schlüssel, elektronische Türöffner, Objektschutzdienste und/oder Sicherheitspersonal am Eingang, Alarmanlagen, Video/CCTV-Systeme.

  Unbefugten wird der physische Zugang zu Grundstücken, Gebäuden oder Räumen verwehrt, in denen sich Datenverarbeitungsanlagen befinden, die personenbezogene Daten verarbeiten und/oder nutzen.

  Die Infrastruktur befindet sich auf der Amazon Web Services Cloud („AWS-Cloud") in nach ISO 27001 zertifizierten Rechenzentren in Deutschland.

  Sicherheitsmaßnahmen für die AWS-Cloud:

  - Die physischen Sicherheitskontrollen umfassen unter anderem Kontrollen der Umgrenzung wie Zäune, Mauern, Sicherheitspersonal, Videoüberwachung, Einbruchserkennungssysteme und andere elektronische Mittel.
  - Der physische Zugang wird sowohl an der Umgrenzung als auch an den Gebäudeeingängen streng kontrolliert und umfasst unter anderem professionelles Sicherheitspersonal, das Videoüberwachung, Einbruchmeldesysteme und andere elektronische Mittel einsetzt. Autorisierte Mitarbeiter müssen mindestens zweimal eine Zwei-Faktor-Authentifizierung durchlaufen, um Zugang zu den Etagen des Rechenzentrums zu erhalten. Die physischen Zugangspunkte zu den Serverstandorten werden durch CCTV-Kameras („Closed Circuit Television") aufgezeichnet, wie in der Richtlinie für physische Sicherheit im Rechenzentrum von AWS („Data Center Physical Security Policy") definiert. Die physischen Sicherheitsmechanismen von AWS werden von unabhängigen externen Prüfern während der Audits für unsere SOC-, PCI DSS-, ISO 27001- und HiTrust-Zertifizierung überprüft.

  Sicherheitsmaßnahmen für Räumlichkeiten von Roche:
  - Vermögenswerte und Einrichtungen werden mit den geeigneten Mitteln gemäß den Roche-Sicherheitsstandards geschützt.
  - Alle Rechenzentren halten sich an strenge Sicherheitsverfahren, die durch Wachpersonal, Überwachungskameras, Zugangskontrollmechanismen und andere Maßnahmen durchgesetzt werden, um zu verhindern, dass Geräte und Einrichtungen des Rechenzentrums manipuliert werden. Nur autorisierte Vertreter haben Zugang zu den Systemen und der Infrastruktur innerhalb der Rechenzentrumseinrichtungen. Um die ordnungsgemäße Funktionalität zu gewährleisten, werden die physischen Sicherheitseinrichtungen regelmäßig gewartet.

- In der Regel sind die Gebäude durch Zugangskontrollsysteme (z. B. Smartcard-Zugangssystem) gesichert.
- Je nach Sicherheitseinstufung können Gebäude, einzelne Bereiche und das umliegende Gelände durch zusätzliche Maßnahmen weiter geschützt werden.
- Zutrittsrechte werden autorisierten Personen auf individueller Basis entsprechend den Maßnahmen der System- und Datenzugangskontrolle gewährt.
- Gäste und Besucher von Roche-Gebäuden müssen sich am Empfang namentlich registrieren lassen und müssen von autorisierten Roche-Mitarbeitern begleitet werden.
- Roche-Mitarbeiter und externes Personal müssen an allen Roche-Standorten ihre Ausweise tragen.
- Roche und alle Drittanbieter von Rechenzentren dokumentieren die Namen und Zeiten von autorisiertem Personal, das die privaten Bereiche von Roche innerhalb der Rechenzentren betritt.
- Es gibt gesicherte Räume, von denen aus nur autorisiertes Personal auf personenbezogene und vertrauliche Daten zugreifen kann.

- Elektronische Zugangskontrolle

  Keine unbefugte Nutzung der Datenverarbeitungs- und Datenspeichersysteme: (sichere) Passwörter, automatische Sperr-/Verriegelungsmechanismen, Verschlüsselung von Datenträgern/Speichern/Speichermedien.

  Roche gestattet nur autorisiertem Personal den Zugriff auf personenbezogene Daten, soweit dies im Rahmen ihrer Aufgabenerfüllung erforderlich ist.

  Datenverarbeitungssysteme, die zur Erbringung der Dienstleistung eingesetzt werden, müssen vor unbefugter Nutzung geschützt werden.

  Maßnahmen:
  - Bei der Gewährung des Zugriffs auf sicherheitsempfindliche Systeme, einschließlich solcher, die personenbezogene Daten speichern und verarbeiten, werden mehrere Berechtigungsstufen verwendet. Berechtigungen werden über definierte Prozesse gemäß der Roche-Sicherheitsrichtlinie verwaltet.
  - Alle Mitarbeiter haben mit einer eindeutigen Kennung (Benutzer-ID) Zugang zu den Systemen von Roche.
  - Roche verfügt über Verfahren, die sicherstellen, dass beantragte Berechtigungsänderungen nur in Übereinstimmung mit der Roche-Sicherheitsrichtlinie durchgeführt werden (z. B. werden keine Rechte ohne Autorisierung erteilt). Falls ein Mitarbeiter das Unternehmen verlässt, werden ihm die Zugriffsrechte entzogen.
  - Roche hat eine Passwortrichtlinie eingeführt, welche die Weitergabe von Passwörtern verbietet, Reaktionen auf die Offenlegung von Passwörtern regelt und verlangt, dass regelmäßig neue Passwörter verwendet und Standardpasswörter geändert werden. Zur Authentifizierung werden personalisierte Benutzer-IDs vergeben. Alle Passwörter müssen die Anforderungen an die Komplexität und die Mindestanforderungen an die Sicherheit erfüllen und werden in gehashter Form gespeichert.
  - Das Roche-Netzwerk ist durch Firewalls vor dem öffentlichen Netzwerk geschützt.
  - Anhand eines Sicherheits-Patch-Managements wird eine regelmäßige Bereitstellung relevanter Sicherheits-Updates in bestimmten Zeitabständen gewährleistet.

- Der Zugriff auf personenbezogene Daten und vertrauliche personenbezogene Daten durch autorisiertes Personal erfolgt über VPN. Alle VPN-Anmeldungen werden überwacht.

- Interne Zugriffskontrolle (Berechtigungen für den Zugriff auf und die Änderung von Daten durch Benutzer)

  Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten innerhalb des Systems, z. B. Berechtigungskonzept, bedarfsgerechte Zugriffsrechte, Protokollierung von Systemzugriffsereignissen.

  Für jedes System werden eine Roche-ID und entsprechende Zugriffsrechte verlangt. Nur autorisiertes Personal, das Zugriff auf das System benötigt, um seine Aufgaben zu erfüllen (Need-to-know-Prinzip), ist berechtigt. Ein Protokollierungssystem ist vorhanden, um die Rückverfolgbarkeit der durchgeführten Aktionen zu gewährleisten, zudem werden Prüfprotokolle geführt.

2. Pseudonymisierung und Verschlüsselung von Daten (Artikel 32 Absatz 1 lit. a DSGVO; Artikel 25 Absatz 1 DSGVO)

Die Verarbeitung personenbezogener Daten in dieser Version erfolgt derart, dass die klinisch-medizinischen Daten in einer anderen Datenbank gespeichert werden als die Daten, über die das Datensubjekt identifiziert werden kann. Die Daten werden dementsprechend getrennt gespeichert und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

Klinische und nicht-klinische Datenbanken werden durch IDs miteinander verknüpft, die jedem Benutzer zugewiesen werden und die ohne die personenbezogenen Daten der betroffenen Person generiert werden.

Die Anwendungsverarbeitung in der Lösung erfolgt unter Verwendung von Tokens, die keine personenbezogenen Daten beinhalten und das Datensubjekt nicht identifizieren können.

3. Integrität (Artikel 32 Absatz 1 lit. b DSGVO)

- Kontrolle der Datenübertragung

  Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten bei elektronischer Übertragung oder Transport, z. B. durch Verschlüsselung, virtuelle private Netzwerke (VPN), elektronische Signaturen.

  In dieser Lösung werden HTTPS (HTTP over SSL) und TLS 1.2 (Transport Layer Security) zur Absicherung der Kommunikation über das nicht vertrauenswürdige Netzwerk (Internet) verwendet.

  Der Zugriff auf Backend-Systeme erfolgt über VPN. Für die Verbindung sind Roche-Anmeldedaten (eindeutige Roche-ID) und Zugriffsrechte erforderlich.

- Kontrolle der Dateneingabe

  Überprüfung, ob und von wem personenbezogene Daten in ein Datenverarbeitungssystem eingegeben, geändert oder gelöscht werden, z. B. durch Protokollierung, Dokumentenmanagement.

  Roche hat ein Protokollierungssystem für die Eingabe, Änderung und Löschung von Daten implementiert. Diese Rückverfolgbarkeitsprotokolle beinhalten u. a. Benutzerzugriff, Art des Zugriffs und Datei/Register, auf die/das zugegriffen wurde.

  Roche hat eine Validierung der Dateneingabe in Informationsfelder implementiert, die Eingabedaten von Benutzern akzeptieren, einschließlich Sicherheitskontrollen zusätzlich zu den Validierungen von Informationen anhand von Geschäftslogik.

  Zu den Validierungen anhand von Geschäftslogik gehören u. a.: keine Pflichtfelder sind leer, das Format und die Länge der Eingaben in Felder werden kontrolliert.

  Berechtigungskontrollen sind ebenfalls vorhanden, so dass bei der Validierung überprüft wird, ob jeder angemeldete Benutzer berechtigt ist, eine Aktion im System durchzuführen.

4. Verfügbarkeit und Belastbarkeit (Artikel 32 Absatz 1 lit. b DSGVO)

- Kontrolle der Verfügbarkeit

  Personenbezogene Daten werden vor zufälliger oder unbefugter Zerstörung oder Verlust geschützt.

  <u>Allgemeine Maßnahmen:</u>

  - Roche implementiert regelmäßige Backup-Prozesse, um die Wiederherstellung von geschäftskritischen Daten entsprechend der Backup-Strategie zu gewährleisten.
  - Roche verwendet unterbrechungsfreie Stromversorgungen (z. B. USV, Batterien, Generatoren usw.), um die Verfügbarkeit der Stromversorgung in den Rechenzentren zu gewährleisten.
  - Roche hat Notfallpläne für geschäftskritische Prozesse definiert und kann Notfallwiederherstellungsstrategien für geschäftskritische Dienste anbieten.

  <u>Spezifische Maßnahmen für den Betrieb:</u>

  - Die Anwendung wird durch eine spezielle Sicherheitsarchitektur geschützt, die dem Prinzip der „Defense in Depth“ folgt
    - Perimeter-Firewall in Hochverfügbarkeitskonfiguration. Gestattet nur den Zugriff auf Ports, die für die Anwendung zugelassen sind
    - Externe Web Application Firewall (WAF) in Hochverfügbarkeitskonfiguration
    - Anwendungsdesign ermöglicht hohe Verfügbarkeit und Elastizität

- Segregation des Datenverkehrs auf verschiedenen Ebenen: Firewall, AWS-Sicherheitsgruppen, Container-Richtlinien zur Trennung von Frontend- und Backend-Pods
- Eine Antivirenlösung ist in jeder EC2-Instanz installiert und wird zentral verwaltet. Die Antivirenlösung wird in regelmäßigen Abständen aktualisiert.
- Die Infrastruktur wird in Bezug auf Verfügbarkeit und Leistung überwacht.
- Spezielles Sicherheitsmonitoring und Prozesse zur Verwaltung von Vorfällen vorhanden
- Roche setzt regelmäßige Backup-Prozesse ein, um geschäftskritische Systeme bei Bedarf wiederherstellen zu können. Die gesamte Produktionsinfrastruktur wird täglich (über AWS-Snapshots) gesichert und die Snapshots werden 7 Tage lang aufbewahrt.

- Schnelle Wiederherstellung (Artikel 32 Absatz 1 lit. c DSGVO);

  Roche führt regelmäßige Notfallwiederherstellungs-Testläufe durch, mindestens einmal im Jahr.

5. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung (Artikel 32 Absatz 1 lit. d DSGVO; Artikel 25 Absatz 1 DSGVO)

- Datenschutz-Management:

  Roche hat zum Schutz vor unbefugten Änderungen eine mehrschichtige Verteidigungsstrategie eingeführt.

  Zur Umsetzung der oben beschriebenen Abschnitte zu Kontrollmechanismen und Maßnahmen setzt Roche insbesondere Folgendes ein. Im Einzelnen:
  - Firewalls;
  - Sicherheitsüberwachungszentrum;
  - Antiviren-Software;
  - Backup- und Wiederherstellungsprozesse;
  - externe und interne Penetrationstests;
  - Verschlüsselung von Daten bei der Übertragung und im Ruhezustand;

- Management der Reaktion auf Vorfälle:

  Die Roche-Anwendungen und die zugrunde liegende Infrastruktur werden rund um die Uhr überwacht, um sicherheitsrelevante Ereignisse oder potenzielle Vorfälle zu erkennen. Es gibt einen Prozess für das Management von Sicherheitsvorfällen, der Folgendes sicherstellt:
  - Reaktion auf einen Vorfall ist aktiviert, die richtigen Schritte werden eingeleitet, die Kommunikation wird gestartet usw.;
  - schnelle und effiziente Wiederherstellung nach Sicherheitsvorfällen, um den Verlust oder Diebstahl von Daten und die Unterbrechung von Diensten zu minimieren;
  - Nutzung der bei der Handhabung von Vorfällen gewonnenen Informationen, um sich besser auf die Handhabung künftiger Vorfälle vorzubereiten und einen stärkeren Schutz für Systeme und Daten zu gewährleisten;

- Einleitung von Abhilfemaßnahmen (zur Senkung der Wiederholungsrate) und Präventivmaßnahmen, um Vorfälle zu verhindern.

Sind personenbezogene Daten von einem Sicherheitsvorfall betroffen, wird der Roche-Prozess für Verletzungen des Schutzes personenbezogener Daten aktiviert und der Datenschutzbeauftragte benachrichtigt, um die nach geltendem Recht erforderlichen Maßnahmen einzuleiten, z. B. die Benachrichtigung von Behörden oder Datensubjekten.

- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 Absatz 2 DSGVO):

  In Anbetracht der Vertraulichkeit von Gesundheitsdaten hat Roche die Plattform im Einklang mit den Grundsätzen des Datenschutzes entwickelt, wie z. B. Datenminimierung und Verschlüsselung von Daten, und verpflichtet sich, das Sicherheits- und Datenschutzniveau durch geeignete, im Hinblick auf Effektivität entwickelte technische und organisatorische Maßnahmen kontinuierlich aufrechtzuerhalten und zu verbessern, um die Anforderungen der DSGVO zu erfüllen und die Rechte der Datensubjekte zu schützen.

  Standardmäßig werden nur personenbezogene Daten verarbeitet, die jeweils für den spezifischen Zweck der Verarbeitung erforderlich sind, was die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, die Dauer ihrer Speicherung und ihre Zugänglichkeit betrifft.

- Auftrags- oder Vertragskontrolle:

  Keine Datenverarbeitung durch Dritte gemäß Artikel 28 DSGVO ohne entsprechende Weisungen von Roche.

  Roche sorgt für ordnungsgemäße vertragliche Vereinbarungen, ein formalisiertes Auftragsmanagement, strenge Kontrollen bei der Auswahl des Dienstleisters, die Pflicht zur Vorabbewertung und aufsichtliche Nachkontrollen.