

Patienteninformation zur Speicherung von Daten für das digitale Labor-Ergebnis

Einleitung

Das digitale Labor-Ergebnis ermöglicht die Speicherung von Labor-Ergebnissen (z.B. Corona-PCR-Tests) und deren spätere Bestätigung zum Nachweis der Echtheit des Tests bei Bedarf. Zu diesem Zweck wird aus den Patientendaten, den Probedaten und einem zusätzlichen Geheimnis eine individuelle Zahlenfolge (Hashwert) gebildet und an einen technischen Dienstleister übermittelt. Bei der späteren Bestätigung des Corona-Tests wird von der Patient*in der Hashwert auf dem gleichen Wege erneut gebildet und an den technischen Dienstleister übermittelt. Dieser vergleicht, ob dieser Hashwert in der Datenbank bereits gespeichert ist und prüft so die Echtheit des Tests. Weder die Patientendaten selbst, noch die Probedaten werden dabei an den Dienstleister übermittelt.

Verantwortlicher

Verantwortlich für die Datenverarbeitung ist [LABOR].

Kontaktdaten der Datenschutzbeauftragten

Unseren Datenschutzbeauftragten erreichen Sie unter [XX].

Zweck und Rechtsgrundlage der Verarbeitung

Zweck der Datenverarbeitung ist die jeweils von der Proband*in initiierte Ermöglichung der Verifizierung von Probenergebnissen der Proband*in zum Nachweis der Echtheit eines bestimmten Probenergebnisses gegenüber Dritten.

Rechtsgrundlage der Datenverarbeitung sind Art. 9 Abs. 2 lit. a und Art. 6 Abs. 1 S. 1 lit. a DSGVO.

Erhobene und verarbeitete Datenkategorien

Für die Bildung des Hashwerts werden folgende personenbezogene Daten erhoben:

- Patientendaten
 - Name
 - Geburtsdatum
- Probedaten
 - Probenergebnis
 - ProbenID
 - Probendatum
- vom Labor erzeugte zufällige Zahlenfolge (Geheimnis)

Aus diesen Daten wird über einen Hashalgorithmus ein Hashwert erzeugt (Hashwert 1). Aus dem Hashwert 1 lässt sich ohne die Kombination von Patientendaten, Probedaten und dem Geheimnis nicht auf den Probanden schließen.

Empfänger der Daten

Der Hashwert 1 (nicht aber die Patientendaten, die Probanden oder das Geheimnis) wird unserem technischen Dienstleister, der ubirch GmbH, Gürtelstraße 25, 10247 Berlin übermittelt. Mit diesem Dienstleister haben wir eine Vereinbarung über die Datenverarbeitung im Auftrag geschlossen.

Der Dienstleister speichert den Hashwert 1 erzeugt zum Zwecke der späteren Verifizierung des Hashwerts über einen anderen Hashalgorithmus einen weiteren Hashwert (Hashwert 2). Beide Hashwerte werden zum Zwecke der späteren Verifikation dauerhaft im Corona-Zertifikat-System gespeichert. Der Dienstleister erhält keinen Zugriff auf die Patientendaten oder Probanden selbst.

Bei der Verifikation des Probenergebnisses erzeugt die Proband*in oder die Verifizierungsstelle aus den Patientendaten, den Probanden und dem nur bei ihm gespeicherten Geheimnis erneut einen Hashwert. Auf die Initiative der Proband*in wird dieser Hashwert an den Dienstleister übermittelt und abgeglichen, ob dieser Hashwert im Corona-Zertifikat-System des Dienstleisters bereits gespeichert ist. Der Dienstleister meldet zurück, ob das behauptete Probenergebnis (positiv/ negativ) stimmt, und aus dem angegebenen Labor und von dem angegebenen Zeitpunkt stammt. Der Dienstleister kann aus dem übermittelten Hashwert keinen Rückschluss auf den Probanden ziehen.

Speicherdauer und Löschung

Wir speichern die Daten solange, wie der Proband seine auf die Speicherung gerichtete Einwilligung nicht widerrufen hat. Eine Löschung von Hashwerten ist nur möglich, wenn der Proband diesen Hashwert unter Nutzung der Patientendaten, der Probanden und des Geheimnisses erneut erzeugt und an uns oder den Dienstleister übermittelt und um Löschung dieses Hashwerts bittet. Ohne diese Daten ist eine Zuordnung von gespeicherten Hashwerten zu Probanden nicht möglich und dementsprechend auch eine Löschung weder möglich noch erforderlich.

Weitere Daten mit Personenbezug sind zu dem Probanden nicht gespeichert.

Betroffenenrechte

Der Proband hat das Recht:

- gem. Art. 7 Abs. 3 DSGVO eine einmal erteilte Einwilligung jederzeit gegenüber uns zu widerrufen. Dies hat zur Folge, dass wir die Datenverarbeitung, die auf dieser Einwilligung beruhte, für die Zukunft nicht mehr fortführen dürfen;
- gem. Art. 15 DSGVO Auskunft über seine von uns verarbeiteten personenbezogenen Daten zu verlangen. Insbesondere kann er Auskunft über die Verarbeitungszwecke, die Kategorie der personenbezogenen Daten, die Kategorien von Empfängern, gegenüber denen seine Daten offengelegt wurden oder werden, die geplante Speicherdauer, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts, die Herkunft ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten verlangen;
- gem. Art. 16 DSGVO unverzüglich die Berichtigung unrichtiger oder Vervollständigung seiner bei uns gespeicherten personenbezogenen Daten zu verlangen;

- gem. Art. 17 DSGVO die Löschung seiner bei uns gespeicherten personenbezogenen Daten zu verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist;
- gem. Art. 18 DSGVO die Einschränkung der Verarbeitung seiner personenbezogenen Daten zu verlangen, soweit die Richtigkeit der Daten von ihm bestritten wird, die Verarbeitung unrechtmäßig ist, er aber deren Löschung ablehnt und wir die Daten nicht mehr benötigen, er jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen oder er gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung eingelegt hat;
- gem. Art. 20 DSGVO seine personenbezogenen Daten, die er uns bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen und
- gem. Art. 77 DSGVO sich bei einer Aufsichtsbehörde zu beschweren. In der Regel kann sich der Proband hierfür an die Aufsichtsbehörde seines üblichen Aufenthaltsortes oder Arbeitsplatzes oder unseres Unternehmenssitzes wenden.

Die bei dem Dienstleister gespeicherten Daten können weder von dem Labor noch von dem technischen Dienstleister einem Probanden zugeordnet werden. Die Ausübung von Betroffenenrechten setzt daher voraus, dass der Proband den Hashwert wie oben beschrieben erneut bildet und übermittelt.

Information über Ihr Widerspruchsrecht nach Art. 21 DSGVO

Der Proband hat das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung ihn betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 S. 1 lit. e DSGVO (Datenverarbeitung im öffentlichen Interesse) oder Art. 6 Abs. 1 S. 1 lit. f DSGVO (Datenverarbeitung auf Grund berechtigter Interessen) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling von Artikel 4 Nr. 4 DSGVO

Legt der Proband Widerspruch ein, werden wir seine personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die seine Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Sofern sich sein Widerspruch gegen eine Verarbeitung von Daten zum Zwecke der Direktwerbung richtet, werden wir die Verarbeitung umgehend einstellen. In diesem Fall ist die Angabe einer besonderen Situation nicht erforderlich. Dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

Möchte der Proband von seinem Widerspruchsrecht Gebrauch machen, genügt eine E-Mail an datenschutz@ubirch.com.

Datensicherheit

Wir bedienen uns geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, um die Patientendaten und Probandendaten gegen zufällige oder vorsätzliche Manipulationen, teilweisen oder vollständigen Verlust, Zerstörung oder gegen den unbefugten Zugriff Dritter zu schützen. Unsere Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert.

Keinen Einfluss haben wir auf die Sicherheit der lokalen Speicherung von personenbezogenen Daten auf den Endgeräten des Probanden. Dort bestehende Sicherheitsrisiken (insbesondere Risiken im

Umgang mit dem jeweiligen Endgerät) können von uns nicht kontrolliert werden. Lokal gespeicherte Daten können nur vom Probanden selbst gegen unbefugten Zugriff und Verlust geschützt werden.

Stand: 5.6.2020