QuoVadis Datenschutzhinweise – Digitale Zertifikate und Signaturlösungen (Schweiz)

Diese Datenschutzhinweise von QuoVadis beziehen sich auf die für die Schweiz erbrachten Zertifikats- und Signaturdienstleistungen der QuoVadis Trustlink Schweiz AG (QVTLSAG). Bezüglich Zertifikaten und Signaturlösungen für EU-Länder lesen Sie bitte unsere separaten Datenschutzhinweise hier.

Wir nehmen den Schutz Ihrer Daten sehr ernst und nutzen Ihre personenbezogenen Daten ausschließlich dazu, um die angeforderten Produkte und Services bereitzustellen.

Wer sind wir?

Die QVTLSAG ist ein Schweizer Vertrauensdienstanbieter gemäß dem Schweizer Bundesgesetz über die elektronische Signatur (ZertES). Wir stellen verwaltete PKI-Dienste (Public Key Infrastructure) zur Verfügung, unter anderem digitale Zertifikate und digitale Signaturen. Die QVTLSAG ist eine Tochtergesellschaft der DigiCert, Inc., die Teil der DigiCert Group ist.

Wer sind unsere Datenschutzbeauftragten?

Unser Datenschutzbeauftragter ist Aaron Olsen (E-Mail: privacy@digicert.com).

Welche Daten werden erfasst?

Wir erfassen die Daten, die für die Bereitstellung der Dienstleistungen erforderlich sind, die wir erbringen.

Zertifikatsinhalt

Folgende personenbezogene Daten können möglicherweise in persönlichen digitalen Zertifikaten enthalten sein:

- Vorname
- Nachname
- Pseudonym (gegebenenfalls)
- Common Name
- E-Mail-Adresse
- Titel (z. B. Herr/Frau/Dr.)
- Position (berufliche Stellenbezeichnung)
- Unternehmen/Firma (gegebenenfalls)
- Kennung der Rechtsform des Unternehmens/der Firma (gegebenenfalls)
- Abteilung (gegebenenfalls)
- Seriennummer (gegebenenfalls)
- Adressenattribute (gegebenenfalls)
- Nummer eines von staatlicher Seite ausgegebenen Ausweisdokuments (z. B. Reisepass, Führerschein). Nur falls ausdrücklich vom Kunden angefordert.

Registrierungsdaten

Personenbezogene Daten, die nicht in persönlichen digitalen Zertifikaten enthalten sind, aber im Rahmen der Ausstellung von Zertifikaten angefordert werden können (zum Beispiel zur Überprüfung der Identität einer Person). Diese Daten können Folgendes beinhalten:

- Adressenattribute
- Telefonnummer
- Ausweisdokumentdaten (zur Identitätsüberprüfung)
- Handelsregisterdaten und Berechtigungsnachweis

Kontodaten

Personenbezogene Daten werden auch benötigt, um ein Benutzerkonto in unserem Zertifikatsverwaltungssystem oder im Rahmen unserer Signaturlösungen zu erstellen. Diese personenbezogenen Daten bestehen aus:

- Vorname
- Nachname
- Benutzername (vom Nutzer ausgewählt)
- E-Mail-Adresse
- Telefonnummer
- Passwort (vom Nutzer ausgewählt)
- Mobiltelefonnummer
- Geheime PIN und/oder Einmalpasswort

Bestimmte digitale Zertifikate, zum Beispiel Gerätezertifikate, enthalten keine personenbezogenen Daten. Es können aber im Rahmen der Beantragung solcher Zertifikate personenbezogene Daten angefordert werden: unter anderem Name, Position, E-Mail-Adresse und Telefonnummer der in die Zertifikatsanforderung und in den Genehmigungsprozess eingebundenen Personen.

Personen, die sich über eine Remote-Identitätsprüfung registrieren, sollten unsere Datenschutzhinweise hier lesen.

Bitte beachten Sie, dass wir nicht die zu unterzeichnenden Dokumente erhalten, sondern lediglich einen kryptografischen Hash des Dokuments. Unsere Signaturlösungen protokollieren die Systemnutzung und die Informationen der stattfindenden Dokumentensignierung.

Warum erfassen wir diese Informationen?/Rechtliche Grundlage für die Verarbeitung

Wir benötigen eine Reihe von Informationen, um unseren Geschäftsbetrieb zu unterhalten. In einigen Fällen können diese Informationen Daten enthalten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Diese werden als personenbezogene Daten bezeichnet.

Der Grund für die Erfassung Ihrer personenbezogenen Daten ist, dass wir diese benötigen, um Ihnen unsere Produkte und Dienstleistungen bereitzustellen, unter anderem die Bereitstellung von digitalen Zertifikaten und Signaturdiensten.

Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Zusammenhang mit diesen Dienstleistungen durch uns ist die Erforderlichkeit der Datenverarbeitung für die Erfüllung eines Vertrags oder für Verarbeitungsvorgänge, die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind (bei Kunden, die als natürliche Person handeln), oder unser berechtigtes Interesse und das berechtigte Interesse unserer Kunden für den Zweck der Bereitstellung von Services für unsere Kunden, wenn diese Services voraussetzen, dass Daten von natürlichen Personen als Vertreter unserer Kunden verarbeitet werden (bei Kunden, die als juristische Person handeln). Personen, die sich über eine Remote-Identitätsprüfung registrieren, sollten unsere Datenschutzhinweise hier lesen.

Wer erfasst diese Informationen?

Wir erfassen Daten direkt von Ihnen oder indirekt von den Organisationen, die mit uns Verträge geschlossen haben (zum Beispiel zur Anforderung von Zertifikaten für deren Mitarbeiter oder zur Bereitstellung von digitalen Onboarding-Dienstleistungen). Wir können auch die Dienste Dritter für die Erfassung Ihrer Daten nutzen (zum Beispiel Dienstleister zur Überprüfung von Ausweisdokumenten). Wenn wir solche Dritten einsetzen, dann handeln diese gänzlich auf unsere Weisung und als Datenverarbeiter. Sie speichern Ihre Daten nicht und nutzen sie auch nicht zu anderen Zwecken als uns diese bereitzustellen.

Wie werden diese Daten genutzt?

Wir verwenden personenbezogene Daten nur für Produkte und Dienstleistungen, zu deren Bereitstellung wir uns vertraglich verpflichtet haben.

An wen werden die Daten weitergegeben?

Wir leiten Ihre personenbezogenen Daten nicht an andere weiter, außer zur Erbringung der vereinbarten Dienstleistungen. Gelegentlich können Informationen innerhalb der DigiCert Group weitergegeben werden, um bei Bedarf die Einhaltung von Audit- und Compliance-Vorgaben sicherzustellen bzw. Probleme an Vorgesetzte zur Klärung weiterzuleiten. Telefonnummern können an internationale SMS-Dienstleister gesandt werden, um Einmalpasswörter im Rahmen des Signaturverfahrens zuzusenden, wenn Kunden dies anfordern.

Wo werden die Daten gespeichert?

Personenbezogene Daten, die im Rahmen unserer Schweizer Zertifikate und Signaturlösungen für die Zwecke von digitalen Zertifikaten und elektronischen Signaturen zur Verfügung gestellt werden, werden in der Schweiz und im EWR (Niederlande) gespeichert und verarbeitet.

Informationen, die in unseren Büros aufbewahrt werden, umfassen unter anderem Verträge, Kundenkontaktdaten und Nachweise als Belege für die Ausstellung der digitalen Zertifikate. Dies gilt sowohl für physische Dokumente als auch für elektronische Daten.

Wie werden Ihre Daten geschützt?

Wir nutzen eine Kombination aus technischen, administrativen, organisatorischen und physischen Schutzmechanismen, um Ihre personenbezogenen Daten sicher zu halten. Es haben nur die Personen Zugang zu Ihren personenbezogenen Daten, für die dies zum Zweck der Servicebereitstellung erforderlich ist. Diese Schutzmechanismen werden im Rahmen unserer jährlichen Audits und Akkreditierungsverfahren geprüft. Einzelheiten entnehmen Sie bitte den Details zu unseren Akkreditierungen und technischen und organisatorischen Maßnahmen.

Aufbewahrungsfristen

Die Zertifikatsrichtlinie (CP) bzw. Zertifizierungspraxiserklärung (CPS) von QuoVadis (siehe https://www.quovadisglobal.com/repository/) fordert, dass Audit-Logs im Falle von Schweizer qualifizierten/regulierten Zertifikaten über einen Zeitraum von mindestens elf Jahren archiviert werden. Bitte beachten Sie, dass diese Frist zu laufen beginnt, wenn das Zertifikat abgelaufen ist.

Ihre Rechte

Wir halten uns an alle maßgeblichen Datenschutzgesetze und -vorschriften. Diese Regelungen sehen

eine Reihe von Rechten in Bezug auf Ihre personenbezogenen Daten vor.

Sie haben das Recht, von uns Zugang zu Ihren personenbezogenen Daten und deren Berichtigung oder Löschung zu fordern, sowie das Recht auf Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und unter bestimmten Umständen auch das Recht auf Datenübertragbarkeit.

Wenn Sie Ihre Zustimmung zur Verarbeitung Ihrer Daten erteilt haben, haben Sie (unter bestimmten Umständen) das Recht, diese Zustimmung jederzeit zu widerrufen. Dies wirkt sich jedoch nicht auf die Rechtmäßigkeit der Verarbeitung vor Widerruf Ihrer Zustimmung aus.

Sie haben das Recht, Beschwerde bei der entsprechenden Datenschutzbehörde einzureichen, falls Sie glauben, dass wir unsere gesetzlichen Pflichten nicht erfüllt haben. Nähere Informationen zu den EU-Datenschutzbehörden finden Sie hier. Nähere Informationen zu den Schweizer Datenschutzbehörden finden Sie hier.

Wenn Sie Ihre oben besprochenen Rechte ausüben möchten, stellen Sie Ihren Antrag bitte über unser Formular für Datenschutzanträge; Sie können sich, falls Sie Fragen haben, auch per E-Mail an die folgende Adresse wenden: privacy@digicert.com

Automatisierte Entscheidungsfindung und Profiling

Eine automatische Entscheidung wird als eine Entscheidung definiert, die nach Verarbeitung von personenbezogenen Daten alleine durch automatisch ablaufende Prozesse getroffen wird, bei denen kein Mensch in den Entscheidungsfindungsprozess eingebunden ist. Außer im Fall unserer optionalen Remote-Identitätsprüfung nutzen wir keine automatisierte Entscheidungsfindung bei der Verarbeitung von personenbezogenen Daten. Personen, die sich über eine Remote-Identitätsprüfung registrieren, sollten unsere Datenschutzhinweise hier lesen.

Wir nutzen kein Profiling.

Zu diesen Datenschutzhinweisen

So wie sich unsere Organisation weiterentwickelt, werden sich auch unsere Datenschutzhinweise über die Zeit ändern. Diese Datenschutzhinweise können regelmäßig aktualisiert werden, um unseren sich ändernden Umgang mit personenbezogenen Daten widerzuspiegeln. Sie sollten unsere Website regelmäßig besuchen, um Kenntnis der jeweils aktuell gültigen Datenschutzhinweise zu haben.

Diese Datenschutzhinweise wurden zuletzt am 8. Juni 2023 aktualisiert.

Kontakt

Falls Sie Fragen zu diesen Datenschutzhinweisen haben, wenden Sie sich bitte per E-Mail an: privacy@digicert.com