PRIVACY POLICY

For certificate products ordered via the request website or WebRA

ENGLISH

DATENSCHUTZERKLÄRUNG

Für Zertifikatsprodukte, die über die Antragswebseite oder die WebRA bestellt werden.

DEUTSCH

INFORMATION FOR DATA SUBJECTS

PRIVACY POLICY

For certificate products ordered via the request website or WebRA

We are extremely committed to protecting your data. This Privacy Policy contains comprehensive information on how D-TRUST GmbH, a subsidiary of Bundesdruckerei GmbH, uses your data.

1. How to contact us:

D-TRUST GmbH
Kommandantenstr. 15
10969 Berlin
https://www.bundesdruckerei.de
info@d-trust.net
Tel.: +49 30 25 98 0
Company data protection officer: Uta Roßberg datenschutz@d-trust.net

2. Scope of processing

a) Categories of personal data that is processed

The following information of the requester is processed: certificate, contact, order and invoice data, revocation password hashes, identification data, results of sanction list checks and export controls, if necessary, copies of the ID document (passport, ID card or other ID documents) as well as documentation of support/service cases.

In the case of ID copies that have not been redacted, the access number (CAN) and special categories of personal data will be transmitted in the form of a photograph (biometric photo). The photograph is so-called biometric data that enables clear identification. In cases like these, consent to data processing also refers to this data.

In addition, authorized signatories, third parties authorized to revoke and the identifying persons (government employees, chamber employees, notaries (NotarIDENT), officers (WebRA), postal employees (PostIDENT), embassy employees) process contact data and the confirmation that they have carried out identification.

IP address pairs, access times and encrypted input content of all users of our Internet service are processed.

In legally justified cases, inquiries regarding data subject rights and data transfers will be documented in accordance with section 8 (2) of the German Trusted Services Act (VDG, *Vertauensdienstegesetz*).

b) Sources of personal data

The data of the requesters, authorized signatories and third parties authorized to revoke is collected directly via the request page or within a WebRA procedure managed by an officer. Within the scope of verifying the request data, identifying persons, authorized signatories, the personnel department or superiors are contacted and involved in clarifying the correctness of the certificate data and authorizations.

The data of persons involved in the identification or confirmation process is collected directly during the course of their work.

Service and support requests as well as any queries regarding data subject rights shall be sent to us directly by the data subjects.

© D-TRUST GmbH

c) Data storage period

The traceability of the identification which serves as the basis for issuing a certificate is a quality feature of the certificate. The statutory storage periods or those specified in certifications depend on the specific product.

In the case of qualified signature and seal certificates, the provisions of section 16 (4) VDG on permanent storage apply to certificates, identification data, including contact data. This corresponds to the entire duration of operations by the trust service provider. Before discontinuing its operations, the trust service provider is required to hand over the data to the Federal Network Agency or another qualified trust service provider.

All other identification data will be deleted eight years after the validity of the last certificate issued on the basis of this data has expired. The same applies to certificates. The revocation password hash is deleted at the latest one year after the validity of the last certificate issued on the basis of this data has expired. The paper copy of the ID card is scanned and will be destroyed 21 days after receipt. The scan will be deleted after the certificate has been activated or the request cancelled.

Invoice data is deleted after ten years.

Documentation of information provided pursuant to section 8 (2) VDG is stored for twelve months.

IP address pairs and access times are kept for two years due to the certification requirement and are then deleted.

d) Purpose of processing

Your data will be processed for the following purposes: to establish the identity of the requester, to check a request and for handling, billing, observing documentation obligations, to warrant the certificate life cycle including revocation and operation of the repository service (status information service), checking cost efficiency and quality, for statistical purposes (anonymised) and in individual cases for troubleshooting, especially in the case of support requests.

Data processing is also carried out as part of measures to maintain information security, especially to detect and ward off attacks, including internal and external audits, export control and sanctions list checking.

In the case of enquiries pursuant to section 8 (2) VDG, the information provided is sent to the competent offices.

e) Legal basis for processing

Certificates and identification data, contact data, order data, invoice data, revocation password hashes, documentation of support/service cases are processed in order to perform the contract with the data subject.

eIDAS Regulation (No. 910/2014) and the Trusted Services Act provide the legal framework for trust services.

The consent of the data subject is obtained in order to copy the ID card, passport or other ID document.

Section 8 (2) VDG provides the legal basis for sending the information provided to competent offices.

Data subject requests are processed pursuant to Art. 12 - 23 GDPR or sections 32 - 37 of the Federal Data Protection Act (BDSG, *Bundesdatenschutzgesetz*).

The information provided is sent to affiliated group companies after weighing up the interests of all sides.

f) Legitimate interests

D-TRUST has a legitimate interest within the meaning of Art. 6 (1) f GDPR in the following cases:

Information security and preventive measures are carried out using technical and organizational measures, including incident handling, in order to assess and prevent possible damage to the company (D-TRUST), the data subjects whose data has been processed and to the trust service users.

The controller is part of a company group. Within the meaning of Recital 48 EU GDPR, Bundesdruckerei GmbH, as the parent company, has a legitimate interest in processing certain data centrally. Sanctions list and export control checks, dunning, sales activities and parts of the support service are performed by Bundesdruckerei.

g) Necessity to collect data

As a trust service provider, the controller is obliged to ensure the identity of the subscriber. The data marked as mandatory fields must be processed in order to meet with this obligation. If data is incorrect or not provided, it will not be possible to issue the certificate. The same applies to submitting proof, such as organizational affiliation or professional attributes. Without proof, the data cannot be included in the certificate.

3. Forwarding and foreign reference

In order to perform support services, the necessary data will be sent to the customer service unit of Bundesdruckerei GmbH and iNCO Spólka z o.o. (subsidiary of Bundesdruckerei in Poland).

In addition, officers and identifying persons, auditors, supervisory authorities and, if necessary, competent authorities pursuant to section 8 (2) VDG can access the respective data.

Within the scope of export control, the name and organization are sent to Bundesdruckerei's sanctions list server. If matches fail, the date of birth, place of birth and nationality as well as the name at birth are used. In addition, the dispatch address, the country of dispatch, the invoice recipient’s address and, if applicable, other partners are assessed by Bundesdruckerei with a view to export control law.

Sales activities and dunning procedures are also carried out by Bundesdruckerei.

There is no procedure in place nor the intention to transfer personal data to a third country or to an international organization.

4. Rights of data subjects

If you have any requests for information regarding your data and its correction, deletion or restriction regarding processing, please send this to the postal address shown above or signed to datenschutz@d-trust.net. The same applies if you wish to object to processing within the meaning of Art 21 of the GDPR or if you have a query regarding data portability.

If you wish to revoke your consent to the processing of your ID card copy, please send your signed revocation request to Bundesdruckerei GmbH, c/o D-TRUST GmbH, Antragsbearbeitung, Kommandantenstraße 15, 10969 Berlin, Germany, stating your request ID for authentication. The copy of your ID card will then be deleted immediately.

If you have any questions or complaints regarding a procedure, please contact us using one of the contact options listed above. If you have any other reason for complaint, you can also contact our supervisory authority (Berlin Commissioner for Data Protection and Freedom of Information, Friedrichstr. 219, 10969 Berlin, Germany).

INFORMATIONEN FÜR BETROFFENE

DATENSCHUTZERKLÄRUNG

Für Zertifikatsprodukte, die über die Antragswebseite oder die WebRA bestellt werden

Der Schutz Ihrer Daten ist uns sehr wichtig. Mit dieser Datenschutzerklärung erhalten Sie umfassende Informationen zur Verwendung Ihrer Daten bei der D-TRUST GmbH, einer Tochter der Bundesdruckerei GmbH.

1. So können Sie uns kontaktieren:

D-TRUST GmbH
Kommandantenstr. 15
10969 Berlin
https://www.bundesdruckerei.de
info@d-trust.net
Telefon: +49 30 25 98 0
Betriebliche Datenschutzbeauftragte: Uta Roßberg datenschutz@d-trust.net

2. Verarbeitungsrahmen

a) Kategorien personenbezogener Daten, die verarbeitet werden

Vom Antragssteller werden Zertifikats-, Kontakt-, Bestell- und Rechnungsdaten, Sperrpassworthashs, Zertifikatsnachweisdaten, Ergebnisse von Sanktionslistenprüfungen und Exportkontrolle, ggf. Ausweiskopien (Reisepass, Ausweis und andere ID-Dokumente), Dokumentationen zu Support-/Servicefällen verarbeitet.

Bei Ausweiskopien, die nicht geschwärzt wurden, werden die Zugangsnummer (CAN) und besondere Kategorien personenbezogener Daten in Form eines Lichtbilds (biometrisches Foto) übermittelt. Es handelt sich bei dem Lichtbild um sogenannte biometrische Daten, die eine klare Identifizierung erlauben. In einem solchen Fall bezieht sich die Einwilligung zur Datenverarbeitung auch auf diese Daten.

Außerdem werden von Zeichnungsberechtigten, Sperrberechtigten Dritten und den identifizierenden Personen (Behördenmitarbeiter, Kammermitarbeiter, Notare (NotarIDENT), Officer (WebRA), Postmitarbeiter (PostIDENT), Botschaftsmitarbeiter) Kontaktdaten und die Bestätigung ihrer Identifizierungsleistung verarbeitet.

Von allen Nutzern unseres Internetangebots werden IP-Adress-Paare, Zeitpunkte des Zugriffs, verschlüsselte Eingabeinhalte verarbeitet.

In rechtlich begründeten Fällen werden Anfragen zu Betroffenenrechten und Datenübermittlungen gemäß §8 Abs. 2 VDG dokumentiert.

b) Quelle der personenbezogenen Daten

Daten der Antragsteller, Zeichnungsberechtigten und sperrberechtigten Dritten werden über die Antragsseite oder innerhalb eines durch einen Officer geführten WebRA-Verfahrens direkt erhoben. Im Rahmen der Verifikation der Antragsdaten werden identifizierende Personen, Zeichnungsberechtigte, Personalabteilung bzw. Vorgesetzte kontaktiert und in die Klärung der Korrektheit der Zertifikatsdaten und Berechtigungen einbezogen.

Die Daten von am Identifikations- oder Bestätigungsprozess beteiligten Personen werden im Zuge ihrer Tätigkeit direkt erhoben.

Service- und Supportanfragen sowie Anfragen zu Betroffenenrechten stellen Betroffene uns gegenüber direkt.

© D-TRUST GmbH

c) Dauer der Speicherung

Die Nachvollziehbarkeit der Identifizierung auf deren Grundlage ein Zertifikat ausgestellt wird, ist ein Qualitätsmerkmal des Zertifikates. Die gesetzlichen oder in Zertifizierungen vorgegebenen Aufbewahrungsfristen sind produktabhängig umgesetzt.

Für qualifizierte Signatur- und Siegelzertifikate gelten für Zertifikate, Zertifikatsnachweisdaten, einschließlich der Kontaktdaten die Vorgaben des § 16 Abs. 4 Vertrauensdienstegesetz zur dauerhaften Aufbewahrung. Dies entspricht der gesamten Dauer des Betriebes des Vertrauensdiensteanbieters. Vor Aufgabe des Betriebs ist, die Übergabe an die Bundesnetzagentur oder einen anderen qualifizierten Vertrauensdiensteanbieter vorgeschrieben.

Alle anderen Zertifikatsnachweisdaten werden 8 Jahre nach Ablauf der Gültigkeit des letzten auf den Daten ausgestellten Zertifikates gelöscht. Gleiches gilt für die Zertifikate. Der Sperrpassworthash wird spätestens ein Jahr nach Ablauf der Gültigkeit des letzten auf den Daten ausgestellten Zertifikates gelöscht. Die Ausweiskopie wird nach Posteingang eingescannt. Die Papierkopie wird 21 Tage nach Posteingang vernichtet. Der Scann wird nach Freischaltung des Zertifikates oder Stornierung des Antrags gelöscht.

Rechnungsdaten werden nach 10 Jahre gelöscht.

Dokumentationen zu Übermittlungen gemäß §8 Abs. 2 VDG werden zwölf Monate aufbewahrt.

IP-Adress-Paare und Zeitpunkte des Zugriffs werden aufgrund der Zertifizierungsanforderung zwei Jahre aufbewahrt und anschließend gelöscht.

d) Zwecke der Verarbeitung

Ihre Daten werden für die folgenden Zwecke verarbeitet: zur Feststellung der Identität des Antragstellers, Antragsprüfung und -abwicklung, Abrechnung, Wahrung der Dokumentationspflichten, Gewährleistung des Zertifikatslebenszyklus einschließlich Sperrung und Betrieb des Verzeichnisdienstes (Statusauskunftsdienst), Wirtschaftlichkeits- und Qualitätsprüfung, für statistische Zwecke (anonymisiert) und in Einzelfällen zur Fehlerbehebung insbesondere bei Supportanfragen.

Im Rahmen der Maßnahmen zur Aufrechterhaltung der Informationssicherheit insbesondere zum Erkennen und Abwehren von Angriffen, einschließlich interner und externer Auditierung, der Exportkontrolle und der Sanktionslistenprüfung findet ebenfalls Datenverarbeitung statt.

Im Fall von Anfragen gemäß §8 Abs. 2 VDG werden Übermittlungen an zuständige Stellen vorgenommen.

e) Rechtsgrundlage für die Verarbeitung

Zertifikate und Zertifikatsnachweisdaten, Kontaktdaten, Bestelldaten, Rechnungsdaten, Sperrpassworthashs, Dokumentation zu Support-/Servicefällen werden verarbeitet zur Erfüllung des Vertrags mit dem Betroffenen.

Die eIDAS-Verordnung (Nr. 910/2014) und das Vertrauensdienstegesetz stellen den gesetzlichen Rahmen für die Vertrauensdienste.

Für die Kopie des Ausweises, Reisepasses oder sonstigen ID-Dokuments wird die Einwilligung des Betroffenen eingeholt.

Rechtsgrundlage für Übermittlungen an zuständigen Stellen ist §8 Abs. 2 VDG.

Betroffenenanfragen werden auf Grundlage der Art. 12 – 23 DSGVO bzw. § 32-37 BDSG verarbeitet.

Die Übermittlungen an die verbundenen Konzernunternehmen erfolgen aufgrund von Interessensabwägungen.

f) Berechtigte Interessen

Ein berechtigtes Interesse der D-TRUST im Sinne von Art. 6 Abs. 1 lit. f DSGVO liegt in folgenden Fällen vor:

Es werden Maßnahmen der Informationssicherheit einschließlich der Prävention durch technische und organisatorische Maßnahmen einschließlich der Vorfallsbehandlung durchgeführt, um mögliche Schäden für das Unternehmen (D-TRUST), für die von der Datenverarbeitung Betroffenen und für die Nutzer der Vertrauensdienste abzuschätzen und zu verhindern.

Die Verantwortliche ist Teil einer Unternehmensgruppe. Die Bundesdruckerei GmbH als Mutterunternehmen hat im Sinne EW 48 DSGVO ein berechtigtes Interesse bestimmte Verarbeitungen zentral abzuwickeln. Die Sanktionslisten- und Exportkontrollprüfung, Mahnwesen, Vertriebstätigkeit und Teile des Supports werden durch die Bundesdruckerei erbracht.

g) Erforderlichkeit der Daten

Die Verantwortliche ist als Vertrauensdiensteanbieter verpflichtet die Identität der Zertifikatsnehmer sicherzustellen. Die Verarbeitung der als Pflichtfelder gekennzeichneten Daten ist notwendig, um dieser Verpflichtung nachzukommen. Bei Nichtangabe oder Falschangabe kann das Zertifikat nicht ausgestellt werden. Gleiches gilt für die Einreichung von Nachweisen, wie beispielsweise Organisationszugehörigkeit oder Berufsattribute. Ohne Nachweis können die Daten nicht in das Zertifikat aufgenommen werden.

3. Weitergabe und Auslandsbezug

Zur Erbringung der Supportdienstleistung werden die erforderlichen Daten dem Customer Service der Bundesdruckerei GmbH sowie der iNCO Spólka z o.o. (Tochterunternehmen der Bundesdruckerei in Polen) übermittelt.

Des Weiteren erhalten Officer und identifizierende Personen, Auditoren, Aufsichtsbehörden, ggf. zuständige Stellen gemäß §8 Abs. 2 VDG Zugriff auf die jeweils erforderlichen Daten.

Im Rahmen der Exportkontrolle werden Name und Organisation an den Sanktionslistenserver der Bundesdruckerei übermittelt. Im Fall von Fehltreffern werden Geburtsdatum, Geburtsort und Staatsangehörigkeit sowie Geburtsname herangezogen. Zusätzlich werden Versandadresse, Versandland, Adresse des Rechnungsempfängers und ggf. weiterer Partner durch die Bundesdruckerei exportkontrollrechtlich bewertet.

Vertriebstätigkeit und Mahnwesen werden ebenfalls durch die Bundesdruckerei erbracht.

Es besteht weder die Praxis noch die Absicht die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln.

4. Betroffenenrechte

Sollten Sie Anfragen zur Auskunft über Ihre Daten oder deren Berichtigung, Löschung oder Einschränkung der Verarbeitung haben, richten Sie diese bitte an die obenstehende Postadresse oder signiert an datenschutz@d-trust.net. Gleiches gilt, falls Sie im Sinne des Art. 21 DSGVO Widerspruch gegen die Verarbeitung einlegen wollen oder eine Anfrage zur Datenübertragbarkeit haben.

Sollten Sie Ihre Einwilligung zur Verarbeitung Ihrer Ausweiskopie widerrufen wollen, senden Sie uns bitte Ihren unterschriebenen Widerruf an Bundesdruckerei GmbH, c/o D-TRUST GmbH, Antragsbearbeitung, Kommandantenstraße 15, 10969 Berlin unter Angabe Ihrer Antrags-ID zur Authentifizierung. Ihre Ausweiskopie wird dann unverzüglich gelöscht.

Sollten Sie Fragen oder Beschwerden zu einem Verfahren haben, wenden Sie sich bitte über die oben genannten Kontaktmöglichkeiten an uns. Sollten Sie darüber hinaus Grund für Beschwerden sehen, besteht für Sie die Möglichkeit, sich an unsere Aufsichtsbehörde (Berliner Beauftragte für Datenschutz und Informationsfreiheit, Friedrichstr. 219, 10969 Berlin) zu wenden.