



Federal Ministry
of the Interior
and Community

Privacy Policy

for users of the Online Access Act-compliant Invoice Submission Portal
(OZG-RE)

Last updated: 08 December 2021

General note

Handling personal data responsibly is a top priority for the federal administration. We want to ensure that users know when and which data are collected and used when using the Invoice Submission Portal which complies with the Online Access Act (OZG-konforme Rechnungseingangsplattform – hereinafter referred to as the “OZG-RE”).

1. Name and address of the controller

The Federal Ministry of the Interior and Community (BMI) is responsible for processing personal data:

Federal Ministry of the Interior and Community (BMI)

Alt-Moabit 140
10557 Berlin

Tel.: 030 / 18 681-0
Fax: 030 / 18 681-12926
E-Mail: poststelle@bmi.bund.de

2. Name and address of the processor

Bundesdruckerei GmbH (bdr)

Kommandantenstr. 18
10969 Berlin
Germany

3. Obligation of the controller

The Federal Ministry of the Interior and Community (BMI) is responsible for the care and maintenance of the OZG-RE and undertakes to fulfil all data privacy requirements for the portal.

The BMI is also responsible for the portal as a website and for registration and authentication for the service account of the Federation. The BMI undertakes to fulfil all data privacy requirements for the portal and the service account, in particular:

- ensuring that data is processed lawfully,
- establishing, amending, developing and complying with specialist and technical requirements,
- protecting the rights of data subjects, and
- fulfilling the information requirements.

4. Name and address of the data protection officer

Data Protection Officer (BDS) for the Federal Ministry of the Interior (BMI)

Alt-Moabit 140
10557 Berlin

Tel.: 030 / 18 681-0

E-Mail: bds@bmi.bund.de

5. Which personal data are processed when using the OZG-RE?

5.1. Visiting the OZG-RE website

The OZG-RE website is accessed via an encrypted HTTPS connection. When the website is accessed, the following technical processes and events are recorded and stored in a log file:

- destination address
- user's IP address
- date and time of access
- protocol version, HTTP method, referrer, user agent string (generally includes the name and version of the browser and possibly also the operating system of the accessing device)
- name of file retrieved, and amount of data transferred in bytes
- notification of whether the request was successful or not (HTTP status code)

Technical and organisational safeguards ensure that only a defined group of suitably instructed administrators have access to log files. The stored data is not linked to the user's other personal data.

Storage period

The data are recorded in log files, where they are stored for a period of 90 days. After that time, the data are automatically deleted. Technical and organisational safeguards ensure that only a defined group of suitably instructed administrators have access to these data. These data are not combined with other data sources.

Legal basis and purpose of data processing

Article 6 (1) (e) of the GDPR in conjunction with section 3 of the Federal Data Protection Act (Bundesdatenschutzgesetz) provides the legal basis for the storage of personal data for the purposes of tracing and analysing possible errors in the system so that these errors can be swiftly rectified in the public interest, thus safeguarding the operation of the OZG-RE.

5.2. Use of cookies

Cookies are small pieces of data that a website can place locally in the memory of your web browser on your computer. They contain identifiers (randomly generated identification numbers), which the server can use to clearly identify requests coming from your access device. In this way, a request can also be clearly attributed to a specific user.

The OZG-RE website uses cookies in order to recognise your browser for the current session. Some of the functions of the website cannot be used without cookies. In order to provide these functions, it is essential that the user's browser can still be recognised after the user navigates to a different page on the site.

User data collected by cookies which are required for technical reasons are not used to compile user profiles.

Storage period

The cookies used in order to recognise the user's browser session are deleted either when the browser session ends or no later than 60 minutes after active use of the OZG-RE website.

Legal basis and purpose of data processing

The legal basis for the use of cookies in providing an invoice submission portal is Article 6 (1) (e) of the GDPR in conjunction with section 3 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*) and section 3 (2) of the Ordinance on Electronic Invoicing in Federal Public Procurement (*E-Rechnungsverordnung*).

Please note: *With any internet browser, you can see when cookies have been set and what they contain. Depending on which browser you use, you can set your browser to accept cookies in general, to accept only certain cookies or to reject all cookies. Your browser will usually also show you which cookies are stored on your access device so that you can delete all or some of them. This can also be done automatically. If cookies are deactivated for the OZG-RE website, however, it may not be possible to fully use all the functions of the website.*

5.3. Registering a company account / user account

In order to use the OZG-RE submission portal, the user must register via the OZG-RE website. This registration results in the creation of a company account and at least one associated user account. Additional user accounts can be added to the same company account.

Personal and company-related user data are collected and stored during the registration process and when creating accounts.

When a **company account** is created, the following data are stored:

- company account ID (automatically generated, hidden)
- company name (required)
- administrator rights (automatically linked to account)
- company address – street (optional)
- company address – postcode (optional)
- company address – town (optional)
- company language (required)
- company address – country (required)
- either VAT ID number or tax number (required)

Administrator rights enable the user to manage the company account that they have set up.

The following data are stored during the registration process when setting up a **user account for sending invoices**:

- first name and last name (required)
- password (required)
- email address (required)
- telephone number (optional)
- user ID (automatically generated, hidden)
- activation period (automatically generated, hidden)
- activation link ID (automatically generated, hidden)
- expiry date for activation link (automatically generated, hidden)
- language (default is German)
- After the user signs into their user account, the following data about the user's activity are stored:
 - user ID
 - date and time of user activity
 - description of user activity
 - description of result of user activity

Storage period

The data are deleted as soon as they are no longer needed for processing purposes. This is the case if the user's company account and associated user accounts are deleted. If changes are made to the details of the company account and associated user accounts, the new information is stored and the original information is deleted. A company account / user account will be suspended after 365 days of inactivity, and the user will be notified of this via email. The user will then be granted the option of lifting the suspension within a period of 30 days. If the user does not lift their suspension within this period, they will be removed entirely from the OZG-RE. Regardless of this, the user can re-register at a later date.

Please note that if a company account is deleted, the user accounts linked to that company account will also be deleted automatically.

At any time, the user may delete the company account or any of its associated user accounts or make changes to stored personal data.

Legal basis and purpose of data processing

The legal basis for the use of cookies in providing an invoice submission portal for the transmission of invoices to recipients who have access to the OZG-RE is Article 6 (1) (e) of the GDPR in conjunction with section 3 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*) and section 3 (2) of the Ordinance on Electronic Invoicing in Federal Public Procurement (*E-Rechnungsverordnung*).

6. Sharing your data with third parties

6.1. Transmitting invoices to recipients who have access to the OZG-RE

The user, via their user account, can submit electronic invoices to recipients who have access to the OZG-RE. The user can send invoices using various transmission methods, namely:

- web submission
- upload
- email
- Peppol

When an electronic invoice is submitted using one of the aforementioned transmission methods, the OZG-RE processes the following data in addition to the invoice content itself:

- date of receipt of the electronic invoice
- link between the electronic invoice and the user account of the user issuing the invoice
- record of receipt of the invoice

Please note: *From the moment when an invoice is sent via the OZG-RE, the invoice recipient is responsible for data privacy issues in the further processing of that invoice. Thereafter, the OZG-RE is only responsible for the technical platform through which the invoice recipient collects the invoice.*

Storage period

If an invoice was marked “Delivered” 28 days ago, or if there has been no change in status for 28 days, all documents, data from dashboards and logs from the database, including all personal data, are deleted from the metadata. Data required for producing monthly and quarterly reports, on the other hand, are deleted after 100 days. These data required for reporting purposes include the name of the organisation, the buyer reference (*Leitweg-ID*), status of the document, date of status changes, transmission method, etc.

Data connected to the processing of an invoice (invoice and invoice data) will generally be stored for five years by the invoice recipient in accordance with section 4.7 of the “administrative regulation for payments, accounting and invoicing” of the Federal Budget Code (*Verwaltungsvorschrift für Zahlungen, Buchführung und Rechnungslegung – Bundeshaushaltsordnung*). To allow for individual agreements in special cases, the storage period for electronic invoices may be extended in such cases by the competent authority.

Legal basis and purpose of data processing

The legal basis for the storage of data is Article 6 (1) (e) of the GDPR in conjunction with section 3 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*), section 3 (2) of the Ordinance on Electronic Invoicing in Federal Public Procurement (*E-Rechnungsverordnung*), and section 90 of the Federal Budget Code (*Bundeshaushaltsordnung*).

The processing of data serves the purpose of a) validating a submitted electronic invoice in accordance with the XRechnung standard in its current version, b) logging the status of a submitted electronic invoice, c) enabling a connection to be made between the electronic invoice and the user submitting the invoice, and d) forwarding the invoice to the competent federal authority to which it is addressed.

Invoice data is further processed by the invoice recipient solely with the purpose of processing the invoice in accordance with current budget and economic management regulations and to document adherence to these regulations (see section 90 of the Federal Budget Code).

6.2. Other recipients of your data

On the basis of Article 6 (1) (e) of the GDPR in conjunction with section 5 of the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*), the Federal Ministry of the Interior and Community (BMI) is required to store data beyond the time of your visit to the OZG-RE website in order to protect against attacks on the BMI's internet infrastructure and federal communications technology. Data logged when you access the BMI's websites are only shared with third parties if there is a legal requirement for this to be done, or if the data are needed for legal or criminal proceedings in case of attacks on federal communications technology. Otherwise, these data are not shared with third parties. The BMI does not combine these data with other data sources, for example to create user profiles.

Other recipients of personal data:

Data processing for the OZG-RE is carried out on behalf of the BMI by the government printing office Bundesdruckerei GmbH (Kommandantenstraße 18, 10969 Berlin). A contract on the basis of Article 28 (3) of the GDPR has been concluded with the Bundesdruckerei; the BMI is responsible for data privacy.

7. Contact

Questions relating to data privacy may be addressed to the Federal Ministry of the Interior and Community (BMI), which is the controller of the OZG-RE (see 1 and 3 above).

Users with specialist/technical questions related to the OZG-RE can contact the help desk by email (sendersupport-xrechnung@bdr.de).

You can contact the BMI by email using the address set up for questions and error reports (sendersupport-xrechnung@bdr.de) or the following central email address: poststelle@bmi.bund.de.

Personal data sent to the central email addresses and stored by the organisational unit responsible for distributing mail are deleted one year after being forwarded to the responsible organisational units within the BMI.

8. Your data privacy rights

You have the following rights vis-à-vis the BMI with regard to personal data concerning you:

- **Right of access, Article 15 of the GDPR**

This right gives data subjects comprehensive access to data concerning them and to a few other key criteria, such as the purpose of processing or the length of storage. Exceptions to this right are governed by section 34 of the Federal Data Protection Act (Bundesdatenschutzgesetz).

- **Right to rectification, Article 16 of the GDPR**

The right to rectification includes the option of having inaccurate personal data concerning the data subject corrected.

- **Right to erasure, Article 17 of the GDPR**

The right to erasure includes the option of having data concerning the data subject deleted by the controller. However, such data may be deleted only if they are no longer needed, if they were processed unlawfully or if consent covering their processing has been withdrawn. Exceptions to this right are governed by section 35 of the Federal Data Protection Act.

- **Right to restriction of processing, Article 18 of the GDPR**

This right enables data subjects to temporarily prevent further processing of personal data concerning them. Such a restriction is used above all when data subjects are examining whether to claim other rights.

- **Right to object to collection, processing and/or use, Article 21 of the GDPR**

The right to object includes the possibility for data subjects to object, in a particular situation, to the further processing of their personal data if this processing is justified by the performance of public tasks or of public and private interests. Exceptions to this right are governed by section 36 of the Federal Data Protection Act.

- **Right to data portability, Article 20 of the GDPR**

The right to data portability gives data subjects the option of receiving from the controller the personal data concerning them in a commonly used and machine-readable format in order to have them transmitted to another controller. According to Article 20 (3) sentence 2 of the GDPR, this right does not apply if the data processing is necessary to perform a task carried out in the public interest.

- **Right to withdraw consent, Articles 13 and 14 of the GDPR.**

If the personal data are processed on the basis of consent, data subjects can withdraw their consent at any time for the purpose in question. The lawfulness of processing on the basis of the consent remains unaffected until notification has been received that consent has been withdrawn.

You can claim these rights in writing using the contact information provided under number 1 above.

The right to lodge a complaint with a supervisory authority

If you think that the processing of your personal data infringes on your rights, you can lodge a complaint with the competent data protection supervisory authority (Article 77 GDPR):

Federal Commissioner for Data Protection and Freedom of Information (BfDI)

Husarenstraße 30
53117 Bonn

E-Mail: poststelle@bfdi.bund.de
<https://www.bfdi.bund.de/>