terranets bw

# » Data protection information according to Art. 13ff. GDPR in connection with the Telecommunications Act (TKG) and the Act to Regulate Data Protection and Privacy in Telecommunications and Telemedia (TTDSG) of terranets bw GmbH

**Data protection information**

| **Data protection information according to Art. 13 GDPR in connection with TKG and TTDSG** | |
|---|---|
| **Area** | **Data protection information in connection with contracts pertaining to the provision of telecommunication services (esp. internet and telephony) as well as services related thereto.** |
| **Short explanation** | Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following:<br>We take protecting your personal data very seriously. On the following pages, we wish to inform you on how your data is processed and what rights you have in connection with your personal data.<br>Within the scope of our business relationship, you are only required to provide the personal data that is necessary for establishing, executing and terminating the business relationship and for fulfilling the related contractual obligations or that we are legally obliged to collect.<br>This data protection information shall apply from 1 December 2021 as a result of the TKG legislative amendment and the new TTDSG. |

## I. Definitions

The General Data Protection Regulation and the Federal Data Protection Act that is based thereupon protect personal data. However, legal entities are not protected by this regulation. In this respect, the following information, insofar as it is based on the General Data Protection Regulation and/or the Federal Data Protection Act, shall apply to your rights exclusively in the case that you are not a legal entity.

This data protection declaration uses terms that are used in the General Data Protection Regulation (GDPR). Moreover, the terms of the Telecommunications Act (TKG) and the Act to Regulate Data Protection and Privacy in the Telecommunications and Telemedia (TTDSG) shall apply. The terms are listed, inter alia, in Art. 4 GDPR, Section 2 of the TTDSG and Section 3 of the TKG.

## II. Who is responsible for processing my data

Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following:
This data protection information shall apply for data processing by:

terranets bw GmbH
Am Wallgraben 135
70565 Stuttgart

## III. Data Protection Officer

You can reach the Data Protection Officer at the following address:

terranets bw GmbH
Am Wallgraben 135

70565 Stuttgart
Email: datenschutz@terranets-bw.de
Tel.: +49 711 7812 1312

**PLEASE NOTE:**
We are legally obliged to inform you of any breach of personal data protection if the conditions set out in Art. 34 GDPR are met and in cases specified in Section 168 TKG (amended by TKModG), i.e. when such a breach of personal data protection seriously affects or is likely to seriously affect your rights or legitimate interests.

For questions, uncertainties or complaints you can – irrespective of this – reach the Data Protection Officer at the contact address provided.

Pursuant to Section 168 (4) of the Telecommunications Act (TKG), we are obliged to inform you when disruptions originate from your data processing system. Insofar as it is technically possible and reasonable, we have the right to inform you of appropriate, effective and accessible technical means by which you can recognise and eliminate these disruptions. In this case, we are also allowed to redirect parts of the data traffic from and to you insofar as this is necessary to be able to inform you about the disruptions.

Pursuant to Section 168 (5) of the Telecommunications Act (TKG) the following shall apply: If we are informed by the Federal Office for Information Security about specific significant risks emanating from your data processing systems, we are obliged to inform you about them without delay. Insofar as it is technically possible and reasonable, we are required to inform you of appropriate, effective and accessible technical means by which you can recognise and prevent these risks.

**IV. Collecting and processing personal data**
Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following:
The categories of personal data set out below are collected by us and originate from the following data sources:

| **Category of personal data** | **Data source** |
|---|---|
| Master and inventory data in the sense of Section 3 No. 6 of the TKG and Section 2 (2) No. 2 of the TTDSG<br><br>Inventory data is data of an end user (i.e. a user according to Section 3 No. 13 of the TKG, who neither operates public telecommunication networks nor provides publicly accessible telecommunication services), that is required for establishing, structuring content, amending or terminating a contractual relationship pertaining to telecommunication services.<br>Inventory data includes among other things:<br>– Company name (if applicable, for sole traders also surname, first name)<br>– Address<br>– Name, address, date of birth of authorised representatives, commercial register numbers, competent register court, VAT ID<br>– Contractual data (e.g. customer number)<br>– Passwords (insofar as they are assigned by us for the customer)<br>– Billing data<br>– Bank data | We have received this data from you |

| | |
|---|---|
| – Contact data (email address, telephone number and, if applicable, fax number)<br><br>Inventory data – as far as it is required – is also processed prior to concluding the contract insofar as this is necessary within the scope of the pre-contractual creation, processing and performing of a contract summary.<br><br>Insofar as it is required in connection with establishing identity for establishing and amending the contract and recording inventory data, we reserve the right to request presentation of an official identification document. Proof of identity can be provided as follows:<br><br>– By presenting the official identification document, of which we are allowed to make a copy (Section 7 of the TTDSG).<br>– By means of electronic identify verification acc. to Section 18 of the Identity Card Act<br>– Acc. to Section 12 of the eID Card Act or<br>– Acc. to Section 28 (5) of the Residence Act<br><br>Within the scope of changes to the contract party position (e.g. because of an inheritance case or after establishing/terminating a registered civil union or liquidation of a company) or change of (company) name, the corresponding following documents are required as means of proof:<br>– Marriage/Divorce certificate (for natural persons)<br>– Change of name certificate (for natural persons)<br>– Confirmation of establishing/terminating the civil registered union (for natural persons)<br>– Death certificate (for natural persons)<br>– Excerpt from the commercial register as well as excerpt from the trade register and, if applicable, additional required company-law documents (e.g. shareholder resolutions, shareholder contract etc.)<br><br>Insofar as the participants are legal entities, the additional following inventory data shall apply:<br>– Name and address of the company<br>– Authorised representative bodies<br>– If applicable, commercial or trade register<br><br>In the case of terminations because of moving or changing the company address (and if as we are unable to provide the service at the new location) we reserve the right to request a corresponding deregistration/registration or commercial and trade register registration as proof of the completed move or the completed change of address. | |
| **Traffic data** in the sense of Section 9 of the TTDSG in connection with Section 3 No. 70 of the TKG | We have collected this data from you within the scope of the actual service provision. |

| | |
|---|---|
| Traffic data is any data whose collection, processing or use is required to provide a telecommunication service.<br><br>Traffic data includes:<br>– Number or identification of the connections involved (IP address, MAC address, access data to the connection) or of the end devices, personal authorisation identifier, also the card number when using customer cards, for mobile connections also the location data (Section 9 (1) No. 1 of the TTDSG)<br>– Start and end of the respective connection by date and time and – if the fees depend on it – the transmitted data volume (Section 9 (1) No. 2 TTDSG)<br>– The telecommunication service you use (Section 9 (1) No. 3 of the TTDSG)<br>– The end points of dedicated connections, their start and end by date and time and – if the fees depend on it – the transmitted data volumes (Section 9 (1) No. 4 of the TTDSG)<br>– Other traffic data required for setting up and maintaining the telecommunication services and billing (Section 9 (1) No. 5 of the TTDSG).<br><br>IMPORTANT INFORMATION:<br>– Section 9 (1) No. 1-3 of the TTDSG, also includes itemised bills (insofar as requested by end user prior to the relevant billing period)<br>– The traffic data will only be processed insofar as this is required for setting up or maintaining the telecommunication, for billing purposes or for setting up additional connections (Section 9 (1) of the TTDSG)<br>– Using the internet generates a large amount of data. We store only general traffic data such as the times of use and used bandwidth. Personal data is not evaluated.<br>– We collect your telephony data to provide telephone services (VoIP) and for the billing. As a basic principle, no content is stored, but only the information with which telephone numbers a connection was established and for how long. In detail, these are the date and time, duration of the call, outgoing call numbers and incoming call numbers.<br>Message content (e.g. SMS, MMS, voice messages) are only stored when this is required for providing the special service you have ordered.<br>– Insofar as a number display is offered in the specific product and service description, your telephone number can be blocked from being displayed either permanently or temporarily for the called party providing your end device supports this feature. If you do not have a suitable end device or do not wish your number to be displayed, transmission of your telephone number can be permanently suppressed. | |

| | |
|---|---|
| – Moreover, we use your IP address to detect misuse such as spam or the sending of malware.<br>– Furthermore, pursuant to Section 12 of the TTDSG we are allowed to process end-user traffic data as well as control data of an information technology protocol for data transmission that is transmitted independently of the content of a communication process or that is stored on servers involved in the communication process and is required to ensure communication between recipient and sender in order to detect, localize or to resolve disruptions or errors in telecommunication systems. This also applies to disruptions that could lead to a restriction of the availability of information and telecommunication services or to unauthorised access to the users´ telecommunication and data processing systems.<br>Access data for end-user routers is used for remote access to support the configuration process within the framework of Section 24 of the TTDSG (e.g. setting up DECT, setting up WIFI) and if necessary, also to assist in eliminating disruptions (e.g. to retrieve system data to detect the cause of the disruption). | |
| | |
| In individual cases, we process the following **other data:**<br>– Residents´ registration office data (esp. for relocation) or trade register excerpt or commercial register excerpt (for address changes or change of the company)<br>– Credit score<br>– Third-party recommendations (customers/friends – e.g. as part of a customer referral programme<br>– Information from customer surveys, esp. customer satisfaction surveys<br>– Porting data (in connection with a change of provider)<br>– Information connected to telecommunication market processes (via the Federal Network Agency); more specific information available on the Federal Network Agency´s website at **www.bnetza.de**. | Residents´ registration office or commercial register or trade register<br>Other customers / friends<br>Customer information<br>Other market participants<br>Federal Network Agency |

**V. Purpose of data processing and legal basis**

Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following:
We process your data only when we have your consent to dos so or the processing is legally permitted.

| **Purpose of processing** | **Legal basis** |
|---|---|
| **Consent cases** | |
| Processing inventory data for **marketing purposes**<br><br>IMPORTANT INFORMATION:<br>This is only permitted if you have given your prior consent and to the extent you consented to. Consent can be withdrawn (revoked) at any time with future effect. Such revocation does not affect the legality of the processing performed up to the revocation. We inform you of the option to revoke within the scope of the consent process. | Art. 6 (1) (a) GDPR |

| | |
|---|---|
| **Contract initiation and contract fulfilment cases** | |
| Processing of inventory and traffic data for the purpose of contract **initiation and contract fulfilment**<br><br>INFORMATION:<br>Additional details are provided in the respective specific product and service descriptions. This includes the processing of inventory and traffic data as part of detecting, localising and eliminating disruptions and errors in telecommunication systems as well as for securing entitlement to fees in cases of unlawful use of a telecommunication network or service. | Art. 6 (1) (b) GDPR |
| **Performing a legal obligation** | |
| **Legal obligations** – Prevention and investigation of criminal offences<br><br>Insofar as we are requested to provide data by a competent authority in legally permissible cases, we are obliged to pass on the data to them. Depending on the nature and scope of the request, this also includes your connection and usage data.<br>In individual justified and legitimate cases, we are also obliged to grant a competent authority access to your usage behaviour of telecommunication services provided by us and to enable audio monitoring of your connection. The respective national and EU provisions for protecting the secrecy of telecommunication shall apply. | Art. 6 (1) (c) GDPR, Sections 22, 23 TTDSG |
| We are subject to various legal obligations such as the Money Laundering Act, tax laws and stipulations of the telecommunications regulations, especially of the Telecommunications Act and the (future) ePrivacy Regulation. The purposes of processing include fulfilling tax-related checking and reporting obligations, fulfilling the telecommunications industry requirements, sanctions list check as well as prevention of fraud and money laundering. | Art. 6 (1) (c) GDPR |
| **Existence of a legitimate interest** | |
| **Improving the service and quality control**<br><br>Your data is also used by us to improve and make our services more efficient. We are thus able to offer you better services in the future. We also measure the quality of our services by means of your data.<br><br>In addition, your contract data is also used for the purpose of generating analyses. These analyses assist us in improving our products for you. Before we use your contract data for these purposes, we anonymise or pseudonymize the data. In this way, (by looking at the data), you as an individual person are either no longer identifiable (anonymisation) or are identifiable only with additional information (pseudonymisation). As part of the pseudonymisation we replace your first name, for example, with another, randomly chosen value. | Art 6 (1) (f) GDPR |
| **Direct marketing, market and opinion research**<br><br>In addition to processing your data for the purpose of direct marketing (by post), we also use your data for the purpose of market | Art. 6 (1) (f) GDPR |

| | |
|---|---|
| or opinion research in order to find out what interests and demands exist with respect to future products. | |
| **Credit checks**<br><br>Based on our legitimate interest in protecting ourselves from payment defaults, we carry out credit checks for payment methods that pose a payment default risk for us prior to concluding a contract. For this purpose, we transmit your data (name, address) to a credit agency that provides us with a stored credit score for your person. Based on your credit score, it is decided on whether to conclude a contract with you. For credit checks, we use the following credit agencies:<br>Creditrefom Boniversum GmbH, Hellersbergerstr. 11, 41460 Neuss. Further information on data processing at Creditrefom Boniversum is available online via the information sheet "Boniversum-Informationen gem. Art. 14 DSGVO" at **https://www.boniversum.de/eu-dsgvo/Informationen-nach-eu-dsgvo-fuer-verbraucher/.**<br><br>For the same reason, we transmit data related to behaviour not in line with the contract or fraudulent behaviour to the above-mentioned credit agency as part of the application, performance and termination of the business relationship.<br><br>Information with regard to data processing by the credit agency and on automated decision-making is available at the link provided above. | Art. 6 (1) (f) GDPR in connection with Section 31 BDSG |

**VI. Data recipients or recipient categories**

Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following:

We process your data in a confidential manner, only the departments and employees who need this data to fulfil the aforementioned purposes have access to your data.

This also means that data is only transmitted to third parties when this is required and legally permissible for the aforementioned purposes or you have granted prior consent.

| **Data recipients** | **Remarks** |
|---|---|
| **Third-party recipients with no corporate affiliation (within the scope of the normal contract fulfilment)** | |
| – IT service providers<br>– IP address managers<br>– Marketing service providers<br>– Printing service providers<br>– Advisory and consulting providers<br>– Credit agencies<br>– Debt collection agencies<br>– Sales partners<br>– Suppliers of mailing and internet services<br>– Selected specialist companies, service technicians for commissioning and fault clearance of your connection<br>– Logistics service providers<br>– Analysis specialists | |

| | |
|---|---|
| – Document and data carrier disposal companies<br>– Authorities<br>– Legal guardians and persons with a power of attorney | |
| **Third-party recipients with no corporate affiliation (special cases)** | |
| Transmission occurs to public authorities when there is a legal obligation to do so. This includes for example law enforcement authorities, tax authorities and local authorities.<br>Transmission also occurs to legal guardians and persons who have a power of attorney. | |
| **Third-party recipients with corporate affiliation** | |
| terranets bw GmbH is part of the EnBW Energie Baden-Württemberg AG and works together with other corporate group companies. Transmission of personal data to other corporate companies only occurs when there is a legal basis for doing so and it is required for one of the aforementioned purposes.<br>In this case, within the corporate group, there is always either:<br>– an agreement on commissioned data processing or<br>– a group-wide agreement on the handling of personal data. | |

**VII. Transmission to a non-EU jurisdiction**

Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following:
The data is transmitted in this case to the following non-EU jurisdictions. In this regard, it must be ensured that the following non-EU jurisdictions have an adequate data protection level. This is subsequently provided as follows:

| Non-EU jurisdiction | Adequate level of data protection by means of |
|---|---|
| Andorra, Argentina, Faroe Islands, Israel, Isle of Man, Canada, Guernsey, Jersey, Switzerland, Uruguay, New Zealand.<br><br>Recipient category: | Establishment of an adequate data protection level by means of standard contractual clauses pursuant to Art. 46 (2) (b) GDPR as well as additional contractual guaranties (cf. Schrems II). |
| USA<br><br>Recipient category: | Establishment of an adequate data protection level by means of standard contractual clauses pursuant to Art. 46 (2) (b) GDPR as well as additional contractual guaranties (cf. Schrems II).<br><br>Information available at:<br><br>**http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32001D0497&from=DE**<br>**http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:DE:PDF**<br>or<br>**http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF** |

**INFORMATION:**
Your data will not be stored by us outside the European Economic Area. However, access from a country outside the European Economic Area is possible by way of administration access as the operable capability of the systems is often

ensured by the follow the sun model. In these cases, data access only occurs when either an adequacy decision exists for the respective country, we have agreed with the service providers on the standard contractual clauses provided by the EU Commission for such cases including more far-reaching guarantees that have been required since CJEU (Schrems II), or the respective company has set up its own internal binding data protection regulations that have been recognised by data protection authorities.

**VIII. Storage period**

We store personal data for as long as it is required for the aforementioned purposes and/or to comply with statutory retention obligations and until all mutual claims are fulfilled. If the purpose for which the data was collected has been fulfilled, the data is deleted regularly unless their temporary further processing is required. This means that – insofar as no special cases exist (please see information below the following table) – your data will be deleted as follows:

| **Category pf personal data** | **Deletion deadline** |
|---|---|
| **Master and inventory data *)** in the sense of Section 3 No. 6 of the TKG as well as Section 2 (2) No. 2 of the TTDSG (for existing contract) | 6 months after termination of the contract **) |
| **Master and inventory data *)** in the sense of Section 3 No. 6 of the TKG as well as Section 2 (2) No. 2 of the TTDSGG (for non-existing contracts – e.g. for exercised revocation rights or the customer does not send the order after transmission of the contract summary or after the subsequent transmission of the contract summary does not approve it) | 1 month after it is determined that the contract will not be concluded or was revoked. **) |
| | |
| **Copy of identity document** for purposes of establishing and changing a contractual relationship in the sense of Section 7 of the TTDSG | Immediate destruction after establishing the end user´s details required for concluding the contract. |
| **Traffic data *) – Telephone service** (insofar as relevant for billing and no dispute exists) ***) | A maximum period of 6 months after dispatching invoice **) |
| **Traffic data – telephone service** (insofar as not relevant for billing and purpose fulfilled – e.g. itemised bill transmitted) ***) | Immediately **) |
| **Traffic data – internet service (login, user ID etc.)** | 7 days |
| **Contents of messages** | Erasure by customers themselves or in accordance with respective agreement/ service description |

| | |
|---|---|
| **Special case data on the customer portal** | In the case that invoices are stored in an account for downloading, invoices are stored there until the respective download is carried out by the customer (however, no longer than 6 months after the end of the contractual relationship).<br>In the case that traffic data is stored in an account for downloading, this traffic data is stored for a maximum period of 6 months and then automatically erased. |

**) for certain data in individual cases, retention periods of up to 10 years can also apply under the Commercial Code, the Fiscal Code and the Money Laundering Act. Furthermore, statutory limitation periods of up to 30 years can make is necessary to retain certain data for evidentiary purposes.*
***) unless you have granted consent to a longer storage, e.g. because you explicitly want connection data to be sent another ten (10) weeks after the invoice is dispatched. A right to storage for misuse and fraud analysis remains reserved for up to 7 days.*
****) the data is not erased if longer storage is required by valid legal regulations or by judicial order.*

**IX. Your rights as data subject**

Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, you have the following rights with respect to the processing of your personal data:

| Your rights | Remarks |
|---|---|
| **Information**<br>Pursuant to Art. 15 GDPR you have the right to information on the data processed about your person. | |
| **Rectification**<br>Pursuant to Art. 16 GDPR you have the right to rectify inaccurate or incomplete personal data. | Please observe the restrictions set out in Section 34 of the BDSG |
| **Erasure**<br>Pursuant to Art. 17 GDPR you have the right to erasure of personal data. | Please observe the restrictions set out in Section 35 of the BDSG |
| **Restriction of processing**<br>Pursuant to Art. 18 GDPR you have the right to restrict processing. | |
| **Data portability**<br>Pursuant to Art. 20 DSGVO you have the right to data portability. | |

| | |
|---|---|
| **Right to object (direct advertising)**<br>Pursuant to Art. 21 (2) GDPR you can object without restriction to processing for direct advertising purposes at any time. | |
| **Right to object (for processing on the basis of public or legitimate interests)**<br>Insofar as the data is processed on the basis of legitimate interests (Art. 6 (1) (f) GDPR) or to perform a task carried out in the public interest, the right to object to the processing exists pursuant to Art. 21 (1) GDPR. | In this case, the data is no longer processed for this purpose unless we can demonstrate compelling legitimate grounds for the processing that prevail over your interests, rights and liberties or the processing serves to assert, exercise or defend legal claims. |
| **Revocation (of a consent)**<br>You have the right to revoke a granted consent pursuant to Art. 6 (1) (a) GDPR at any time. | |
| **Right to lodge a complaint**<br>Insofar as you are of the opinion that the processing of your personal data breaches applicable law, you have the right to lodge a complaint with a data protection authority pursuant to Art. 77 GDPR at any time.<br>This is:<br>The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg<br>Postfach 10 29 32<br>70025 Stuttgart<br>Tel. 0711 6155 410<br>poststelle@lfdi.bwl.de | This right shall apply irrespective of other administrative or judicial remedies. |

You may submit your objection or consent revocation to us at any time. This can be without any specific form. In order to be able to process your objection or revocation in an orderly way and to avoid delays, we kindly ask you to use the following contact address:
terranets bw GmbH
Am Wallgraben 135
70565 Stuttgart
info@terranets-bw.de

**X. Provisioning requirements or obligations**

You must provide only the personal data that is required for concluding, performing and terminating the contractual relationship or specific purpose or that we are obliged to collect because of legal regulations. If you do not provide this data, we will be forced to decline concluding the contract or will no longer be able to fulfil the contract.

**XI. Automated decision-making (Art. 22 GDPR)**

Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following: We would like to point out that we do not make use of automated decision-making. With regard to the credit check, please refer to the link given in Section V.

## XII. Amendment clause

As our data processing is subject to changes, our data protection information is adapted from time to time. We will inform you of changes in a timely manner. You can find the respective current version of this data protection information at **https://www.terranets-bw.de/datenschutz**.

## XIII. Information on your right to object pursuant to Art. 21 GDPR

Insofar as the GDPR is applicable to you, i.e. insofar as you are not a legal entity, we inform you of the following: **Right to object in individual cases**
You have the right to object, for reasons arising from your particular situation, at any time to the processing of personal data related to you that occurs based on Art. 6 (1) (e) GDPR (data processing in the public interest) and Art. 6 (1) (f) GDPR (data processing based on a balancing of interests). This shall also apply to profiling based on these provisions in the sense of Art. 4 No. 4 GDPR (insofar as it is applicable).
In this case, in the case of an objection, we will refrain from processing your personal data with future effect unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and liberties or the processing serves to assert, execute or defend legal claims.

**Right to object to data processing for direct marketing purposes**
In individual cases, we process your personal data in order to conduct direct advertising. You have the right to object to the processing of data related to your person for the purpose of such advertising at any time. This shall also apply to profiling insofar as it is connected to such direct advertising.

If you object to data processing for direct advertising purposes, we will refrain from processing your data for these purposes with future effect.

**Status: October 2023**