# Privacy notice for enterprise customers



## I. Notes for all Corporate Customers

### 1. Your data – our responsibility

Your privacy is important to us! Read here how we, Vodafone GmbH, and Vodafone West GmbH, both of Ferdinand-Braun-Platz 1, 40549 Düsseldorf, and Vodafone Deutschland GmbH, Betastrasse 6 - 8, 85774 Unterföhring (jointly referred to as Vodafone companies or we) handle your personal data in our capacity as data controllers.
In providing you with telecommunications services, such as Internet and telephone products, our handling of your and the users' personal data is, in particular, based on sections 9--13 of the German Telecommunications and Telemedia Data Protection Act (TTDSG), as well as on Article 6 para. 1 lit. b) of the General Data Protection Regulation (GDPR).
If we offer you products that we provide as a processor, the regulations of the respective, product-specific contract processing agreement apply to the personal data that we process on your behalf.
You and the users of our services can find this privacy notice online at any time at www.vodafone.de/business/digitalisierung/datenschutz-privatsphaere.html .

### 2. Contract data

We process your contract data for all types of contracts that we conclude with you.
Contract data is personal data that is required for the establishment, amendment and development of the content of our mutual contract. This includes, for instance, your contact details or those of our contact persons at your premises, such as the name, address, telephone number and e-mail address.
We delete your contract data after the end of the contract, unless the law requires that we retain it, e.g. for audits. Archiving can last up to 10 years and starts at the end of the year following the end of the contract. After that, we delete your data permanently. In the meantime, we will severely restrict the possibilities of access. This ensures that only a few employees can access the data as necessary.

### 3. Legitimate interest and analyses

We use your personal data primarily to fulfil the contract with you and to provide you with the service you expect from us. We also process your personal data within the scope of our legitimate interest for the following purposes:
- Ensure technical availability and information security
- Assertion of legal rights
- Debt collection and risk management
- Prevention and investigation of criminal acts
- Video surveillance to enforce house rules
- Sales and business management
- Optimisation of internal processes
- Review and optimisation of needs analyses
- Advertising, market research, opinion research, satisfaction surveys
- Improvement of advertising campaigns for new Customers using analytical and statistical
- Improvement of products and services using analytical and statistical methods
- Improvement of service quality using analytical and statistical methods
- Improvement of Customer satisfaction using analytical and statistical methods

The legal basis for this is Article 6 (1) f) GDPR unless – e.g. for certain types of advertising – your separate consent is required. This data processing takes place in compliance with the principle of data minimisation and, as far as possible, in anonymised, pseudonymized or aggregated form. As a result, you can no longer be identified as the person behind the data or can only be identified with highly protected additional information. For this purpose we replace your name with another randomly chosen value, for example. You can object to the processing of your contract data for the purposes of advertising, market research, opinion research and satisfaction surveys at any time. In the other aforementioned cases, please state the grounds relating to your particular situation.
Contact details to exercise your right to object can be found in Clause 8.

### 4. Disclosure of your data

If you have not given us separate consent, we will only pass on your personal data if we are permitted or required to do so under German or European law. We have various companies working for us in the fields of contract processing and support, if necessary printers (e.g. for invoicing), sales agencies, billing service providers, collection agencies, service partners who are responsible for troubleshooting or installation, logistics partners (for sending hardware), maintenance service providers for the support and maintenance of IT systems, as well as auditors from the public and private sectors. In order for these partners to meet the obligations under data protection law in the processing of your data, we set out detailed contract provisions.
In certain situations we are required to disclose your personal contract, traffic, usage or location data and the content of your communication to German authorities. We only do this, however, if we are required to do so by law. For example, this may be the case due to a court order in criminal proceedings.

### 5. Data processing in the group

The Vodafone companies share your contract data with each other in order to inform you of the products and services of the Vodafone companies, including on a mutual basis for each other. The Vodafone companies will only contact you with such information using means of communication to which you have given your consent or which are allowed under law, unless you have objected to this. We also send contract and other legally relevant information to you regardless of whether you have given your consent or have objected and to all contact details known to the Vodafone companies.
In addition, the Vodafone companies share your contract data with one another in order to prepare analyses. The analyses help us to improve our products together for you and to make robust decisions. Before we use your contract data for this purpose, we anonymize or pseudonymize it. As a result, you can no longer be identified as the person behind the data or can only be identified with highly protected additional information. For this purpose we replace your name with another randomly chosen value, for example.
The legal basis for this is provided by Article 6 (1) f) GDPR in conjunction with the legitimate interest of the Vodafone companies in individually relevant information on their products and services as well as joint analyses. You can object to this processing of your contract data at any time. However, if you object to joint analyses, you must state the grounds relating to your particular situation.

### 6. Forwarding of data abroad

Unless we have agreed otherwise with you in the contract, we store your contract data in the European Union and in the United Kingdom, and particularly sensitive data, such as traffic data, only in Germany. If we cooperate with contracting partners outside the EU area who may have access to your data, we do so in accordance with the rules set up by the European Commission.
What this means for you is that we either include so-called standard contract clauses in the contract, or the European Commission has expressly determined that the level of data protection in the country of our contractual partner is adequate.

### 7. Your data protection rights

**a. Right of access, of rectification and right of deletion with regard to the data**

Do you want to know what data we store about you? Do you ask yourself what we use your personal data for and or where we got it from? Talk to us. We are happy to answer your questions. Has your data changed? Let us know. We will provide you with the information you require. Or has an error found its way into your Customer data? We will change this for you. Do you want to have your personal data erased? Tell us what data precisely you would like to have erased. We will then erase all data we no longer need to store.

**b. Objection to advertising**

We use as your contract partner your telephone number and e-mail address in order to send you information by Messenger, SMS and e-mail for the purpose of providing advice and advertising of our own similar offers.
You can object to the use of your telephone number and e-mail address for this purpose at any time.

**c. Unsubscribing from the newsletter**

If you no longer wish to receive our newsletter, you can unsubscribe directly via a link at the end of the newsletter.

### 8. Your data protection service

Whether information, correction, deletion or objection – our data protection specialists are here for you. Use our online data protection service for all issues relating to your data protection rights. www.vodafone.de/business/digitalisierung/datenschutz-privatsphaere.html

Or write to:
Dr. Dirk Herkströter, Data Protection Officer Vodafone GmbH,
Dr. Anastasia Meletiadou, Data Protection Officer of Vodafone Deutschland GmbH, Data Protection Officer of Vodafone West GmbH, Ferdinand-Braun-Platz 1, 40549 Düsseldorf.
If we are unable to resolve your data protection concerns, please feel free contact the supervisory authority responsible for us.
For data protection issues relating to telecommunications:
The Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153, 53117 Bonn
Data protection issues relating to our website:
The State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia
PO Box 20 04 44, 40102 Düsseldorf
Other data protection issues relating to Vodafone Deutschland GmbH:
Bavarian State Office for Data Protection Supervision
PO Box 606, 91511 Ansbach

## II. Telephone or Internet contract

If you have entered into an Internet or telephone contract with us, the following supplementary privacy notice applies.

### 1. Traffic and location data

We process your traffic data to provide our internet and telephone services. Traffic data is data that is processed during the provision of a telecommunications service, such as the beginning and end of a connection, the call number of the calling and the called line, the amount of data transmitted and the telecommunications services used, as well as your location in the case of mobile phone connections. The content of the message does not count as traffic data and is not stored by Vodafone.
Traffic and location data will be deleted directly after the respective retention periods have ended: Internet traffic data will be erased by us after 7 days at the latest. We erase your telephone traffic data immediately, if it is no longer relevant for billing and at the latest 3 months after the bill was sent.

### 2. SMS spam protection

If you have a mobile phone tariff with us, we check your SMS for signs of spam or malware. For this purpose, we analyse criteria such as the number of recipients of the same message or suspicious links. If we determine that an SMS is spam or malware, it will not be delivered. We use these measures to protect the recipients of SMS messages from unwanted messages, damage to their IT systems and to protect our network from disruptions.

### 3. Itemised statements

For future billing periods, you can choose whether or not you want an itemised statement (IS) for the chargeable connections.
If you have opted for an IS, the following rules shall apply:
- You can choose whether the IS should show the complete destination numbers or the destination numbers shortened by the last three digits
- The itemised bill must be requested before the respective billing period.
- For connections in companies and public authorities, a written declaration is required that all employees have been or will be informed about this and that the participation of the works council or the staff or employee representatives has been ensured in accordance with the statutory regulations.
- Since the IS only serves as proof of chargeable connections, the connections subject to a flat rate charge (e.g. in the case of billing according to flat rate tariffs) are not listed in the IS. We will delete your itemised statement no later than 6 months after sending it.

### 4. Inclusion in telephone directories

Upon request, Vodafone may arrange for the inclusion of your telephone number(s), address, name or company name and additional details such as occupation, industry, type of connection and co-users (consent required) in public subscriber directories. You can choose between printed and electronic directories for publication or to refuse publication. You can also choose to make your data available only to directory enquiries. Vodafone may also provide the data released by you for the relevant subscriber directories to third parties (network operators, service providers) for the purpose of producing and publishing subscriber directories and for the provision of directory enquiry services. You can limit the scope of your entry or object to publication altogether at any time by making a declaration to this effect to Vodafone.

### 5. Inquiry services

Vodafone and/or third parties may provide information about the Customer data available in public subscribed directories in individual cases – e.g. a provider of telephone inquiry services. If you have been included in a directory
- information about your telephone number will be provided unless you object to this information being provided If you have opted for information to be provided, you can also decide whether information should be provided about your entry in its entirety.
- your name and address will be provided to information seekers who only know your telephone number ("reverse information") unless you object to this information being provided.

### 6. Display of the phone number

The Vodafone connection allows your call number to be suppressed permanently or on a case-by-case basis for the called subscriber, provided your terminal device supports this feature. If you do not have a suitable terminal device or do not wish to have your call number displayed, the transmission of your call number to the called lines can be permanently excluded.

### 7. Protection of your mobile identity

You can use your mobile phone number as an additional security factor with many online services, for example with online banking or in your social media profile. For instance, if you use the mTAN process with a bank which carries out such an identity check, Vodafone GmbH will, upon request by your bank, check your mobile phone number and other security-relevant indicators in order to protect you against fraudulent transactions.
Security-relevant indicators are information which suggest the fraudulent use of your mobile phone number or identity

theft, for example if a SIM card replacement, change of telephone number or number porting has taken place shortly before the online transaction or if the name and mobile phone number given for an online transaction do not match the data we have stored about you. As a result of our check, your provider will receive an answer as to whether such security-relevant features are present and, if so, since when or whether or not you have an active contract (prepaid or fixed-term contract) with us for the mobile phone number used. Beyond this, we do not forward any other personal data about you.
If any security-relevant indicators are present, your provider will offer you alternative ways to complete your online transaction. Information on whether your online provider carries out such a security check can be found in your provider's privacy notice. For increased protection of your personal data, we do not forward security-relevant indicators relating to your mobile phone number directly to your online provider, but to a data custodian who acts as an intermediary. When our response is forwarded to your online provider, they remove the information about the mobile phone provider from whom the details about you originated. The legal basis for this is provided by Article 6 (1) f) GDPR in conjunction with our and your online provider's legitimate interest in protecting you against fraudulent misuse of your mobile phone number or identity theft. You can object to this processing at any time; however you must state the grounds relating to your particular situation. Contact details to exercise your right to object can be found in Clause 8.
In cases other than those described above, we will only check for security-relevant indicators if your online provider has obtained your express consent for us to do this. This applies in particular if processing of your traffic or location data is required for this purpose.

**8. Processing of anonymous data for statistics and research purposes**
We anonymize your aforementioned personal data for statistics and research purposes. This is also the case for your traffic and location data. Such anonymous analysis results can, for example, be projections of traffic flows or maps which show the movement of groups of mobile phone devices. For example, we support researchers and statisticians to better understand the effects of pandemics or tourism and to develop strategies to better deal with them. Under no circumstances will your personal data be disclosed to third parties for these purposes. This means the following: The analysis results are abstract findings which are independent from specific persons. These results will not allow us to draw any conclusions about you as a person. This is ensured by our anonymised process. For this purpose, for example, several mobile phone devices are consolidated into groups.

**9. SMS service „Corporate Customer faults"**
On our website https://www.vodafone.de/business/stoerungen/ you will find information about the most significant faults currently affecting Corporate Customers. You can also subscribe to have SMS notifications sent to your mobile phone number each time a fault occurs.
Once you have entered your mobile phone number we will send you a confirmation SMS to confirm that you have activated the service yourself. After you have replied by messaging „Start", the SMS subscription will begin. The subscription ends automatically once the fault you have subscribed to has been rectified.
If you wish to cancel the SMS service before this, simply message „Stop" to the fault SMS sender. Only your mobile phone number is processed for providing the SMS service. We store and use your mobile phone number for the duration of the subscription. As soon as the subscription ends (automatically or upon request), we will store your mobile phone number for another 30 days, after which we delete your data permanently.

**III. F-Secure**
If you use the security package powered by F-Secure, you enter into a contract directly with our cooperation partner: F-Secure Corporation, Tammasaarenkatu 7, PL 24, 00181 Helsinki, Finland. We therefore forward your contract data to F-Secure. We and F-Secure are both responsible for the processing of your personal data. You can find out more about data protection at F-Secure at:
https://www.f-secure.com/de/legal/privacy/statement .
If you as a Customer of Vodafone West GmbH purchase the security product "F-Secure", we will process the user data (primarily your Customer number in order to associate it with an F-Secure licence key from our contingent) which is necessary for the provision, execution and billing of your services and for ensuring their technical availability and the security of information (protection against viruses and other malware) within the confines of the law.

**IV. Information concerning credit checks and fraud detection**
If we carry out any credit check or fraud detection procedures relating to the product you have ordered, the following additional privacy notice shall also apply.

**1. Check by SCHUFA and CRIF GmbH**
We forward personal data collected within the scope of the contractual relationship relating to the application for, execution and termination of the contract, for example your name, date of birth and your IBAN, as well as data relating to any behaviour that is in breach of the contract or fraudulent to CRIF GmbH, Leopoldstraße 244, 80807 Munich ("CRIF GmbH"). Vodafone GmbH and Vodafone Deutschland GmbH also forward the aforementioned data to SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden ("SCHUFA"). The legal basis for this transfer of data is provided by Article 6 (1) b) and Article 6 (1) f) GDPR in conjunction with our legitimate interest in minimising the risk of payment default and in preventing fraud. By sharing data with SCHUFA and CRIF GmbH, we also meet our statutory obligation to carry out credit checks with regard to Customers (sections 505a and 506 of the German Civil Code (BGB). SCHUFA and CRIF GmbH process the data received and use it for profiling purposes (scoring) in order to provide their contracting partners within the European Economic Area and in Switzerland as well as in some other third countries (if an adequacy decision for these countries has been adopted by the European Commission) with information on, among other things, credit checks on natural persons („credit scoring").
Independently of the credit scoring, SCHUFA supports its contracting partners with profile building services upon identifying any suspicious circumstances (for example for the purpose of preventing fraud in mail-order business). For this purpose, enquiries of SCHUFA contracting partners are analysed to check these for potentially suspicious circumstances. This check, which is carried out individually for the respective contracting partner, can also take into account address data, information on whether and in what capacity there is an entry for a public figure in generally available sources with matching personal data, as well as aggregated statistical information from the SCHUFA database. This procedure has no effect on the credit checking and credit scoring processes.
Further information on the activities of SCHUFA can be viewed online at www.schufa.de/datenschutz .
Further information on the activities of CRIF GmbH can be viewed online at www.crif.de/datenschutz .

**2. Checking by Infoscore**
We forward your data (name, address and if applicable date of birth) for the purpose of credit checking, to obtain information to assess the risk of payment default on the basis of mathematical-statistical methods using address data, and to verify your address (check deliverability) to Infoscore Consumer Data GmbH, Rheinstr. 99, 76532 Baden-Baden ("ICD"). The legal basis for the forwarding of this data is provided by Art. 6 (1) b) and Article 6 (1) f) GDPR. Detailed information on ICD within the meaning of Article 14 GDPR, i.e. information on the object of this company, the purposes of data storage, the data recipients, the entitlement to have a credit report issued to oneself, as well as the right to have one's data erased or rectified can be found at:
https://finance.arvato.com/icdinfoblatt .

**3. Preliminary check by Vodafone companies (whitelist)**
The Vodafone companies also share information on your positive payment history with us. This information is taken into account in the credit check or results in no credit check being carried out by the aforementioned credit agencies. This is also our legitimate interest pursuant to Article 6 (1) f) GDPR. This also ensures that Customers with a positive payment history are not rejected. You can object to this processing at any time; however you must state the grounds relating to your particular situation.

**4. Preliminary check by Vodafone companies (blacklist)**
The Vodafone companies also keep a shared blacklist, in which (former) Customers with a negative payment history or those who have received support are listed. (Former) Customers with a negative payment history are either Customers whose contracts have already been or could be terminated due to non-payment, or Customers in the reminder/instalment payment process. The latter will be removed from the blacklist as soon as the outstanding payments have been settled. Supported customers are added to the blacklist if the supervisor provides written proof of support. Supported customers are also removed from the blacklist as soon as a Vodafone company is informed that support has been cancelled. The following data is processed here: first name, surname, address, e-mail address, telephone number, date of birth, Customer number, IBAN and the characteristic. The legal basis for this is provided by Article 6 (1) f) GDPR in conjunction with our legitimate interest in protecting ourselves with preventive action against payment default and possible cases of fraud as well as protecting persons who do not possess legal capacity against unjustified claims. You can object to this processing at any time; however you must state the grounds relating to your particular situation.

**5. Fraud prevention in the case of online orders**
If you place an order with us online, we carry out the following additional checks:
Before we accept your online order, we check information about the device you use to place the order with us. We forward this information to Risk Ident GmbH, Am Sandtorkai 50, 20457 Hamburg ("Risk Ident"). Risk Ident operates a database on devices which have drawn attention in the past in connection with online fraud. In order to identify an individual device, Risk Ident uses so-called browser fingerprinting on our website and in doing so establishes the technical configuration of the device. If online fraud is suspected, we are sent a warning. We use this together with the other checks referred to in this Clause 4. in order to decide whether to accept your order.
If our check with CRIF GmbH described in Clause 4. a. provides an inconclusive result on the probability of fraud and the information that you are an online Customer, we may ask you to verify your personal details via your bank. You then decide with your separate consent whether you want to authorise your bank to carry out online verification of your order details.
The legal basis for this is provided by Article 6 (1) f) GDPR in conjunction with our legitimate interest in preventing fraud and protecting ourselves against payment default as well as in the case of online verification via your bank your separate consent pursuant to Article 6 (1) p.1 a) GDPR.

**V. Dow Jones Risk & Compliance**
Before we conclude or extend a contract with a Corporate Customer or supplier, or if there is any other reason (e.g. publication of new sanctions lists), we use the „Research Tool" of Dow Jones & Company, Inc., 1211 Avenue of the Americas New York, NY, 10036 USA, to check whether the Corporate Customer or supplier has violated regulations aimed at combating money laundering, bribery, corruption or economic sanctions, among others. Donors and sponsorship partners are also subjected to Dow Jones screening. Screening is performed by comparing company data (company name, address and commercial register number) with the Dow Jones database and international sanctions lists. Personal data is only processed if this initial comparison returns a positive result. Only then is an in-depth check of the company owner or other authorised representative performed. The processed data is as follows: First name, surname, date of birth, details of the person authorised to represent the company and the respective violation. In the case of donations and sponsorships, the company owners or other authorised representatives are checked during the initial screening.
Finally, the results of screening are summarised in a due diligence report.
Depending on the individual case, the legal basis for data processing is either Article 6 (1) p.1 c) GDPR, insofar as the processing is necessary to fulfil a legal obligation. Should this legal obligation not apply to the specific relationship, the processing is based on Art. 6 (1) p.1 f) GDPR in conjunction with our legitimate interest in complying with applicable law, protecting, enforcing or defending our legal rights or property, protecting ourselves against fraud and other unlawful acts and for risk management purposes.
This enables us to identify transactions that we are not prepared to enter into for reasons of compliance with applicable law, our endeavours to achieve global compliance, corporate social responsibility and sustainability aspects when considering which Corporate Customers and suppliers we wish to do business with.
We store your personal data for as long as is necessary for the stated purposes, unless a longer retention period is required or permitted by law.
You can object to this processing at any time; however you must state the grounds relating to your particular situation. Contact details to exercise your right to object can be found in Clause 8.
Information on processing by Dow Jones & Company, Inc. can be found in the privacy notice at:
www.dowjones.com/pibcontentprivacynotice/.

**VI Notes on the use of Operator Connect**
The service provides an interface between MS Teams and the Public Switched Telephone Network („PSTN"). Vodafone enables Corporate Customers to call landline and mobile numbers directly from within MS Teams. The service is a telecommunications service pursuant to Section 2 (1) of the German Telecommunications Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutz-Gesetz – „TTDSG") in conjunction with Section 3 No. 24 of the German Telecommunications Act (Telekommunikationsgesetz – „TKG"). Insofar as Vodafone processes personal data in line with providing this telecommunications service, the strict requirements of the TKG and the TTDSG shall apply. The legal basis for data processing is the telecommunication service provision contract and the relevant statutory provisions, including Sections 9 et seq. TTDSG in conjunction with the TKG. Insofar as Vodafone processes data of Corporate Customers' contact persons for the purpose of contract data processing, administering the customer account or data for the purpose of Corporate Customer support, this processing is based on Art. 6 (1) f) GDPR. Vodafone's legitimate interest here lies in fulfilling the contractual obligations vis-à-vis our Corporate Customers.