Privacy notice for enterprise customers

I. Privacy notice for all enterprise customers

1. Your data – our responsibility

Your privacy is important to us. In the following we, Vodafone GmbH and Vodafone West GmbH, both of Ferdinand-Braun-Platz 1, 40549 Düsseldorf, and Vodafone Deutschland GmbH, Betastrasse 6-8, 85774 Unterföhring (hereinafter referred to as "the Vodafone companies" or "we"), explain how we, as data controller, handle your personal data.
When we provide telecommunications products and services, such as internet and telephony products, we handle your personal data and the personal data of users in accordance with sections 9-13 of the German Telecommunications-Telemedia Data Protection Act (Telekommunikations- und Telemedien-Datenschutzgesetz, TTDSG) and Art.
6 (1) b of the EU General Data Protection Regulation (GDPR).
When we provide products and services as a data processor, the personal data that we process for you are subject to the provisions of the product-specific contract for commissioned processing of personal data concluded with you.
You and the persons who use our services can find this privacy policy online at
www.vodafone.de/business/digitalisierung/daten-schutz-privatsphaere.html.

2. Contract data

If you conclude any type of contract with us we process your contract data.
Contract data are personal data necessary for the establishment, amendment and formulation of your contract with us. They include, for example, your contact details or the details of our contact at your company, such as name, address, telephone number and e-mail address.
Your contract data are deleted upon termination of the contract unless we are required by law to retain them for purposes such as financial audits. The retention period can extend to 10 years and commences at the end of the year after the termination of the contract. At the end of the retention period we permanently erase your data. Until that time we impose stringent restrictions on access. Only a few members of staff have access to the data, and only then in the event that access is necessary.

3. Legitimate interest and analyses

We primarily use your personal data to execute the contact with you and to provide the services that you expect of us. We also process your personal data in connection with our legitimate interests for the following purposes:

- Ensuring technical availability and information security
- Assertion of legal claims
- Debt collection and risk management
- Prevention and investigation of criminal acts
- Video surveillance to uphold domiciliary rights
- Sales and business management
- Internal process optimisation
- Review and optimisation of requirements analyses
- Advertising, market and opinion research, satisfaction surveys
- Improvement of new customer advertising campaigns by means of analytical and statistical procedures
- Improvement of products and services by means of analytical and statistical methods
- Improvement of service quality by means of analytical and statistical methods
- Improvement of customer satisfaction by means of analytical and statistical methods

The legal basis for the above is Art. 6 (1) f) GDPR unless separate consent is necessary – e.g. for certain types of advertising. In the processing of the data the principle of data minimisation is taken into account and, whenever possible, the data is used in anonymised, pseudonymised or aggregated form. This ensures that the persons to whom the data pertain are either not identifiable or can only be identified with specially protected additional information. For example, we replace names with randomly selected values. You can object to the processing of your contract data for the purposes of advertising, market and opinion research and satisfaction surveys at any time. In the other cases, please state the reasons relating to your particular situation in your objection.
The contact details for objections are provided in section 8.

4. Transfer of your data

If you have not provided your explicit consent we only transfer your personal data if we are permitted or obliged by German or European law to do so. Various companies are involved in the execution and management of our contracts, including, when required, printing companies (e.g. to print invoices), marketing agencies, billing service providers, debt collection companies, partners for fault remedy and installation services, logistics partners (to deliver hardware), maintenance service providers for support and the maintenance of IT systems as well as official auditors and certified public accountants. To ensure that these partners comply with data privacy obligations in the processing of your data we provide detailed contractual instructions.
In certain situations we are required to disclose your contract, service, usage or location data, and the content of your communications, to the German authorities. However, we only do this if we are under a legal obligation to do so, for example, if a court decision in criminal proceedings mandates it.

5. Data processing in the Vodafone Group

The Vodafone companies share your contract data in order that they can inform you individually and reciprocally about Vodafone products and services. The Vodafone companies will only contact you with this information if you have given your consent or they are permitted by law to provide it, and you have not objected to the provision of such information. Contract data and other legally relevant information is sent to all known contacts at Vodafone companies irrespective of whether you have consented or objected.
Furthermore, the Vodafone companies share your contract data in order to prepare reciprocal analyses. The analyses help us to collectively improve our products for you and to make well-informed decisions. Before we use your contract data for these purposes we anonymise or pseudonymise it. This ensures that you are either not identifiable or can only be identified with specially protected additional information. For example, we replace names with randomly selected values.
The legal basis is Article 6 (1) f of the GDPR, since processing is necessary for the purposes of the legitimate interests pursued by the Vodafone companies to provide customised information about products and services and to implement joint analyses. You can object to the processing of your contract data at any time. However, you can only object to joint analysis if you provide reasons relating to your particular situation.

6. Data transfers outside Germany

In the absence of any contractual agreements concluded with us which specify otherwise, we store your contract data in the European Union and in the United Kingdom. Particularly sensitive data, such as traffic data, are only stored in Germany. Where contract partners outside the EU could have access to your data, we work in accordance with the rules of the European Commission.
For you, this means we either include standard clauses in our contracts with our partners, or the European Commission has explicitly confirmed that the level of data protection in our partner's country is appropriate.

7. Your rights under data protection laws and regulations

a. Right to obtain information, to rectification and to erasure

If you would like to know which data we store about you, or have questions about what we use your personal data for or where we obtained it, contact us. We will be happy to provide the requested information. Have your personal data changed? Let us know and we will amend our records. Or have you discovered an error in your customer data? We will rectify it. If you would like to have personal data concerning you erased tell us which personal data those are and we will erase it, unless we are required by law to retain it.

b. Objecting to advertising

As your contract partner, we use your telephone number and e-mail address to send you information via Messenger, SMS, MMS and e-mail for advisory, advertising and similar purposes.
You can object to the use of your telephone number and e-mail address for these purposes at any time

c. Unsubscribe to the newsletter

If you no longer wish to receive our newsletter, click on the link that is provided at the end of the newsletter to unsubscribe.

8. Your data protection service

Our data protection specialists are here to help you with your requests for information, correction and erasure, and your objections. Use our online data protection service for all data protection-related enquiries: www.vodafone.de/business/digitalisierung/datenschutz-privatsphaere.html
Or write to
Dr Dirk Herkströter, Data Protection Officer, Vodafone GmbH
Dr. Anastasia Meletiadou, Datenschutz-Beauftragte Vodafone Deutschland GmbH/Vodafone West GmbH
Ferdinand-Braun-Platz 1, 40549 Düsseldorf.
If we are not able to help you with your data protection enquiry, you can contact our supervisory authority.

For telecommunication-related data protection enquiries:
The Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Husarenstrasse 30, 53117 Bonn
For website-related data protection enquires: The North Rhine-Westphalian State Commissioner for Data Protection and Freedom of Information,
Postfach 20 04 44, , 40102 Düsseldorf
For other data protection enquiries relating to Vodafone Deutschland GmbH, contact the
Bavarian State Office for Data Protection Supervision, Postfach 606, 91511 Ansbach.

II. Telephone or internet contract

If you have an internet or phone contract with us the following privacy notice also applies.

1. Traffic and location data

We process your traffic data to provide our internet and telephony services. Traffic data comprises data which are processed during the provision of the telecommunications service, such as time of connection establishment and termination, calling and called numbers, volumes of data transmitted, telecommunications services used and, in the case of mobile calls, your location. Message content is not traffic data and therefore not stored by Vodafone.
We erase all traffic and location data upon expiry of the legally prescribed retention periods. Internet service data are deleted after 7 days at the latest. We delete voice service data which are not relevant for billing immediately, and otherwise 3 months at the latest after the invoice is issued.

2. SMS spam protection

When you subscribe to one of our mobile tariffs we check your text messages to see if they contain spam or malware. These checks are performed by analysing the number of recipients of the same message and suspicious links. If we ascertain that a text message contains spam or malware, it is not delivered. This serves to protect the recipients of text messages from unsolicited messaging or damage to their IT systems and it protects our network against incidents.

3. Itemised call statements

You can request to receive or not receive an itemised call statement for charged calls in future billing periods.
If you request an itemised call statement, please note the following:

- You can choose whether you want to have the entire number or just the last three digits of called numbers listed.
- The itemised call statement must be requested by you before the relevant billing period.
- If the subscriber has a business or organisation line, a written declaration is necessary confirming that all employees have been or will be informed and that the works council or the HR/employee representative has been notified as is required by law.
- The itemised call statement only includes charged connections. Calls placed under flatrate arrangements are not listed. We erase your itemised call statements 6 months at the latest after the invoice is issued.

4. User directory listings

You can request Vodafone to list your number, address, name/company name and additional information such as occupation, sector, type of connection and co-users (subject to their consent) in public phone directories. There is a choice of a listing in printed or electronic directories, or you can also opt for no listing at all. It is also possible to list your data for directory enquiries purposes only. Vodafone may provide the data you have approved for publication to third parties (network operators, service providers) for the purpose of publishing subscriber directories and providing information services. At any time, by way of declaration, you can instruct Vodafone to restrict the scope of your listing or object to the publication of your listing.

5. Directory services

In some cases Vodafone or a third party may disclose customer data contained in public subscriber directories, e.g. when your telephone number is requested. If you are included in a directory,

- your number will be made available by the directory enquires service unless you have requested it not to be. If you do wish your number to be disclosed, you can decide whether or not the entire entry is disclosed.
- Your name and address will be disclosed to persons who only know your number (reverse search) unless you instruct otherwise.

6. Caller line identity presentation

The Vodafone service allows you to partially or permanently hide your number, provided that your device supports this feature. If your device does not support Calling Line Identity Presentation (CLIP) or you do not want to present your number it can be permanently hidden.

7. Protection of your mobile identity

In many online services, such as online banking or your social media profile, you can use your mobile number as an additional security factor. For example, if you use mTAN for banking, which requires such ID verification, Vodafone GmbH will check your mobile phone number and other security relevant criteria at to protect you from fraudulent transactions at your bank's request.
Security relevant criteria are information that indicate use of your mobile number for fraudulent purposes or identity fraud, e.g. if a SIM card is replaced or a number is changed or ported shortly before an online transaction, or when the name and mobile number provided for an online transac-

tion do not correspond to the information that we have on file about you. After our check your retailer will receive information about whether such security relevant criteria exist and, if yes, whether and for how long you have had an active contract (prepaid or fixed-term) for the mobile phone number. Other than that we do not share any of your personal data.
If security relevant criteria exist your retailer will then offer you an alternative way of concluding your online transaction. Your online provider's privacy policy contains information about whether such a security check is made. We do not directly disclose security relevant criteria to the online retailer in order to more effectively protect your personal data. Instead, we disclose it to an intermediary data custodian. The custodian removes the information about the mobile services provider when passing these data to the online retailer. The legal basis is Art. 6 (1) f) GDPR in conjunction with our legitimate interest, and the legitimate interest of the online retailer to protect you against the fraudulent use of your mobile phone number and identity theft. You can object to this processing at any time if you state the reasons particular to your situation. The contact details for objections are provided in section 8.
In all other cases, security relevant criteria are only checked by us if your online retailer has obtained your explicit consent. This particularly applies if it is necessary to process your service or location data for this purpose.

8. Processing of anonymous data for statistical and research purposes

We also anonymise your personal data for statistical and research purposes. The same applies to your traffic and location data. These kinds of anonymous analyses can include extrapolations of traffic flows or SIM cards to show how groups of mobile devices move. For example, we support researchers and statisticians to understand the impacts of pandemics on tourism and develop strategies to deal with them more effectively. Under no circumstances are your personal data transferred to third parties for these purposes. In other words, the analysis results are abstract insights which cannot be linked to specific people and it is therefore impossible for you to be identified in this way. We ensure this with our anonymisation process which involves, for instance, creating groups of multiple mobile devices.

III. F-Secure

If you subscribe to the 'powered by F-Secure' security bundle you enter into a contract with our cooperation partner: F-Secure Corporation, Tammasaarenkatu 7, PL 24, 00181 Helsinki, Finland.
For that reason we transfer your contract data to F-Secure. We and F-Secure are responsible for the processing of your personal data. Further information about data protection at F-Secure can be found at:
https://www.f-secure.com/de/legal/privacy/statement . If you are a customer of Vodafone West GmbH and you buy the security product 'F-Secure' we process your master data (mainly your customer number to assign an F-Secure licence from our contingent to it) for the performance, implementation and billing of services, to ensure technical availability and for information security (virus protection/ malware protection) to the extent that is permitted by law.
Information about credit assessments and fraud checks
If we perform a credit assessment or fraud check in connection with a product you have ordered, the following privacy notice also applies.

SCHUFA and CRIF GmbH credit assessments
We transfer personal data provided during the conclusion, execution and termination of the contract, such as your name, date of birth and IBAN number, as well as information about incidents of non-compliance or fraudulent acts to CRIF GmbH, Leopoldstrasse 244, 80807 München ('CRIF GmbH'). Vodafone GmbH and Vodafone Deutschland GmbH also transfer the above-stated data to SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden ('SCHUFA'). The legal bases for transferring the data are Art. 6 (1) b) and Art. 6 (1) f) GDPR in conjunction with our legitimate interest to minimise the risk of payment default and fraud. Data exchange with SCHUFA and CRIF GmbH also serves the purposes of meeting statutory obligations to perform customer credit assessments (section 505a and 506 of the German Civil Code). SCHUFA and CRIF GmbH process the data they receive and use it for scoring to provide their contractual partners in the European Economic Area, Switzerland and third countries (the latter only if a Commission adequacy decision exists in their respect) with information for their assessment of the creditworthiness ('credit scoring') of natural persons.
Independently of credit rating scoring, SCHUFA supports its contract partners by creating profiles to identify potential fraud patterns (e.g. for the purpose of fraud prevention in mail order transactions). Contract partner enquiries to SCHUFA are analysed to identify such anomalies. This calculation, which is carried out individually for the respective business partner, may also include address data, information whether and in which function an entry on a person in public life with matching personal data is included in generally accessible sources, as well as aggregated statistical information from the SCHUFA database. The procedure has no impact on SCHUFA's credit assessment or credit rating scoring.
Further information about SCHUFA's activities can be found online at www.schufa.de/datenschutz .
Further information about CRIF GmbH's activities can be found online at www.crif.de/datenschutz .

1. Infoscore checks

We transfer your data (name, address and possibly date of birth) to infoscore Consumer Data GmbH, Rheinstr. 99, 76532 Baden-Baden ("ICD") for the purpose of credit assessments, to request information enabling us to assess the default risk based on mathematical-statistical methods and use address data to verify your address (deliverability check). The legal bases for the transfer of the data are Art. 6 (1) b) and Art. 6 (1) f) GDPR. Detailed information on ICD pursuant to Art. 14 GDPR, i.e. information about the business object, the purpose of data storage, data recipients, right to information, right to erasure or correction etc. can be found in the appendix or at the following link:
https://finance.arvato.com/icdinfoblatt .

2. In-house pre-check (whitelist)

Vodafone companies share information about your positive payment behaviour in the past with us. Such information is taken into account in the credit assessments and, in some cases, positive payment behaviour information results in a waiver of the credit assessments at the above credit rating agencies. It is also in our legitimate interest to do this pursuant to Art. 6 (1) f) GDPR. Furthermore, it ensures that customers with positive payment behaviour are not rejected. You can object to this processing at any time if you state the reasons particular to your situation.

3. In-house pre-check (blacklist)

Vodafone companies additionally maintain a common blacklist of (former) customers with negative payment behaviour or persons under guardianship. Blacklisted (former) customers are either customers whose contracts were or may be cancelled due to payment default or customers in a dunning/ payment by instalments process. The latter are removed from the blacklist as soon as the debt is cleared. Persons under guardianship are included in the blacklist if the guardian provides written proof of the guardianship. They are also removed from the blacklist as soon as a Vodafone company is informed that the guardianship has ended. The data processed in these cases are: first name, surname, address, e-mail address, telephone number, date of birth, customer number, IBAN and the listing criterion. The legal basis is Art. 6 (1) f) GDPR in connection with our legitimate interest to take preventative action to protect ourselves against payment default, fraud and to protect persons without the capacity to contract against unwarranted claims. You can object to this processing at any time if you state the reasons particular to your situation.

4. Fraud prevention in online orders

If you place an online order with us, we perform the following additional checks.
Before accepting the online order we check the information about the device you are using to place the order. We transfer this information to Risk Ident GmbH, Am Sandtorkai 50, 20457 Hamburg ("Risk Ident"). Risk Ident operates a database of devices that have been identified as having been involved in online fraud in the past. Risk Ident uses browser fingerprinting on our website to identify a specific devices and the device's technical configuration. If the device is suspected of having been used for online fraud, we are sent a warning. We use this in conjunction with the other checks set out in this section 4. as the basis for our decision on whether to accept the order.
If the assessment performed by CRIF GmbH in accordance with section 4 a) does not provide an unambiguous result on fraud probability, or it reveals that you are an online banking customer, we may request you to verify your personal banking details. You then decide on the basis of a separate consent form whether to authorise your bank to provide online verification of your order data.
The legal basis for this is Art. 6 (1) f) GDPR and our legitimate interest to prevent fraud and protect ourselves against payment default, and the legal basis for the online verification by your bank is your separate consent in accordance with Art. 6 (1) 1a) GDPR.