BT privacy policy

Central Eastern Europe

Current version - applicable from 18 May 2018

Contents

Welcome

Why do we have a separate privacy policy for CEE?

Although BT has a BT.com Privacy Policy that applies to all BT entities and all of its employees globally, in order to comply with the relevant local regulations BT needs to set some additional rules.
This addendum serves as a complementary policy to the BT.com Privacy Policy and only amends and adds information that is relevant for BT in the CEE countries. Therefore, the present policy must be interpreted in line with the BT.com Privacy Policy. The present policy will prevail in every case if it differs from the BT.com Privacy Policy, however, the BT.com Privacy Policy remains applicable.

Common rules for CEE

Hereby we list the rules and pieces of information that are additional to the BT.com Privacy Policy and that apply throughout the CEE region. Please note that we have further specific rules for some countries that we list below.

Additional information

Please note that the present policy and the BT.com Privacy Policy give a general overview of BT's data processing. In case of certain products and services you will receive more detailed information when taking the given service or purchasing the product. You should interpret this policy in line with the specific notices you receive. In case there is a deviance between the two, BT applies the rules indicated in the specific notices.

Who do we involve when processing your information

When providing the service BT uses several other service providers that assist BT in doing so. This is necessary to maintain the quality of the service but this means that in certain occasions other entities have access to your personal data other than BT who become BT's data processors. In this case BT ensures that they protect and process your personal data in line with BT's high standards. You are entitled to ask BT what data processors it employs in case of the given product you use.

Hungary

Instead of the credit and fraud prevention checks information detailed in the BT.com Privacy Policy BT applies the following rules in Hungary.

To run credit and fraud prevention checks

Before we provide you with a product or service (including upgrades or renewals), or sometimes when you use our products and services, we'll use personal information you have given us together with information we have collected from other electronic communication service providers directly or via the aggregated customer database made under section 158 of the Hungarian Act No. C of 2003 on electronic communications and other publicly available sources. We use this information to manage our credit risk, and prevent and detect fraud. We might also use these databases to confirm your identity. When they get a search from us, a 'footprint' goes on your file which other organisations might see. We might also share the information with other electronic communications service providers. We do this because it's in our, and the organisations', interests and the Hungarian law allows us to acquire personal data to prevent fraud and money laundering, and to check identities, to protect our business and to keep to laws that apply to us.
Details of the personal information that will be used include your identifying information and credit risk you pose to electronic service providers.

If you don't become one of our customers, we'll still keep the result of our credits checks about you if we have a legal obligation and it's in our legitimate interests to help prevent or detect fraud. Your personal information can be retained in the database for a limited periods of time, and if you are considered to pose a fraud or financial risk, your information can be held in the database for a 1 year period from the due date of claim that resulted in your data being represented in the database.
If you give us false or inaccurate information which we identify as fraudulent we might share it with law enforcement agencies, as may the agencies we have shared the information with.
If you tell us you're associated with someone else financially (for example, by marriage or civil partnership), we'll link your records together. So you must make sure you have their agreement to share information about them.
If we fraud or credit risk, we may refuse to provide the services or financing you have asked for, or we may stop providing existing services to you.
The electronic communications service providers keep a record of any fraud or credit risk of their clients voluntarily and this may result in other organisations refusing to provide services to you. If you have any questions about this, please contact us using the details below.
We might send other electronic communications service providers information about fraudulent customers and those with credit risk, and they keep that information. This includes telling them about your account balances, what you pay us and if you miss a payment (going back in the past, too). We might also share these details with the common database of electronic communications service providers. So if you don't pay your bills on time, other electronic communications service providers will be aware of that.

Please note that there are no data brokers operating in Hungary, therefore BT does not apply them when providing services to Hungarian clients.

Remedies

Data Subjects may, in the event of an infringement of their rights, file a petition to any Hungarian courts.
Requests for remedy and any complaints may also be addressed to the Hungarian data protection authority:
Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information)
Registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Postal address: 1530 Budapest, Pf. 5.
Telephone: +36 1 391 1400
Facsimile: +36 1 391 1410
E-mail: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu

Local legal environment:

Besides the GDPR BT applies the following statutes when processing your personal data:
Act CXII of 2011 on the right to information self determination and the free flow of information
Act CXXXXIII of 2005 on the rules of security activities and private detectives

Poland

Instead of the credit and fraud prevention checks information detailed in the BT.com Privacy Policy BT applies the following rules in Poland.

To run credit and fraud prevention checks

Before we provide you with a product or service (including upgrades or renewals), or sometimes when you use our products and services, we'll use personal information you have given us together with information we have collected from bureaus of economic information, operating due to provisions of the statute on disclosing economic information and exchange of economic information dated on 9 April 2010. We use this information to manage our credit risk, and prevent and detect fraud. We might also use these pieces of information to confirm your identity. When they get a search from us, a 'footprint' goes on your file which other organisations might see.

Details of the personal information that will be used include your identifying information and credit risk you pose to an electronic service provider.

If you give us false or inaccurate information which we identify as fraudulent we might share it with law enforcement agencies, as may the agencies we have shared the information with.

If you tell us you're associated with someone else financially (for example, by marriage or civil partnership), we'll link your records together. So you must make sure you have their agreement to share information about them.

If we identify fraud or credit risk, we may refuse to provide the services or financing you have asked for, or we may stop providing existing services to you.

The electronic communications service providers keep a record of any fraud or credit risk of their clients voluntarily. If you have any questions about this, please contact us using the details below.

If you don't pay your bills on time, we might submit information about it to bureaus of economic information, which means that any business entity using their services will be aware of that.

Remedies

Data Subjects may, in the event of an infringement of their rights, file a petition to any Polish courts.

Requests for remedy and any complaints may also be addressed to the Polish data protection authority:
Urząd Ochrony Danych Osobowych (Personal Data Protection Office)
Registered office: ul. Stawki 2, 00-193 Warszawa, Poland
Telephone: +22 531 03 00
Fax +22 531 03 01
Website: https://www.uodo.gov.pl

Local legal environment

Besides the GDPR BT applies the following statutes when processing your personal data:
Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 13 czerwca 2016 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Czech Republic

Instead of the credit and fraud prevention checks information detailed in the BT.com Privacy Policy BT applies the following rules in the Czech Republic.

What information we collect and what we use it for

In the Czech Republic we use some of the information processed for the conclusion of the contract and the provision of the services to maintain an up-to-date database of all our customers to the publicly available telephone service as required by the Act No. 127/2005 Coll. on Electronic Communications (§61).
In line with the Act No. 127/2005 Coll. (§90), we will use your traffic data related to services used by you for marketing purposes only upon your prior consent.

To run credit and fraud prevention checks

Before we provide you with a product or service (including upgrades or renewals), or sometimes when you use our products and services, we'll use personal information you have given us together with information we have collected from credit reference information database (such as SOLUS),, other electronic communication providers or publicly available sources (such as public business registers). We use this information to manage our credit risk, and prevent and detect fraud and money laundering. We'll also use these database to confirm your identity. When they get a search from us, a 'footprint' goes on your file which other organisations might see. In line with the Act No. 634/1992 Coll. on the Consumer Protection, we can register in a credit reference information database (such as SOLUS), which brings together companies from different economic sectors, including banks, non-bank financial institutions, and others and enables to share negative information about the clients who are not interested in paying their contractual liabilities and/or about the clients who have trouble with paying their debts.

We might also share with other electronic communication service providers data related to the provision of the service, namely data about the subscribers being connected, data needed to ensure interconnection and access to the network, data needed for mutual billing, and for identification of any abuse of the electronic communications network (malicious and/or annoying calls) and services (consistent late payment). We do this because it's in our, and the organisations', legitimate interests to prevent fraud and money laundering, and to check identities, to protect our business and to keep to laws that apply to us.
Details of the personal information that will be used include your identifying information, financial information and credit risk.
If you don't become one of our customers, we'll still keep the result of our credits checks about you if we have a legal obligation and it's in our legitimate interests to help prevent or detect fraud.
If you give us false or inaccurate information which we identify as fraudulent, we might also share it with law enforcement agencies, as may the organisations we have shared the information with.
If you tell us you're associated with someone else financially (for example, by marriage or civil partnership), we'll link your records together. So you must make sure you have their agreement to share information about them.
If we decide that you are a credit, fraud or money laundering risk, we may refuse to provide the services or financing you have asked for, or we may stop providing existing services to you.
The organisations providing a credit reference information database will keep a record of any fraud or money laundering risk and this may result in other organisations refusing to provide services, or financing to you. If you have any questions about this, please contact us using the details below.
We might send to a credit reference information database details of your accounts and bills, including how you manage them. This includes telling them about your account balances, what you pay us and if you miss a payment (going back in the past, too). So if you don't pay your bills on time, it will be recorded in the credit reference information database.
Please note that there are no data brokers operating in the Czech Republic, therefore BT does not apply them when providing services to Czech clients.

To meet our legal and regulatory obligations

We might have to release personal information about you to meet our legal and regulatory obligations.

To law enforcement agencies

Under investigatory powers legislation, we might have to share personal information about you to government and law-enforcement agencies, such as the police, to help detect and stop crime, prosecute offenders and protect national security. They might ask for the following details.

☐ Your contact details. This includes your name, gender, address, phone number, date of birth, email address, passwords and credentials (such as your security questions and answers) needed to confirm your identity and your communications with us.

☐ Your communications with us, such as calls, emails and webchats.

☐ Your payment and financial information.

☐ Details of the products and services you've bought and how you use them – including your call, browser (including IP address) and TV records

We may be requested by certain authorities such as law enforcement authorities, the Czech National bank, intelligence service to submit them traffic and location data related to services used by you for purposes determined by separate acts (such as to prevent crime, identify a person).

According to the Act No. 127/2005 Coll. on Electronic Communications (§97) and Act No. 141/1961 Coll. Criminal Procedure Code (§88, §88a) we must set up and secure interfaces at specified points of our network to to enable the Police and Intelleigent services to connect their terminal equipment and carry out interception and recording of messages in criminal proceeding specified by the Criminal Procedure Code.

The balance between privacy and investigatory powers is challenging. We share your personal information when the law says we have to, but we have strong oversight of what we do and get expert advice to make sure we're doing the right thing to protect your right to privacy. You can read more about our approach to investigatory powers in our report on Privacy and free expression in UK communications
https://www.btplc.com/Thegroup/Ourcompany/Ourvalues/Privacyandfreeexpression/index.htm

You can find the terms of reference for our oversight body here
https://www.btplc.com/Thegroup/Ourcompany/Theboard/Boardcommittees/InvestigatoryPowers/index.htm

We'll also share personal information about you where we have to legally share it with another person. That might be when a law says we have to share that information or because of a court order.
In limited circumstances, we may also share your information with other public authorities, even if we do not have to. However, we would need to be satisfied that a request for information is lawful and proportionate (in other words, appropriate to the request). And we would need appropriate assurances about security and how the information is used and how long it is kept.

For regulatory reasons

We'll also use your call, browser (including IP address) and TV records to find the best way of routing your communications through the various parts of our network, equipment and systems as required by our regulator.
If you order a phone service, we'll ask if you want your details included in any directory services such as our Phone Book and to what extent. If you do, we'll publish your details in our directory service and share that information with other providers of directory services or directory enquiry services. Ex-directory numbers aren't included and will not appear in The Phone Book.

Protecting your information and how long we keep it

How do we protect your personal information?

We have strict security measures to protect your personal information. We check your identity when you get in touch with us, and we follow our security procedures and apply suitable technical measures, such as encryption, to protect your information.

How long do we keep your personal information?

We'll keep:

- a summary copy of your bills for six years from the date of the bill;

- your contact details on file while you're one of our customers, and for six years after; and
- details relating to any dispute for six years after it was closed.

According to the Act No. 127/2005 Coll. on Electronic Communications (§97) we must store traffic and location data related to services used by you for a period of 6 months. We can further store your traffic data (including location) for the period:

- during which the bill may be legally challenged or the claim for the payment may be asserted or the payment collected;
- of ongoing dispute resolution.

In other cases we'll store personal information for the periods needed for the purposes for which the information was collected or for which it is to be further processed. And sometimes we'll keep it for longer if we need to by law. Otherwise we delete it.

Remedies

Data Subjects may, in the event of an infringement of their rights, file a petition to any Czech courts.
Requests for remedy and any complaints may also be addressed to the Czech data protection authority:
Úřad pro ochranu osobních údajů (The Office for Personal Data Protection)
Registered office: Pplk. Sochora 27, 170 00 Praha 7, Czech Republic
Telephone: +420 234 665 800
E-mail: posta@uoou.cz
Website: http://www.uoou.cz

Local legal environment

Besides the GDPR BT applies the following statues when processing your personal data:
Zákon č. 101/2000 Sb.Zákon o ochraně osobních údajů a o změně některých zákonů
Zákon č. 106/1999 Sb. Zákon o svobodném přístupu k informacím