openreach

Openreach Data Processing Guidelines for CPs

Openreach Information Assurance

January 2019

Contents

Welcome

We've created this documentation to reflect the changes in data-protection laws.

Our main role is as a wholesaler providing services to communications providers to connect homes, mobile phone masts, schools, shops, banks, hospitals, libraries, broadcasters, governments and businesses – large and small – to the world.

What is this document for?

We always need a good reason to process end customer personal data provided by you. This document explains the reasons we collect information as set out in our product contracts.

We receive information from you to install or maintain a connection to your end customer premises under an order from you. This involves the use of personal information. And we believe that it's very important for our customers to trust us with that information. We want you to be confident that we'll keep it secure and use it both lawfully and ethically, respecting your customer's privacy.

We've included a glossary which explains the meaning of any technical terms we use.

Our support for the right to privacy, as part of our broader commitment to human rights, is stated in our human rights policy. And our privacy policy explains in detail how we use personal information where we are a Data Controller.

What's not included?

This guidance doesn't apply to information about our employees or shareholders.

What about cookies?

You can read our cookie policy here for information about how we use cookies on our website.

If your customer asks you to update how we use their information

We won't respond to requests directly from your customers or your resellers. If your customers contact us we will reject the request and inform them they need to contact you.

Applications on behalf of your customers will need to adhere to the following process:-

You need to use our online form. Once we've looked at your request, we'll let you know when you can expect to hear from us.

We'll always try to help you with your request but we can refuse if we believe doing so would have a negative effect on others or the law prevents us. And even though we have to complete your request free of charge, we're allowed to reject requests if:

- they're repetitive;
- you don't have the right to ask for the information; or
- the requests made are excessive.

If that's the case, we'll explain why we believe we don't have to fulfil the request.

We'll respond to a request electronically unless you advise us otherwise.

In some cases, we might decide to keep information, even if you ask us not to. This could be for legal or regulatory reasons, so that we can keep providing our products and services, or for another legitimate reason. For example, we keep certain billing information to show we've charged you correctly.

We aim to provide our products and services in a way that protects information and respects your, or your end customers, request. Because of this, when you delete or change (or ask us to delete or change) personal data from our systems, we might not do so straight away from our back-up systems or copies on our active servers. And we may need to keep some information to fulfil your request.

What information we process and why

To provide you with products and services

We'll use end customers personal data provided by you to enable us to provide and maintain the products and services you order from us.

This means we'll receive:

- The address where you want us to provide service
- The on the day contact name and telephone number
- Information you give us if you have a vulnerable customer

We use this information to carry out our contract and provide products or services to you.

To run fraud prevention checks, prevent and detect crime (including contact with law enforcement agencies) and to meet our legal and regulatory obligations

We'll use your customer's personal data and your employee data to help prevent and detect crime and fraud. We'll also use it to prevent and detect criminal attacks on our network or against your equipment. We monitor traffic over our network, trace nuisance or malicious calls, and track malware and cyber-attacks. We might have to release personal data about you or your customers, to meet our legal and regulatory obligations. Under investigatory powers legislation, we might have to share personal data about you, or your customers, to government and law enforcement agencies, such as the police, to help detect and stop crime, prosecute offenders and protect national security.

To do that we use the following information, but only where strictly necessary.

- Details of the products and services you, or your customers, have bought and how you, or they, use them
- Information on the individual services provided to your customers
- CCTV footage in and around our buildings.
- Your communications with us, such as calls, emails and webchats.

We use this personal information because we have a legitimate interest in protecting our network and business from attacks and to prevent and detect crime and fraud. We also share it with other organisations who have the same legitimate interests. Doing this helps make sure our network works properly and helps prevent attacks. The balance between privacy and investigatory powers is challenging. We share your customer's 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 the BT report on Privacy and free expression in UK communications. And you can see the terms of reference for the BT oversight body here.

We'll also share personal information about you or your customers 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.

We have to report certain information to our regulators, such as Ofcom, which might include personal information. We'll only do so in confidence and where it is necessary to fulfil our obligations.

Sharing end customer personal data provided by you

Who do we share end customer personal data provided by you with, why and how?

We may share end customer personal data provided by you with other companies within the BT Group. We have a group-wide arrangement, known as binding corporate rules. Openreach has signed and committed to work within these rules to make sure end customer personal data provided by you is protected. You can ask for a copy of our binding corporate rules by emailing our Information Assurance team, contact details can be found here.

We use suppliers in order to provide and maintain our products and services to you. Details of how they handle end customer personal data provided by you are set out below.

Using other service providers

We use suppliers to carry out services on our behalf or to help us provide products and services to you.

Where we use another organisation, we still protect end customer personal data provided by you. And we have strict controls in place to make sure it's properly protected.

.

If we need to transfer end customer personal data provided by you to another organisation for processing in countries that aren't listed as 'adequate' by the European Commission, we'll only do so if we have model contracts or other appropriate safeguards (protection) in place.

If there's a change (or expected change) in who owns us or any of our assets, we might share personal information to the new (or prospective) owner. If we do, they'll have to keep it confidential.

The countries we share personal information to

BT Group is a large multinational organisation. Our binding corporate rules reflect how we operate. They include a list of countries (below) which are structured to allow us to transfer personal information to the countries where we have a presence. For us, after the UK and wider EU, India and the Philippines are where most of our processing of personal information takes place. While our binding corporate rules allow us to transfer personal information to these countries, the information won't always include the personal information you provide to us in every case.

Algeria, Argentina, Australia, Bahrain, Bangladesh, Barbados, Bermuda, Bolivia, Bosnia and Herzegovina, Botswana, Brazil, Canada, China, Colombia, Costa Rica, Cote d'Ivoire, Dominican Republic, Ecuador, Egypt, El Salvador, Ghana, Gibraltar, Guatemala, Honduras, Hong Kong, India, Indonesia, Isle of Man, Israel, Jamaica, Japan, Jersey, Jordan, Kazakhstan, Kenya, Republic of Korea, Lebanon, Macedonia, Malawi, Malaysia, Mauritius, Mexico, Moldova, Montenegro, Morocco, Mozambique, Namibia, Nicaragua, Nigeria, Norway, Oman, Pakistan, Panama, Paraguay, Peru, Philippines, Puerto Rico, Qatar, Russian Federation, Serbia, Singapore, South Africa, Sri Lanka, Switzerland, Taiwan, Tanzania, Thailand, Trinidad and Tobago, Tunisia, Turkey, Uganda, Ukraine, United Arab Emirates, United States, Uruguay, Venezuela, Vietnam, British Virgin Islands, Zambia and Zimbabwe.

When we make a change to the suppliers we share the personal information provided by you we'll notify you. We'll issue a briefing to inform you of the change and the template is shown in Annex 1. The details of the change will be set out in a spreadsheet which will set out the company name, a summary of the services they provide and the countries they process data in. The list can be accessed here

If you disagree with the new supplier processing the personal data provided by you to Openreach, you can object if you have concerns on its ability to adhere to data privacy legislation. You'll need to raise your concerns by emailing dataprivacy@openreach.co.uk, setting out the details of your objection. This needs to be sent within 90 days of Openreach notifying Communications Providers.

Protecting end customer personal data provided by you and how long we keep it

How do we protect end customer personal data provided by you?

We have strict security measures to protect end customer personal data provided by you. We follow our security procedures and apply suitable technical measures to protect end customer personal data provided by you.

How long do we keep end customer personal data provided by you?

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data and the purpose for which we process the personal data and the applicable legal requirements.

Unless there is a specific regulatory or legal requirement for us to keep your information longer, we'll keep your information for no longer than is necessary and only for providing and maintaining products and services to Communications Providers.

How to contact us and further details

You can get in touch with us in three ways:

- Email the BT Data-Protection Officer at cpo@bt.com
- Email the Openreach Head of Information Assurance at dataprivacy@openreach.co.uk, or
- Write to the address below and mark it for their attention.

pp 3.55F
Kelvin House
123 Judd Street
London WC1H 9NP

Glossary

We have included a description of how the technical terms we use are generally interpreted.

- **BT Group companies and BT Group plc** means EE Ltd, Plusnet plc, Openreach Limited, BT Communications Ireland Ltd, BT Business Direct Ltd, BT Cables Ltd, Tikit Ltd, BT Fleet Ltd, Pelipod Ltd and BT Law Ltd and the areas that make-up BT: Consumer, EE, Business and Public Sector, Global Services, Wholesale and Ventures, Technology, Service and Operations, Group Functions, BT Wifi, BT Shop and MyDonate.
- **Binding corporate rules** are designed to allow multinational companies to transfer personal information from the European Economic Area (EEA) to their affiliates outside of the EEA and to keep to data protection legislation.
- **Cookies** are small text files (up to 4KB) created by a website and stored in the user's connected device – either temporarily for that session only or permanently on the hard disk (called a persistent cookie). Cookies help the website recognise you and keep track of your preferences.
- **Model contracts** are standard contractual clauses set by the European Commission. They offer enough protection of people's privacy, fundamental rights and freedoms when their personal information is moved from within the EEA to outside of it. The contracts keep to data protection legislation.
- **Openreach, we** or **our** means Openreach Limited.
- **Personal data** means how the term is defined in the GDPR.
- **Regulatory obligations** means our obligations to regulators such as Ofcom and the Information Commissioners Office.