

AT&T Business Customer GDPR Privacy Notice

This Notice explains AT&T's commitment to compliance with the European Union's General Data Protection Regulation (GDPR) and how GDPR affects you as a user of AT&T business services. This Notice defines key terms and answers important questions, such as who is covered by GDPR, what GDPR requires, and how AT&T operates within those requirements.

AT&T's Commitment to Data Protection

AT&T is committed to fulfilling our responsibilities in relation to collection, retention, use, and other processing of personal data that is within the scope of the General Data Protection Regulation. Such personal data will be processed only for lawful and appropriate purposes. AT&T has implemented measures designed to ensure security of personal data and to prevent unauthorized or accidental access, erasure, or other misuse of personal data. AT&T will facilitate the exercise of data subject rights in an effective and transparent manner.

Definitions

Term	Meaning
GDPR	The European Union's (EU) General Data Protection Regulation (EU 2016/679)
AT&T Business Customer	A legal entity (excluding AT&T affiliates) that has contracted with AT&T to provide Services
Customer Data Subject	An identified or identifiable individual authorized by an AT&T Business Customer to use the Services or to interact with AT&T on behalf of the AT&T Business Customer
Data Controller	An entity that determines the purposes and means of the Processing of Personal Data
Personal Data	Any information relating to an identified or identifiable natural person
Processing	Any operation(s) performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Services	The products and services provided by AT&T under a contractual agreement between AT&T and the AT&T Business Customer
Special Categories of Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Processing of Personal Data relating to criminal convictions and offenses may also have additional safeguards under Member State law.



Who is covered by this Notice?

This AT&T Business Customer GDPR Privacy Notice applies when:

1. A Customer Data Subject creates Personal Data through use of AT&T Services within the European Union (EU) or the European Economic Area (EEA) in connection with the Customer Data Subject's relationship with an AT&T Business Customer or AT&T otherwise Processes Personal Data of a Customer Data Subject who is in an EU or EEA country;
2. Such Services are within the scope of GDPR; and
3. AT&T functions as a Data Controller when Processing the Personal Data of such Customer Data Subject.

Additional information for the Customer Data Subject may be available directly from the AT&T Business Customer. AT&T maintains other policies and notices, including the [AT&T Privacy Policy](#), that address data protection. Unless specifically stated otherwise, where another notice or policy conflicts with the purposes of this AT&T Business Customer Privacy Notice, this AT&T Business Customer Privacy Notice will prevail as to Customer Data Subject in the EU or EEA.

What Personal Data about Customer Data Subjects does AT&T Process?

AT&T generally Processes the following categories of data, which may include Personal Data of Customer Data Subjects:

- **Business Contact Data:** Data for general contact or administration purposes, which may include name, job title, employer, address, phone number, email address, instant messaging user name, and similar data.
- **Device Identification Data:** Data that identifies a device from which (or to which) electronic communications are sent (or received); may include Internet Protocol (IP) address, Media Access Control (MAC) address, International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, Serial Number, and Unique Device Identifier (UDID).
- **Electronic Communications Metadata:** Data processed in an electronic communications network for the purposes of transmitting, distributing, or exchanging electronic communications content (but not including electronic communications content); includes data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration, and type of communication.
- **Authentication Data:** User name, password, personal identification number, password hints, and similar data to authenticate users in connection with use of the Services or access to information related to the Services.

Why does AT&T Process Personal Data about Customer Data Subjects?

AT&T Processes Personal Data when a Customer Data Subject uses the Services or when the AT&T Business Customer provides the Personal Data to AT&T. In connection with the provision of Services, AT&T will generally Process Personal Data of Customer Data Subjects for the purposes of:

- Providing the Services to the AT&T Business Customer
- Performing obligations and exercising rights with respect to the Services and AT&T's contract with the AT&T Business Customer, including performing related activities and functions
- Complying with legal obligations
- Evaluating, supporting, and enhancing the performance, efficiency, and security of the Services.

AT&T Processes Personal Data of Customer Data Subjects only pursuant to appropriate lawful bases for Processing as necessary for:

- Performing a contract to which the Customer Data Subject is a party;
- Complying with a legal obligation(s) to which AT&T is subject; and/or
- Legitimate interests pursued by AT&T, such as performing its contract obligations to, or exercising its legal or contract rights with, the AT&T Business Customer, or for improving services and network operations.



In limited circumstances, AT&T may Process Personal Data as necessary for:

- Protecting the vital interests of the Customer Data Subject or another natural person; and/or
- Performing a task carried out in the public interest.

AT&T will not Process “Special Categories” of Personal Data about Customer Data Subjects unless specifically authorized by law, for example where the Customer Data Subject has given explicit consent; as necessary for carrying out obligations and exercising specific rights in the field of employment and social security and social protection law; and/or as necessary for the establishment, exercise, or defense of legal claims.

Who has access to Personal Data about Customer Data Subjects?

Personal Data about Customer Data Subjects will be disclosed, to the extent required for Service delivery, to appropriate and authorized recipients. Recipients may include: AT&T personnel; third party service providers and subcontractors; and/or other third parties performing services for any of the AT&T companies. Personal Data may also be provided to the AT&T Business Customer and its agents.

Third parties given access to Personal Data about Customer Data Subjects will be required to use appropriate security measures consistent with GDPR requirements when Processing Personal Data and, where the third party is Processing such Personal Data on behalf of AT&T, to do so only pursuant to AT&T’s instructions.

AT&T may disclose Personal Data if compelled to do so by a court of law or lawfully requested to do so by a relevant governmental authority using the appropriate means of request. AT&T may disclose Personal Data if AT&T determines it is necessary or appropriate to comply with the law or to protect or defend AT&T’s rights, property or employees.

Where is Personal Data about Customer Data Subjects Processed?

AT&T has centralized business activities to better manage a global business. That centralization may result in the transfer of Personal Data to countries outside of the EEA. For example, a Customer Data Subject’s Personal Data may be transferred for Processing in the United States of America, by AT&T and/or third party service providers.

AT&T generally transfers Personal Data about Customer Data Subjects between AT&T affiliates on the basis of our Intra-Group Agreement, which is based on the EU’s standard contractual clauses for export of Personal Data to third countries. A Customer Data Subject may request to access or review the safeguards AT&T uses for cross border transfers.

AT&T may additionally rely on other approved mechanisms for export of Personal Data the EEA, such as a determination by the European Commission that the recipient country offers adequate protection of Personal Data or pursuant to established derogations for specific situations.

Wherever Personal Data is Processed, AT&T uses appropriate security measures consistent with GDPR requirements.

When is Personal Data about Customer Data Subjects deleted?

Personal Data will be retained as needed for business administration, tax, or legal purposes and as consistent with applicable law, including GDPR. In many cases, this will require retention through the period of the contract between AT&T and the AT&T Business Customer, or through the period of the relationship between the AT&T Business Customer and the Customer Data Subject. After that, Personal Data will be destroyed by making it unreadable or undecipherable. While Personal Data is retained, AT&T implements appropriate technical and organizational measures designed to make the Personal Data collected secure. Such measures include:

- Maintaining and protecting the security of computer storage and network equipment and using security procedures that require user names and passwords to access sensitive data;
- Applying encryption or other appropriate security controls to protect Personal Data when stored or transmitted; and
- Limiting access to Personal Data to only those with jobs requiring such access.



What rights does a Customer Data Subject have to manage Processing of Personal Data?

GDPR grants the Customer Data Subject certain rights regarding Processing of Personal Data. AT&T is committed to honoring these rights and has established effective and transparent policies and procedures to do so. A Customer Data Subject's rights with respect to his or her own Personal Data include:

- **Right to Notice.** AT&T provides Customer Data Subjects with this GDPR Customer Privacy Notice detailing how Personal Data is Processed.
- **Right of Access.** A Customer Data Subject may obtain confirmation of whether Personal Data is being Processed and, if it is, access the Personal Data and additional information about the Processing of that data.
- **Right to Rectification.** A Customer Data Subject may have inaccurate Personal Data corrected and have incomplete Personal Data made complete.
- **Right to Erasure.** A Customer Data Subject may have Personal Data erased, in certain circumstances.
- **Right to Restriction of Processing.** A Customer Data Subject may have additional Processing of Personal Data temporarily prohibited while the accuracy or Processing of Personal Data is contested.
- **Right to Data Portability.** A Customer Data Subject may be able to receive Personal Data for the purpose of providing that Personal Data to another Controller.
- **Right to Object.** A Customer Data Subject may object to Processing of Personal Data at any time and on grounds relating to his or her particular situation.
- **Right to Information Regarding Automated Individual Decision-Making.** AT&T's Processing of Personal Data generally does not include automated decision-making that produces legal effects concerning the Customer Data Subject or similarly significantly affects the Customer Data Subject. In the event AT&T implements such automated-decision making, AT&T will provide meaningful information about the logic involved and the significance and the envisaged consequences of such Processing for the Customer Data Subject.

Whether and how a right applies will depend upon the lawful basis pursuant to which the data is Processed, the nature of the Personal Data, and AT&T's ability to determine that it holds responsive Personal Data. As the Personal Data is processed as part of AT&T's contract obligations to the AT&T Business Customer, for authentication purposes AT&T will coordinate responses to requests of Customer Data Subjects with the AT&T Business Customer. AT&T therefore recommends the Customer Data Subject directly contact the AT&T Business Customer to initiate a rights request. AT&T will work with the AT&T Business Customer to determine the appropriate response to a request. Provision of Personal Data in response to a Customer Data Subject's request shall not adversely affect the rights and freedoms of others.

Additional Information

A Customer Data Subject may file a complaint with the relevant data protection regulator, also known as a "supervisory authority." The relevant supervisory authority would likely be, but is not necessarily limited to, the supervisory authority of the country in which the Customer Data Subject is located. A Customer Data Subject may additionally or alternatively seek judicial redress for alleged infringements of applicable law by AT&T.

Questions on this AT&T Business Customer GDPR Privacy Notice may be sent to AT&T's Data Protection Officer at AskPrivacy@att.com. Please include "customer data subject question" in the email's subject line.

