Privacy Policy

This privacy policy (“Privacy Policy” or “Transatel Privacy Policy”) describes how Transatel (as defined below) uses, shares and protects personal data (“Personal Data”) collected and/or processed by Transatel. It summarises the organisational and technical measures, as well as the principles, that are in place to protect the confidentiality of personal data.

As Transatel’s registered office is located in France, Transatel complies primarily with the General Data Protection Regulation (No. 2016/679) of 27 April 2016 (“GDPR”) and the “Personal Data Protection Act” of 14 May 2018.

Transatel may also have subsidiaries that may collect and/or process personal data in accordance with applicable local regulations.

Ubigi is a trade mark under which Transatel markets mobile connectivity packages for the general public (including eSIM plans). Ubigi is not a separate legal entity: Transatel remains the data controller for personal data collected via the Ubigi website, app and services. This Privacy Policy therefore applies in full to the processing carried out in connection with the operation of the Ubigi brand, including where the term “Ubigi” appears on its own in the user interface.

Contact

Transatel

SAS (RCS Nanterre 432 786 432)

1, Passerelle des Reflets 92400 Courbevoie
FRANCE

Data Protection Officer (DPO)

dpo@transatel.com

If you have any questions, please contact our DPO.

If you have any queries regarding a service subscribed to under the Ubigi brand, you may also contact Ubigi’s customer service via the app or the ubigi.com website; your enquiry will, where appropriate, be forwarded to Transatel’s DPO.

What personal data does Transatel control and/or process?

Transatel’s activities are diverse. The information required varies depending on the specific activity. Transatel endeavours to collect and/or process only the information necessary for its employment relationships with its staff and for the operation of Transatel’s services.

Personal data comprises only information relating to natural persons who:

- who can be identified or are identifiable directly from the information in question (for example, their name); or
- can be indirectly identified from that information when combined with other information (for example, the MSISDN).

Personal data may also include special categories of personal data or data relating to criminal convictions and offences. Such data is more sensitive and you may only process it in more limited circumstances.

Pseudonymised data can help to reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

If personal data can be genuinely anonymised, the anonymised data is not subject to the GDPR. Information relating to a deceased person does not constitute personal data and is therefore not subject to the GDPR.

Information relating to businesses or public authorities does not constitute personal data. However, information relating to natural persons acting as sole traders, employees, partners and company directors, where they are individually identifiable and the information relates to them as natural persons, may constitute personal data.

The GDPR provides a non-exhaustive list of identifiers, including

- surname;
- identification number;
- location data; and
- an online identifier.

'Online identifiers' include IP addresses and cookie identifiers, which may constitute personal data.

Transatel may collect and/or process the following information:

As an employer, Transatel collects and processes information relating to employees and job applicants:

- Identification details (e.g. name, address, telephone number, copy of ID document, etc.)
- Financial information (e.g. IBAN, etc.)
- Application-related information (e.g. CV, cover letter, etc.)

As a provider of mobile services for businesses (MVNx, IoT), Transatel processes:

- Information about individuals representing Transatel's customers (name, address, telephone number, email address, etc.)
- Information on traffic usage by the end users of Transatel's customers:
    - Provisioning information
    - xDR (e.g. MSISDN, ICCID, numbers dialled, etc.)
    - Voice messages
    - SMS content
    - Data traffic information (e.g. IP address, websites visited, etc.)

As a retail mobile service provider for end-user customers (Ubigi brand, operated by Transatel), Transatel collects and processes the following data:

- Identification details (e.g. name, address, telephone number, copy of ID document, etc.)
- Financial information (e.g. IBAN, etc.)
- Information on data usage by Transatel subscribers:
    - Provisioning information
    - xDR (e.g. MSISDN, ICCID, numbers dialled, etc.)
    - Voice messages
    - SMS content
    - Data traffic information (e.g. IP address, websites visited, etc.)
- VIN (vehicle identification number)

- Device and eSIM identifiers (e.g. IMEI, EID)
- Country of connection to the visited mobile network (location data at country level, derived from roaming)
- Account and usage data for the Ubigi website and app (login credentials, data plan purchase history, preferences)
- Payment data, processed by our payment service providers and, where applicable, by the Apple App Store and Google Play platforms
- Cookies and trackers placed on the Ubigi website and app
- Customer support data (communications with Ubigi customer service via chat, email or telephone)

Information processed by Transatel in the course of its M2M business is not covered by the GDPR, unless it relates to individuals representing Transatel's M2M client.

Purpose of collection and/or processing

As a data controller, Transatel collects and processes personal data to employ its own staff and to provide a mobile service to its own end users (notably under the Ubigi brand).

As a data processor, Transatel processes personal data on behalf of its MVNO clients, who are data controllers, in order to provide them with integrated mobile solutions which they use to provide mobile services to their own subscribers.

Legal bases for processing (Article 6 of the GDPR)

Transatel ensures that all processing of personal data, including that carried out under the Ubigi brand, is based on one of the legal bases set out in Article 6 of the GDPR. These legal bases vary depending on the purpose pursued:

- Performance of a contract (Art. 6(1)(b)): provision of the mobile and Ubigi services subscribed to, customer account management, billing and customer service.
- Legal obligation (Article 6(1)(c)): combating fraud and crime, retention of traffic data, compliance with accounting, tax and regulatory obligations.
- Legitimate interests (Article 6(1)(f)): network security and integrity, fraud prevention, service improvement, and the compilation of aggregated and anonymised statistics.
- Consent (Art. 6.1.a): placement of non-essential cookies, sending of marketing communications and newsletters and, where applicable, precise geolocation.

Where processing is based on your consent, you may withdraw it at any time, without this affecting the lawfulness of the processing carried out prior to such withdrawal, by amending your account settings or those of the Ubigi app, or by contacting our DPO.

Marketing communications and newsletters

Data subjects and data processed

When you subscribe to our newsletter, create an account or make a purchase, Transatel may process your data in order to send you marketing communications (offers, news, advice relating to our services). This applies to both customers and individuals who have subscribed to our communications but are not customers (prospects).

For this purpose, we process, in particular: your email address, your name, your language and country, your communication preferences, as well as data relating to your interactions with our messages (see point C below).

Purpose and legal basis

This data is used to send you our communications, manage their frequency and personalise their content. This processing is based on your consent. For existing customers, sending communications relating to similar services may be based on our legitimate interest, subject to the conditions set out in the applicable regulations. In all cases, you may withdraw your consent or object to receiving these communications at any time (see the 'Individuals' rights' section).

Tracking our emails (tracking pixels and links)

Our marketing emails may contain tracking technologies, namely tracking pixels and personalised tracking links.

- Purposes. These technologies enable us to determine whether our emails are opened and whether the links they contain are clicked on. This information is used to measure the performance of our campaigns, adjust the frequency of our mailings, and personalise our content according to your interests.
- Legal basis. The use of these technologies for measurement and personalisation purposes is based on your consent. This consent is separate from the consent you give to receive our communications: you can receive our emails without being subject to this tracking.
- Scope. Where you give your consent, these trackers may be placed on all devices from which you view the relevant emails.
- Cases not requiring your consent. Certain limited technical measures, such as deliverability tracking designed to identify inactive email addresses so that they can be removed from our lists, may be carried out without your consent, to the extent strictly necessary for this purpose. In such cases, only the date of the last time the email was opened is retained, and this is overwritten each time the email is opened again.
- Retention. Data resulting from this tracking is retained for 13 months from the date of collection, in accordance with the CNIL's recommendations applicable to trackers.
- Withdrawal and objection. You may object to this tracking at any time, without this resulting in your unsubscription from our communications.

Retention

Your marketing data is retained for 3 years from our last contact for prospective customers, and for the duration of the contractual relationship followed by the applicable statutory period for customers.

Your rights

You have the rights described in the 'Rights of natural persons' section above, in particular the right to object and the right to withdraw consent, which may be exercised by contacting our DPO (see the 'Contact' section), as well as via the unsubscribe link included in each of our communications.

Location of personal data

The personal data collected and/or processed by Transatel is primarily located within the European Union. However, some of our data processors (notably those providing CRM, marketing, B2B prospecting or analytics tools) may host or process data outside the European Union, in particular in the United States. In such cases, Transatel ensures that an adequate level of protection is provided, notably through standard contractual clauses approved by the European Commission or, where applicable, the provider's certification under the EU-US Data Privacy Framework.

Transatel's customers are informed that when they use Transatel's services worldwide, they may roam on the mobile networks of Transatel's partner mobile network operators (MNOs) and that these MNOs collect and

process their personal data in order to provide them with local access to their mobile network, in accordance with applicable local regulations.

Transatel's subsidiaries may also collect and/or process personal data of local customers; in such cases, the Transatel subsidiary complies with the applicable local regulations.

Sharing data with third parties

Your personal data is only shared with third parties to ensure the proper functioning of our services, and in accordance with the following provisions.

Types of Third Parties and Data Processing

The following are the main third parties with whom we collaborate and the specific processing of your data that they carry out:

- Payment Service Providers

Purpose: to enable the secure processing of your payments made directly on our website or via our customer service team (excluding purchases made via app distribution platforms; see below).

Data processed: transaction data, banking details.

Third parties involved: our payment service providers.

- Email and Marketing Services

Purpose: to send marketing communications and newsletters to individuals who have consented to receive them.

Data processed: email address, name, communication preferences.

Third parties involved: our email service providers.

- Analytics Service Providers

Purpose: to analyse website traffic and optimise the user experience.

Data processed: IP address, browsing data, pages visited.

Third parties involved: our analytics service providers.

- Cloud Service Providers

Purpose: data storage and security backups.

Data processed: user data, backup files.

Third parties involved: Our cloud service providers.

- Data and artificial intelligence platforms

Purpose: analysis of network data and development of anomaly detection and artificial intelligence models, to improve the quality and security of our services.

Data processed: technical traffic data (e.g. IMSI, MSISDN, ICCID), without any other associated personal data.

Third parties involved: our cloud-based data and analytics platform.

- Application distribution platforms

Purpose: distribution of the Ubigi app and processing of payments made via these platforms.

Data processed: platform account ID, transaction data relating to in-app purchases.

Third parties involved: Apple (App Store) and Google (Google Play).

- Customer relationship management (CRM) tools

Purpose: management of leads, sales opportunities and customer relations for Ubigi for Business activities.

Data processed: business contact details (name, email, company, telephone number).

Third parties involved: our CRM and marketing automation tools.

- B2B lead generation and campaign service providers

Purpose: to identify business contacts and carry out targeted email campaigns aimed at businesses, based on our legitimate interest in prospecting for new business clients.

Data processed: business contact details (name, job title, business email address, company).

Third parties involved: our B2B prospecting and email campaign service providers, selected for their compliance with the GDPR.

- Website and contact form providers

Purpose: to manage the website and contact forms used to collect enquiries from visitors, with their consent.

Data processed: name, email address and telephone number provided voluntarily via the form.

Third parties involved: our website and contact form provider.

- IoT and automotive connectivity partners (Auriga solution)

Purpose: to provide analytical dashboards and a support pathway (onboarding, in-app questionnaires) to car manufacturers using the Auriga solution.

Data processed: vehicle usage and connectivity data linked to the VIN, data relating to interactions with the app or the in-vehicle questionnaire.

Third parties involved: our dashboard analytics partner and our in-app onboarding service provider.

Data Protection Measures and Data Transfer

We select third parties that maintain high security standards to protect your personal data. Where personal data is transferred outside the European Union, we ensure that appropriate safeguards are in place, such as standard contractual clauses approved by the European Commission or other protective mechanisms.

Retention of Personal Data

The retention period for your personal data depends on the performance of your contract or applicable legal and regulatory obligations. In all cases, you will be informed of the retention period for your personal data.

Please also note that Transatel may retain your personal data for statistical purposes. In such cases, Transatel will anonymise your personal data.

The retention period for your personal data held by Transatel is as follows:

- Employment information:
    - Employee information: 5 years from the date the contract ends
    - Candidate information: 2 years from the date the candidate's profile was submitted
- Traffic usage information: 10 years from the date of the traffic
- Customer information: 5 years from the contract end date
- Financial documents: 10 years from the date of invoicing

- External communications information: 3 years from the date of the communication

Principles

Transatel's privacy policy is governed by the principles set out below. These principles guide Transatel's work in protecting data privacy.

Staff training

We dedicate time to training and informing our staff about GDPR compliance issues. We regularly organise specific training sessions to ensure that our staff are fully aware of the applicable regulations.

Privacy by Design

From the very outset of a project, Transatel always bears in mind that the collection of personal data must be limited to what is strictly necessary. Our staff strive to minimise the use of personal data to what is strictly necessary. We have a document that outlines the process by which we assess the need for personal data in new projects.

Privacy by default

Transatel is committed to protecting individuals' privacy. To achieve this objective, Transatel always defaults to the option that offers the greatest protection for customers. Transatel may only change this option with the customer's consent.

Minimisation

Transatel collects only the information necessary for the operation of its services. Transatel limits the data collected. Furthermore, Transatel deletes data when it is no longer necessary for the operation of the service. Transatel regularly carries out data purges across all systems to ensure that only necessary data is retained.

Cooperation

Transatel cooperates fully with the data protection authorities in order to comply with the legislation in force in the country in which it operates. Transatel has various documents detailing its security measures in order to comply with its 'accountability' obligation.

Restricted access

Transatel restricts access to personal data to authorised staff only. We control access to personal data. Transatel grants access to individuals who have been trained to handle this type of sensitive data. Transatel has put systems in place to protect access to its system.

Individuals' rights

Right of access

You have the right to access your information at any time. We will provide you with all the information we hold about you in our system.

Right to lodge a complaint

If you believe there has been a breach in the way we process your data, you have the right to lodge a complaint with the French data protection authority: the Commission Nationale de l'Informatique et des Libertés (CNIL).

Right to rectification

If we hold incorrect information about you, you may ask us to amend or update it. In such cases, for certain types of information, we may ask you to provide justification.

Right to data portability

You have the right to receive your personal data in a machine-readable format. Please note that, with regard to Transatel's activities, this right does not apply to any of our operations.

Right to restriction

You have the right to prevent Transatel from processing your personal data. We are permitted to store your data, but we cannot use it. This right applies only in certain circumstances.

Right to erasure ("right to be forgotten")

You have the right to have your personal data erased from our database. Please note, however, that for regulatory reasons, the continued provision of the service requires certain data to be retained. Erasure will result in the suspension of the service.

Right to object

You have the right to object, at any time and without giving a reason, to your personal data being used for commercial marketing purposes, in particular for sending our marketing communications and newsletters. You may also object, on grounds relating to your particular situation, to processing based on Transatel's legitimate interests. You may exercise this right at any time via the unsubscribe link included in each of our communications, or by contacting our DPO.

Changes to our privacy policy

Transatel reserves the right to amend its privacy policy. Should this occur, you will be notified by email or by any other means. Any future amendments will always comply with the applicable regulations.