



[Last update: 29th November 2022]

# Privacy Notice

At INFOBIP, we care about your personal data. It is very important to us to be transparent about the data we collect about you, how we use such data and with whom we share it. Therefore, we advise you to read the following Privacy Notice to be informed about the processing of your personal data.

Through our worldwide network of over 600 direct carrier connections, we reach more than 7 billion people and things. Our local presence, of more than 60 offices across six continents, enables us to react faster, support better, engage more, and offer tailor-made solutions creating communications solutions of the future with our clients. We believe that the responsible use of data supports business growth and builds strong relationships between partners, consumers, and brands. As a business, we are committed to respecting and protecting the privacy of all individuals with whom we interact.

1. DEFINITIONS .....	2
2. ABOUT INFOBIP SERVICES .....	2
3. CONTROLLER’S CONTACT DETAILS .....	3
4. HOW DO WE OBTAIN PERSONAL DATA? .....	3
5. WHAT PERSONAL DATA DO WE COLLECT, WHY AND ON WHICH LEGAL BASIS, HOW DO WE USE IT AND FOR HOW LONG DO WE KEEP IT? .....	4
5.1. When we provide the Services to our customers.....	4
5.1.1. To create the customer’s account and enable the customer to start using our Services: .....	4
5.1.2. To enable customers to exchange their communications by the use of our Services and to ensure the security of our network and Services: .....	5
5.1.3. To improve our products and Services .....	6
5.2. When you provide your products or services to us .....	7
5.3. When you contact us with a question about our products and services and when we are looking for new business opportunities.....	8
5.4. When we send you our email marketing communications .....	8
5.5. When you register to attend our webinar, business breakfast, or other events .....	9
5.6. When we perform research activities .....	11
5.6.1. When we perform market research activities .....	11
5.6.2. When we perform user experience research .....	11
5.7. When you visit our webpage .....	12
5.8. When you apply for a job or internship with us or when you sign up to receive job posting updates .	12
6. HOW AND WITH WHOM DO WE SHARE YOUR PERSONAL DATA? .....	14
7. HOW DO WE CARRY OUT INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA? .....	15
8. HOW DO WE SECURE YOUR PERSONAL DATA? .....	15
9. WHAT ARE YOUR RIGHTS IN RESPECT OF YOUR PERSONAL DATA? .....	16
10. HOW CAN YOU OBJECT TO THE PROCESSING OF YOUR PERSONAL DATA? .....	16
11. HOW CAN YOU EXERCISE YOUR RIGHTS? .....	17
12. DO WE CONDUCT AUTOMATED DECISION-MAKING, INCLUDING PROFILING, THAT SIGNIFICANTLY AFFECTS YOU? .....	17
13. HOW LONG DO WE KEEP YOUR PERSONAL DATA? .....	17
14. INFORMATION FROM CHILDREN .....	17
15. SUPPLEMENTAL NOTICE FOR CALIFORNIA RESIDENTS.....	18
16. HOW OFTEN DO WE UPDATE THIS PRIVACY NOTICE? .....	19

# 1. DEFINITIONS

In the text, we use specific data protection terms, and their definitions are the following:

The term “**INFOBIP**” or “**us**” or “**we**” or “**our**” refers to the company **INFOBIP LIMITED**, with its registered office at the United Kingdom, London EC4V 6BW, Fifth Floor, 35-38 New Bridge Street and registration number 7085757, as well as to its **subsidiaries and affiliates** (the full list of INFOBIP subsidiaries and affiliates with contact details can be found at: <https://www.infobip.com/offices>).

The term “**Applicable Data Protection Law**” means all laws and regulations applicable to the processing of personal data under this DPA, including, where applicable, the GDPR (General Data Protection Regulation (EU) 2016/679), the UK GDPR, the UK Data Protection Act 2018, and any laws and regulations implementing the foregoing, as amended, or superseded from time to time.

The term “**personal data**” means any information about you by which you can be identified, directly or indirectly.

The term “**controller**” means the natural or legal person which determines the purposes and means of the data processing and is responsible for processing such data in a manner consistent with the Applicable Data Protection Law.

The term “**processor**” means a natural or legal person who processes personal data on behalf of the controller.

The term “**Services**” means INFOBIP’s cloud-based communication products and services (CPaaS – Communications Platform as a Services and CCaaS – Contact Centre as a Services).

The term “**you**” refers to a natural person (an individual) whose personal data INFOBIP collects and processes.

## 2. ABOUT INFOBIP SERVICES

INFOBIP is a Communications Platform as a Services (CPaaS) and Contact Centre as a Services (CCaaS) provider. While providing Services to our customers and processing personal data, we act either as the controller or the processor, depending on the situation.

Our customers are mainly companies that integrate our Services into their business operations through their own software applications (via API) or using INFOBIP Portal (“Customer User Portal” or “CUP”), our website interface. By using our cloud communications platform, our customers are able to send or exchange their communications with their end users using different communication channels (for example, SMS, email, Voice). We are not in direct relationship with our customers’ end users, so we will distribute these communications through telecom operators and other communications providers.

We act as the processor when processing personal data of individuals on behalf of our customers, and for the sole purpose of providing our Services to them. We do that within limits and according to customers’ instructions and in line with the Service terms and conditions, agreement for Services and/or data processing agreement concluded with the customer.

For example, when you, as an end user of our customer are the recipient of communication that our customer sent you by using our platform (such as an SMS message), we send that customer’s communications acting on behalf of our customer. That means that the customer is the controller, and INFOBIP is the processor.

Any request we may receive from customers’ end users regarding their rights related to our activities taken on behalf of our customers will be forwarded to customers, or the end users will be asked to contact them directly.

In situations when we process personal data for our own purposes and do not act on behalf of someone else, we act as the controller and we are committed to processing that data as described in this Privacy Notice and respecting all obligations arising from the Applicable Data Protection Law.

### 3. CONTROLLER'S CONTACT DETAILS

INFOBIP LIMITED, 35-38 New Bridge Street, Fifth Floor, London EC4V 6BW, United Kingdom

Contact details of all INFOBIP subsidiaries and affiliates (INFOBIP group companies) are available at: <https://www.infobip.com/offices>.

If you have questions regarding this Privacy Notice or about the INFOBIP Group's privacy practices, you may reach our Privacy team and Data Protection Officer via the email address [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com).

### 4. HOW DO WE OBTAIN PERSONAL DATA?

Most of the personal data we process is provided to us directly by you for one of the following reasons:

- You created an account and started using our Services
- You visited our website, registered for more information on a specific Service, took steps to enter into a business relationship with us and/or you initiated communication with us
- You registered to attend or have attended an event organised by INFOBIP
- You subscribed to our e-newsletter, blog or a webinar
- You accepted to participate in our market research activities
- You applied for a job or internship with us.

We also receive personal information indirectly, such as in the situations where:

- Our customer or supplier provided us with the contact details of its representatives and personnel who will be our business contact points
- Our customer provided us with the contact details of individuals authorized to use its account to access our Services,
- Our customer provided us with the contact details of its personnel who will attend our event
- Our customer provided us with contact details of its end users (such as telephone number or email address) when using our Services
- An employee of ours gave us your contact details when naming you as a referee
- From providers of background check services when you apply for a job offer
- We have collected your information from LinkedIn or other publicly available sources or from data enrichment providers
- We automatically collect certain information, such as your Internet protocol (IP) address, user settings, cookie identifiers, and other unique identifiers, browser or device information, location information (including approximate location derived from IP address ), and when you use our Services.

# 5. WHAT PERSONAL DATA DO WE COLLECT, WHY AND ON WHICH LEGAL BASIS, HOW DO WE USE IT AND FOR HOW LONG DO WE KEEP IT?

<a href="#">5. WHAT PERSONAL DATA DO WE COLLECT, WHY AND ON WHICH LEGAL BASIS, HOW DO WE USE IT AND FOR HOW LONG DO WE KEEP IT?</a> .....	4
<a href="#">5.1. When we provide the Services to our customers</a> .....	4
<a href="#">5.1.1. To create the customer’s account and enable the customer to start using our Services:</a> .....	4
<a href="#">5.1.2. To enable customers to exchange their communications by the use of our Services and to ensure the security of our network and Services:</a> .....	5
<a href="#">5.1.3. To improve our products and Services</a> .....	6
<a href="#">5.2. When you provide your products or services to us</a> .....	7
<a href="#">5.3. When you contact us with a question about our products and services and when we are looking for new business opportunities</a> .....	8
<a href="#">5.4. When we send you our email marketing communications</a> .....	8
<a href="#">5.5. When you register to attend our webinar, business breakfast, or other events</a> .....	9
<a href="#">5.6. When we perform research activities</a> .....	11
<a href="#">5.6.1. When we perform market research activities</a> .....	11
<a href="#">5.6.2. When we perform user experience research</a> .....	11
<a href="#">5.7. When you visit our webpage</a> .....	12
<a href="#">5.8. When you apply for a job or internship with us or when you sign up to receive job posting updates</a> ..	12

## 5.1. When we provide the Services to our customers

### 5.1.1. To create the customer’s account and enable the customer to start using our Services:

#### What personal data do we collect?

We collect customer’s **“account data”**, which is data that relates to the customer’s relationship with INFOBIP.

If you sign up for our Services, in order to create a customer’s **“account”** we ask for your name, contact details (e.g., phone number, email address, country), and certain related information such as your company’s name, industry and your business role, as well as your login details (e.g., username and password, or API key).

We also collect names, contact details and login details of customer’s personnel or any other individual authorised by the customer to log into and utilise our Services connected with the customer’s account (a **“user”** of the customer’s account).

Within the customer’s account we also collect billing information (such as billing address, information on whether the customer is a legal entity or an individual, prepaid or postpaid subscriber, and further information if we are legally required to, and depending on each country’s legislation).

When doing business with legal persons, we may collect personal data (such as name, business contact details, position in the company) related to their representatives and other personnel that will be our contact points.

Collecting your name, contact details, login details, and billing information **is necessary** for us in order to enter into an agreement for Services with you. Therefore, we will not be able to provide you with our Services

without collecting this basic information. If you sign up for a free trial account, you are not required to enter your billing information unless and until you decide to continue with a paid subscription to our Services.

#### **How do we collect personal data?**

If you are our customer as an individual, we obtain this data directly from you. If your organisation is our customer, we may obtain your personal data either directly from you or via your organisation.

#### **Why do we collect personal data, under which legal basis, and how do we use it?**

We collect and use collected data for agreement signing and agreement administration purposes, to create your account and enable you to access and use our Services, to keep your account secure, to provide you with customer care and technical support, to share relevant information about our products and services and to exercise our rights and fulfil our obligations arising from the business relationship that we may have with you or with your organisation.

Conducting these activities is our legitimate interest in the sense of providing our Services to your organisation. However, if you personally are our contractual counterpart, we process your data because it is necessary for the performance of an agreement for Services, or in order to take steps, at your request, prior to entering into the agreement.

### **5.1.2. To enable customers to exchange their communications by the use of our Services and to ensure the security of our network and Services:**

#### **What data do we collect?**

We collect **traffic data**. Traffic data is data that is processed for the conveyance of a communication exchanged by using our Services or for billing related to that communication, and it includes data on the routing, type, duration, and time of the communication. So, this data encompasses data used to trace and identify the source and destination of a communication (including customer end user's telephone number or email address, depending on the Service provided).

We also collect the commands your application communicates to INFOBIP (such as your IP addresses, information on your usage, routing information), as well as logs on your activities created during your use of our tools and Services and we connect this information with your account details.

#### **How do we collect this data?**

We receive the customer's end user's telephone number or email addresses from our customer, while other traffic data are automatically generated or unveiled during the process of conveyance of a communication.

We collect data related to your activities on our platform directly from you when you use our Services.

#### **Why do we collect this data, under which legal basis, and how do we use it?**

We collect and process traffic data to provide customers with our Services, that is, to manage traffic with the purpose of transmitting customer's communications toward or from telecom operators and other communication networks, in order to handle customer's enquiries and to calculate charges.

If you, as our customer, are an individual, the processing of your personal data is necessary for the performance of our agreement for Services. If our customer is a legal person, we rely on our legitimate interest to process personal data.

We also process traffic data to prevent spam and fraud, for troubleshooting and detecting problems with the network, and to settle interconnection payments with telecom operators and other communications providers. Should we have a billing dispute with our customer or with telecoms or other communications providers, we may need to use traffic data related to routing (including the end user's telephone number or email address, as well as the customer's IP address) in order to resolve it. The carrying out of these activities is our legitimate interest.

In order to comply with our legal obligations, we may be obliged to retain records containing communications related data as stipulated in the relevant national data retention provisions regulating the law enforcement matter, and to share them upon government request.

We collect logs on your activities created during your use of our Services and connect this information with the customer's account details in order to secure customer's account, to prevent or detect fraudulent activities, and to ensure the security of the INFOBIP network. This information is necessary to construct the timeframe of user's activities in the case of security-related incidents, and to be able to take adequate steps for mitigation. IT security is crucial for us, so for these activities we rely on our legitimate interest and on the legitimate interest of our customers to maintain and improve the security of our network and Services.

### 5.1.3. To improve our products and Services

#### **What data do we collect?**

We collect the data you generate during your activity on our platform (e.g. your behaviour records inside our web interface, such as time spent, pages visited, history of your visits and features used).

#### **How do we collect this data?**

We obtain this data directly from you. When you browse our website and use our Services, we automatically collect data by placing necessary cookies and trusted tracking technologies on your browser. For more information on how we collect you data through cookies, please visit our [Cookie Policy](#).

#### **Why do we collect this data, under which legal basis, and how do we use it?**

The information we collect helps us maintain and improve our website and business. It usually includes your IP address, browser type, the pages you have visited and the order you visited them in as well as whether you are a new or a returning visitor.

If you are already our customer, we'll use the data collected from your account to gain insight into the way you use our platform and Services, what your business needs are, past support issues, and so on. This information makes it possible for us to tailor our assistance and product offers and provide the best possible support.

We analyse your activities on our platform and collect data that is useful for the improvement of our products and Services, relying on our legitimate interest. This may include using your personal information to create de-identified and / or aggregated information, such as de-identified demographic information, de-identified location information, information about the device from which you access our Services or other de-identified analyses we create. We take partially automated measurements that include human intervention in order to analyse the way you use the features and tools available on our platform (e.g., by tracking and recording your behaviour inside our web interface, including time spent, pages visited and features used) in order to give you recommendations to improve your performance (e.g. how to better access some feature). Also, we create statistics on the use of our tools to understand which tools have a user-friendly design and which should be enhanced. The general goal of such activities is to enhance your and your company's messaging execution when communicating with your end users.

#### **How long do we keep your personal data?**

We will erase all information collected about our customers (basic identification data, contact details, business details and account details) within 7 years after the closure of the account. Moreover, information about reseller's customers and account users (basic identification data, contact details, business details and account details) will be kept 12 months after the account closure.

In order to maintain records of our business relationship and to comply with the applicable financial and tax regulations, we keep business agreements related to Infobip Services for 10 years after the end of the year when the account was closed and invoices for 10 years after the end of the invoicing year. Longer periods may apply when required by the local legislation.

Customers' requests and other communication exchanged with our support team via our help desk (support ticketing) system may be kept for 7 years upon the ticket closure.

Traffic data containing end users' information (such as MSISD-number, telephone number, IMSI, IMEI) will be kept, in our communication detail records, for 12 months after the date of communication. Longer periods may apply if INFOBIP needs to comply with applicable national legislation regulating retention of data in electronic communications for law enforcement purposes. In addition, as we may need to keep traffic data in order to calculate charges, we will keep them for billing and to settle our payments towards telecoms and

other communications providers until payments are settled, the longest until the end of the period during which the bill may lawfully be challenged or payment pursued. In case that a bill remains unpaid or has been challenged before being paid, we will keep data to establish, exercise or defend our legal rights, the longest until the court or other legal procedure is finally closed.

Customers' and reseller's customers traffic data (such as sender name, sender ID, time, type, duration of communication, routing details) are kept for 10 years after the date of communication, since they can be checked by auditors and tax authorities, and they are necessary in order to demonstrate compliance with the relevant financial, audit, and tax legislation.

Behaviour analytics i.e. data generated during your activity on our platform are kept for twenty-five months.

In case that legal matters such as litigation, law enforcement requests or government investigations acquire us to preserve records, including those containing personal information, we will delete the impacted records when no longer legally obligated to retain them.

## **5.2. When you provide your products or services to us**

### **What personal data do we collect?**

If you as our supplier are an individual, we collect your name, contact details (such as address, phone number, email address), certain related information such as your company's name, industry and your business role, and your billing information (e.g., billing address, information on whether you are a business or an individual, your VAT number, bank account details, and further information if we are legally required to and in accordance with applicable national legislation).

Collecting this data is necessary for us in order to enter into an agreement with you. Therefore, we will not be able to purchase your products or services without collecting this personal data.

When doing business with legal entities, we collect personal data related to their representatives and other personnel that will be our contact points (such as their name, business contact details, position in the company).

### **How do we collect personal data?**

If you as an individual are our supplier, we obtain this data directly from you. If your organisation is our supplier, we may obtain your personal data either directly from you or via your organisation.

### **Why do we collect personal data, under which legal basis, and how do we use it?**

We collect and will use this data for agreement signing and agreement administration purposes, to maintain and improve our business relationship, to get relevant information about our supplier's product or services, or to share relevant information about our business and services with you, as well as to exercise our rights and fulfil our obligations arising from the business relationship that we may have with you or your organisation.

Conducting these activities is our legitimate interest in the sense of purchasing products or services from a supplier that is a legal person. However, if you personally are our contractual counterpart, we process your personal data because it is necessary for the performance of an agreement or in order to take steps, at your request, prior to entering into an agreement.

### **How long do we keep your personal data?**

When you provide your products or services to us, we keep your business-related personal data (basic identification data, contact details and business details) for 7 years after the end of our business relationship. However, we keep business agreements for 10 years after the end of our business relationship and invoices for 10 years after the end of the invoicing year. Longer periods may apply when required by the local legislation.

Customers' requests and other communication exchanged with our support team via our help desk (support ticketing) system may be kept for 7 years upon the ticket closure.

Personal data of the supplier's personnel (basic identification data, contact details, business details) that were our contact points during the business relationship we had obtained from our supplier will be deleted or made anonymous within 12 months after the end of the business relationship.



If legal matters such as litigation, law enforcement requests or government investigations require us to preserve records, including those containing personal information, we will delete the records in question when we are no longer legally obligated to retain them.

### **5.3. When you contact us with a question about our products and services and when we are looking for new business opportunities**

#### **What personal data do we collect?**

We may collect your name, surname and basic contact and business information such as your email address, phone number, country, company, industry, and business role or job title. We will also collect any other information you choose to provide us, depending on the nature of our communication.

#### **How do we collect your personal data?**

We may collect this information directly from you through our “Contact Sales” or other forms available on our website. After submitting your details, we will send you an email to confirm that our sales team will contact you.

We may also collect your information directly from you when you register on our website to learn more about our business and services, start chatting with us via our chat channel, take steps to enter into a business relationship with us, submit Startup or Shift Sponsor/Partner application form and when you provide us your contact information when requesting further information.

We are constantly searching for new business opportunities. Therefore, we may collect your contact and business information indirectly, through business and professional networks and databases (such as LinkedIn) or we may employ third parties that supply us with information collected from publicly available sources and data enrichment providers. We only retain the information that will help us reach potential customers and suppliers that could benefit from our services and products, or if we are interested in their products and services.

#### **Why do we collect personal data, under which legal basis, and how do we use it?**

We collect this information to contact you, answer your questions, find out if you or your organisation are interested in further cooperation with us.

We use your personal data to provide you with the requested information about our products and services and to see if you are interested in using them, or if we can benefit from using your products and services, as well as to provide you with all the necessary information and support required to ensure the mutually beneficial and satisfying cooperation if you become our customer or supplier. Any further processing of your personal data will be based on the business relationship established with you or your organisation and on the lawful processing ground.

Such activities represent our legitimate interest.

If there will be a mutual interest in entering into an agreement, we will process your personal data within the presales and purchasing process to ensure adequate technical and administrative support (tender procedures, negotiating, and concluding agreements), and it is our legitimate interest to conduct this process properly. If you personally are our contractual counterpart (as an individual), we process your data because it is necessary for the performance of a contract or in order to take steps, at your request, prior to entering into a contract.

#### **How long do we keep your personal data?**

If we do not enter into an agreement, we will delete your personal data collected for this purpose within six months after our last communication.

In any case, if you no longer wish to be contacted by our sales or procurement team, you can always object by sending an email to [sales@infobip.com](mailto:sales@infobip.com).

### **5.4. When we send you our email marketing communications**

#### **What personal data do we collect?**

We collect your name and email address.

#### **How do we collect personal data?**

We collect this information directly from you if you subscribe to receive our newsletters, blogs or our other email marketing communication by which we provide the information about our business and services. This data is collected through the webforms available on our website.

For business to business (B2B) marketing, if we have an existing business relationship (our customers, suppliers and their staff), we may use data collected from you or your organisation when entering into an agreement or during our business relationship.

#### **Why do we collect personal data, under which legal basis, and how do we use it?**

Our purpose for collecting the information is the provision of the services to you and informing you about news, webinars and upcoming events.

We use your details only to provide these services. We also gather statistics around email opening and clicks using industry standard technologies, including clear gifs to help us improve our e-newsletter.

If you subscribe to our email marketing communication, we rely on your consent provided to us when submitting such webforms. You will receive a confirmation email once you have submitted your details.

For B2B (business to business) direct marketing, we may rely on our legitimate interest. For the purpose of maintaining and improving our business relationship, it is our legitimate interest to inform our existing business partners (customers and suppliers, including their staff) about our products and services, news, webinars, and upcoming events via email newsletters, blogs or other forms of email communication.

In any case, you may proactively manage your preferences or opt-out of communications (unsubscribe) with INFOBIP at any time using the unsubscribe link provided in all INFOBIP's email marketing communications. In case that you have unsubscribed from our marketing communications (i.e. withdraw your consent or object to the processing) we will stop sending you any marketing materials.

However, we maintain a so-called "suppression list" that contains only your email address just to be sure that we will not contact you with unwanted content in the future. We retain this information relying on our legitimate interest.

#### **How long do we keep your personal data?**

If we send you marketing communications based on our legitimate interest (B2B) we will do so only during the business relationship with you or your organisation (existing agreement for products or services is in place), or until you object to the processing of your personal data for this purpose. We will keep a suppression that contains email addresses of individuals that objected to receiving our marketing communications until the end of the business relationship with you or your organisation.

If you subscribed to receive our email marketing communications, we will provide you this service until you unsubscribe, i.e. withdraw your consent.

In order to prevent you from receiving unwanted content after you had opted-out from marketing communications, your email in the suppression list is kept until you decide to subscribe again to our marketing communications.

## **5.5. When you register to attend our webinar, business breakfast, or other events**

#### **What personal data do we collect?**

When you register to attend a business breakfast, webinar or any other event (hereinafter: event), you will be asked to provide your name and contact details (email, phone number, country), as well as your company's name, industry, and your business role.

We may also ask you information about the time and place of your arrival as well as accommodation details and dietary requirements you may have.

If you require us to provide you with an invitation or support letter, or you need to get letter of guarantee to be able to get a visa, we will collect the necessary information required by applicable law (such as your name, address, date of birth, passport details).

We may collect photos, audio, and video material from our events.

### **How do we collect your personal data?**

We collect your personal data directly from you when you fill in our registration forms.

Sometimes your organisation will send us your contact details to attend our event on their behalf, and we will send you an invitation with the link for registration.

### **Why do we collect personal data, under which legal basis, and how do we use it?**

If you register for a webinar, we will use your contact details to provide you with the webinar details in advance, to remind you of the webinar and email you the recording of the webinar subsequently.

If you register to attend our event, we will use gathered information to ensure your place at the event, to be in touch with you, to provide you (via email or by SMS on the phone number you provided in the registration form) all relevant information before your arrival and during the event, to facilitate the event and ensure all organisational support that you may need. For example, help you with information about the location of our event, accommodation, travel or other logistic details related to the event.

The legal basis we rely on for processing your personal data is your consent, provided when you submit your details through our registration forms. When we collect any information about dietary requirements, we also rely on your consent .

If you will need an invitation or support letter or letter of guarantee to be able to get a visa, we have to collect the necessary information about you as defined by the applicable legislation. We collect this information just to respond to your request and support you with the necessary documentation and we rely on your consent provided when you submit us your personal data for this purpose. Such information will not be processed for any other purpose than issuing such a document upon your request. However, we may be legally obliged to share such a document with government authorities and to keep it for a certain period of time, as defined by applicable legislation.

In order to be able to facilitate the event, we rely on your consent to process your personal data and this means you have the right to withdraw your consent at any time by sending an email to [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com).

We also keep events' participants lists containing only your name, contact details, your company's name, industry and your business role. In this case, the processing purpose is to maintain a list of former participants in order to invite them to future events we consider they might be interested in. To be able to stay in touch with you, invite you to our other events, and inform you about our products and services, we rely on our legitimate interest . You may object to these communications at any by time using the **unsubscribe link** provided in all INFOBIP's emails and we will stop sending you event invitations.

We also conduct promotion activities of the events we held. In this case, the processing purpose is to promote our events, and it consists of publishing photos, videos, audios, and texts in online and offline media. These activities represent our legitimate interest.

### **How long do we keep your personal data?**

Personal data collected when you register for our webinar are kept for 18 months after the webinar.

For off-line events, we keep events' inviting lists for three years after the event day.

All other personal data collected will be kept only for the duration of the event (accommodation and other logistic data) are erased within 60 days after the event day. Invitation, support letter or letter of guarantee will be kept for a period of time determined by the applicable legislation.

## 5.6. When we perform research activities

### 5.6.1. When we perform market research activities

#### **What personal data do we collect?**

We collect your name and contact information (email address). The idea of the researches we conduct is to gather anonymous information. Therefore, our intention is to collect only your personal data necessary to send you a questionnaire but not to link the anonymous answers with you in any way.

#### **How do we collect your personal data?**

We collect your name and contact data (email address) from business and professional networks (for example LinkedIn), or from our databases if you or your organisation are our customers, suppliers or business contacts.

#### **Why do we collect your personal data, under which legal basis, and how do we use it?**

We conduct market research activities in order to receive anonymous information and feedback for improving our products and services and targeting potential.

Firstly, we invite you to take a survey sending a generic untraceable URL to a survey questionnaire. If you decide to participate and answer our questions, we will not ask you to unveil any personal data, and our intention is to keep the answers anonymous.

When searching for your email address, we rely on our legitimate interest. Our intention is to collect anonymous information. However, if you disclose any information about you in your answers, we will rely on your consent.

Keep in mind that we respect your privacy rights, so we do not carry out any activity to link the answers provided with you, and we do not inform other organisations (e.g. your employer) on the answers you provided in any way.

#### **How long do we keep your personal data?**

We will process the answers you provided in order to have general feedback on our products and services. However, we will never ask you to reveal any personal data in your answers, our intention is not to collect personal data within this activity, and if you reveal any personal data in your answers, it will be promptly deleted.

### 5.6.2. When we perform user experience research

#### **What personal data do we collect?**

We collect your personal data such as name, surname, email, and job title. We are committed to collecting and processing only personal data necessary to fulfill the aim of our research. The aim of the research we conduct is to collect feedback from users of our products to improve them based on users' practical experience and needs.

#### **How do we collect your personal data?**

We collect your name and contact data (email address) from our databases if you or your organization are our customers, suppliers, or business contacts to invite you to be part of our research hub.

If you apply to be part of our research hub and participate in our research, we will collect the personal data directly from you through a third-party provider who will process it on our behalf.

#### **Why do we collect your personal data, under which legal basis, and how do we use it?**

We conduct user experience research activities to receive feedback for improving our products and services.

Firstly, we invite you to be part of our research hub via email by sending you a link to apply. When inviting you to be part of our research hub, we rely on our legitimate interest.

Your participation is completely voluntary, and if you decide to be part of our research hub and participate in our research, we will rely on your consent for personal data collected and further processed. We will contact you only about research related to the product you already use or have used.

The research may be recorded, and we will take notes of your comments and actions. The research results, recordings, and notes are used only for improving our products and would be shared with the responsible teams, such as product design and development teams.

#### **How long do we keep your personal data?**

Data deletion deadlines are applied to ensure data is erased once no longer necessary for research purposes.

### **5.7. When you visit our webpage**

We use third-party services such as Google Analytics when you visit [www.infobip.com](http://www.infobip.com) in order to collect standard internet log information and details on visitor behaviour patterns. We do this to find out information such as the number of visitors to various parts of the site. This information is only processed in a way that does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of visitors to our website. We also use LinkedIn Analytics. For more information, please consult the relevant privacy notice.

When you browse our website, we automatically place necessary cookies on your browser. You can opt in to accept advertising or analytical cookies. The information we collect helps us maintain and improve our website and business. It usually includes your IP address, browser type, the pages you've visited and the order you visited them, as well as whether you're a new or returning visitor. For more information please read our [Cookie Policy](#).

### **5.8. When you apply for a job or internship with us or when you sign up to receive job posting updates**

#### **What personal data do we collect?**

When you apply for a job or internship with us, we collect your first and last name, contact information (email address and telephone number) and place of residence as well as information about your education, previous work experience, and any other information you choose to share with us in your resume (CV) or application when expressing interest in joining our team.

When permitted by applicable law, we may also collect professional information about you from the business networking sites you use (such as LinkedIn) and we may search their content in order to find out more professional information about you if your resume or application contains links to other sources (e.g. web pages).

If we arrange an interview and you go through our selection process, we may collect further information gathered from you during the interviews, results of conducted evaluation tests, interview notes and reviews of our colleagues who interviewed you. We may also collect information about your professional experience from your referees, if you indicated them. If you are a successful candidate, we might also conduct a background check if permitted by the legislation. We will provide a separate privacy notice to you prior to conducting it.

When you sign up to receive job posting updates, we collect your first and last name as well as your email address.

## **How do we collect your personal data?**

We collect your personal data directly from you when you submit your resume or application directly into our recruitment software or when you create an account there to receive job posting updates.

We may collect your personal data from recruitment agencies we have engaged in order to help us find potential candidates for open positions or from business networking sites you use such as LinkedIn.

We may collect further information about you during the selection process. This information will be generated by you and by us. For example, you might complete an evaluation test or we might take interview notes or contact your referees.

If you are a successful candidate, we might also collect your personal data from a background check agency if permitted by the legislation.

## **Why do we collect personal data, under which legal basis, and how do we use it?**

As we are a young and growing company, we are in constant need of new, talented individuals who will become part of our global team.

You can find information on open positions and internships in our offices all around the world on our Careers web page (<https://www.infobip.com/careers>), where you can follow the link to our recruitment software and submit your resume or application if you are interested in joining us. You can also create a profile in our recruitment software to receive job posting updates. When submitting your resume, you will be asked to provide us your consent to store and process your personal data for recruitment purposes for the period of time specified in the consent form.

We rely on your consent to collect and process your personal data. We use your personal data for recruitment purposes, e.g. in order to let you know of new open positions or internships and check if you are interested, and if you are, to conduct the selection process and assess your suitability.

If you do not submit your resume directly into our recruitment software (e.g. when we receive it from a recruitment agency or when we find your professional details on business networking sites you use), we will send you an email with a link to our recruitment software and you will be asked to provide us your consent to keep your personal data for recruitment purposes. In such cases, we collect your personal data and contact you with an email based on our legitimate interest, in order to find potential job candidates. However, we need your consent for any further processing of your personal data. If you do not provide us with the consent within thirty days following the receipt of the email, we will erase your personal data from our database.

During the selection process we collect further information in order to review your professional qualifications and interests and be able to choose the best candidate. We also conduct the relevant background checks, to the extent permitted by applicable laws, which include identity verification, right of work verification, education, professional license and previous employment checks, verification of recommendations, checks of company registers and criminal checks. Moreover, for executive roles we will also carry out a reputational check from publicly available sources. For the processing of this information, we rely on our legitimate interest, your consent, or legal obligation depending on the circumstances.

If you have been selected as the most suitable candidate for a job position or internship, you will be presented an offer. If you accept it, we will collect further information so as to be able to conclude and execute an agreement with you. The further collection and processing of your personal data will be carried out to conclude an employment or internship agreement with you or in order to take certain steps, at your request, prior to entering into that agreement. You will be presented with an Infobip privacy notice that applies to our staff where you can find relevant privacy information.

We collect and process your personal data through the recruitment platform of our processor, Workday Ltd. Your personal data are collected and stored on servers maintained by Workday in data centers located in the European Union. It will be processed by authorized members of the Infobip recruitment team. However, if there is a problem with the platform, the Workday support team may also have access to your personal data in order to help us resolve the problem. If you want to know more details about Workday's privacy practices, you can refer to the [Workday's Privacy Policy](#).

We may share your personal data within Infobip Group companies ([subsidiaries and affiliates](#)). Since we are a global company, we may engage our subsidiaries and affiliates in which we have employed members of our recruitment team in order to complete the recruitment process.

#### **How long do we keep your personal data?**

Your recruitment-related personal data will be deleted after the expiration of the period for which you have provided us with your consent (or earlier if you withdraw it). These periods might differ across countries due to local legislation.

If legal matters such as litigation, law enforcement requests or government investigations require us to preserve records, including those containing personal information, for longer periods than you have consented to, then we will delete the records in question when we are no longer legally obligated to retain them.

Please note that **you have the right to withdraw your consent at any time**. If you want to withdraw your consent or to edit your profile, you can do so yourself directly by [accessing your profile](#) in our recruitment software. Otherwise, you can always withdraw your consent as well as exercise your other rights by contacting our Data Protection Officer. More information regarding your rights is listed in sections 9 and 11 below.

## **6. HOW AND WITH WHOM DO WE SHARE YOUR PERSONAL DATA?**

We may engage [processors](#) to facilitate us in the processing of your personal data through CRM (Customer Relationship Management), marketing, recruitment and other tools necessary for conduct our business activities or to assist us in providing you with our Services.

We maintain an up-to-date list of them [here](#), including reference to the special safeguards on which we rely on when transferring your personal data outside the EEA.

Before engaging a new processor, we perform security & privacy assessment of the processor, and we ensure that the processing of personal data is always regulated with written data processing agreements. If the personal data during the provision of the services of our processor is being transferred outside the European Economic Area (EEA), INFOBIP will always ensure that the transfer is in line with the Applicable Data Protection Law.

We may share your personal data within INFOBIP Group companies ([subsidiaries and affiliates](#)). Since we are a global company, we may share your personal data with our subsidiaries and affiliates to complete internal procedures within our offices, to perform certain processing activities on a global scale or to support you in the use of our products and services. INFOBIP subsidiaries and affiliates can be engaged as processors or in certain situations can act as joint controllers.

All INFOBIP subsidiaries and affiliates will only use the personal data as described in this Privacy Notice. All intercompany processing of personal data is regulated by the INFOBIP Group intercompany agreements on personal data processing and transfer and where applicable with standard contractual clauses of all relevant jurisdictions.

Notwithstanding the foregoing, as a rule, we do not share personal data with third parties except when necessary, such as:

- With telecom operators and other communications service providers when necessary for the set-up of proper routing and connectivity. We are able to deliver messages that our customers send to their end users, independent of where they are located, through our connections with telecoms and other communications providers operating all over the world, especially OTT ones such as Whatsapp, Viber, Facebook, Kakaotalk, Line, Telegram, V Kontakte.
- With third-party service and technology providers, to the extent strictly necessary for them to perform specific actions on our behalf. We may share personal information with our trusted and verified third-party service providers, for example, in order to enable them to process payments for us or to prevent fraud.
- Due to relevant legislation. If we are presented with the legal obligation, we will share the data with third parties that are legally entitled and authorized to request it, such as for criminal procedures or because of threats to public security. As a communications provider, we are required to retain certain communications-related data for law enforcement purposes and will be required to share that data with authorized law enforcement authorities upon their request. Also, if we are under an obligation to demonstrate compliance with relevant accounting, financial and tax legislation, your data can be shared with auditors and tax authorities for those purposes.
- Targeted Advertising. We do not and will not sell, rent, or share in any other shape or form any information to a third party for advertising or similar marketing purposes. We do, however, use direct marketing through Google Adwords for our own purposes. You can visit our [Cookie Policy](#) or adjust the advertising settings in your browser. There you will be able to find out more about how to manage your advertising preferences to suit your needs.
- APIs/SDKs. We may use third-party Application Program Interfaces (“APIs”) and software development kits (“SDKs”) as part of the functionality of our Services. For more information about our use of APIs and SDKs, please contact us as set forth below.
- Disclosure in the event of merger, sale, or other asset transfer. If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, purchase or sale of assets, or transition of service to another provider, your information may be transferred as part of such a transaction, as permitted by law and/or contract.

## 7. HOW DO WE CARRY OUT INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA?

We conduct our business operations globally, and sometimes we need to carry out international transfers of your personal data by providing your personal data to the parties specified in the section above. All international transfers are carried out ensuring the confidentiality and security of your personal data.

In addition, the international transfers of your personal data are subject to contractual restrictions in accordance with the Applicable Data Protection Law, including, where necessary, the implementation of contractual mechanisms such as standard contractual clauses for data transfers.

## 8. HOW DO WE SECURE YOUR PERSONAL DATA?

Infobip values your privacy. In order to protect personal data collected and processed by INFOBIP we have invested in development, implementation, and constant improvement of a wide range of technical and



organisational measures. Our technical and organisational measures have been implemented in accordance with ISO 27001:2013 standard requirements, and you can read more about them [here](#). The list of our current and up-to-date certificates can be found [here](#).

We take care to train all our staff in the field of privacy and security, starting from their first day in INFOBIP through the onboarding process and continuously throughout their stay at INFOBIP.

Before we engage any third-party vendor and service provider, we check their security practices and alignment with the Applicable Data Protection Law, and regularly conduct our vendors' and service providers' security and privacy assessments.

## 9. WHAT ARE YOUR RIGHTS IN RESPECT OF YOUR PERSONAL DATA?

Under the Applicable Data Protection Law you have rights we need to make you aware of.

Where permitted by the Applicable Data Protection Law, you have the right to:

- withdraw your consent to our processing of your personal data (to the extent such processing is based on your consent and consent is the only permissible basis for processing), without affecting the lawfulness of processing based on consent before its withdrawal,
- request from us to access your personal data, which means request a copy of the personal data we hold about you,
- ask us to rectify (correct) your personal data that you think is inaccurate and to complete your personal data that you think is incomplete,
- ask us to erase your personal data in certain circumstances,
- ask us to restrict the processing of your personal data in certain circumstances,
- if we process your personal data by automated means based on your consent or upon a contractual relation with you, you can exercise the right of data portability,
- if we process your personal data upon our legitimate interest, you have the right to object to the processing, and we will reassess the legitimacy of the processing,
- you may also have specific rights in exceptional cases when we may carry out automated decision-making operations, including profiling,
- you also have a right to file a complaint with us and/or the relevant data protection authority.

You can exercise these rights within limits stipulated by the Applicable Data Protection Law.

## 10. HOW CAN YOU OBJECT TO THE PROCESSING OF YOUR PERSONAL DATA?

If we process your personal data upon our legitimate interest, you have the right to object to the processing. In such a case we will reassess its legitimacy and will no longer process your personal data unless we are able to demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms, or for the establishment, exercise or defence of legal claims.

However, when we process your personal data for direct marketing purposes, you have the right to object at any time to such processing of your personal data, and in this case, your personal data will no longer be

processed for marketing purposes. You can exercise this right by using the unsubscribe link provided in all INFOBIP's email marketing communications.

## 11. HOW CAN YOU EXERCISE YOUR RIGHTS?

If you have any questions on how we use your personal data or if you wish to exercise a certain right (as specified under 9 and 10 of this Notice) or resolve a complaint regarding the processing of your personal data, you can contact our Data Protection Officer by sending an email to the following email address: [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com) or by sending a written request via the postal address: INFOBIP d.o.o., attn. Data Protection Officer, Istarska 157, 52 215 Vodnjan, Croatia.

You can exercise your rights in accordance with the Applicable Data Protection Law.

If applicable, you can lodge a complaint with the supervisory authority of the EU member state of your habitual residence, place of work, or place of the alleged infringement. If you want to file a complaint or contact the relevant data protection authority for any other reason, you may find contact details of EEA data protection authorities at: [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en).

## 12. DO WE CONDUCT AUTOMATED DECISION-MAKING, INCLUDING PROFILING, THAT SIGNIFICANTLY AFFECTS YOU?

No. We do not conduct any operation under which you would be subject to a decision based solely on automated processing that has legal or similarly significant effects for you, including profiling.

## 13. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

Your personal data that has been collected and saved in our database in accordance with your consent and will be saved in our database for a period specified in the consent. If you wish to withdraw your consent for the processing of your personal data for any purpose and to delete your data from our database, you can do that at any time by sending an email to [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com).

Regarding your personal data that is not subject to your consent, we will process it for the period necessary to fulfil the purposes outlined in this Privacy Notice, unless a longer period for the processing of such personal data is required or permitted by law. We have provided relevant information under section 5 of this Privacy Notice. Any storage of data beyond the deletion deadlines will encompass only non-personal data (aggregated or anonymized data).

## 14. INFORMATION FROM CHILDREN

Children under 16 cannot use our products and services as our customers. If we learn or are notified that it is the case, we will immediately take reasonable steps to delete that information from our records as quickly as possible. If you consider a child under 16 is using our products or services as a customer, please contact us at [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com).

# 15. SUPPLEMENTAL NOTICE FOR CALIFORNIA RESIDENTS

This Supplemental California Privacy Notice only applies to our processing of personal information that is subject to the California Consumer Privacy Act of 2018 (“CCPA”). The CCPA provides California residents with the right to know what categories of personal information Infobip has collected about them and whether Infobip disclosed that personal information for a business purpose (e.g., to a service provider) in the preceding 12 months. California residents can find this information below:

Category of Personal Information Collected by Infobip	Category of Third Parties Information is Disclosed to for a Business Purpose
<b>Identifiers</b> A name, alias, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.	<ul style="list-style-type: none"> <li>Advertising networks</li> <li>Communication service providers</li> <li>Data analytics providers</li> <li>Service providers</li> <li>Social networks</li> </ul>
<b>Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))</b> A name, signature, contact information, legal eligibility to work in US (for job applicants), experience and any other information you provide us in your resume (for job applicants), bank account number or any other financial information (for clients only)	<ul style="list-style-type: none"> <li>Service providers</li> </ul>
<b>Protected classification characteristics under California or federal law</b> A name, contact (email)	<ul style="list-style-type: none"> <li>Service providers</li> </ul>
<b>Internet or other electronic network activity</b> Browsing history, search history, information on a consumer's interaction with an internet website, application, or advertisement.	<ul style="list-style-type: none"> <li>Advertising networks</li> <li>Data analytics providers</li> <li>Service providers</li> <li>Social networks</li> </ul>
<b>Geolocation data</b> Physical location (over IP) or movements.	<ul style="list-style-type: none"> <li>Advertising networks</li> <li>Data analytics providers</li> </ul>
<b>Professional or employment-related information</b> Current or past job history or performance evaluations.	<ul style="list-style-type: none"> <li>Service providers</li> </ul>
<b>Inferences drawn from other personal information to create a profile about a consumer</b> Profile reflecting a consumer's preferences, behaviour on web site or web based interface	<ul style="list-style-type: none"> <li>Advertising networks</li> <li>Data analytics providers</li> <li>Service providers</li> <li>Social networks</li> </ul>

**Disclosure to Protect Us or Others.** We may access, preserve, and disclose each of the categories listed above to external parties if we, in good faith, believe doing so is required or appropriate to: comply with law enforcement or national security requests and legal process, such as a court order or subpoena; protect your, our, or others’ rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.

## “Sales” of Personal Information under the CCPA

For purposes of the CCPA, Infobip does not “sell” personal information, nor do we have actual knowledge of any “sale” of personal information of minors under 16 years of age.

#### **Additional Privacy Rights for California Residents**

**Non-Discrimination.** California residents have the right not to receive discriminatory treatment by us for the exercise of their rights conferred by the CCPA.

**Authorized Agent.** Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. To designate an authorized agent, please contact us [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com).

**Verification.** To protect your privacy, we will take steps the following steps to verify your identity before fulfilling your request. When you make a request, we will ask you to provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative, which may include contact information. We will only ask for the minimum data and only what is relevant in the given context.

If you are a California resident and would like to exercise any of your rights under the CCPA, please contact us [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com).

We will process such requests in accordance with applicable laws.

**Accessibility.** This Privacy Policy uses industry-standard technologies and was developed in line with the World Wide Web Consortium’s Web Content Accessibility Guidelines, version 2.1. If you wish to print this policy, please do so from your web browser or by saving the page as a PDF.

#### **Contact Information**

Infobip

email address: [data-protection-officer@infobip.com](mailto:data-protection-officer@infobip.com)

the postal address: INFOBIP d.o.o., attn. Data Protection Officer, Istarska 157, 52 215 Vodnjan, Croatia.

## **16. HOW OFTEN DO WE UPDATE THIS PRIVACY NOTICE?**

The most current version of this Privacy Notice will govern our practices for collecting, processing, and disclosing personal data. We will provide notice of any modifications by posting a written notice on our website.