Blip Compliance FAQ - GDPR

We've received a lot of questions about Blip's compliance with the General Data Protection Regulation (GDPR), so we've created this guide to address frequently asked questions. For more information about Blip's security, privacy, and compliance programs, visit the Blip Trust Center.

Does Blip have a Privacy Program?

Blip has a formal privacy and data protection program, which includes structuring a privacy team, establishing Standards, Policies, processes and technological controls, among other requirements for compliance with the main privacy laws.

This program is based on best practices in data governance and personal information protection, seeking to ensure that all data processed by Blip is done in a transparent, secure manner and in accordance with current legislation.

Blip's privacy program includes, among other actions:

- Ongoing training for employees, ensuring that everyone understands the importance of data protection and the legal obligations associated with the processing of personal information.
- Consent management (Blip as Controller): Implementation of clear mechanisms for collecting and storing user consent, when necessary, ensuring that consent is free, informed and explicit.
- Privacy Impact Assessment (DPIA): Conducting assessments to identify and mitigate risks related to the processing of personal data.
- Access control and security: Implementing controls to ensure that only authorized individuals have access to personal data, including the use of encryption and other technologies to ensure data security.
- Data retention policy: Clear definition of retention and disposal periods for personal data, ensuring that data is kept only for the time necessary to fulfill the legitimate purposes of processing.
- Communication channels and data subject rights: Implementation of easily accessible channels so that data subjects can exercise their rights, such as the right to access, correct, delete or transfer their personal data.
- Involvement of all areas of the company: The privacy program involves all areas of Blip, ensuring that data protection is considered in all business processes, from the development of new products to the execution of contracts with partners and suppliers.

With these practices, Blip not only ensures compliance with privacy legislation, but also reinforces its commitment to protecting the privacy of its users and public trust in our services.

Is Blip compliant with the General Data Protection Regulation (GDPR)?

Yes, Blip is in the process of adapting to the GDPR (General Data Protection Regulation). We have an infrastructure in Europe that allows us to process personal data to offer our products and services, including the Blip Platform, to customers and users within the European Economic Area (EEA). This means that, regardless of where our headquarters are located, we are subject to European legislation whenever we process personal data of EEA citizens or offer products and services in the region.

To ensure this compliance, Blip had the support of a specialized consultancy, which helped adapt regulations, contracts, data processing agreements and other adjustments necessary to comply with the legislation. This work included the implementation of technical and organizational measures to ensure that all data processing activities are carried out securely, ethically and within legal requirements.

Who are the data controllers?

In the case of a Blip Platform licensing relationship, the **customer** is considered the "**CONTROLLER**" and **Blip** is the "**PROCESSOR**" of the personal data provided by the customer and transferred to the Blip Platform.

Who is the Data Protection Officer (DPO)? And what is the contact channel?

Blip has appointed **Marcelo Lopes** as **Data Protection Officer (DPO)**, responsible for ensuring compliance with GDPR, as well as ensuring that personal data is processed in accordance with the best privacy and protection practices. The Officer also monitors respect for the rights of data subjects, such as access, correction, deletion and other rights provided for by law.

To contact the Data Protection Officer, simply send an email to **privacy@blip.ai**. This channel is available to clarify doubts, request information or make requests related to the protection of your personal data.

Are there records of personal data processing activities (ROPA)?

Blip maintains a complete inventory of personal data processing activities, which includes a Record of Personal Data Processing Activities (ROPA). This inventory documents in detail all operations carried out with personal data, such as collection, storage, sharing, processing and deletion, ensuring full transparency and compliance with the main privacy laws.

Blip's ROPA is updated regularly and includes information on the purpose of the processing, the legal basis used, the types of personal data processed, the data controllers and recipients of such data, among other aspects.

In addition, Blip adopts controls and processes to ensure that all processing activities comply with data protection standards and are carried out in a secure and transparent manner.

How is our infrastructure organized?

The security of the storage infrastructure is ensured through default encryption for all data at rest, using keys managed internally or by the customer. Data transmission is protected by secure protocols, ensuring integrity and confidentiality. Additionally, mechanisms such as role-based access control (RBAC), integrated authentication, and network restrictions, including firewalls and private network integration, enhance protection against unauthorized access.

How is personal data processed by Blip?

As Controller, the customer is responsible for defining which data will be collected, based on the specific needs of its business or scope of activity.
Blip will process Personal Data for the purposes indicated by the customer (controller), as established in the contract signed between the parties.

Where is personal data processed and stored?

The application is hosted on the cloud. It has three environments to meet the needs of data storage locations:

- Europe - Germany
- USA
- Brazil - São Paulo

Does Blip have access to the data of customers who use the Platform?

In attention to the principles of confidentiality, integrity and availability, access to data is granted and limited only to those who really need access, such as the Platform Support team, for example, and with due transparency to the customer.

How do we protect your data?

Blip adopts best practices and security measures to ensure the privacy, confidentiality and integrity of information, protecting your data against unauthorized access, improper changes and destruction. Our security policies and controls comply with legal and regulatory standards, including GDPR requirements.
Data in transit on the Blip Platform is protected by encryption using, by default, the TLS 1.2 protocols (without weak ciphers) and TLS 1.3 in all data communication. This encryption applies to all interactions, including communication with database systems, ensuring that information remains secure against interception or alteration during transmission.

Stored data (data at rest) is also protected by encryption using, at least, the AES-128 algorithm. This measure ensures the confidentiality and security of information, even in the

event of unauthorized access to the systems. In addition, the management of encryption keys is monitored and audited through independent external audits.

Reinforcing our commitment to data protection, Blip is certified under ISO 27001:2022, one of the most recognized international standards for information security management.

In addition to technical measures, we continually invest in training and raising awareness among our employees through regular training on information security and privacy. This way, we ensure that everyone understands the importance of data protection and follows the established policies and procedures, promoting a safe environment for both our users and customers and for Blip.

Does Blip process sensitive personal data?

Blip does not intend to process sensitive personal data for its own operations. However, when providing the Blip Platform, we collect and process the data transmitted by the smart contact, as defined by the customer ("**CONTROLLER**"). This means that, if the scope of the smart contact involves the collection of personal data or sensitive data, such data will be processed in accordance with the settings established by the customer.

We emphasize that the responsibility for defining the business rules and for the appropriate processing of the data collected lies with the customer, who must ensure compliance with applicable laws, including the GDPR. Blip provides the necessary mechanisms for its customers to manage the privacy and security of the data processed on the platform.

More information can be found in the **Personal Data Processing and Information Security Agreement**.

Does Blip have subprocessors?

Blip may subcontract third-party data processors with whom it may share Personal Data received from Customers, such as cloud providers and service tools. Prior to any subcontracting, Blip carries out a careful risk assessment, considering factors such as information security, GDPR compliance and the ability of the subprocessor to meet the requirements necessary to guarantee the protection of personal data.
In all cases, Blip will be responsible, within legal limits, for all its subprocessors and will require them to comply with Information Security obligations and levels in accordance with the provisions of the DPA.

Who are Blip's subprocessors?

We have a formal and constantly updated register of Blip sub-processors, which undergo a rigorous due diligence process. The updated list of sub-processors can be requested at any time.

How can I exercise my rights as a data subject?

As a data subject, you can exercise your rights easily through our Privacy and Data Security Portal. Simply access the "Privacy Rights" section, where we provide a form so you can make requests, such as access, correction, deletion, portability or revocation of consent, among other rights provided for by the GDPR. As the customer is the data controller, deletion will be preceded by notification to the customer, so that the appropriate measures can be taken.

Our team is prepared to respond to your request quickly, ensuring transparency and security in the process. If you need any additional guidance, you can also contact our team directly by email at **privacy@blip.ai**.

If you are one of our customers (Data Controller), you can send your request to our support team who will respond as soon as possible.

Your request can be registered here: Submit a request

What is the deadline for receiving a response to a request?

As the "**CONTROLLER**", Blip will respond to a request within 30 (thirty) days from the date of receipt of the request sent by the data subject. If more time is needed to analyze or process the request, the data subject will be informed of the additional period in a transparent and clear manner. Blip is committed to ensuring that all requests are handled with due attention, agility and in compliance with current legislation.

As the "**PROCESSOR**", we are committed to responding to requests as quickly as possible from the date of receipt of the request.