Stay GDPR compliant with Bigin

What is GDPR?

General Data Protection and Regulation defines new set of rules on how to collect and handle personal information of EU citizens.

Who does this law apply to?

1. A company, established in EU, that processes personal data of individuals (eg. customers).
2. A company, established outside EU, that processes personal data of individuals present in EU.

In simple words, if your organization has its base in EU or you process the data of EU residents, you come under the GDPR radar.
This does not depend on the size of your company, but the nature of the activities.

Data Collector - Determines the purpose and means by which personal data is processed
Data Processor - Processes the personal data on behalf of the controller.
Data Subject - The person whose personal information you collect are the data subjects.

Bigin as a Data Processor

Bigin complies with GDPR as the data processor, with fully equipped tools to help secure the personal data.

Data Collection

GDPR requires the purpose and get consent when collecting personal information.

Lawful bases of Data Processing

GDPR defines 6 lawful bases of processing personal data.

1. **Consent** - When you have consent from the data subject to process their personal data. There must be a deliberate action on the part of the data subject to opt in or give consent.
   Example: Collecting and processing personal data for marketing purposes or for sending newsletters.
2. **Contract** - When you have a contract with an individual to supply goods or services requested by them. In this case, you process data to fulfil the contract.
   Example: During a contract, when the customer asks for more information via email, the organization processes their personal data to respond to the request.

3. **Legal Obligation** - When you have to process the data to comply with the law.
   Example: An employee's salary details are needed by a government institution or an investigation requires the processing of the personal data.
4. **Vital Interests** - When you need to process data to protect someone's life or in an emergency.
   Example: Collecting personal details of the people to ensure their safety during an emergency or a fire.
5. **Public Interests** - When you need to carry out tasks in the public interest, usually as a government institution, political party, etc.
   Example: As a public authority who processes data for scientific research, surveys, or public health studies.
6. **Legitimate Interests** - When your organization holds a genuine, legitimate reason to process data and the purpose does not harm the data subject's rights. Example: A customer has not paid their invoice and so the company needs to process the customer's data to collect payment. Or, for administrative purposes, when an organization processes an employees' personal data for payroll.

Data Source

Data subject's information can be pushed into Bigin in many ways. You can also enter the information manually. Data source keeps a record of how the information landed in Bigin.

Consent

Before the data is processed, consent should be obtained from the respective individuals. Data Controllers should explicitly state the reason why they are obtaining consent.

Bigin allows you to get consent from data subjects in 2 ways.

1. **Consent form** - The consent form available in Bigin can be customized with various fields that ask for communication preferences, consent statements by the data subjects, etc. The link to this form can be used in email templates and sent to get consent.
   You can send individual emails from a record, or mass email to a list of records.
2. **Update manually** - When you get consent during a call or in person, you can update it manually in the *Data Privacy* section of a record.

Rights of a Data subject

1. **Right of access**: The subject's right to obtain from the controller, the confirmation as to the processing of their data and furthermore request to access their personal information.
2. **Right to rectification**: The subject's right to ensure that their personal data is accurate and updated as needed.
3. **Right to erasure or be forgotten**: The subject's right to ask the controller for the erasure of their personal data without undue delay.
4. **Right to object and restriction of processing**: The subject's right to object to the processing of their data and even restrict it if they so desire.
5. **Right to data portability**: The subject's right to obtain their information in a structured and machine-readable format or have their data transferred to another organization if feasible.

6. **Right to be informed**: The subject's right to be informed of how and why their personal data is being processed. Also, they have the right to know if the data is being shared with other third-party. This can be addressed by identifying the appropriate lawful bases to process data. In case of a consent being , getting proper
7. **Right to be notified**: In case of a data breach, the data subjects need to be informed within 72 hours of first having become aware of the breach.