



Data Subject Rights

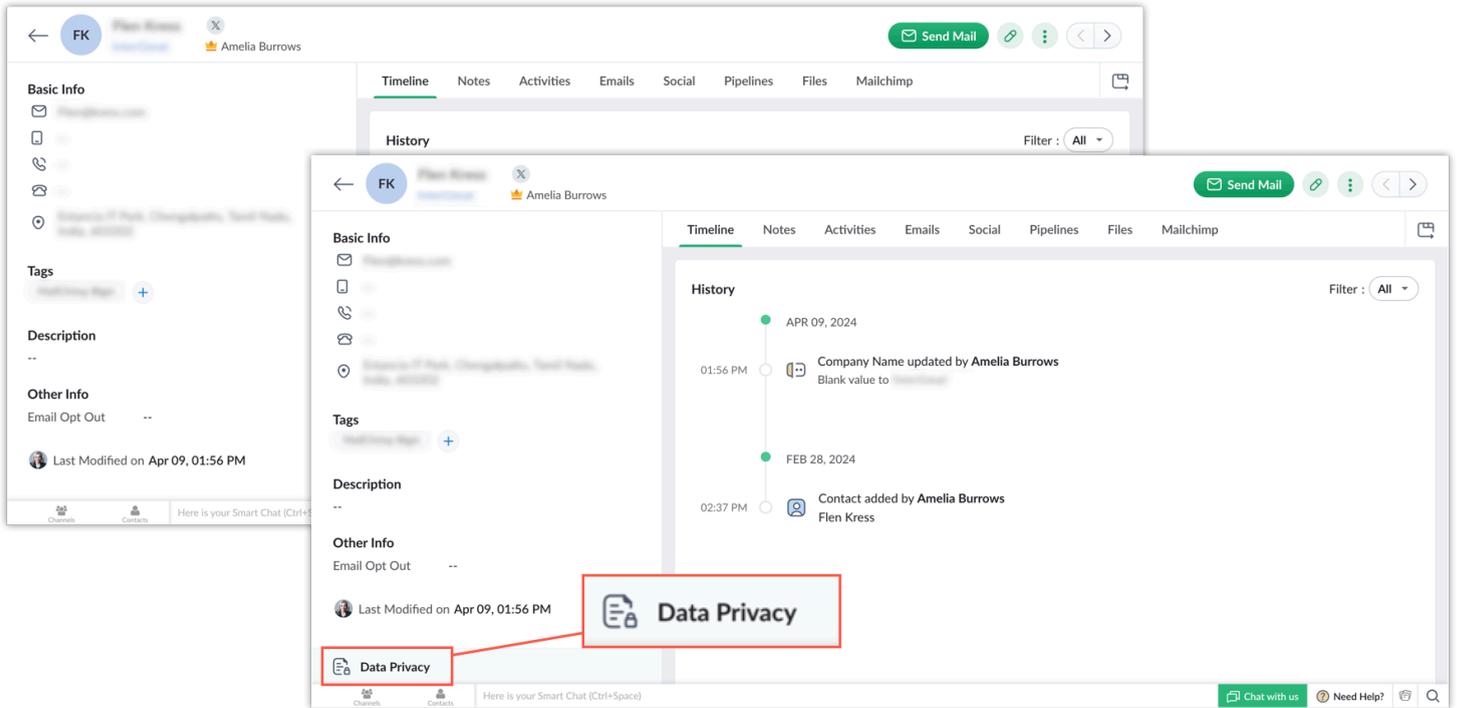
As per GDPR [Articles 12 to 23](#), individuals have specific rights concerning their personal data. Organizations must understand and meet these rights when individuals seek to exercise them.

- **Right of access:** Individuals have the right to ask the controller to confirm if their data is being used and to request access to their personal information.
- **Right to rectification:** Individuals have the right to make sure their personal data is accurate and up to date. They can ask for corrections or updates when needed.
- **Right to erasure or be forgotten:** Individuals have the right to request the deletion of their personal data from the controller's records without delay.
- **Right to object and restriction of processing:** Individuals have the right to say no to their data being used and can ask for limits on how it's used if they want.
- **Right to data portability:** Individuals have the right to receive their information in a structured, machine-readable format or to have their data transferred to another organization, if feasible.
- **Right to be informed:** Individuals have the right to know why and how their personal data is being used. They also have the right to know if their data is being shared with others. This is done by following the right legal rules for using data. If consent is needed, it's important to get it right.
- **Right to be notified:** In the event of a data breach, individuals must be notified within 72 hours of the controller becoming aware of the breach.

To enable data subject rights, the initial step is to activate GDPR compliance in your account. This regulatory framework ensures the protection of personal data and grants individuals rights over their data. To initiate this process, follow the steps mentioned in this [help document on managing compliance](#). Once GDPR compliance is successfully enabled, a new feature becomes accessible within the contact's detail page, known as *Data Privacy*.

Upon accessing the Data Privacy section, you will have a set of options designed to facilitate data subject rights.

Before enabling GDPR Compliance



After enabling GDPR Compliance

To add a data subject's request to your account, go to any **Contact > Data Privacy > Data Subject Requests > + Request button**. You can gather requests via email, through a call, or face-to-face.

New Request

- Request to access data**
Data subject will have an option to view their personal data on sending an email with personal fields information.
-
- Request to rectify data**
Data subject will have an option to rectify personal fields by sending a .CSV file containing personal information and updating changes manually.
-
- Request to export data**
Data subject will have a copy of their personal data in CSV format, which can be used in other systems.
-
- Request to stop processing data**
Subject's data should be locked from further use or processing once this request is received.
-
- Request to delete data**
Subject's data should be deleted and moved to block list to prevent data being re-entered.

Cancel

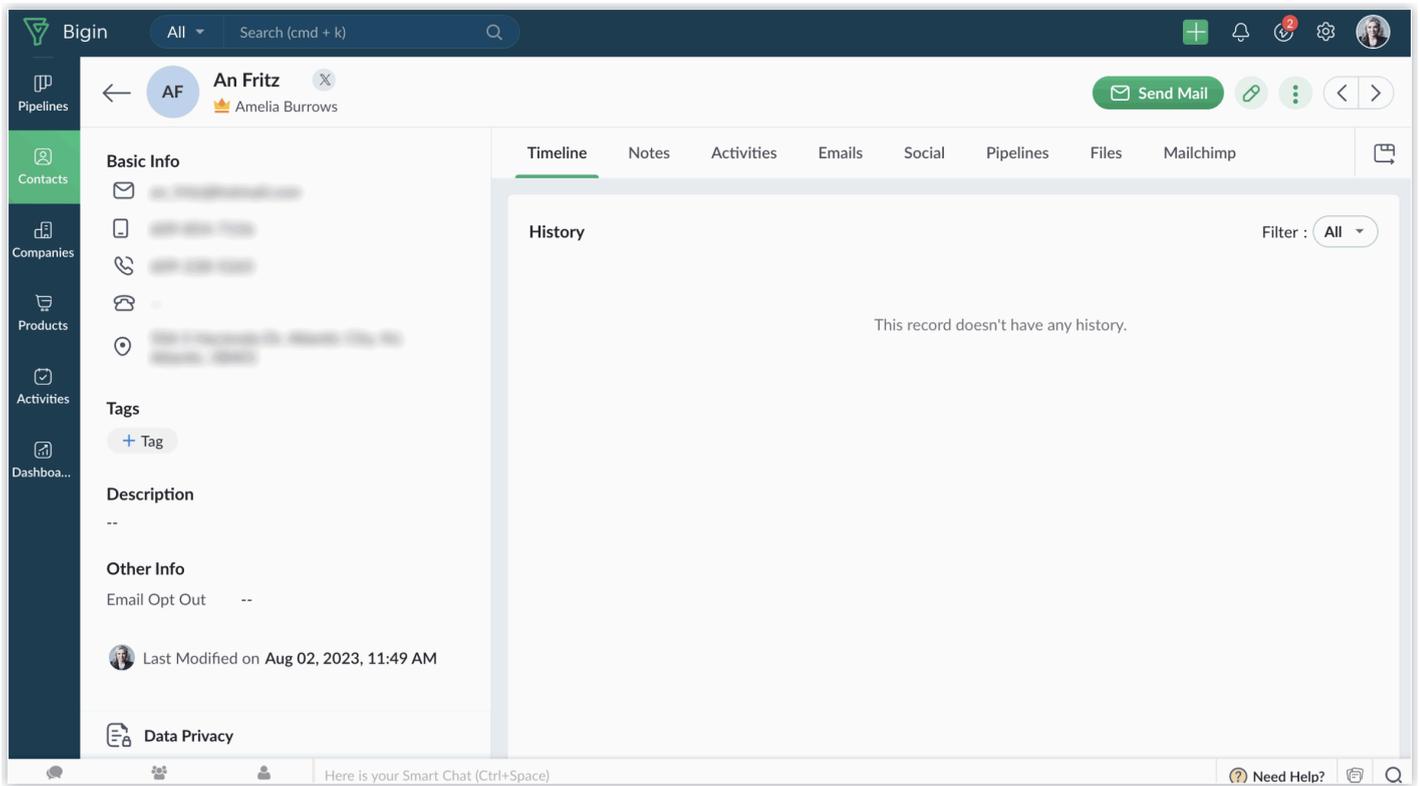
Save

Request to access data (Right to access)

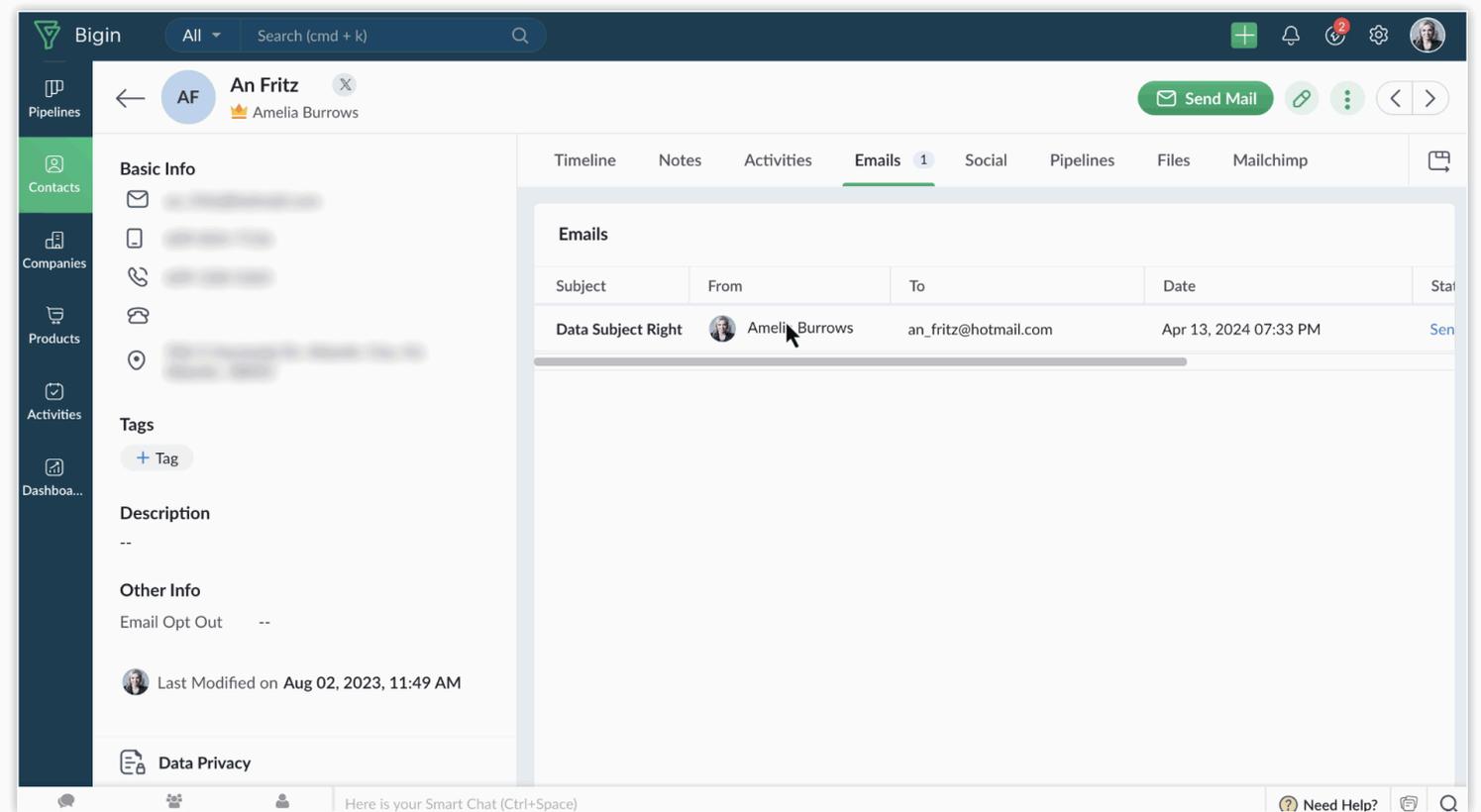
With the consent forms created, you can send emails in CSV format when data subjects request access to their information.

To send an email with the data subject's information:

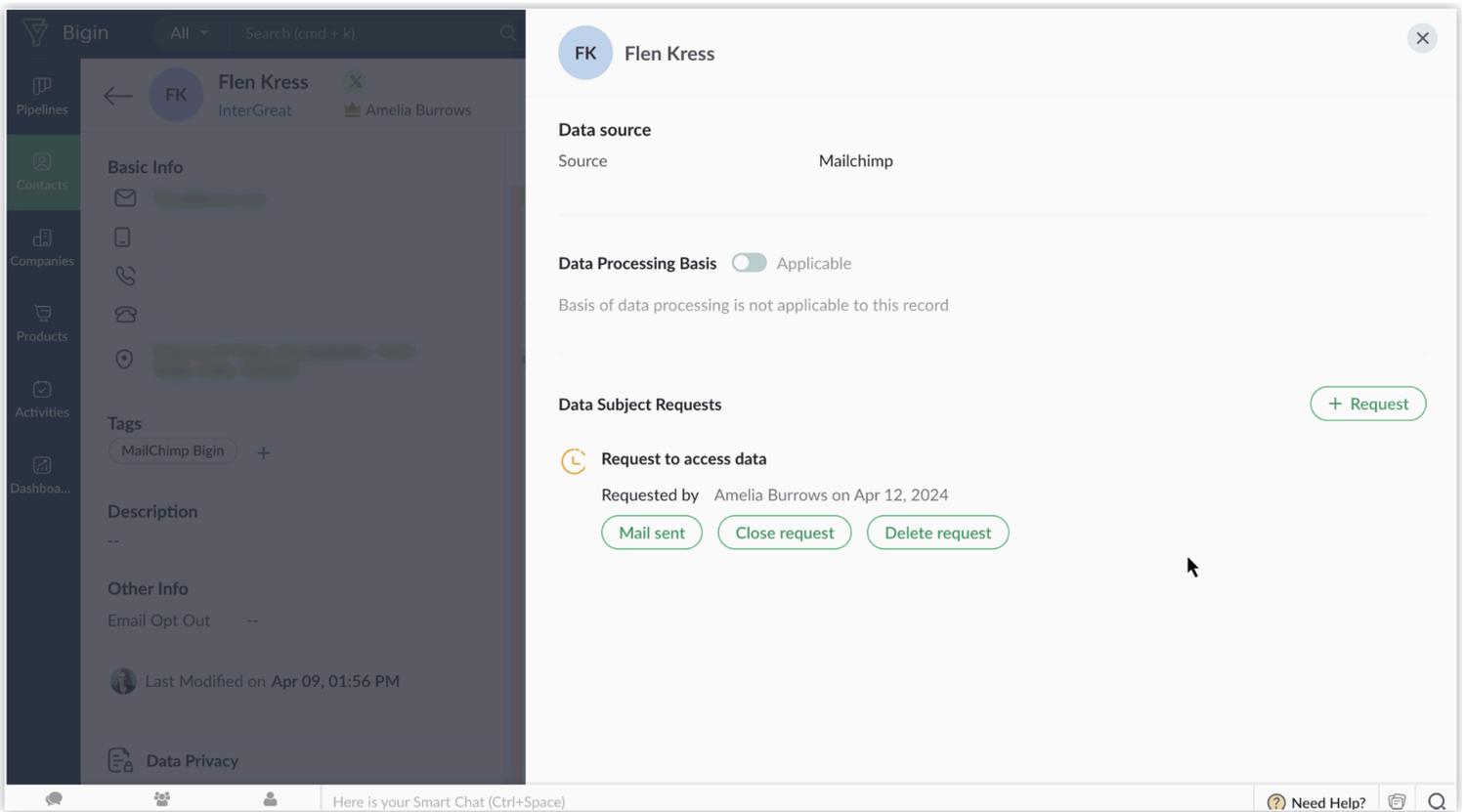
1. Open the user's record and click **Data Privacy**.
2. Under the Data Subject Requests section, click + **Request**.
3. In the New Request pop-up, select **Request to access data**.
4. Click **Save**, and the request will be added to the record.
5. Click **Send email** for the request to access data.
6. In the email composer, compose an email or select the email template with which you want to send the email, and send the email.



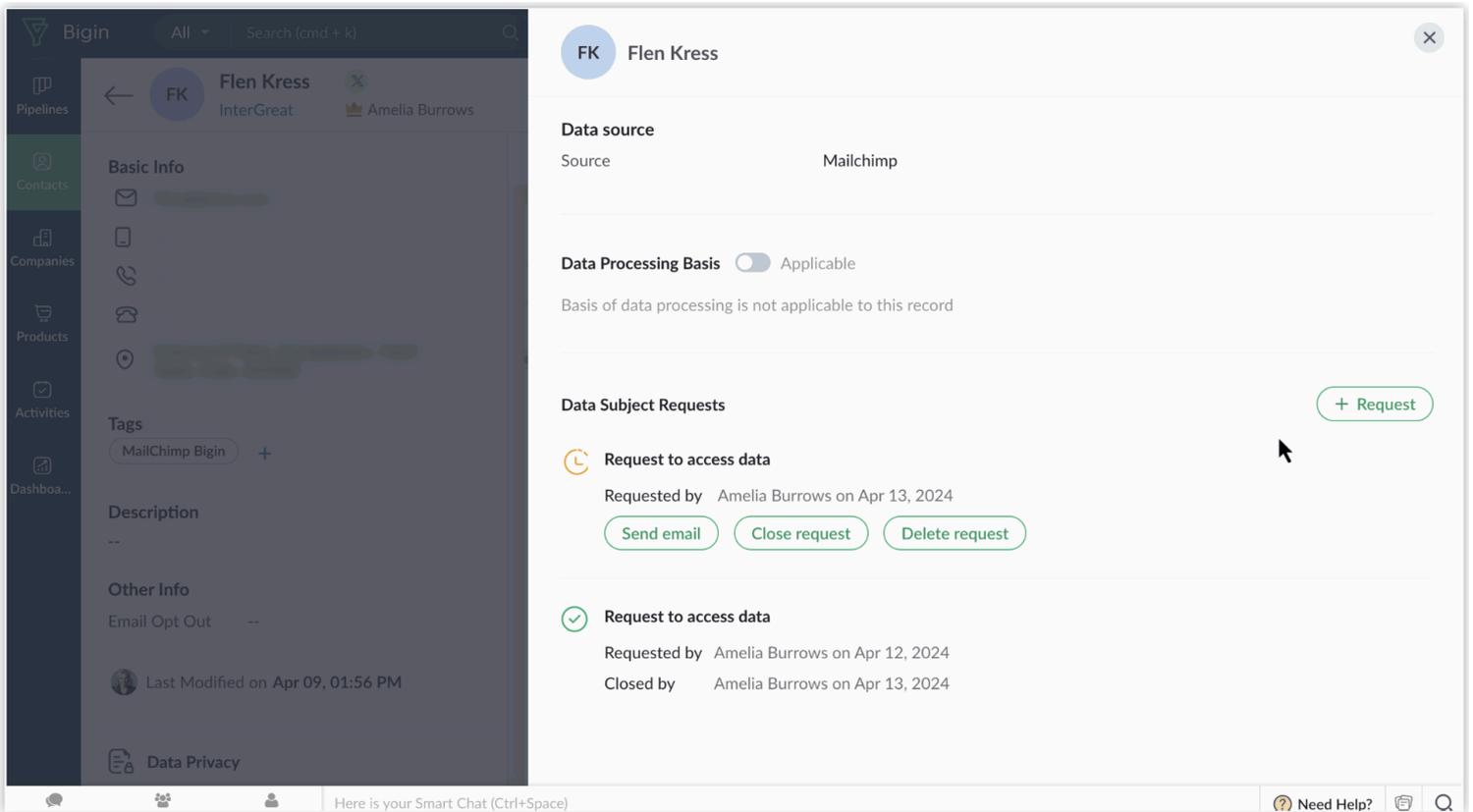
You can view the email sent from the related list tab. You can also download the CSV file that you send from here.



You can close the request created once you are done. To close the request, click on **Close Request**. You can create a new request only after you close the existing request.



If you have sent the request by mistake, or if you need to revert the request, you can delete the request. Remember, you cannot delete the request once you close the request. To delete the request, click on **Delete Request**.

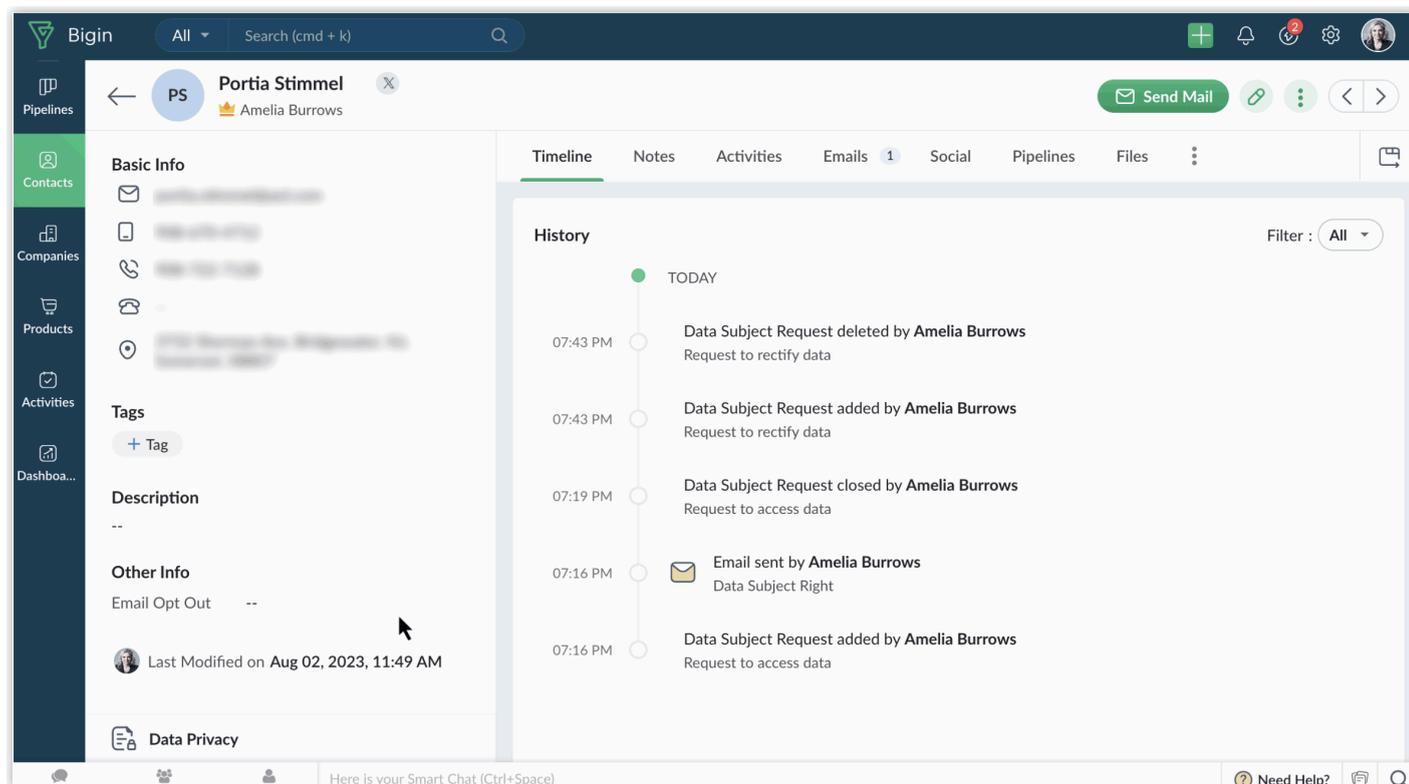


Request to rectify data (Right to rectify)

You can send an email with a CSV file containing the data subject's information. They can then correct the information in the CSV file and send it back to you. Afterward, you can import it into your account to update the information.

To send an email to rectify the data subject's data:

1. Open the user's record and click **Data Privacy**.
2. Under the Data Subject Requests section, click + **Request**.
3. In the New Request pop-up, select **Request to rectify data**.
4. Click **Save**, and the request will be added to the record.
5. Click **Send email** for the request to rectify data.
6. In the email composer, select the email template with which you want to send the email, and send the email.



Similar to request access data, you can view the email sent from the related list tab. You can also download the CSV file that you send from here. You can also close the request and delete the request.

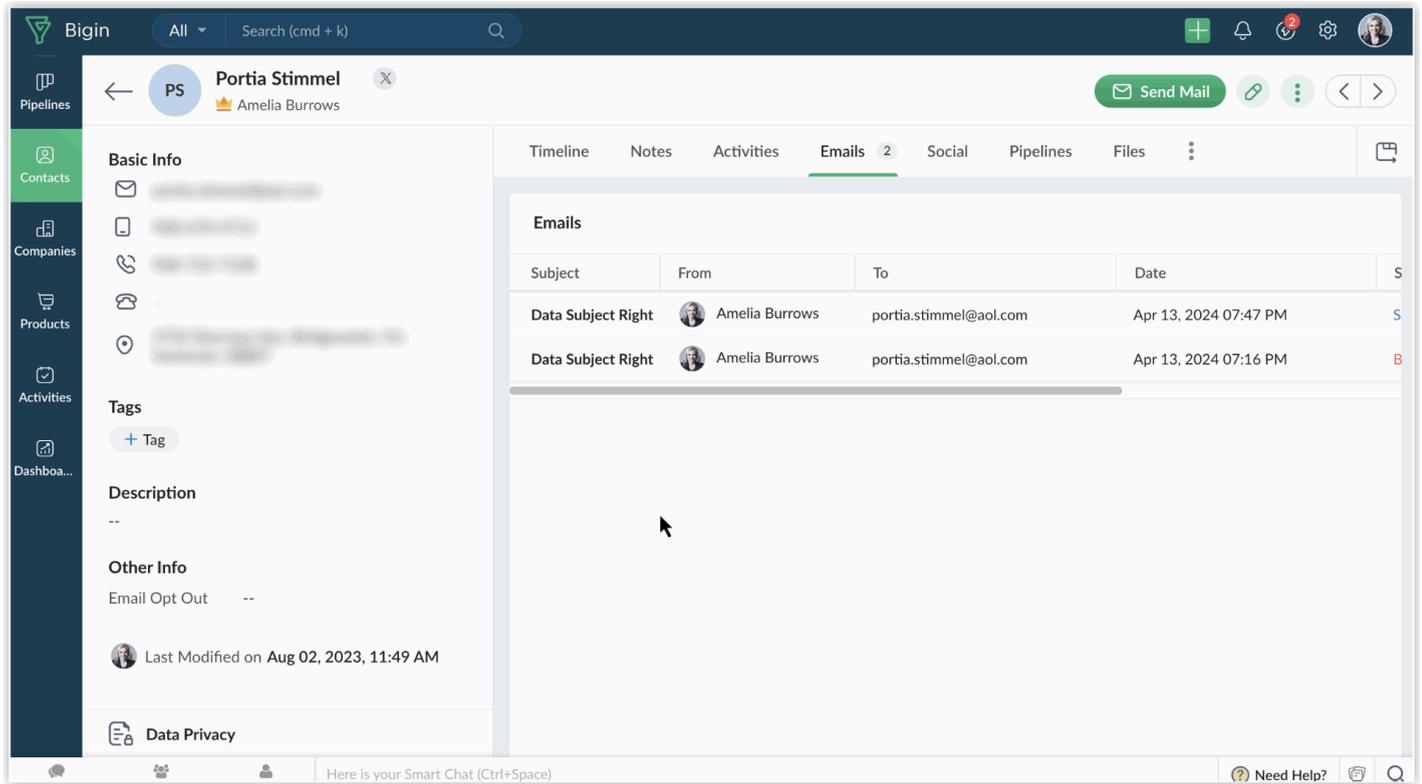
Request to export data (Right to portability)

You can export data subject information in a machine-readable CSV format, attach it to an email, and send it, all without downloading it onto the Controller's device.

To send a copy of the data subject's data:

1. Open the user's record and click **Data Privacy**.
2. Under the Data Subject Requests section, click + **Request**.

3. In the New Request pop-up, select **Request to export data**.
4. Click **Save**, and the request will be added to the record.
5. Click **Send email** for the request to export data.
6. In the email composer, select the email template with which you want to send the email, and send the email.



Similar to request access data, you can view the email sent from the related list tab. You can also download the CSV file that you send from here. You can close the request and delete the request, too.

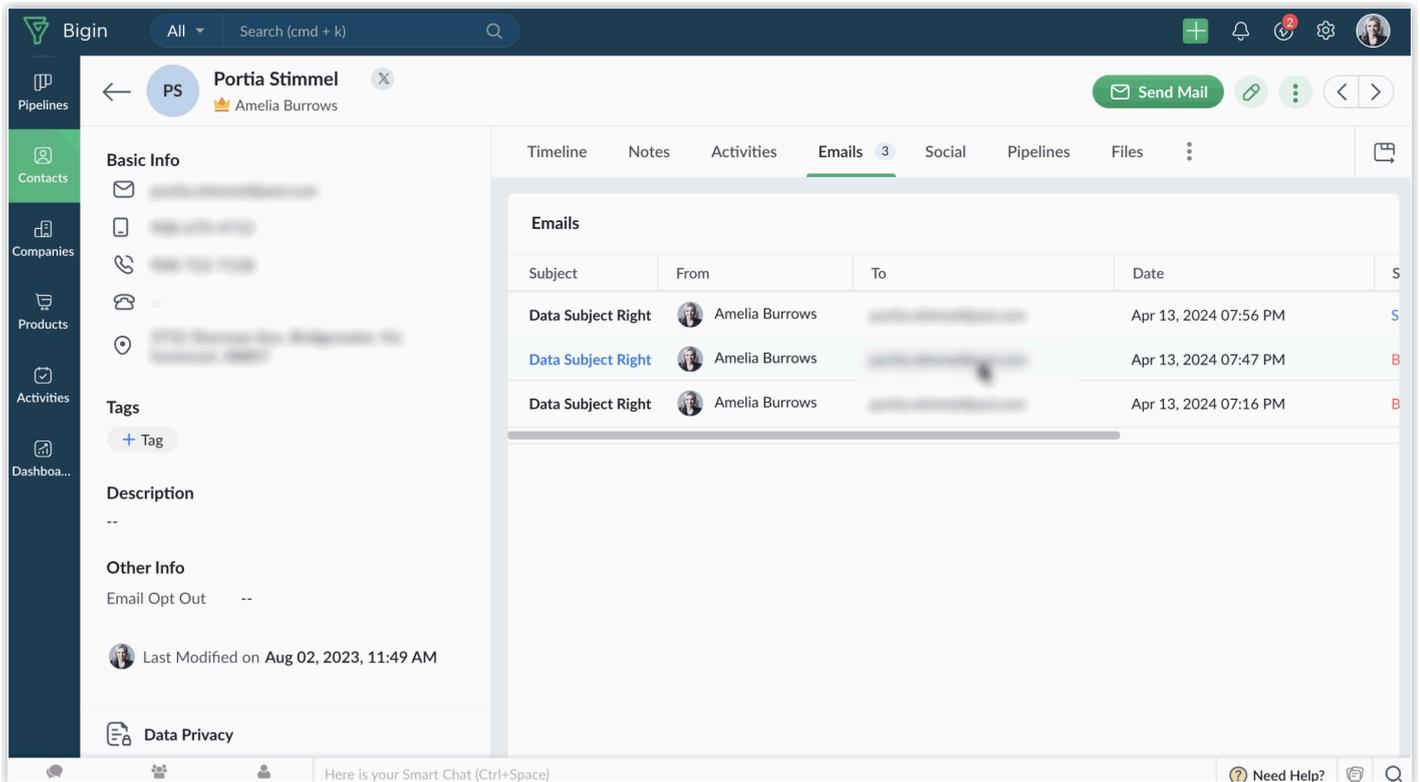
Request to stop processing data (Right to stop processing)

Once they exercise this right, you can halt the processing of the data subject's information in Bigin. You can also lock the data subject's information, halting any further processing. When a record is locked, all its details are also restricted from further use or processing within Bigin. For example, you cannot send emails, edit the record, make calls, and so on.

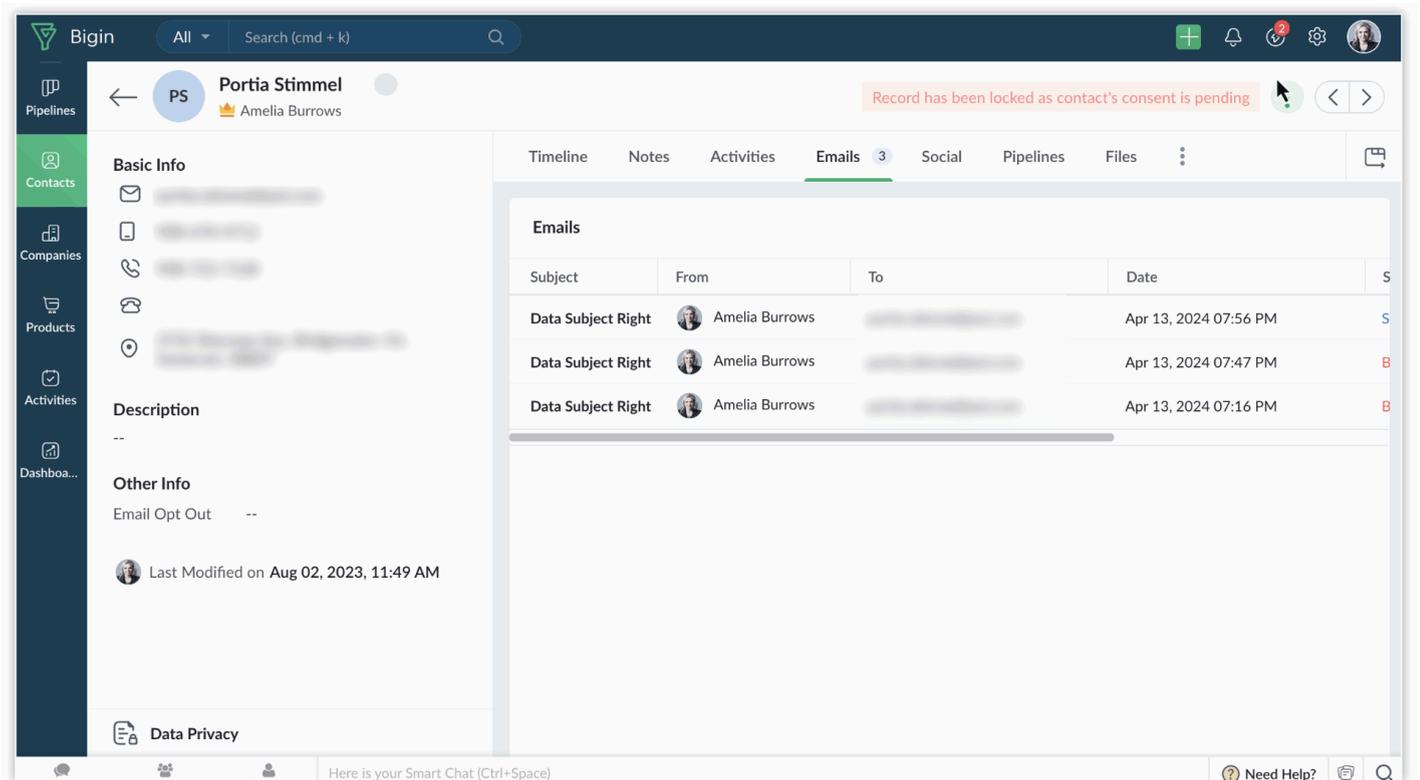
To lock the record:

1. Open the user's record and click **Data Privacy**.
2. Under the Data Subject Requests section, click **+ Request**.
3. In the New Request pop-up, select **Request to stop processing data**.
4. Click **Save**, and the request will be added to the record.
5. Click **Lock** for the Request to stop processing data.

6. The record will be locked, and you cannot perform any actions for the record, as mentioned earlier.



7. You can unlock the record when a contact requests you to do so. To unlock the record, click **Unlock**. Once it is unlocked, you can edit the records, make calls, and send emails.



Request to delete data (Right to be forgotten)

Once requested, the data subject's information can be locked in Bigin for the retention period set in the Data Controller's terms of service. During this time, the data won't be processed. Afterward, the controller can choose

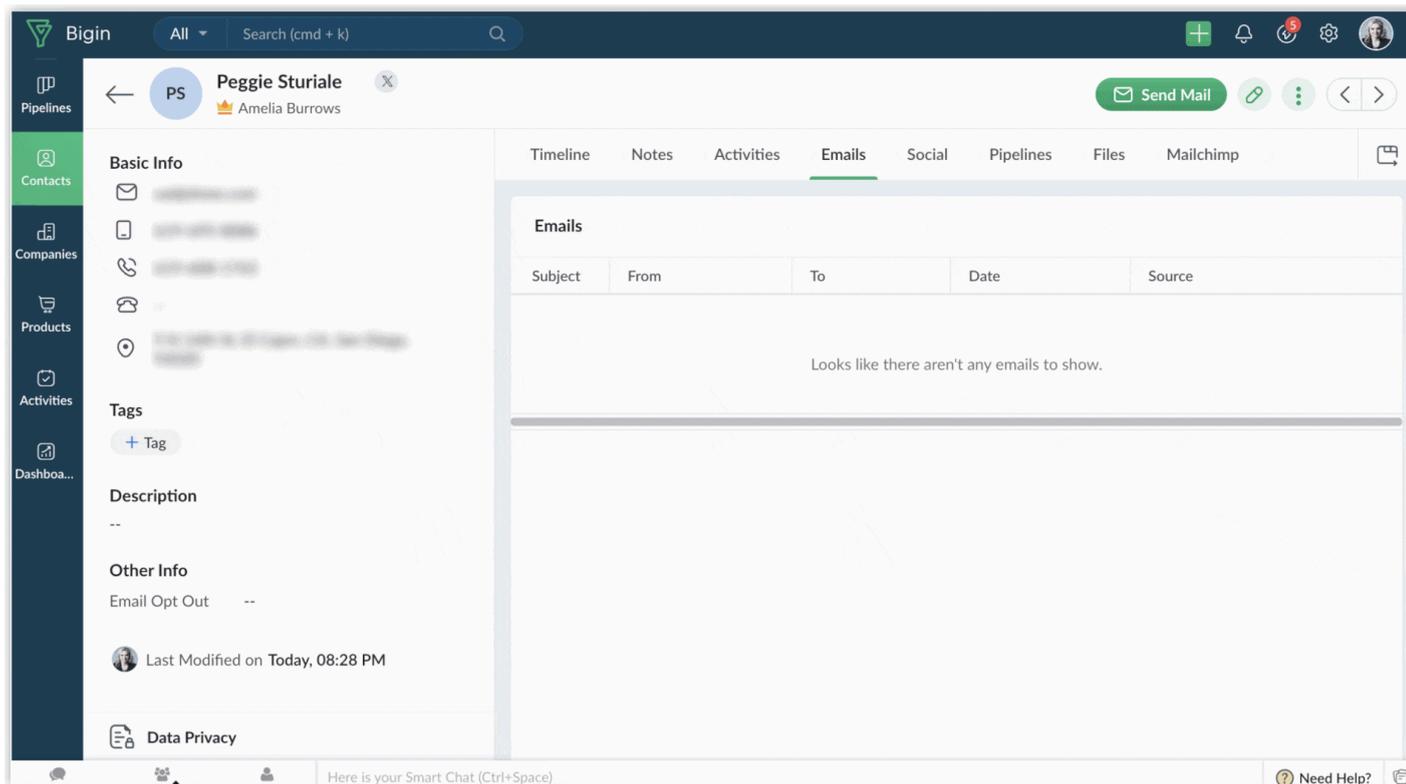
to delete the data subject's info. When deleted, the email address will be added to a block list, stopping re-entry through import or synchronization.

Note:

- You need valid permission to put a record on the block list.
- When a record is on the block list, all records with the same email address are deleted.

To lock and block-list the record:

1. Open the user's record and click **Data Privacy**.
2. Under the Data Subject Requests section, click + **Request**.
3. In the New Request pop-up, select **Request to delete data**.
4. Click **Save**, and the request will be added to the record.
5. Click **Lock** for the Request to stop processing data.
6. Click the **Move to block list** button to remove it from your account.
7. In the Blocklist Record pop-up, select **Move to block list**; the record will be removed, and the email address will be added to the block list.



8. Nonetheless, you can manually add a record with the same email address if needed; you will be warned with a notification.

Block list record

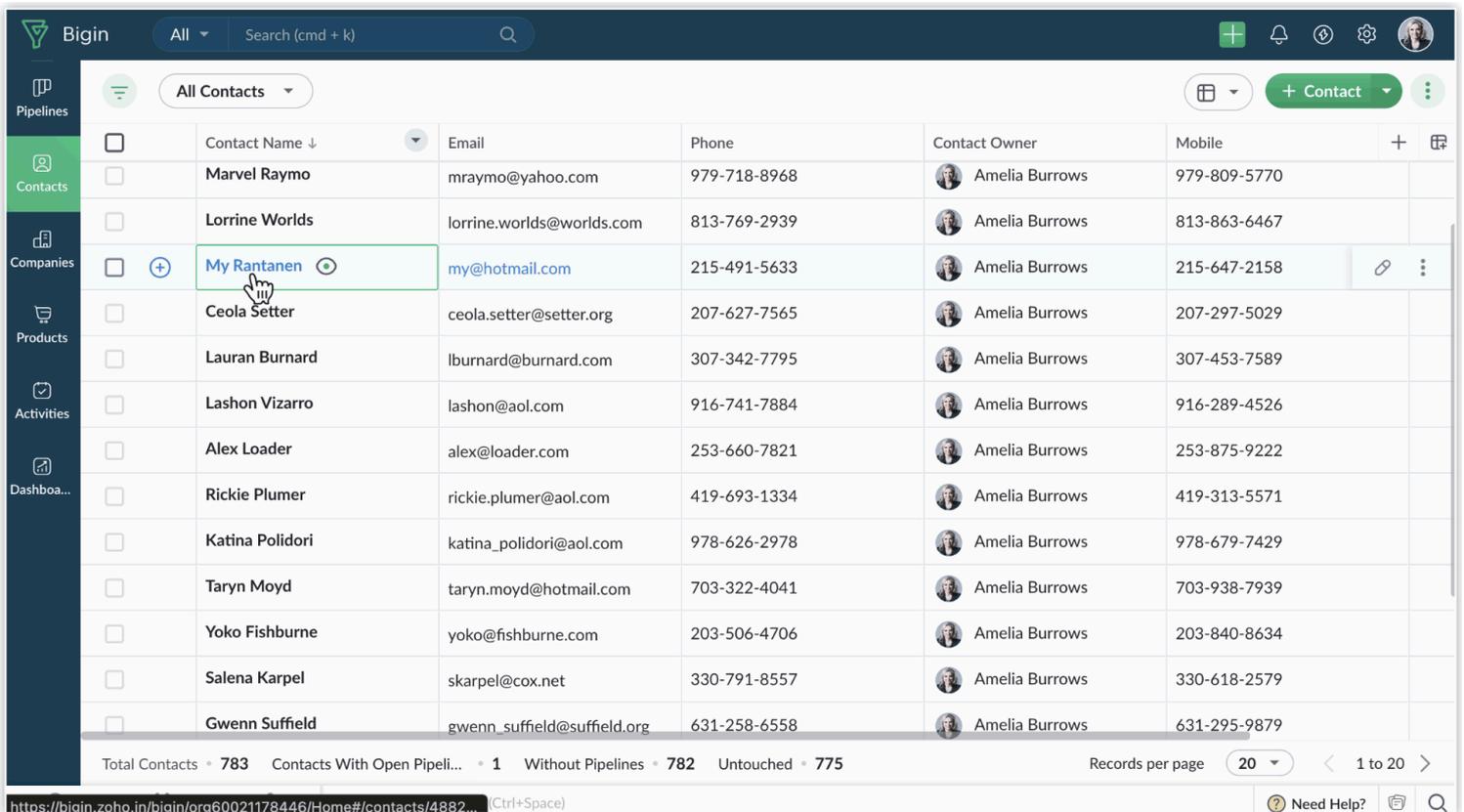
You are trying to add a record that has been block listed under the right to be forgotten. Do you still want to proceed?

No

Yes, Continue

Lawful basis of data processing

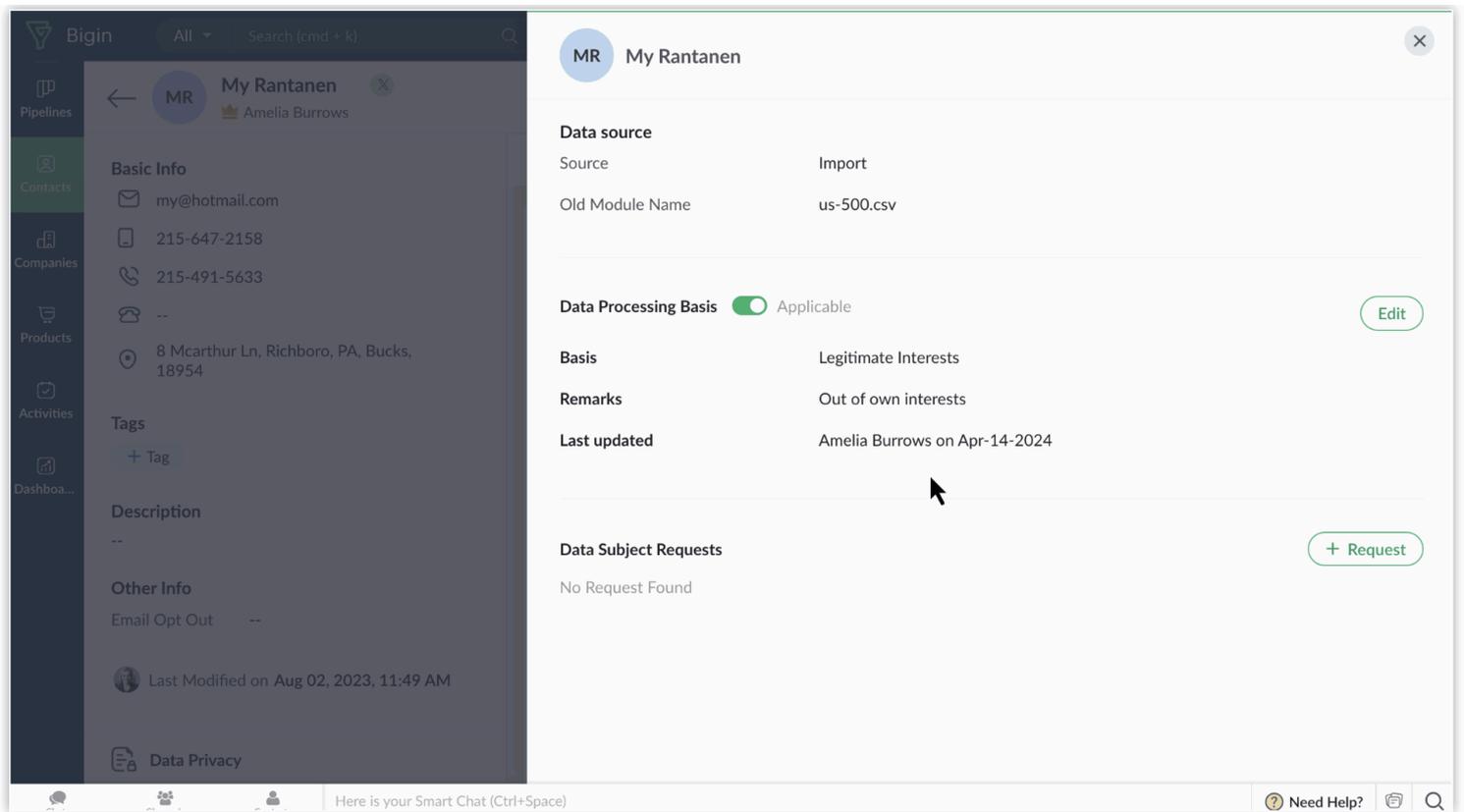
GDPR defines six lawful basis for processing personal data. To activate Data Processing Basis, go to **Contacts > Any record > Data Privacy > Data Processing Basis > Enable > Choose the Data Processing Basis.**



The screenshot shows the Zoho CRM interface. The top navigation bar includes the 'Bigin' logo, a search bar, and user profile icons. The left sidebar contains navigation options: Pipelines, Contacts, Companies, Products, Activities, and Dashboards. The main content area displays a table of contacts under the 'All Contacts' filter. The table has columns for Contact Name, Email, Phone, Contact Owner, and Mobile. The contact 'My Rantanen' is highlighted in blue, and a mouse cursor is pointing at the 'Edit' button (a circle with a right-pointing arrow) next to the contact name. Below the table, there are summary statistics: Total Contacts (783), Contacts With Open Pipelines (1), Without Pipelines (782), and Untouched (775). The bottom of the interface shows the browser address bar with the URL 'https://bigin.zoho.in/bigin/org60021178446/Home#/contacts/4882...' and a 'Need Help?' button.

| Contact Name | Email | Phone | Contact Owner | Mobile |
|-----------------|-----------------------------|--------------|----------------|--------------|
| Marvel Raymo | mraymo@yahoo.com | 979-718-8968 | Amelia Burrows | 979-809-5770 |
| Lorraine Worlds | lorrine.worlds@worlds.com | 813-769-2939 | Amelia Burrows | 813-863-6467 |
| My Rantanen | my@hotmail.com | 215-491-5633 | Amelia Burrows | 215-647-2158 |
| Ceola Setter | ceola.setter@setter.org | 207-627-7565 | Amelia Burrows | 207-297-5029 |
| Lauran Burnard | lburnard@burnard.com | 307-342-7795 | Amelia Burrows | 307-453-7589 |
| Lashon Vizarro | lashon@aol.com | 916-741-7884 | Amelia Burrows | 916-289-4526 |
| Alex Loader | alex@loader.com | 253-660-7821 | Amelia Burrows | 253-875-9222 |
| Rickie Plumer | rickie.plumer@aol.com | 419-693-1334 | Amelia Burrows | 419-313-5571 |
| Katina Polidori | katina_polidori@aol.com | 978-626-2978 | Amelia Burrows | 978-679-7429 |
| Taryn Moyd | taryn.moyd@hotmail.com | 703-322-4041 | Amelia Burrows | 703-938-7939 |
| Yoko Fishburne | yoko@fishburne.com | 203-506-4706 | Amelia Burrows | 203-840-8634 |
| Salena Karpel | skarpel@cox.net | 330-791-8557 | Amelia Burrows | 330-618-2579 |
| Gwenn Suffield | gwenn_suffield@suffield.org | 631-258-6558 | Amelia Burrows | 631-295-9879 |

You can edit your basis any time you want by just clicking on the **Edit** button.



Here are each of them in detail.

- **Legitimate interests:** Processing personal data is allowed when it's needed for the controller's or a third party's legitimate interests, unless it goes against the rights and freedoms of the individual.
 - **Example:** An organization may process customer data for direct marketing purposes if it can demonstrate a legitimate interest, such as promoting relevant products or services to existing customers. Similarly, employers may process employee personal data for administrative purposes, such as payroll processing or performance management, as long as it's done in a way that respects the rights and freedoms of the employees.
- **Contract:** Personal data can be processed if it's necessary for fulfilling a contract with the individual or for taking steps at their request before entering into a contract.
 - **Example:** When someone purchases a product online, their personal data, such as name, address, and payment information are necessary for the organization to fulfill the order.
- **Legal obligation:** Processing personal data when it's required to comply with the law.
 - **Example:** Businesses may need to process personal data for tax purposes or to comply with employment laws, such as providing employee salary details to tax authorities.
- **Vital interests:** Personal data can be processed when it's necessary to protect someone's life.
 - **Example:** During a medical emergency, healthcare providers may need to access and process a patient's medical records to provide life-saving treatment.
- **Public interests:** Processing personal data is permitted when it's in the public interest or for official functions performed by public authorities.
 - **Example:** Government agencies may collect and process personal data for statistical purposes, public health surveillance, or national security.

Note:

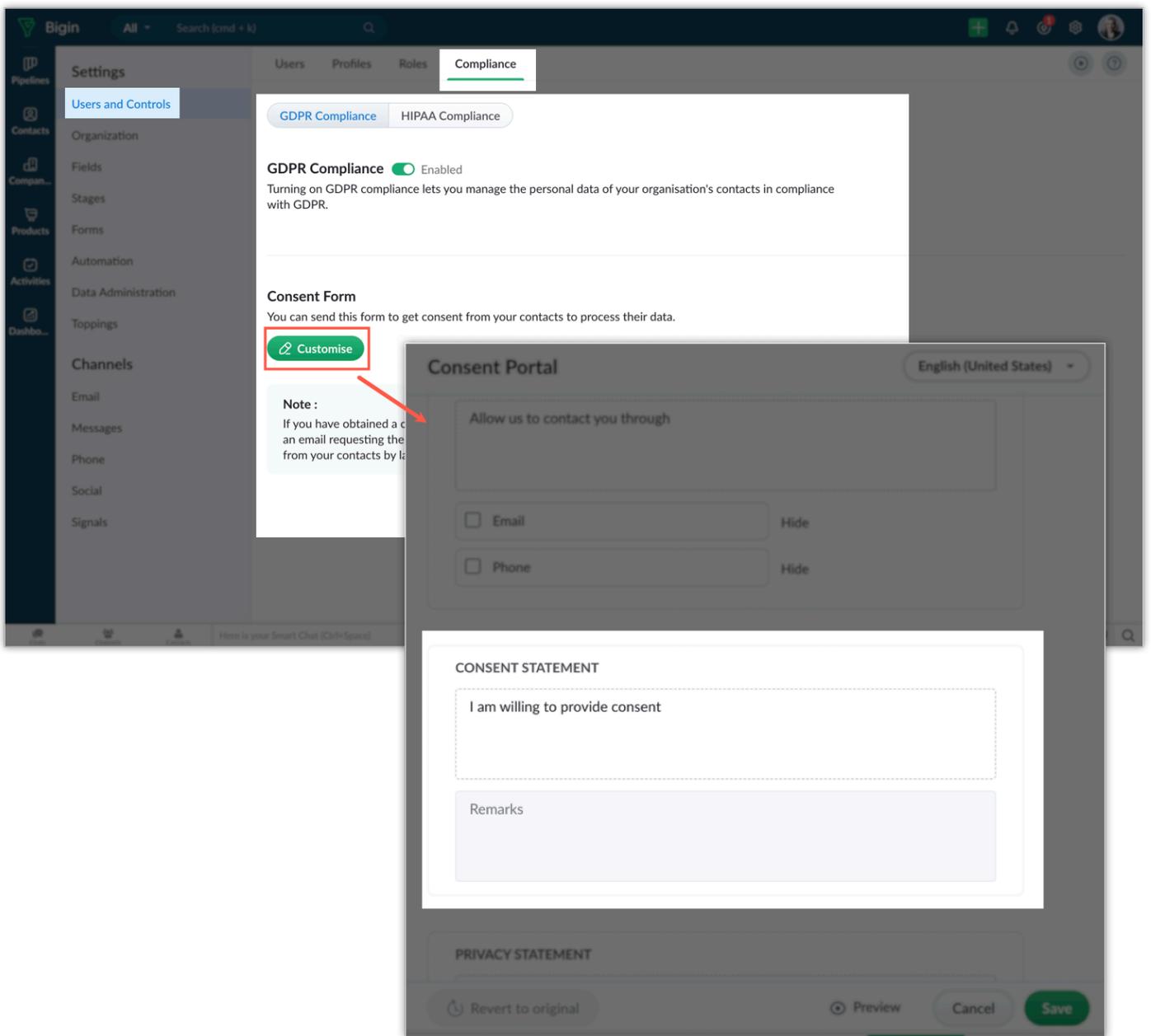
- For the above-mentioned data processing basis, you can add Consent remarks, if required.

- **Consent:** This is when individuals give clear permission for their personal data to be used for specific purposes. It requires an affirmative action from the individual, such as ticking a box or signing a form.
 - **Example:** If a user subscribes to a newsletter by providing their email address and ticking a consent box, they are allowing the organization to send them marketing emails.

Ways to get consent

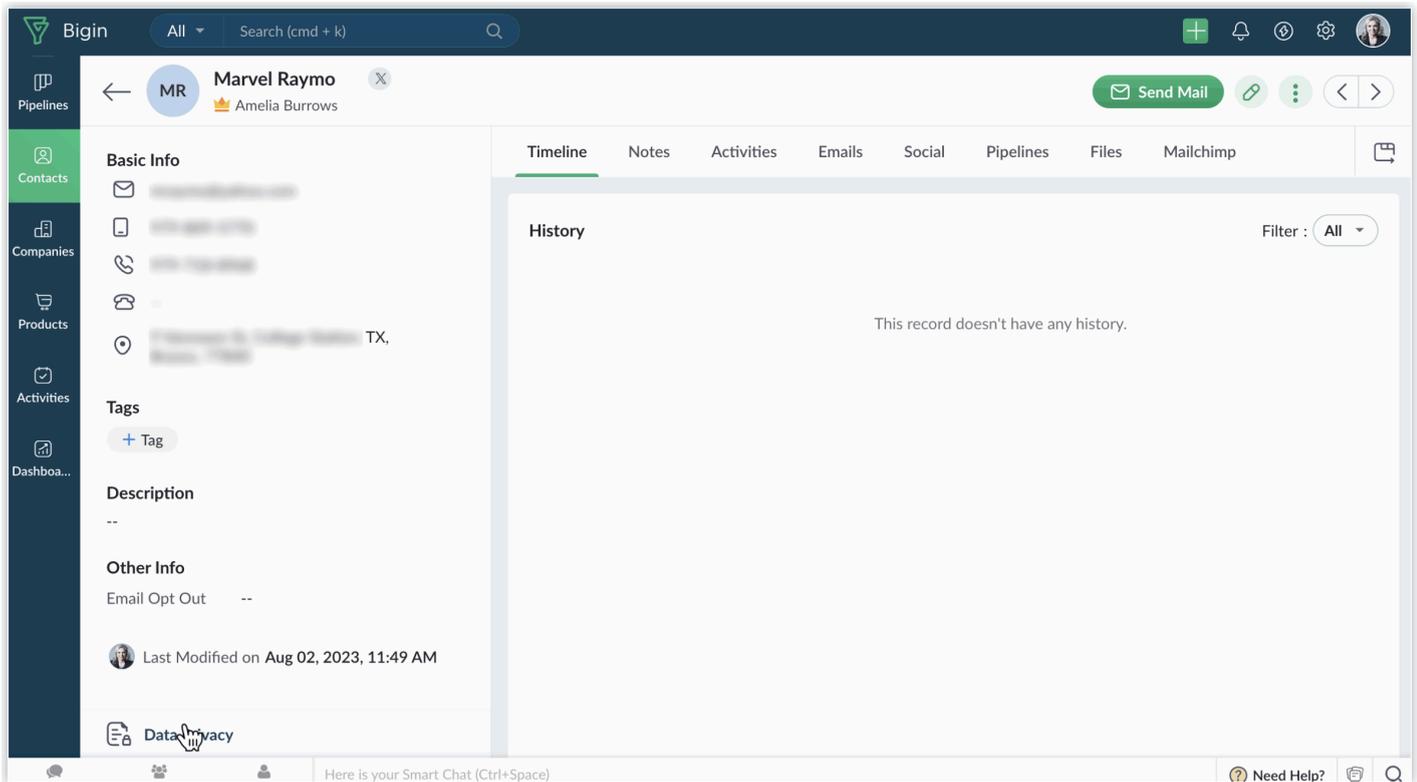
In Bigin, there are two ways to obtain consent from data subjects.

- **Consent Form:** In Bigin, you can personalize consent forms with fields for communication preferences and consent statements. To create a consent statement, go to **Settings > User and Controls > Compliance > Consent Form > Customize > Consent Statement.**

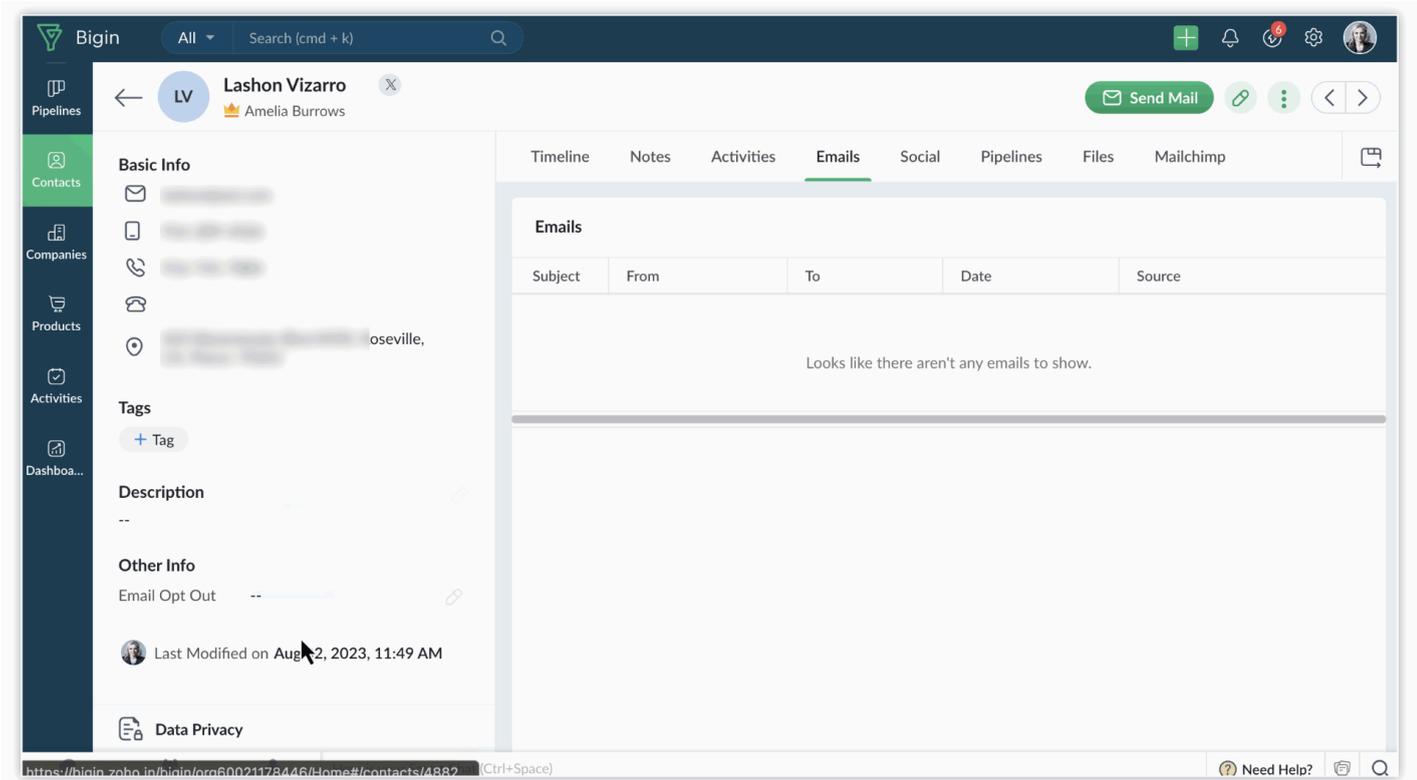


These forms can be shared via email templates, allowing you to request consent from individuals. Additionally, you have the option to send individual emails from a record or send mass emails to a list of

records.



- **Manual Update:** If you obtain consent during a phone call or face-to-face meeting, you can manually update the consent status in the Data Privacy section of a record.



Stages in consent management

Based on the customer response, the status of the consent request is processed; the stages involved here are as mentioned below.

- **Pending:** When a consent request hasn't been sent to data subjects.

- **Waiting:** After sending the consent form, while awaiting a response.
- **Obtained:** When consent is received from the data subject.
- **Not responded:** When consent isn't received within the defined waiting period in Consent Settings.

Data Processing Basis Applicable Edit

Basis Consent

Status Pending Waiting Obtained Not Responded

