

Trivacy - Installation and Configuration Guide

Introduction

Trivacy is an on-platform Salesforce app that allows organizations to view and manage all personal data in a Salesforce org. With this app, your organization can comply with personal data protection regulation (GDPR, CCPA, HIPAA, etc.) for your Salesforce data with just a few clicks of a button. The app automates the laborious process of locating, viewing, exporting, anonymizing and deleting personal data on your Salesforce organization, and enhances Salesforce's existing data protection functionality, such as the Individual object and the ability to delete field history.

Overview

Personally Identifiable Information (PII) can be stored in many different places in Salesforce; in Contact and Individual records, Attachments (e.g., a passport scan), Email Messages, Tasks (e.g., notes on a medical condition), Chatter (discussing that call with a colleague) and many more. Dealing with all this personal data to comply with privacy regulation requires expert technical knowledge of Salesforce administration and the Salesforce data model and security. Even if you have this expertise in your organization, handling this manually as per the long list of [manual steps recommended by Salesforce](#) is very time consuming and error prone.

Trivacy massively simplifies personal data management by bringing personal data spread out over different objects in a single page, and allows users without special administrative permissions to review, edit, export, obfuscate, anonymize or delete data across linked records in a few clicks. Trivacy uses configurable object linkages that indicate how to control personal data from one object to another, e.g., from `Contact` -> (converted) `Lead` -> `Attachment`. Links are based on Salesforce lookup or master-details fields, and can point the same direction as the Salesforce data model (e.g., from `Contact` to `Account`), but also the opposite direction (from `Account` to `Contact`). This allows all objects with personal data to be brought together under a single object from which that data can be managed.

Trivacy can mask or delete personal data across linked records based on the policies configured for the organization. Whereas removing personal data may involve deleting records and clearing field values, Trivacy also offers less intrusive options, such as partial removal or reversible obfuscation. All Salesforce field types are supported, including text, rich text, binary, email, url, geolocation and dates. Tracked changes, such as field history or Chatter items for these fields are also cleared.

Trivacy comes pre-configured with a full personal data inventory for the standard Salesforce data model, covering more than 150 fields over 25 objects. Additional settings can be added for standard and custom fields and objects.

Trivacy can also anonymize, mask or delete personal data in sandboxes in bulk, so your in-house or external developers can work in full or partial Salesforce sandboxes, without exposing personal data.

With these features, your organization can easily comply with the various requirements of data protection regulation, including the rights of access, portability, rectification, and erasure, and reduces the exposure to leaking personal data inadvertently.

Installation

Overview

Start by installing Trivacy from the [AppExchange](#). It is recommended to install for Administrators only, and then later assign the relevant Trivacy permissions to other users as per the instructions below.

After the installation completes, a few more steps need to be performed to set up Trivacy in your organization. Trivacy does not perform these steps automatically, because we want you to be in control of your organization's security settings and user experience. Trivacy does come with detailed installation wizard that takes you through the steps that need to be performed, and also checks whether you have set up things correctly. While these are the steps for the default Trivacy configuration, you can also take a different approach that fits better with your organization standard practices, e.g., use a separate profile instead of adding a permission set, or set up the batch job at a different schedule. Either way, the `Trivacy Settings` page will provide feedback on whether the relevant configuration requirements for the correct operation of Trivacy have been met.

To check the post-installation steps, open the `Trivacy App`, then navigate to the `Trivacy Settings` tab.

Your Permissions

Trivacy requires a number of permissions to ensure it can access all personal data. As a managed package, Trivacy will not change your security settings automatically, but instead leaves you in full control of the security settings in your organization.

To ensure Trivacy can access all personal data, it requires the following System Permissions:

- 'Modify All Data'
- 'Enable "Delete From Field History"'
- 'Enable "Delete From Field History Archive"'.

You must first enable these permissions in your organization:

- **Go to:** Setup -> User Interface -> User Interface.
- **Check** Enable "Delete from Field History" and "Delete from Field History Archive" User Permissions.
- **Click** Save.

Enable the required permissions in a permission set, and assign the permission set to the user under which the Trivacy scheduled job should run:

- Go to: Setup -> Users -> Permission Sets.
- Clone the permission set `Trivacy - Administrator Template`.
- On the new permission set page, enter Label: `Trivacy - Administrator` and API Name: `Trivacy_Administrator`.
- Click `Save`.
- Open the permission set `Trivacy - Administrator` you just created.
- Go to `System Permissions` and click `Edit`.
- Check the items:
 - `Modify All Data`
 - `Enable "Delete From Field History"`
 - `Enable "Delete From Field History Archive"`
- Click `Save`.
- While still on `Trivacy - Administrator` permission set, click `Manage Assignments`.
- Click `Add Assignments`.
- Select the user under which the Trivacy scheduled job should run.
- Click `Assign`.

Check that the logged in user has the right permissions:

- Log in as the user under which the Trivacy scheduled job should run, and navigate to the `Trivacy Settings` tab in the `Trivacy App`. If you are already logged in as that user, click the `Reload` button on the `Trivacy Settings` page, to ensure it displays the latest information.
- The message box on the page should turn green.
- If the box is not green, review the error message that is shown, and check the steps above to ensure nothing has been missed.
- Contact the Trivacy team if you need further assistance.

Scheduled Job

Users can schedule personal data to be masked or deleted, even if they don't have the System Permissions to process all personal data. Scheduled items will instead be handled by the processing job, which runs as a (different) user that has the required permission to access all the relevant data. These permissions are not available by default, and Trivacy can therefore not set up this job automatically on installation. The processing job is a Salesforce scheduled job that runs at 4:00AM daily (local time of the scheduling user), and you can schedule it with the `Schedule Job` button on the `Trivacy Settings` page.

Follow these steps to set up the processing job:

- Ensure you are logged in as the user under which the Trivacy scheduled job should run.

- The `Schedule Job` button on the `Trivacy Settings` page will become available once the permissions are correctly set up. If this button is not available, review the instructions in the 'Your Permissions' section above.
- Click the `Schedule Job` button to schedule the processing job.
- The message box on the `Trivacy Settings` page should turn green.
- If the box is not green, review the error message that is shown, and check the steps above to ensure nothing has been missed.
- Contact the Trivacy team if you need further assistance.

Add Trivacy to the User Interface

Once the scheduled job and permissions are correctly set up, start rolling out Trivacy for your users.

The simplest way to make Trivacy available to your users is by adding the `Trivacy` button to the main objects from which your organization manages personal data. Typically, these are: `Contact`, `Account`, `Lead`, `User` and `Case`. Again, you are in control on how to best fit Trivacy within your organization, and so Trivacy will not overwrite your pages on installation.

Add the `Trivacy` button to the main objects from which personal data is managed. Typically, these are: `Contact`, `Account`, `Lead`, `User` and `Case`.

Follow these steps for each object and page layout on which you want to add the Trivacy button, replacing `[Object Name]` with the Object on which you want to add the Trivacy Button, e.g., `Contact`:

- Go to: `Setup -> Object Manager -> [Object Name] -> Page Layouts`.
- Select the Page Layout where you want to add the `Trivacy` button.
- Select `Buttons` under the `Save` button.
- Drag the `Trivacy` button onto the `Custom Buttons` section below.
- Click `Save`.
- The Trivacy button should now be available on your Page Layout. Depending on how many buttons are on the page, the Trivacy button may be in the dropdown list next to the standard buttons.

Repeat these steps for each Object and Page Layout for which you want to add the Trivacy Button.

Assign User Licenses and Permission Set

By default, Trivacy is installed only for Administrators. To allow additional users to work with Trivacy, you need to grant them a Trivacy License and the right permissions.

To assign a Trivacy License to your users:

- Go to: `Setup -> Apps -> Installed Packages`.
- Click `Manage Licenses` next to the `Trivacy` app.
- Click `Add Users`.

- Select the users that need Trivacy access and click `Add`.
- Contact the Trivacy team if you need more licenses.

Trivacy comes with a default permission set for non-Administrator users, called `Trivacy - User`, which grants access to Export and to schedule Masking of personal data. To grant this permission set to users:

- Go to: `Setup -> Users -> Permission Sets`.
- Select the Permission Set `Trivacy - User`.
- Click `Manage Assignments`.
- Click `Add Assignments`.
- Select the Users that need Trivacy access and click `Assign`.

Usage

Trivacy Personal Data Manager

Users can manage an individual's personal data from a single page, called `Trivacy - Personal Data View`. To access this page, navigate to a record where you have added the `Trivacy` button (as per the previous section), and click the `Trivacy` button. This loads and displays the `Trivacy - Personal Data View`, with personal data on that record, as well additional records linked to this record (as per the Trivacy linkages configuration).

Linked records are grouped by object type, e.g., for a Lead record, the list of Chatter items is grouped separately from the list of Emails. To navigate through the list of records more easily, a group of records or an individual record can be collapsed (or expanded). When collapsing a group or individual records all the records controlled by those records are also hidden. E.g., when collapsing an Email record, its Attachments are also hidden.

`Trivacy - Personal Data View` shows each record in its own section, with a title, an (optional) edit link, and a number of fields that contain personal data. To view a record separately, click on the record's title. To edit a record directly from `Trivacy - Personal Data View`, click the  link next to the record's name (only available for objects that support the edit action).

To export the personal data that is displayed in `Trivacy - Personal Data View`, click the `Export to PDF` button. This shows the page as a pdf, which allows for saving the results and potentially send them to the individual that the personal data is about (e.g., in case of a subject access request).

While viewing `Trivacy - Personal Data View`, changes made to records either directly from the page, or outside of `Trivacy - Personal Data View` will not be immediately updated. To show the latest data, click the 'Reload' button.

Depending on the user access settings, the `Mask`, `Unmask` and `Delete All` buttons may be available. These buttons schedule an action that is handled at a later time by a Salesforce scheduled job that runs with the full permissions to process all personal data. If the user already has all the permissions to

process personal data, they can tick the `Process Immediate` checkbox. `Mask`, `Unmask` and `Delete All` actions will be executed immediately when the `Process Immediate` checkbox is ticked, rather than scheduled to be picked up later by the scheduled job.

Clicking the `Mask` button will mask the record and all linked records as per the configured policies. For masked records, or records where the masking status is unknown, the `Unmask` button is available (if the user has permissions to unmask), which restores the original data. However, note that not all policies are reversible; see the description of the masking policies below. Clicking the `Delete All` button will delete the record and all linked records. Note that deleting records in Salesforce is not always straightforward due to dependencies between different objects. Trivacy will work out the correct order of deletion without triggering dependency errors (where possible), so that no records are inadvertently left in the system.

After scheduling an action, a message will be shown indicating whether the scheduling was successful, and when the record is expected to be processed. To change the scheduled action, simply click another available action button. When an action is scheduled, the `Unschedule` button becomes available, which can be used to unschedule the scheduled action.

Scheduled actions and their results are stored in `Data Action` records. When something goes wrong during processing a record, the error message will be written on a `Data Action` record, which can then be reviewed by a System Administrator or another User that has access to this Object.

Trivacy can track whether a record is masked using a custom checkbox field. It will still work fine without such a field, but will not be able to establish whether a record is already masked or not, and hence, it will be possible to apply the `Mask` operation on already masked records and vice versa. To allow Trivacy to track whether a record is masked, add a checkbox field with API name `Masked` (note that the API name of this field can be configured in settings).

Full Sandbox Masking

Full Sandbox Masking can only be used in Sandboxes and Developer Edition organizations (and when running tests). When trying to run this in any other type of organization, such as a Production organization, an exception will be thrown.

To mask personal data in sandboxes, go to the `Trivacy Settings` tab, then click `Sandbox`. If you are indeed in a Sandbox or Developer Edition organization, and you have the correct permissions for processing all personal data, you can press the `Start` button to initiate full sandbox masking. This will schedule a batch job to process the action according to the configured policy for the first object in the configured list of objects. After processing all records for the first object, the next object in the configured list of objects will be scheduled, and so on, until all configured objects have been processed. Note that full processing may take several hours, depending on the amount of data in the sandbox.

To view the progress of the batch jobs, check the debug logs (it is recommended to set a low debug level to prevent exceeding the allowed Salesforce log size, e.g., 'Debug'), or the `Apex Jobs` list in the `Salesforce Settings`.

In some cases, the Trivacy may be unable to update a record, e.g., if a custom validation rule prevents an update, or if a configuration leads to invalid field values. Exceptions are written to Data Action records, the system debug logs, and can also be sent in an email to users with the System Administrator profile and/or users that are subscribed to Apex exception emails. Note that Email Deliverability is standard disabled in sandboxes, and will need to be set to 'System Email Only' or 'All Email' to work.

To restart the Trivacy batch job for a subset of objects, provide a list of object names other than the standard list obtained from the settings. You can only provide object names for which an object setting is present in the custom metadata configuration. Note that objects are processed in the order of the list. For example:

```
Boolean skipAlreadyMasked = true; // whether to skip records that are already masked
List<String> objects = new List<String>{'Account', 'Contact'}; // list of objects to process
pdm.Batch.maskAll(objects, skipAlreadyMasked);
```

processes only Account and then Contact records.

Actions and Policies

Policies determine how records and fields are processed, and are configured in custom metadata.

Policies can be set for an object (object policies) and for each field on that object (field policies). Actions determine which policy to execute, and are provided at runtime; by clicking a button on the `Trivacy - Personal Data View` in interactive mode, or by specifying an action in code in batch mode. Actions may execute or override the policy configured in metadata. For example, when executing the `Mask` action on an Account with an `Update` policy, the Account will be updated according to its field policies. However, when executing the `Delete All` action on an Account with a policy set to `Update`, the Account will be deleted instead. See the documentation of the policies below on which actions can override them.

The following actions can be initiated:

- `View`: load and display records. Default action for `Trivacy - Personal Data View`; not available in batch mode.
- `Mask`: execute the configured object policy.
- `Unmask`: execute the reverse operation for the configured object policy (if available).
- `Delete All`: delete records with the following record policies: `Update`, `Version` and `Delete`.

The following object policies can be specified:

- `View`: Show records in `Trivacy - Personal Data View`, but do not mask or delete.
- `Delete`: Delete records. Ignores any field policy settings.

- **Update:** Apply configured field policies and update existing record.
- **Version:** Delete old record, store new version of record with configured field policies applied. Note that any links to the original record are not updated.

Some policies are not supported on all objects. E.g., `Content Document Versions` and `Chatter Items` cannot be updated using DML, and would instead need to be deleted.

The following field policies can be specified:

- **Delete:** Delete the field's content.
- **Obfuscate:** Reversible masking.
- **Randomize:** Irreversible masking.
- **View:** Show field, but don't update.
- **Clear History Only:** Only delete the field's history. Use this for lookup fields that track a record name. E.g., the lookup to `Account` on the `Contact` object tracks the history of the `Account Name`. Using `Clear History Only` clears tracked changes that include that name, but leaves the lookup intact.

For all policies except `View`, the field history, field history archive and Chatter tracked change items are also cleared.

The standard configuration for Trivacy takes into account the limitations on standard Salesforce objects and fields, and specifies the least-intrusive way to mask personal data. However, not all records support reversible masking, and are deleted instead as part of masking data. `Trivacy - Personal Data View` shows a warning symbol [⚠] on records that will be deleted as part of the `Mask` action.

Security

Trivacy is intended to operate on existing records in the subscriber's organization, including Salesforce standard objects and custom objects. Special care has been taken in the app's design to follow the subscriber's access security model for field-, object- and record-level access, while at the same time ensuring that all personal data is handled as expected.

The `Trivacy - Personal Data View` page only shows the records and fields to which the running user has access. For avoidance of doubt, `Trivacy - Personal Data View` fully respects sharing rules, field and object-level security settings, and does therefore not expose any information that would not otherwise be visible to the user. Bear in mind that there may be other personal data to which the running user does not have access, and hence, could not be exported and shared with the individual in case of a subject access request.

When masking or removing personal data, it is important to handle all personal data for an individual. This typically involves fields and objects that are only accessible to System Administrator users. Normal users can therefore schedule personal data to be masked or deleted, but the actual processing of those

actions is handled in a separate scheduled job. See the Installation section in this document on how to set up the scheduled job.

User access to the different Trivacy actions (Mask, Unmask, Delete All and Export) can be controlled with Custom Permissions. The Trivacy - Administrator Template permission set comes standard with all these permissions, while the Trivacy - User permission set comes with Mask and Export by default. Should you want to add the Unmask or Delete All permissions for your users, simply clone the permission set Trivacy - User (e.g., following the instructions in section 'Assign User Licenses and Permission Set') enable the relevant Custom Permissions, and assign this new Permission Set to your users.

Note that there is not currently as separate Custom Permission for the View action, as this can simply be controlled using Trivacy licenses or access to the Trivacy - Personal Data View Visualforce page.

Options

The application is configured using custom metadata records. Settings can be updated in the subscriber's organization, and configurations for additional objects and fields can be added. To check that configuration is correct, navigate to the Trivacy Settings; tab, and then to Options. Any issues with your configuration will be displayed here.

Application

Overall application settings are configured as key-value pairs in the Settings custom metadata object. The following settings are available:

Name	Default Value	Description
Debug	FALSE	Set the Value to 'TRUE' to run the app in debug mode. Debug mode provides stack traces in on-screen error messages, and additional logging.
Alphanumeric Character Range	09,AZ,az,À¸	Comma-separated groups of Unicode character ranges that are processed by the masking algorithms. Each group has the start and end character of the Unicode range, e.g., '09' for all the numbers. Where applicable, add the Unicode ranges for your writing system.
Feed History Events	accountCreatedFromLead, accountMerged, accountUpdatedByLead, personAccountUpdatedByLead, contactCreatedFromLead, contactMerged, contactUpdatedByLead, leadConverted, leadMerged, opportunityCreatedFromLead	Comma-separate list of action values in [Feed Tracked Change].[Field Name], that are removed as part of clearing Feed Item Tracked Change history. The Field Name field on the Feed Tracked Change record may contain actions other than actual field names, and these records may contain personal data.
Is Masked Field Name	Masked__c	The 'Is Masked' checkbox field is used to determine which records to mask or unmask, and

		will be ticked / unticked after record masking / unmasked succeeds. If the 'Is Masked' field is not present on an object, the masking algorithms will process records of the object type regardless.
All Admin Exception Email	TRUE	Set to true to send Trivacy exception emails to all active users with the System Administrator profile.
Subscribed Apex Exception Email	TRUE	Set to true to send Trivacy exception emails to those subscribed to Apex Exception emails.

Object Settings

`SObject Setting` custom metadata records determine how to show and process an object. A default configuration for standard Salesforce objects is included with Trivacy. The default configuration can be overridden in subscriber organizations, and new records can be created for other standard or custom objects. Each object must only have one `SObject Setting` record. The following fields can be specified:

Name	Default	Description
SObject Name		Object developer name.
Parent Clause		Semi-SOQL WHERE clause, with lookup to parent records enclosed in curly braces. Semi-join subselects are supported as {{field IN table.reference}}, which are translated into WHERE field IN (SELECT reference FROM table WHERE ...)
View Clause		Additional SOQL conditions that are applied to determine which records to show.
Update Clause		Additional SOQL conditions that are applied determine which records to process.
Requires Parent Clause	Unchecked	Tick if this record cannot be queried standalone, and always needs to be related to a set of parent records.
Policy	View	Processing policy. See object policies above.
Override Dependencies		Objects are processed before their parents in the Parents Clause field. Enter a comma-separated list of object names to consider as parents for processing order instead. Enter 'First' or 'Last' to process this object first or last, respectively.
Batch Size		Maximum number of records to show or process in a transaction. Used for batch processing, as well as loading and updating records elsewhere. Leave empty to use default batch size (200).
Comments		Comments.
Active	Checked	Inactive settings are ignored.
Display Option	Section	Determines how to display records for this object: Options are: Section: Show each record with its configured fields distributed over columns. Table: Show records as table rows with configured fields as table.

		columns; children are not shown. Skip: Don't display; record's children are still shown.
Columns		Number of columns used to show records. Leave empty to use default (2).
Title Field	Name	Developer name of the field that is displayed as the title when showing this record.
Title Action	View	Select the standard object action that is to be called when clicking the record title. If the selected action is not valid for the object, an error occurs when loading the page. Leave empty to not display a hyperlink on the record title.
Edit Action		Select the standard object action that is to be called when clicking the edit icon next to the record title. If the selected action is not valid for the object, an error occurs when loading the page. Leave empty to not display the edit icon.

Field Settings

`SObject Field Setting` custom metadata records determine how to show and process object fields. A default configuration for standard Salesforce fields is included with Trivacy. The default configuration can be overridden by subscribers, and new records can be created for other standard or custom fields. Each object field must only have one `SObject Field Setting` record. The following fields can be specified:

Name	Default	Description
Label		Naming convention is [SObject Settings Name].[Field Name], e.g.; 'Account.Name'.
Field Name		Field developer name.
SObject		Lookup to SObject Setting record.
Policy	View	Policy applied in case the object's policy is 'Update'. See Field Policies above.
Keep		Number of characters to keep when processing. The field type determines whether to keep characters from the left (e.g., Text, TextArea, Number) or the right (e.g., Email, URL). This can be used to identify processed records in sandboxes.
Do Not Display	Unchecked	Include field content when processing, but do not display this field when viewing the record graph.
Active	Checked	Inactive settings are ignored.

Limitations

Governor Limits

Trivacy is intended to be used for dealing with personal data in designated fields, including free text fields and even binary data. However, some operations can exceed Salesforce's governor limits for CPU and/or Visualforce View State when applied to large amounts of data in big free text fields or binary data. Around 100,000 characters per transaction can be processed before breaching the Salesforce

governor CPU or Visualforce View State limits. When encountering these limits, evaluate whether a less CPU and/or storage intensive solution (such as clearing the fields or records) would be more appropriate.

The app has been designed to work efficiently within Salesforce governor limits, such as chunking of database updates, and limiting the number of queries, but in extreme scenarios other Salesforce Governor limits may be reached. Exceptions will typically be displayed on the `Trivacy - Personal Data View` page and recorded on Data Action records, so the user can adjust the configuration, or take the relevant manual actions.

Error Handling

In some cases, exceptions may occur, e.g., when subscribers have added invalid configurations, or when other code or settings in the organization prevent record updates. For example, a validation rule may prevent storing a record when Trivacy clears a field. Exceptions are written to `Data Action` records, the system debug logs, and can also be sent in an email to users with the System Administrator profile and/or users that are subscribed to Apex exception emails. To provide maximum clarity to the user, other Apex exceptions are caught and displayed on the `Trivacy - Personal Data View` page.