

Data Privacy README

The Data Privacy application helps you manage requests to remove personal data from your systems. This app replaces email-based approaches often used by companies. It not only streamlines the process of handling requests, but it provides monitoring and traceability to ensure requests are handled in a timely manner and can be audited later.

The Appian Data Privacy app leverages Portals to accept data privacy requests via a website. Users are required to confirm ownership of their email to prevent email spoofing. The Portal lets them know what to expect and also sends them a follow-up email so they know their request was received. All the language in the Portal can be adjusted via the Admin interface without needing to make design object changes or republish the Portal.

The system allows Administrators to enter their various systems that will need to be reviewed as part of a data privacy request and specify which users are responsible for handling requests within those systems. When new requests come in, tasks are assigned to each system owner to review their system and complete their part of the data privacy request.

Data Privacy specialists can use the Data Privacy site to monitor all the requests and their status to ensure compliance.

Setup

1. Create a user to serve as your service account named **gdpr.serviceaccount** and make sure it is a member of the [Service Accounts system group](#). For more information, see [Service Accounts in Portals - Appian 23.3](#).
2. Go to your Cloud Database interface, select the Appian database, and import the included SQL to generate the database tables.
3. Edit the included properties file to decide if you want to allow creating new user accounts via the Users & Groups system administration screen
4. Import the attached application

Import

Extend your applications by importing solutions and utilities. [Browse the AppMarket](#)

When inspecting the package for missing precedents, no items are added or modified. The deployments view will be updated when import is completed.

Package (ZIP) ?*

 **Data Privacy**
ZIP - 360.03 KB

Include related import customization file

Import Customization File (PROPERTIES) ?

 **Data Privacy Import Customization**
PROPERTIES - 2.31 KB

5. Go to the Users and Groups Administration page of the new Data Privacy site: <https://<your host url>/suite/sites/privacy/group/admin/page/users-groups>

6. Add users to the following groups:
 - Specialists: these are users who will handle general, non-system-specific data privacy requests
 - Site Viewers: these are users who can view the Data Privacy site
 - Systems Administrators: these are users who can add and edit systems
 - You may create new users from this screen if needed as well
 - **Tip**: To start, add your user account the Systems Administrators group (at least) so you can perform the next step.
7. Click the Systems Administration page: <https://<your host url>/suite/sites/privacy/group/admin/page/systems>
 - Click the Add button and add Systems for each system in your organization that needs to be reviewed for personal information when a data privacy request is received.
 - Assign system owners to each system who will be responsible for reviewing their system and removing data when a data privacy request is received
8. (Optional) Click the Language Administration page: <https://<your host url>/suite/sites/privacy/group/admin/page/language>
 - Update any text shown on the Data Privacy Portal and used by the Data Privacy emails.

Test

1. Go to the Data Privacy Portal in your development environment
 - a. In the development environment, the portal will have an obfuscated URL. You must open the Portal design object to find the URL
2. Create a test submission using an email that you have access to
3. Verify that you receive the email
4. Click the code in the email or copy and paste it into the Portal to complete the Process
5. Verify that a task was assigned to each systems owner group to complete the request
 - a. Note: if you use "testing" in the email address you use for your request, the request will be automatically completed without sending a request to each systems owner group