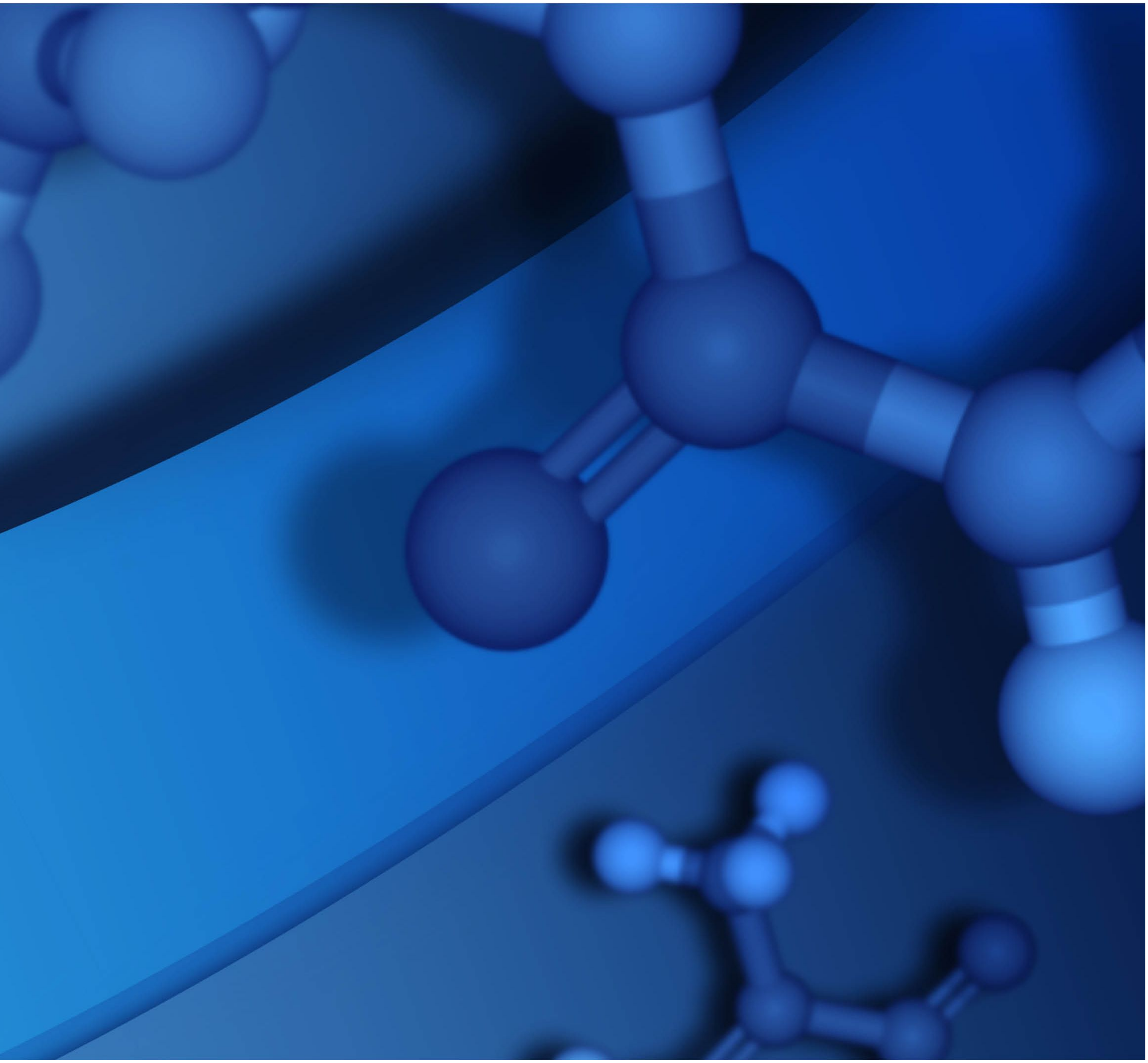
DASSAULT SYSTEMES

BIOVIA

ADMINISTRATION GUIDE

BIOVIA PERSONAL DATA PROTECTION



Copyright Notice

Acknowledgments and References

To print photographs or files of computational results (figures and/or data) obtained by using Dassault Systèmes software, acknowledge the source in an appropriate format. For example:

> "Computational results were obtained by using Dassault Systèmes BIOVIA software programs. BIOVIA Personal Data Protection Administration was used to perform the calculations and to generate the graphical results."

Dassault Systèmes may grant permission to republish or reprint its copyrighted materials. Requests should be submitted to Dassault Systèmes Customer Support, either by visiting https://www.3ds.com/support/ and clicking **Call us** or **Submit a request**, or by writing to:

Dassault Systèmes Customer Support
10, Rue Marcel Dassault
78140 Vélizy-Villacoublay
FRANCE

Contents

Introduction

BIOVIA Foundation Hub, Pipeline Pilot, and the integrated solutions they support capture information that can be considered personal data. The gathering and processing of such information is often subject to privacy legislation, such as the European Union's General Data Protection Regulation (GDPR).

Scope of this Document

The following BIOVIA deployments and applications are covered by this guide:

- On-premise deployments only.
- BIOVIA applications that are integrated with Foundation Hub and/or Pipeline Pilot. Standalone deployments are *not* covered. The following BIOVIA applications are covered:
    - CISPro
    - Compose and Capture
    - Experiment
    - Insight
    - Insight for Excel
    - Notebook
    - Registration (Biological and Chemical)
    - Workbook

Compliance Responsibility

While these products contain features to facilitate GDPR compliance, you, the Customer, are solely responsible and liable for the access to and the use of these products. Therefore, it is your responsibility to ensure that the deployment is GDPR compliant, including provision of a suitable privacy policy.

In order to be compliant with such regulations, it is necessary to:

- Create and maintain a privacy policy.
- Make that policy available to users.
- Allow users to view, correct, and request the deletion of their personal data.

Note: In BIOVIA applications, usernames are **not** considered to be nor treated as personal data. Therefore, we strongly recommend that you do not use information that could be considered to be personal data to create usernames, such as email addresses or full names.

Managing your Privacy Policy

Foundation Hub and Pipeline Pilot allow you to publish a privacy policy that users must consent to in order to log in.

- Your privacy policy should cover all of the applications in your deployment and all users.
- BIOVIA does not provide advice on how to write a privacy policy suitable for your organization. You can, however, use the information provided in this guide to write a privacy policy that explains how your organization uses personal data collected by the applications.
- When a user gives their consent, their consent is considered universal; that is, it applies to both the server and all the applications it hosts. If a user chooses not to consent to the privacy policy, they will not be able to access the server nor any of the integrated applications.
- There is no mechanism to allow users to withdraw their consent. Instead, they must ask for their account and all personal details to be deleted.

Managing the Privacy Policy in Foundation Hub

In Foundation Hub, privacy policies are managed on the Legal Notices page.

To open the Legal Notices page:

1. Log in to Foundation Hub.
2. Click ⚙ in the tool bar.

   The Admin and Settings page is displayed.
3. Select **Settings > Legal Notices**.

   The Legal Notices page is displayed.

On this page, you can publish and modify privacy policies. You can also view the current or a previous policy by clicking its file name in the Legal Notices list.

Publishing a Privacy Policy

- Before you publish a new privacy policy or a new version of an existing policy, you must create a single file containing your organization's policy. For example, this could be a complete document in a PDF or text file, an HTML file with a link pointing to an online location where your policy is published, or even an executable file.
- Write an acceptance message that will be displayed to users when they are prompted to read and consent to the policy. If you are requiring users to re-consent to an updated privacy policy, you can update the Acceptance Message to indicate what is changed and why they need to re-consent to the updated policy.

To publish the policy:

1. Open the Legal Notices page.
2. Click the **Add** ⊕ icon.
3. Complete the fields as required:
   - **Legal Notice Version:** Enter a reference by which the version of the policy can be identified.

     This is a free-text field to use according to your company policy. This value is solely for use by the administrator and is intended to help manage the privacy policies.
   - **File Name:** Browse to and select the privacy policy file.

- **Require User Acceptance:** Check this field to prevent users from signing in without consenting to the policy.
- **Acceptance Message:** Enter a message that will instruct the users to consent to the policy. Once the user reads and accepts the policy, the message is not displayed again unless you update the policy and require re-consent.

4. Click **Save**.

Updating a Privacy Policy

> **Note:** When you edit a published privacy policy, users will *not* be prompted to re-consent to it. To make a change that requires users to re-consent to the policy, you must create and publish a new policy. See Publishing a Privacy Policy on page 2 for more information.

To edit the privacy policy:

1. Open the **Legal Notices** page.
2. In the table, click the current privacy policy.

   > **Note:** Only the currently active privacy policy can be edited.

3. Click **Edit**.
   The details of the policy are displayed.
4. Edit the fields as required.
5. Click **Save**.

Checking User Consent to the Privacy Policy

You can check which users have consented to the privacy policy on the Users page:

1. Log in to Foundation Hub.
2. Click ⚙ in the tool bar.

   The Admin and Settings page is displayed.
3. Select **Security > Users**.

   The Users page is displayed.

   The **Accepted Latest Legal Notice** column indicates whether the user has consented to the most recent policy.
4. Click on a User row.

   The user details are displayed.
5. In **Account Settings > Legal Notices**, you can view the details of the legal notices that the user has accepted including date, file name, and version.

Deactivating the Privacy Policy

You cannot delete privacy policies in Foundation Hub. However, you can change the settings so user consent to the policy is no longer required in order to log in.

1. Open the **Legal Notices** page.
2. Click the row of the current privacy policy.
3. Click **Edit**.

   The privacy policy details are displayed.

4. Deselect **Require User Acceptance**.
5. Click **Save**.

Managing the Privacy Policy in Pipeline Pilot

You will manage your privacy policy in the Pipeline Pilot Admin Portal if the *Authentication Method* you are using for Pipeline Pilot is set to *Any User Name* or *Domain*. If the Authentication Method is set to *Foundation*, you will manage your privacy policy in Foundation Hub as described in this document. See Managing the Privacy Policy in Foundation Hub on page 2.

To open the Privacy Policy page:

1. Log into *Pipeline Pilot Server Home Page*.
2. Click **Administration Portal** and sign in.
3. Open **Setup > Privacy Policy**.

Publishing a Privacy Policy

Before you publish a new privacy policy or a new version of an existing policy, you must create a single file containing your organization's policy. For example, this could be a complete document in a PDF or text file, an HTML file with a link pointing to an online location where your policy is published, or even an executable file.

1. From the **Pipeline Pilot Admin Portal**, open **Setup > Privacy Policy**.

   > **Tip:** The Privacy Policy page is only available when *Authentication Method* is set to an option other than Foundation or 3DPassport.

2. Upload your **Data Privacy Policy file**:
   a. Click **Upload**.
   b. Click **Choose File** and navigate to your privacy policy file.
   c. Set the **Version**. This is a free-text field to use according to your company policy. This value is solely for use by the administrator and is intended to help manage the privacy policies.
   d. Choose **Require re-consent** if you are updating your privacy policy and want your users to consent to the new version before signing in.
   e. Click **Upload File**.
3. Set the **Acceptance Message**:
   a. Enter a message that will instruct the users to consent to the Privacy Policy. Once the user reads and accepts the policy, the message is not displayed again unless you update the policy and require a re-consent.
   b. Click **Save**.
4. Activate the policy by selecting the **The Data Privacy Policy feature is DEACTIVATED** check box.

   The field text changes to indicate the policy is active .

   Clear the check box to deactivate the privacy policy consent requirement.

Viewing an Uploaded Privacy Policy

1. From the **Pipeline Pilot Admin Portal**, open **Setup > Privacy Policy**.
2. In the **Data Privacy Policy File** section, click **View**.

Updating a Privacy Policy

1. From the **Pipeline Pilot Admin Portal**, open **Setup > Privacy Policy**.
2. If the existing policy is active, deactivate it by clearing the **The Data Privacy Policy feature is ACTIVATED** check box.

   The field text changes to indicate the policy is deactived.
3. Upload your new **Data Privacy Policy file**:
   a. Click **Upload**.
   b. Click **Choose File** and navigate to your privacy policy file.
   c. Set the **Version**. This is a free-text field to use according to your company policy. This value is solely for use by the administrator and is intended to help manage the privacy policies.
   d. Choose **Require re-consent** if you want your users to consent to the new version before signing in.
   e. Click **Upload File**.
4. Update the **Acceptance Message** as required. Click **Save**. If you are requiring users to re-consent to an updated privacy policy, you can update the Acceptance Message to indicate what is changed and why they need to re-consent to the updated policy.
5. Activate the policy by selecting the **The Data Privacy Policy feature is DEACTIVATED** check box.

   The field text changes to indicate the policy is active.

Checking User Consent to a Privacy Policy

Note: The policy must be active to see the user report.

1. From the **Pipeline Pilot Admin Portal**, open **Setup > Privacy Policy**.
2. Below the **Data Privacy Policy File** section, click **Show User Report**.

   A grid opens with a list of users.
3. Click the column headers to sort and click the right side of the header for filter options. The following columns are displayed:
   - **Consent is Current:** Icon that indicates whether the user has consented to the active privacy policy.
   - **User Name:** Username of the user who consented.
   - **Date of Consent:** Date that the user consented.
   - **Policy Document Name:** Name of the privacy policy the user consented to.
   - **Policy Version:** Version of the privacy policy the user consented to.

Deactivating a Privacy Policy

You can deactivate your privacy policy by setting the feature to deactivated, or you can delete the privacy policy file altogether.

Deactivating a Privacy Policy without Deleting It

1. From the **Pipeline Pilot Admin Portal**, open **Setup > Privacy Policy**.
2. Clear the check box next to the **The Data Privacy Policy feature is ACTIVATED** warning to deactivate your policy.

The warning text changes to **The Data Privacy Policy feature is DEACTIVATED**.

Select the check box to re-activate the privacy policy consent requirement.

Deleting the Privacy Policy

1. From the **Pipeline Pilot Admin Portal**, open **Setup > Privacy Policy**.
2. In the **Data Privacy Policy File** section, click **Delete**.

Protecting Personal Data

BIOVIA integrated solutions capture personal data items such as first and last name, email address and location information. These personal data items can be stored in Foundation Hub and the integrated applications. This has implications for how the data is managed, modified, and deleted. See Personal Data Items for information on where personal data items are stored and how they propagate to integrated applications.

> **Note:** Some integrated applications offer the ability to create custom fields that can capture personal data. If you configure your application to do this, you are responsible for maintaining that data in accordance with any relevant regulations.

Managing User Data in Foundation Hub

You can manage user data from the Foundation Hub Admin and Settings page. The following personal data items are captured in Foundation Hub:

- First Name and Last Name
- Email address
- Location

See Personal Data Items for information on where personal data items are stored and how they propagate to integrated applications.

Managing Users in Foundation Hub

> **Note:** If you are synchronizing users with external user directories, consult the Foundation Hub documentation for managing users.

1. Log in to Foundation Hub.
2. Click the **Settings** icon ⚙.
3. Open **Security > Users**.
4. For details about managing users, see the *Foundation Hub Administration Guide*:
   a. Click the **Help** icon ?.
   b. Choose **Admin Guide**.

> **IMPORTANT!** In order to create a user account in Foundation Hub, administrators must obtain the name, email address, and location of the user. As this information is considered to be personal data, strictly speaking when you are creating a user, you are handling their personal information prior to gaining their consent to a privacy policy. Therefore, you must consider how this information is handled prior to adding it to Foundation Hub and adhere to your processes for doing so in accordance with your company's policies.

Deleting a User in Foundation Hub

When you delete users in Foundation Hub, the users cannot log in and you cannot add them to groups. However, their account information is retained in the database.

Pseudonymizing a User in Foundation Hub

To protect the user's privacy, Foundation Hub allows you to convert a deleted user's First and Last Name to a pseudonym. This option will convert the First and Last Name fields to *Anonymous_User_*

<*number*>. Note that this operation is *irreversible*.

1. From the Foundation Hub Admin and Settings page, open **Security > Users**.
2. Above the grid of users, click the **Show Deleted** button.
3. Click the row of the user you want to pseudonymize.
4. Click **Pseudonymize User** near the top of the window.

   The Confirm dialog opens.
5. Click **Yes**.

   The Last Name and Full Name fields will contain a pseudonym.

Managing Personal Data in Integrated Applications

The integrated BIOVIA applications that can be accessed through Foundation Hub or Pipeline Pilot all contain personal data items.

The Personal Data Items table lists all the items available and explains whether they are shared from Foundation Hub or maintained in the applications themselves.

To modify or delete the personal data of a user of an integrated application:

1. Consult the Personal Data Items table and the application topic for information on how personal data items are handled.
2. If required, log in to Foundation Hub and modify the data as required.
3. If required, log in to the application as an Administrator user and make further changes.

CISPro

Accessing and Consenting to the Privacy Policy

Users of CISPro deployments that use Foundation Hub must accept the privacy policy that is managed in Foundation Hub in order to access CISPro.

After consenting, users can view the privacy policy from Foundation Hub.

Note: There is no privacy policy functionality available for CISPro deployments that do not use Foundation Hub.

Personal Data - Storage and Usage

When CISPro is connected with Foundation Hub, users and administrators can view their personal data from their user profile in CISPro. The ability to modify the data is split between CISPro and Foundation Hub. For details of which data items are managed by these applications, refer to the *Managing Data in Foundation Hub* topic in the *BIOVIA CISPro Administration Guide*.

CISPro uses personal data to create names in electronic signatures (which is required for FDA Title 21 CFR Part 11 compliance), emails for report subscriptions, and as needed by Foundation Hub. The data is stored either in an Oracle database, which is protected based on the architecture of the given environment, or in Foundation Hub.

Users can view, modify, or anonymize (by deleting or entering dummy information) any of their own personal data. Administrators can view and modify other users' data. They also can access the CISPro Roles and Users information and delete or deactivate user accounts. If CISPro is not connected to Foundation Hub, all personal data is deleted as soon as their account is deleted. If CISPro is connected to Foundation Hub, user account deletion follows the Foundation Hub rules on how personal data items are handled.

Note: The IP address of a connecting user is captured in CISPro's Login Data table.

Personal Data Protection

In CISPro, non-administrator users do not have access to the personal data of other users. Additionally, CISPro's password functionality includes rules for complexity, allowed history of previous passwords, and a password expiration date.

FDA Title 21 CFR Part 11 Compliance

CISPro employs electronic signatures. These signatures are generated from the username, first name, and last name of the user in question. Although usernames are not considered to be personal data in BIOVIA products, the first and last name fields are. Therefore, even if a user account is deleted, the first and last name of that user will persist in any electronic signatures that have been used in order to achieve compliance with FDA Title 21 CFR Part 11 and potentially other regulations.

Compose and Capture

Accessing and Consenting to the Privacy Policy

Compose and Capture users must log into Foundation Hub to view and consent to the privacy policy. After users have consented, they can view the policy by logging into Foundation Hub; it is not possible to view the policy in Compose and Capture.

Personal Data - Storage and Usage

The First and Last name personal data items are used to identify the user who has created or modified a recipe. The data itself is stored in Compose's database.

Compose shares information with Capture and the Review module. Capture and Review use information from the Compose and Capture database and application servers. The Compose database server replicates user information from the Foundation Hub server. Foundation Hub administrators control personal data used in Compose and Capture.

- When a Foundation Hub administrator pseudonymizes a user's first and last name information, the pseudonymization is replicated in the Compose database. See Managing User Data in Foundation Hub on page 7 for information about pseudonymizing a user.
- When a Foundation Hub administrator modifies or deletes a user's first and last name information, the Compose and Capture administrator must update the Compose database schema accordingly.

Personal Data Protection

Any user can view this personal data in the user interface by examining the "Created by" and "Updated by" fields for a recipe. Only Foundation Hub administrators can modify personal data items.

API Access

API client applications can access Compose data only after the user account under which the API client runs has logged on to Foundation Hub or Pipeline Pilot and consented to the privacy policy. Log in attempts fail until consent has been provided.

FDA Title 21 CFR Part 11 Compliance

Compose employs electronic signatures. These signatures are generated from the username, first name, and last name of the user in question. Although usernames are not considered to be personal data in BIOVIA products, the first and last name fields are. Therefore, even if a user account is deleted, the first and last name of that user will persist in any electronic signatures that have been used in order to achieve compliance with FDA Title 21 CFR Part 11 and potentially other regulations.

Experiment

Accessing and Consenting to the Privacy Policy

Users of Experiment are prompted to consent to the privacy policy when they log in to the application.

When a user is logged in, he or she can view the privacy policy at any time by clicking the username in the title bar and then selecting **Privacy Policy** from the menu.

Personal Data - Storage and Usage

User records in Experiment include several fields that can identify users either directly or partially. A user can view these fields by clicking his or her name in the title bar and selecting **Profile** from the menu. This opens the User Profile page, which shows the following user information:

Username, Full name*, Email*, Phone*, Alternative contact*, Location, Business Unit, Manager, Reports, Time zone*

Asterisks indicate details that users can edit themselves in the User Profile page. If a user wants other details to be modified, he or she must contact the Experiment administrator. Instructions for administrators on editing user details are in the *BIOVIA Experiment Administration Guide*.

> **Note:** The **Username** field is not considered to be personal data in BIOVIA applications. It is included in the above list for completeness only.

User records in Experiment are not synchronized at any stage with user records in the application being used for authentication (Foundation Hub or Pipeline Pilot). Therefore, if a change is made to an Experiment user record to comply with personal data protection legislation, a corresponding change might need to be made in Foundation Hub by an administrator of that application. For example, if a user changes his or her email address in Experiment, the Foundation Hub administrator must also change the email address. The administrator of Experiment should be aware of such requirements and communicate any requested change to the Foundation Hub administrator.

Storage of personal data: User data is stored in the Experiment SQL Server database and protected by the usual SQL Server security mechanisms.

Usage of personal data: Experiment uses personal data for the following purposes:

- To allow administrators to communicate with users of Experiment (for example by email or phone).
- To allow collaborators on projects to assign work to each other. (They must know each others' business unit to do this. The business unit could be used in addition to other details to identify users.)

Anonymization and removal of personal data:

- Users can anonymize the value of any field that is editable in the User Profile page.
- Users can remove personal data from any field that is editable in the User Profile page by entering a blank value.
- If a user wants his or her Manager or Reports to be anonymized or removed, he or she must request this from an Experiment administrator. The administrator can perform these actions in the Experiment Administration pages.
- The Business Unit and Location fields are mandatory for every user and cannot contain blank values. Therefore, removal of business unit and location information is not possible. However, anonymization is possible, as explained in the next point.
- If a user wants his or her Business Unit or Location to be anonymized, he or she must request this

from the Experiment administrator. The administrator can create a neutrally-named Business Unit or Location (for example, `Unspecified Business Unit`, `Unspecified Location`), and assign the user to it.

- The Experiment administrator can delete user records. For instructions, see the *BIOVIA Experiment Administration Guide* > Users > "Deleting a User."

  This deletion is "soft". The user record is no longer viewable from anywhere in the Experiment user interface (including the Administration pages), but the record is retained in the SQL database.

  Before a user can be deleted, the administrator must remove all references to the user from other tables in the Experiment SQL Server database. The administrator can do this either in the Administration pages or by modifying the SQL Server database tables directly. (The latter should be done with extreme caution to avoid introducing data errors.)

Personal Data Protection

Location and business unit information are mandatory for every Experiment user. The location and the business unit are classified by BIOVIA as personally identifying. Other personally identifying details can be present in a user record, but are not mandatory and can be removed or anonymized without affecting the user's access to Experiment.

Personal data accessible to non-administrators:

- A user can view the full names (if recorded) of all users who are owners, members, or guest users of the same projects. The full names are visible in the **Project Summary** panel of a project. They are also visible in various menus and lists throughout the project, job, and experiment pages, and in associated workflow windows.

  If a user record does not include a full name, the username is displayed instead in the above-mentioned places. The username is not classified as personally identifying.
- Non-administrator users can infer the business unit of users with whom they share projects because all members of a project have the same business unit.
- Experiment has a Project Creator user role that gives limited administrator privileges to non-administrators. A Project Creator can create and edit users, create and edit projects, and assign users to projects. A Project Creator thus has the same access to personal data as a full Administrator.

API Access

API client applications can access Experiment data only after the user account under which the API client runs has logged on to Foundation Hub or Pipeline Pilot and consented to the privacy policy. Log in attempts fail until consent has been provided.

REST Interface Access

Experiment has a REST interface that is used by the application's Pipeline Pilot protocols, including the ETL protocol that is necessary for searching. Protocols access the REST interface as the service account user that is created in the Experiment configuration pages. Automatic logins of the service account user will fail until the user has accepted the current privacy policy. This acceptance is performed by an Experiment administrator, who logs in to Experiment manually as the service account user, and accepts the uploaded or updated policy.

Insight

Accessing and Consenting to the Privacy Policy

Insight users must log into Foundation Hub to view and consent to the privacy policy. After a user has consented, they can view the policy by logging into Foundation Hub; it is not possible to view the policy in Insight itself.

Personal Data - Storage and Usage

Insight only uses the first and last name and email address of its users, and these are derived from Foundation Hub. Therefore, since all personal data storage and management is performed through Foundation Hub, Insight does not need nor provide storage protections for this data.

Insight uses this personal data to display user information for file ownership and history. As this data is synchronized from Foundation Hub, any changes to it must be made there. So if an Insight user's personal data is anonymized or if their account is deleted in Foundation Hub, this change will propagate to Insight.

Personal Data Protection

Any Insight users can see the first and last names of the users who have modified a data object. Only Foundation Hub administrators can see or modify any other personal data.

API Access

API client applications can access Insight data only after the user account under which the API client runs has logged on to Foundation Hub or Pipeline Pilot and consented to the privacy policy. Logon attempts fail until consent has been provided.

Insight for Excel

Accessing and Consenting to the Privacy Policy

Insight for Excel users must log on to Foundation Hub or Pipeline Pilot to view and to consent to the privacy policy. When users of Insight for Excel for Isentris try to connect to Isentris, they are prompted to log in to the Isentris console to consent to the privacy policy.

Note: There is no privacy policy feature for Insight for Excel when configured in standalone mode.

Personal Data - Storage and Usage

Insight for Excel does not inherit or store any personal data items out of the box.

Personal Data Protection

As no personal data is inherited or stored by Insight for Excel out of the box, there are no special protections in place for such data.

Notebook

> **Note:** This section describes the use of Notebook as part of a Unified Lab Management (ULM) deployment. If you use Notebook as a standalone application, refer to the *BIOVIA Notebook Installation Guide* for information on configuring privacy policies and the *Notebook Help* for information on viewing and consenting to the privacy policy. The same measures to protect personal data should be taken whether Notebook is employed standalone or as part of ULM.

Accessing and Consenting to the Privacy Policy

Notebook users must log into Foundation Hub to view and to consent to the privacy policy. If a user who has not yet consented to the policy attempts to log in, Notebook denies access and displays a dialog instructing them to visit Foundation Hub in a web browser in order to give their consent.

Notebook users must also log into Foundation Hub to view the policy once they have given consent. There is no mechanism to allow them to view the policy directly from Notebook.

Personal Data - Storage and Usage

User email addresses and name information are stored in the database, while the IP address of the device they access Notebook with is stored in the log files. The data is used to identify users, assign roles and actions, track contributions, and create electronic signatures.

Notebook stores the UTC offset which can be used to determine the time zone of a user. Although UTC offset is not considered to be personal data in BIOVIA products, time zone is.

Notebook administrators can amend the first and last names of users in the Notebook Administration tool (ElnAdminWeb).

Notebook administrators can also generate security audit logs reporting changes to users.

User accounts can only be deleted by first removing all their experiments and then employing the Notebook API to delete the user account. To completely delete all user information not related to signatures (see FDA Title 21 CFR Part 11 Compliance on page 15) , the logs must also be deleted from the Notebook server.

Personal Data Protection

The full name and email address of every Notebook user who authors, collaborates on, or reviews a Notebook experiment is recorded in the system. This information is displayed in various locations, including:

- The Author column in libraries
- Experiment collaborator details
- Last changed footer in experiment views
- Submission or signing conditions
- Email notifications
- Experiment audit trail
- System logs

Notebook can also be configured to store user information directly in experiments, typically in the document background form.

Notebook provides granular permissions for each object and users can only see a Notebook experiment (and the personal information associated with it) if they have the appropriate permissions.

API access

API access to Notebook data does not require privacy policy consent.

The Notebook API is built to serve custom automated integration solution. Such integration solutions will normally access Notebook API using a special account not belonging to a physical person, as such privacy policy consent is not appropriate. It is not recommended to employ the Notebook API to make the same changes that would normally be handled through the Notebook web client.

FDA Title 21 CFR Part 11 Compliance

Notebook employs electronic signatures. These signatures are generated from the username, first name, and last name of the user in question. Although usernames are not considered to be personal data in BIOVIA products, the first and last name fields are. Therefore, even if a user account is deleted, the first and last name of that user will persist in any electronic signatures that have been used in order to achieve compliance with FDA Title 21 CFR Part 11 and potentially other regulations.

Registration

Note: Biological Registration and Chemical Registration handle personal data items in identical ways. Therefore, while this topic refers to Biological Registration, it applies to both Registration applications.

Accessing and Consenting to the Privacy Policy

Biological Registration users must log into Foundation Hub to view and consent to the privacy policy. After users have consented, they can view the policy by logging into Foundation Hub; it is not possible to view the policy in Biological Registration itself.

Personal Data - Storage and Usage

Biological Registration does not capture any personal data items out of the box. However, its database schema is customizable by the administrator deploying the application. Additionally, any data stored in the Biological Registration database cannot be deleted or anonymized due to the auditing of all transactions. For example, if you change or delete a data value, the before and after values are recorded permanently in the transaction log.

For these reasons, BIOVIA strongly recommends that you do not define attributes to hold personal data in your data model.

Personal Data Protection

All Biological Registration users can view all fields for all the data records they have access to.

API Access

Biological Registration provides a RESTful API. API client applications can use this to access Biological Registration data only after the user account under which the API client runs has logged on to Foundation Hub or Pipeline Pilot and consented to the privacy policy. Logon attempts fail until consent has been provided.

Workbook

Accessing and Consenting to the Privacy Policy

Workbook users must log on to Foundation Hub to view and to consent to the privacy policy. If a user who has not yet consented to the policy attempts to log on, Workbook denies access and displays a message that instructs the user to visit Foundation Hub in a web browser to consent to the privacy policy.

To view the policy after giving consent, Workbook users must log on to Foundation Hub again. They cannot view the policy directly from Workbook.

Personal Data - Storage and Usage

Standard Workbook installations use only email addresses and first and last names to identify users. This data is propogated and synchronized from Foundation Hub.

Key Points

- Email addresses, first names, last names, and full names of Workbook users are stored in the Foundation Hub database and protected by Foundation Hub protection mechanisms.
- Changes to personal data stored in Foundation Hub are automatically propagated to Workbook.
- Workbook uses personal data to identify the users responsible for various activities, such as experiment creation, and approvals.
- Workbook users can change their personal data by using the User Profile Settings page in Foundation Hub.
- Workbook users who want to remove or anonymize their personal data in existing records such as log files and reports must contact a Foundation Hub administrator.

IMPORTANT! Customers can create custom Workbook fields and property sets, and can use them to collect personal data. Such data is stored in Workbook and can be displayed in items such as forms and exported spreadsheets. BIOVIA cannot provide specific guidance on how to control custom personal data fields and property sets.

Personal Data Protection

The full name and email address of every Workbook user who authors, collaborates on, or reviews a Workbook experiment is recorded in the system. This information is displayed in various locations, including the Created By column, folder names, in-vault messages and email notifications, user access history, audit history, and system logs. Workbook can also be configured to store user information directly in experiments, typically in a form.

Workbook provides granular permissions for each object, and users can see a Workbook document (and any personal data associated with it) only if they have been granted the appropriate permissions.

API Access

API client applications can access Workbook data only after the user account under which the API client runs has logged on to Foundation Hub and consented to the privacy policy. Logon attempts fail until consent has been provided.

Appendix: Personal Data Items

Table key

- **Core:** Owned by Foundation Hub and is available to integrated applications.
- **App:** Owned by and exclusive to the application.
- **Replicated:** Copied from Foundation Hub to the application when the user is created.
- **Synced:** Stored in Foundation Hub and synchronized to the application.

Data item	Foundation Hub	Pipeline Pilot	Capture	Compose	CISPro	Experiment	Insight	Insight for Excel	Notebook	Registration	Workbook
First and Last Name	Core	-	-	Replicated	Synced	App	Synced	-	Replicated	-	Synced
Email	Core	-	-	-	Synced	App	Synced	-	Replicated	-	Synced
Preferred location	Core				App	App	-	-	-	-	-
Secondary location	-	-	-	-	-	-	-	-	-	-	-
Phone number	-	-	-	-	App	App	-	-	-	-	-
Alternative contact	-	-	-	-	-	App	-	-	-	-	-
Business unit	-	-	-	-	App *	App	-	-	-	-	-
Manager	-	-	-	-	-	App	-	-	-	-	-
Reports	-	-	-	-	-	App	-	-	-	-	-
Time zone	-	-	-	App	-	App	-	-	App *	-	-

Data item	Foundation Hub	Pipeline Pilot	Capture	Compose	CISPro	Experiment	Insight	Insight for Excel	Notebook	Registration	Workbook
(custom extension)	App *	-	-	-	-	App *	-	-	-	App *	App *
IP address	App		App	App	App *	-	-	-	-	-	-

* For further information on how this personal data item is handled, see the individual topic for this application.