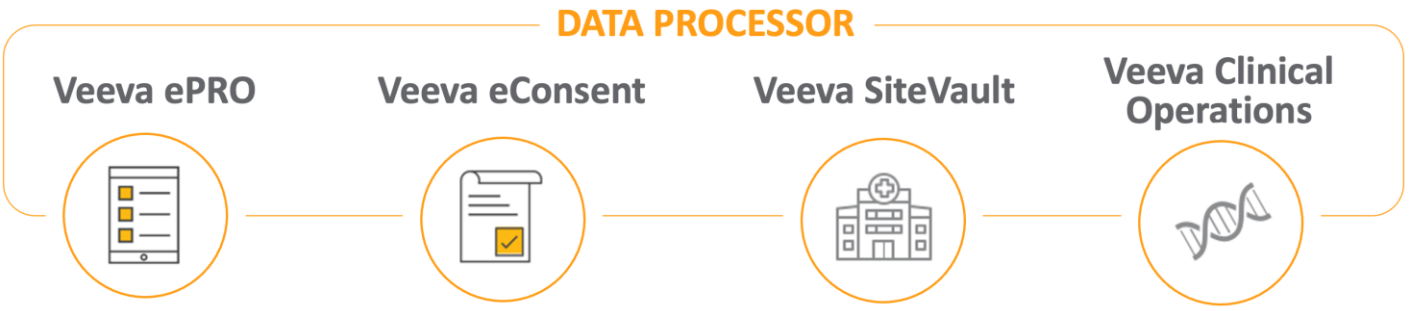
Data Protection Impact Assessment (DPIA) for Veeva Digital Trials

Compliance with the GDPR across Veeva Digital Trials applications

Veeva Digital Trials & GDPR



The Veeva Digital Trials Platform provides a set of software applications for usage by Sponsors, Sites and Patients. The data within these applications is entered and managed by Sponsors or Sites - – this means Veeva acts as a data processor for the Digital Trials Platform.

Purpose of Personal Data Processing for Digital Trials

Our Digital Trials applications process personal data for the following purposes:

User Profile: To allow user access to the applications. There are three kinds of users in the Digital Trial platform: An employee of the sponsor; a research site employee; or a clinical trial patient.

For MyVeeva for Patients:

The MyVeeva for Patients application stores the association between a patient and the studies they are participating in. It stores the participants name, email address and mobile phone number in order to facilitate login and two factor authentication. It also stores copies of signed consent documents.

When ePRO is in use, the user will provide patient reported outcomes via the MyVeeva application. Responses to in-progress forms are stored within the application.

For Sponsor and Site Vaults:

For those applications where clinical trial subject data may be configured, collected and processed, data is processed as approved by the relevant health authority, and for the purposes identified in those approvals.

For those applications supporting processes where health authorities require personal data for clinical trial investigators and other staff, data is processed within the confines of those regulatory and regulated processes.

Patient PHI and PII: Only SiteVault and MyVeeva will store PHI and PII. Any data shared between SiteVault (site) and Clinical Operations (sponsor) is de-identified to ensure sponsor has no access to patient PHI or PII

Build trust and transparency with personal data on Veeva solutions

Duration of Data Processing

Data is processed for as long as a company has a contract with Veeva and requires the data to be retained. For sponsors, the ability to delete all data in their Vault is available at any time.

For Sites, data will be maintained for at least 25 years from study creation.

Further information is available in the Veeva Privacy Policy: **veeva.com/eu/privacy**

Right to be Forgotten

If an individual submits a 'right to erasure' request to a Veeva sponsor or site to have their data deleted from a Veeva database, then that company has the following options:

- Process the data deletion themselves: Vault users can remove data at any time within the security controls configured by our customers.
- Request that Veeva deletes that data: If a Veeva customer requests Veeva's assistance in the removal of subject data, Veeva will respond to such requests within 20 business days and would remove the PHI/PII from the relevant records.

These deletions should only be processed if other global & European regulations (particularly regarding the long-term storage of clinical trial data) permit such data deletion. It is for Veeva customers to make that determination.

Data Access

Digital Trials Platform users can view and edit (with restrictions) their user information at any time once logged in.

For those applications where patient information is collected from individuals (for example, eConsent or ePRO), it is the responsibility of the research site (as data controllers) to make such individuals aware of what data will be collected and processed.

If an individual submits an access request to a Veeva customer to understand the data that is being stored on them, Veeva enables that company to provide a copy of that data, in an electronic format, within 20 business days.

Veeva only discloses individual data to other system users who are authorized by the customer.

Data Storage Locations

Veeva uses data centres in Europe, North America and Asia. For sponsor systems, the sponsor chooses the location of their Vault. Sites are provisioned in the geographic region closest to them – EU sites will be hosted in EU. Patient accounts have an affinity to the location of the site. If the site is in EU, the patients MyVeeva data is also in EU.

Breach Notification

Veeva has a data breach management policy and a security team in place to identify violations and to ensure correct and timely action. If Veeva becomes aware of a data breach, it will contact the customer(s) affected within 72 hours.

Summary

How personal data processing in the Digital Trials Platform complies with GDPR product obligations as a data processor

Fair, Lawful & Limited Purpose

- Core user profile information is required to allow users to access Vault or MyVeeva and provide compliance audit trail information.
- SiteVault users can export a full list of data subjects at any time to provide them notice of the processing.
- Users can access Veeva's Privacy Policy at the bottom of all pages or via the mobile applications.
- Where clinical trial subject data is collected, SiteVault allows tracking of a signed consent form.
- Collection of data is lawful based on the legal grounds of the contract with the customer. No data is processed outside of this purpose.

Controls Data Quality & Security

- **Data Quality:** Data can be updated at any time (subject to user permissions).
- **Data Exports:** Vault users can export data (restricted by user security).
- **Data Backups:** Data backups do not leave the region of data storage. European data is backed up to a different location in Europe.
- **Data Retention:** Data is processed for as long as the company contracts with Veeva and requires the data to be retained. Veeva customers may request the deletion of all their data at any time, per contract. Site data is maintained for 25 years from study creation.
- **Security:** Veeva quality policies, application and AWS security are in place.

Supports Individuals' Rights

- Processes and tools exist to support individuals' rights to access their data, receive an electronic copy and port the data to another Controller, and the right to be forgotten.
- Additional data privacy measures in Vault and MyVeeva:
    - Whilst cookies are used (for security, user experience and user preferences), they do not track or profile individuals, and are not shared with other services.
    - Whilst user profiles cannot be erased from the audit trail, user info can be de-identified.
    - Veeva only sends direct marketing communications to users who mark themselves as '**Opt-in**' in Veeva Vault.

If you require more information on how Veeva complies with GDPR product obligations as a Data Processor, please reference the Veeva Privacy Policy (**veeva.com/eu/privacy**) or contact your Veeva CSM or Site Success Manager (sitesuccess@veeva.com).

This document is a summary of the DPIA, which is available on request. Contact your Veeva CSM or Site Success Manager.