Ivanti User Workspace Manager and GDPR

This document details Ivanti's stance with respect to General Data Protection Regulation (GDPR) when using Ivanti's User Workspace Manager solution. It contains information on the type of personally identifiable information (PII) that is collected, where it is stored and how this data can be removed on request.

Ivanti User Workspace Manager

There are three products within Ivanti User Workspace Manager where users' PII is collected and stored centrally in separate databases:

- Ivanti Management Center
- Ivanti Environment Manager
- Ivanti Insight

Ivanti Management Center

Data Collection

The following PII data is collected by Ivanti Management Center on the user endpoint and is then transferred to the centralized Management Center SQL Database:

- Access credentials for deploying the Client Communication Agent
  - Domain\user info + a FIPs compliant encrypted password
- Domain\user for admin access to the Management Console
- User SID for created objects
- Event data can include username and/or machine name unless anonymized
- The Machines and ScuServers tables also store machine names

Collated data in the Management Center SQL Database is retained indefinitely, or until an administrative user chooses to purge said data.

All "right to be forgotten" requests for data removal should begin with the Ivanti Client Communications Agent being removed from the endpoint device.

Data Removal Requests

Data can be removed from the Management Center SQL Database either by:

- Built-in, scheduled maintenance tasks
- Manually run PowerShell scripted maintenance tasks
- Manually run SQL Scripts

Additionally, event data can be saved out to local endpoint event logs or to local endpoint log files in either CSV or XML format.

These can be deleted manually or through scheduled tasks, as required, by an administrative user.

Ivanti Environment Manager

Data Collection

The following PII data is collected by Ivanti Environment Manager on the user endpoint and is then transferred to a centralized Personalization Server SQL Database:

- User ID
- User Login Name
- User SID
- Group SID
- Distinguished Name (User's AD name) (For List of users authorized to connect to the database only))

If a user has any sensitive data stored within their profile for a managed application, this data will also be stored within the Personalization Server SQL Database and so caution will need to be taken, with respect to GDPR, when storing 3rd party application personalization settings.

Collated data in the Personalization Server SQL Database is retained indefinitely, or until an administrative user chooses to purge said data.

All “right to be forgotten” requests for data removal should begin with the Ivanti Environment Manager Agent being removed from the endpoint device.

Data Removal Requests

Data can be removed from the Personalization SQL Database either by use of:

- The Ivanti Personalization Analysis Tool
- The Ivanti Personalization Operations Web Console
- Manually run SQL Scripts

Additionally, event data can be saved out to local endpoint event logs or to local endpoint log files in either CSV or XML format.

These can be deleted manually or through scheduled tasks, as required, by an administrative user.

Note: Where SQL replication, SQL mirroring or Ivanti GeoSync replication is being utilized across geographically dispersed sites, data may be stored across multiple Personalization SQL Databases. It is therefore recommended to regularly sync databases immediately after a GDPR “right to be forgotten” request has been implemented.

Ivanti Insight

Data Collection

The following PII data is collected by Ivanti Insight on the user endpoint and is then transferred to a central ElasticSearch Datastore on an Insight appliance:

- Logon GUID
- Device ID
- Device Type
- Device Manufacturer
- Device Model
- Computer Name

- Domain\username
- Profile Location
- Parent Username
- File path (could include username)
- File Description (could include username)

Note: By enabling the 'User Data – Individual File Information' option from the Insight Web Console Data Management screen, every file name a user creates and has stored on their endpoint device will be recorded. This could contain PII in the filename.

Collated data in the Insight ElasticSearch Datastore is retained indefinitely, or until an administrative user chooses to purge said data.

All "right to be forgotten" requests for data removal should begin with the Ivanti Insight Agent being removed from the endpoint device.

Data Removal Requests

To permanently remove unwanted data from an Insight server it is possible to purge all collected data or only that which relates to particular data types. Following a purge, data is permanently removed from the server and data collection starts again for purged data types, unless the Insight Agent is removed from the specific user device. You have the following options when removing data:

- Remove data for individual data types - Click **PURGE** for the required data type.
- Remove data for all data types - Click **PURGE ALL**.
- Remove data for all data types based on the age of the data - In the Purge by Age settings, enter the required number of days and click **PURGE NOW**. All data for the applications selected for collection, which is older than the entered period of time, is deleted.

To set up a recurring task based on these settings, select **Automatically run this task daily**, otherwise data is kept indefinitely.

Additionally, raw data reports can be exported from the Insight Web Console to CSV format and can be saved out to local administrative endpoints.

These can be deleted manually or through scheduled tasks, as required, by an administrative user.

Data Deletion and Support Cases

As part of the Ivanti support process customers may be requested to upload log files to the Ivanti portal to assist with troubleshooting. The files are stored securely with the Ivanti Data Center and are retained for no longer than 30 days after the incident is closed. The 30-day period is to give customers the opportunity to reopen their support case without having to re-upload their log files. For further detail please read the Ivanti data processing addendum.

If a customer wishes to remove specific data, that is not currently achievable through a product console or supported tool, details of tools and, where possible, examples of potential SQL /PowerShell API scripts can be provided to customers through a Support Incident.

Other Information

For more detailed information on the data collection features of Ivanti User Workspace Manger please access the relevant product knowledgebase or support portal at https://www.ivanti.co.uk/support/contact.

Ivanti User Workspace Manager does not allow Ivanti to access personal data, as defined in Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter “GDPR”), but personal data may be input into the Ivanti product, such that Ivanti is a processor under GDPR. Ivanti is not a controller under the legislation. Ivanti has addressed its obligations under GDPR through the creation of a customer-focused Data Processing Addendum, found at https://rs.ivanti.com/legal/ivanti-customer-eu-data-processing-addendum.pdf, as well as implementing industry-standard security and privacy protocols.