Ivanti IT Service Management and GDPR

Using Ivanti IT Service Management Products in a GDPR-Compliant Environment

This document applies to all current Ivanti IT Service Management (ITSM) products:

- Ivanti Help Desk Essentials – Cloud only, hosted on Microsoft Azure
- Ivanti Service Manager (ISM) – On-premises or Cloud, hosted on Amazon Web Services
- Ivanti Service Desk powered by Heat – On-premises or Cloud, hosted on Amazon Web Services (AWS)
- Ivanti Service Desk powered by Landesk (ISD) – On-premises or Cloud, hosted on AWS or Netplan
- Ivanti Voice – On-premises only

Including the following legacy products:

- Heat Service & Support (Heat Classic) – On-premises only
- Heat ITSM – On-premises only

Customers can use the Ivanti ITSM products to store personal information for their employees or external end users. Whether the data is imported from data files such as Excel or from external sources such as Active Directory, Ivanti ITSM products have several predefined attributes that customers can use to hold personal information such as names, network logins, email addresses, and phone numbers. Customers can also create extra fields to hold additional data such as payroll number or emergency contact details.

On-Premises Deployments

In on-premises deployments, the product database stores this data behind the customer's firewall. The customer is responsible for restricting direct access to the ITSM products and their database by following standard best practice protocols. All Ivanti products provide auditing capabilities to record all login, logout create, update, and delete activities and all administrator actions.

Cloud-based / SaaS Deployments

The cloud-based Ivanti ITSM products have the same detailed auditing capabilities for all activities.

In addition, for cloud deployments of Ivanti Service Manager, we encrypt all data at the field level in transit and at rest and all backup files. When in transit, data is sent securely through industry standard methods such as HTTPS, using SSL/TLS, AES 256-bit encryption, and 2048-bit certificates. To support backend integration into a customer's network, Ivanti provides VPN connections using industry standard AES (128 or 256) IPsec encryption. Commonly, we use VPNs as an alternative to direct over-the-internet communication for system-to-system processes such as SMTP/IMAP, SCCM, LDAP (both bulk import and authorization) and some file transfers.

Further information regarding GDPR and security settings available to Ivanti cloud-based services hosted on Amazon Web Services (AWS), Microsoft Azure, or Netplan can be found on their respective sites. In addition, the Ivanti Cloud Security white paper outlines Ivanti's comprehensive security model for the cloud-optimized Ivanti Service Manager solution.

Best Practices for Both On-Premises and Cloud-Based Implementations

Leverage Role-Based Privileging

Whether Ivanti ITSM products are deployed on-premises or in the cloud, we recommend using their role-based attribute-level privileging and object-level partitioning capabilities to help ensure sensitive data is available only to users who should be able to see it. All console interfaces (for example, for Service Manager, the Analyst, Self Service, and Mobile interfaces; for Service Desk, the console, Web Access, and Workspaces interfaces) and respective APIs adhere to these restrictions.

Do Not Store Personal Data in Free Text Fields

We recommend that customers restrict personal data to known fields only. This makes it easy to identify and remove that data as necessary to manage GDPR opt-out ("right to be forgotten") requirements. For example, do not store personal data in free text fields such as Incident Description or Note fields. In Service Manager, we further recommend not storing personal data in fields where data input cannot be validated or masked (for example, where an email address might appear as ********or@ivanti.com) to prevent inadvertent exposure.

Other

Some customers have asked whether it is possible to anonymize all personal data stored in Ivanti databases. Doing this would defeat many of the product's capabilities. For an organization to provide superior service to employees and/or external customers, it is important to know who is receiving the services, how to contact them, and what devices they are using. We strongly suggest you review the requirements of the GDPR, because most organizations' use of Ivanti products will qualify under one or more of the lawful reasons to process and handle personal data.

Opt-In Consent vs Legal Basis

GDPR Article 6(1) details lawful reasons for collecting, using, and storing personal data:

"1. Processing [of personal data] shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Article 6(1) covers normal business operations. For example, a business must use employees' personal data to provide services such as payroll and benefits and generally has the employees' express or implied consent to do so. In addition, a business must know who its employees are, where they are based, and what devices they use for work. It is a necessary part of being an employer. A business must also manage and secure its employees' devices, grant and restrict access to IT systems and data, and provide various other IT services. These tasks often require the use of personal data in IT management tools and databases.

Article 6(1) also has application in the following circumstances:

- When handling external customers' personal data as part of a contract (for example, using Service Manager or Service Desk to store and use that data to process external service requests)
- When using a third party to process personal data on behalf of the organization (for example, in a third-party SaaS or MSP offering)

Using Ivanti to Further Support GDPR Compliance Efforts

You may also want to consider the following uses for your Ivanti ITSM product implementation:

1) Create an incident process that models your business process for handling a breach or other security alert, including an SLA to help ensure IT and other parts of the organization respond in a timely manner.
2) Create a request process and service request item in the service catalog to manage opt-out requests. This should model all the steps the organization needs to take to comply and prove compliance. An SLA that meets the GDPR requirements can also be added.
3) Create request processes for managing Data Processing Addendum (DPA) requests and compliance surveys (for example, partner, vendor, or customer requests to provide a copy of the DPA or respond to data handling surveys). This could include processes for tracking the status of incoming and outgoing requests.

Notice

This guidance is not intended as legal advice to our customers. You are responsible for ensuring your organization's compliance with GDPR. We recommend consulting with your legal counsel to interpret the relevant laws and regulations for your business and to guide any actions you may need to take to comply.