Part II: GDPR Compliance Information

Tables of Contents

GDPR Compliance Information

This document is for PID(s): 5725-D14, 5725-F59, 5725-A39, 5725-A40, 5737-B60, 5737-B86

Notice

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of Informix that you can configure, and aspects of the product’s use, that you should consider to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the large variety of ways that the product can be used in itself and with third-party applications and systems. Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. HCL does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Overview

General Data Protection Regulation (GDPR) has been adopted by the European Union ("EU") and applies from May 25, 2018.

Why is GDPR important?

GDPR establishes a stronger data protection regulatory framework for processing of personal data of individuals. GDPR brings:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for processors

- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

For more information on GDPR see,

- EU GDPR Information Portal (https://www.eugdpr.org/)
- hcl.com/GDPR website (https://www.hcltech.com/privacy-statement)

Product Configuration for GDPR

The following section provide considerations for configuring IBM® Informix® to help your organization with GDPR readiness.

Configuration to support data handling requirements

The GDPR legislation requires that personal data is strictly controlled and that the integrity of the data is maintained. This requires the data to be secured against loss through system failure and also through unauthorized access or via theft of computer equipment or storage media.

Informix provides the features and capabilities needed to help our customer meet their GDPR responsibilities and this document is intended to provide guidance as to which capabilities are relevant to the different needs of our customers under this legislation.

Data Life Cycle

GDPR requires that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.
- Kept in a form which permits identification of the data subject for no longer than necessary.

Whether or not an Informix database will contain personal data is dependent on the business needs and objectives of our customer. It is the responsibility of our customer to ensure that appropriate consent is in place for the collection and storage of personal data within an Informix system and to configure Informix appropriately to ensure that the data is secured throughout its persistence in an Informix database.

This document is intended to give insight into how Informix interacts with personal data once it is stored in an Informix database as well as to identify specific aspects that may need to be considered by our customers.

Data Collection

The customer decides when and where personal data is collected within their business processes. SQL statements and Informix utilities are used by the customer to present the data to Informix for any desired processing, access, or storage within Informix as required by their business. How and where such personal data is stored within an Informix database is likewise determined by the customer.

The only personal data required by Informix itself is during the authentication process and this information is not stored within Informix. Authentication occurs during any attempt to connect to a database and Informix requires the presentation of an external user ID and credentials (e.g. password) for authentication purposes. This information is passed by Informix to the external authentication service identified by the customer during Informix configuration and, assuming a successful authentication, this service will then provide Informix with the individual and group Informix authorization IDs associated with that specific user in its records. This latter information is associated in Informix memory with that specific connection for the life of the connection.

Once personal data is stored within a database, Informix processing can interact with it in the following ways:

Backup

Informix provides its customers with the ability to backup the data contents of a database, or part of a database, to an independent file in a customer defined location. This backup file will contain any customer data located in the specified Informix source location (e.g. database or tablespace) at the time of the backup request.

Transaction logs

Informix transaction logs, used for recovering a database after a failure or recovering to a specific point-in-time from a database backup, can contain some of the personal data collected by Informix about the connection which made the change(s) as well as any personal data in the customer-specified data that was changed. Informix provides the customer the ability to define a location where Informix will archive old transaction logs for long-term storage.

Audit logs

If Informix Audit is enabled by the customer, the audit logs will contain some of the personal data associated with the connection by Informix.

Diagnostic information

For diagnostic purposes, the contents of the Informix diagnostic log (location set by MSGPATH) can contain some of the personal data associated with the connection by Informix. As well, in the event of a service event occurring within Informix (e.g. an unexpected error or termination), additional diagnostic files can be created; these files can contain the personal data associated with the connection by Informix as well as any customer-specified personal data revealed through SQL statement text in the form of literals or data arguments provided for host variables or parameter markers in the SQL statement.

Monitoring

Some Informix monitoring interfaces can be used to access both the personal data associated with the connection by Informix as well as any customer-specified personal data revealed through SQL statement text in the form of literals or data arguments provided for host variables or parameter markers in the SQL statement.

Database catalog tables

Certain actions can result in Informix recording the Informix authorization ID associated with the currently connected user into its internal catalog tables as a record of ownership or permanent permission for that authorization ID. Examples of these actions include the creation of a database object or the granting of a database permission by or for the connected user.

Informix configuration files

As part of its database manager and database configuration files, Informix can request information related to IP addresses and user IDs needed to access other (non-Informix) services.

Data Storage

Storage of account data

Account information used by Informix to authenticate individuals is stored in a security facility outside of Informix. The security facility can be part of the operating system or a separate product and the customer is responsible for determining how and where this information is controlled within the security facility. For more information, refer to, Authentication

Storage of client Data

The customer explicitly inserts any collected data to be stored into specific tables that they have created within the database. The physical location of the data in those tables is determined by the definition of the tablespace(s) used in the table definition. For more information, refer to the [CREATE TABLE] and [CREATE TABLESPACE] in the IBM Knowledge Center.

Storage in backups

The customer determines when and where database backups will occur through their configuration of Informix and/or their use of the BACKUP command. For more information, refer to, Data recovery. The customer determines when and where Informix transaction logs are archived through their configuration of Informix. For more information, refer to [Log file management through log archiving].

Data Access

The customer has complete control over what authorities and privileges are made available to any user who can connect to the database.

By default, when a Informix database is created, a number of privileges are granted to public allowing all connected users to use them. If strict control over access is desired, it is recommended to create the database without the PUBLIC keyword (Replacing PUBLIC with Specified Users) or to use security products such as IBM Guardium Data Protection for Databases to evaluate the access control model on the database.

Separation of duties

While Informix provides the ability to implement separation of duties through its granular authorization model, it does not enforce this policy. The customer is responsible for ensuring that is policy is properly implemented and maintained.

Privileged Administrators and Administrators

The highest level of database privilege is database administrator, or DBA. When you create a database, you are automatically the DBA and can grant same level of privilege to other users. If it is necessary to have multiple administrative users, the customer can implement additional protection against inappropriate access by this authority to client data in tables by implementing row and column access control (LBAC) and multi-level security (MLS), to control who has read access and write access to individual rows and columns on the tables containing sensitive data. For more information refer to Security Data .

Activity logs

Informix provides the ability to configure and enable audit logs through its [Auditing facility] Access to the data in these audit log files is controlled by the file permissions on the files. For more information refer to Auditing data security.

Data Processing

Encryption of data in motion

In order to protect all personal data being exchanged to the Informix server, it is recommended that the customer encrypt the communication to and from Informix by implementing secure communications using Transport Layer Security (TLS). For more information, refer to Data Encryption. Similarly, secure communications should also be considered in an HADR environment where personal data may appear in the transaction logs flowing between the primary and standby databases.

Encryption of data at rest

In order to protect database files, transaction logs, and backups while they are at rest on external storage media, it is recommended that this data be encrypted. For more information, refer to (Data Encryption).

Encryption key ownership

If Informix native encryption is chosen as the method to protect at rest data, encryption keys will be generated by Informix and used to encrypt the user data. The keys can be stored in a keystore external to Informix. The keystore is protected by a password which is stored in a stash file. The customer is responsible for the protection of the keystore and stash file.

Data Deletion

Right to Erasure

Article 17 of the GDPR states that data subjects have the right to have their personal data removed from the systems of controllers and processors - without undue delay - under a set of circumstances.

Deletion of data from within a database

Personal data collected by the customer about their clients and stored within Informix can be deleted from individual tables using the DELETE or TRUNCATE SQL statements or by dropping the tables which contain the data. This will make the data inaccessible to future access within the database although it will still potentially exist in database backup images, archived transaction logs, or archived audit files and will continue to do so until those files are removed.

To remove references to a user Informix authorization ID from the system catalog tables, action must be taken to revoke any authorization granted to that authorization ID and to drop or transfer ownership of any object created by that ID.

It is also possible that some references to the deleted personal data could still exist in the Informix diagnostic log or in additional diagnostic files. The customer is responsible for managing these files and removing them if they are no longer needed.

Deletion of an Informix database or instance

To remove the Informix database, the customer can drop the database from the Informix server and then follow standard disk cleaning practices on the storage used by the database. For more information, refer to Dropping databases. To remove the complete Informix installation, the customer can uninstall the product and then follow standard disk cleaning practices on the storage used by the product. For more information, refer to Uninstalling.

Data Monitoring

All changes to data stored in the database are recorded in the Informix transaction logs and these logs can be accessed by authorized users.

Informix provides an optional Auditing facility which can be configured by the customer to view a variety of different activity within the database including access and changes to data in the database. There are also external products such as [IBM Guardium Data Protection for Databases] (https://www.ibm.com/us-en/marketplace/ibm-guardium-data-protection) which can be used to audit database activity.

Informix also provides a number of monitoring interfaces in the form of event alarms and web tools which can be used by the customer to perform ad hoc monitoring of activity on the database. For more information, refer to Database Monitoring.

Responding to Data Subject Rights

Responsibility for meeting data subject rights lies with our customer and should be reflected in their database configuration and design, application logic, and business processes. They must manage and account for the deletion or modification of any personal information data collected by Informix or by customer database application logic.

Ordinary DML SQL statements can be used to delete or modify any identified personal information stored in the database itself but our customers are reminded that the original data may still exist in archived transaction logs and database backup images. Also, the target personal information may also exist in additional files associated with the database such as the audit files and diagnostic files.