LYNQ

Supporting GDPR Compliance

LYNQ MES

DECEMBER 2021

Contents

Introduction

On the 25 May 2018, the General Data Protection Regulations (GDPR) came into effect. GDPR is a European privacy and security law that establishes a new global standard for privacy rights, security and compliance.

The GDPR may require changes to how your organisation gathers, uses and manages personal and sensitive data. GDPR applies to any organisation, whether based in the European Union (EU) or not, which processes the data of individuals residing in the European Union. Since GDPR came into effect, it is more important than ever to ensure the correct procedures are in place to follow the new regulations. If organisations do not adhere to the regulations or lack the adequate IT security to protect personal data, they could be heavily fined.

Key principles of the GDPR include:

- Enhanced personal privacy rights
- Increased duty for protecting personal data
- Mandatory reporting of personal data breaches
- Significant penalties for non-compliance

There are terms within the GDPR that are important to remember as you evaluate how technology companies such as LYNQ can help you meet the requirements of GDPR.

The following terms should be clearly understood:

Term	Meaning
Data Subject	The identified or identifiable living individual to whom personal data relates.
Personal Data	Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Special Category Data (Sensitive)	Special category data includes personal data revealing or concerning racial, ethnic origin, political opinions, religious, philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life and sexual orientation.
Processing	In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).
Controller	A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	A person, public authority, agency or other body which processes personal data on behalf of the controller.

As part of your GDPR compliance, you will need to understand the definitions of personal and sensitive data and how they relate to the types of data held by your organisation within LYNQ.

When LYNQ is installed within an organisation's local environment, the organisation takes on the role as processor. It is the organisation's responsibility to ensure that any processing of personal data is compliant with the GDPR. In the event that LYNQ are requested to process data on behalf of the controller, LYNQ will comply with the GDPR and in accordance with a signed Data Processing Agreement. A Data Processing Agreement can be requested by emailing privacy@lynqmes.com.

The purpose of this document is to provide a basic understanding of the GDPR and how to relate that to LYNQ. As you are the primary custodian of the data, this document includes the features and functions within LYNQ that can help you enhance your overall data and privacy capabilities. LYNQ guarantees data protection safeguards are built into products and services from the earliest stage of development, providing 'data protection by design' in new products and technologies.

This document is reviewed and updated in line with new software releases to ensure any changes made to the storage of personal data is correctly reflected in this document.

What is considered personal data

Organisations must understand what personal data is collected against their data subjects. The table below can help organisations to understand whether LYNQ stores different types of personal data. Personal data in scope of the regulation can include, but is not limited to, the following:

Personal Data	Stored in LYNQ	Location
Name	Yes	Database Files & Text Log Files
Identification number	Yes	Database Files & Text Log Files
Address	No	
Email address	Yes	Database Files
Photo	Yes	Database Files
IP address	Yes	Text Log Files
Location data	No	
Cookie identifiers	No	
RFID tags	No	
Analytics & profiling	Yes (Analytics for OLE)	Database Files
Race	No	
Religion	No	
Political opinions	No	
Trade union membership	No	
Sexual orientation	No	
Biometric data	No	
Genetic data	No	

Tables in LYNQ that store personal data

The tables listed below will help you identify where personal data in LYNQ is stored by default. You will need to consider any customised tables added by LYNQ or your organisation, if required.

Personal Data	Database Name	Table Name	Field Name
Name	ERP DB	Lynq_VP_UserRole	UsrName
	MOM_Data	Lynq_ME_ActivityExtension	AssignedTo
			ResolvedBy
		Lynq_ME_Employee	lName
		Lynq_ME_LinkedURLLog	EmployeeName
		Lynq_ME_Message	FromName
			FromCode
		Lynq_ME_MessageObject	Name
		Lynq_ME_MessageRecipient	ToName
			ToCode
		Lynq_ME_Trace_Employee	lName
		Lynq_ME_HieracrchItem	Code
		Lynq_ME_Interaction	ChangedBy
		Lynq_ME_User	DisplayName
First Name	MOM_Data	Lynq_ME_Employee	lName1
		Lynq_ME_Trace_Employee	lName1
		Lynq_ME_User	FirstName
Last Name	MOM_Data	Lynq_ME_Employee	lName2
		Lynq_ME_Trace_Employee	lName2
		Lynq_ME_User	LastName
Identification Number	MOM_Data	Lynq_ME_Activity	aEmployeeCode
			aErpEmployeeCode
		Lynq_ME_Activity2	aReporterCode
			aEmployeeCode
			aErpEmployeeCode
			aReporterCode
		Lynq_ME_Activity_GeneralLog	aEmployeeCode
			aErpEmployeeCode
		Lynq_ME_Association	EmployeeCode
		Lynq_ME_DO_Container	Reporter
			Employee
		Lynq_ME_DailySummary	dReporterCode
			dEmployeeCode
		Lynq_ME_Employee	lCode
			lErpReporterCode
		Lynq_ME_EventMark	eEmployeeCode

			eReporterCode
		Lynq_ME_LinkedURLLog	EmployeeCode
		Lynq_ME_OfficeTime	oEmployeeCode
		Lynq_ME_Trace_Employee	lCode
		Lynq_ME_Trace_Employee	lErpReporterCode
	MOM_Config	Lynq_ME_DataCollection	Code
		Lynq_ME_EmployeeExt	lCode
		Lynq_ME_EmployeePhoto	Code
		Lynq_ME_Seats	EmployeeCode
		Lynq_ME_UserProfile	UserID
		Lynq_ME_UserProfileEmplStatusSett	UserID
		Lynq_ME_UserProfileFAEventsListFilterSet	UserID
		Lynq_ME_UserProfileFcltStatusSett	UserID
		Lynq_ME_UserProfileMonitorStatusesSett	UserID
		Lynq_ME_UserProfileSeatFilterSett	UserID
	MOM Logic	Lynq_ME_Logic_ANav_Bulk_ReceivedEvent	EEmployeeCode
			EReporterCode
		Lynq_ME_Logic_ANav_ReceivedEvent	EEmployeeCode
			EReporterCode
		Lynq_ME_Logic_Core_FixingMarks	ReporterID
		Lynq_ME_Logic_ZDisc_Evo_All	ReporterID
		Lynq_ME_Logic_ZDisc_Evo_Bulk_All	ReporterID
		Lynq_ME_Logic_ZLabour_Ent_Reporter	Code
		Lynq_ME_Logic_ZLabour_Evo_Membership	MasterReporterID
		Lynq_ME_Logic_ZLabour_Evo_MembershipTask	ByReporterID
		Lynq_ME_Logic_ZLabour_Evo_Reporter	ReporterID
			EmployeeCode
		Lynq_ME_Logic_ZLabour_Evo_ReporterAccountMark	ReporterID
		Lynq_ME_Logic_ZLabour_Evo_ReporterMembership	ReporterID
		Lynq_ME_Logic_ZLabour_State_Membership	MasterReporterID
		Lynq_ME_Logic_ZLabour_State_Reporter	ReporterID
			EmployeeCode
		Lynq_ME_Logic_ZLabour_State_ReporterAccountMark	ReporterID
		Lynq_ME_Logic_ZLabour_State_ReporterMembership	MembershipID
			ReporterID
		Lynq_ME_Logic_ZLabour_State_TaskMembership	MembershipID
			ByReporterID
	LYNQ api	Lynq_PG_UserGroupRel	UserID
Email Address	MOM Config	Lynq_ME_User	Email
Login	MOM Data	Lynq_ME_LinkedURLLog	UserName
	MOM Config	Lynq_ME_User	UserName
		Lynq_ME_UserProfile	UserName
	LYNQ api	Lynq_PG_User	UserName

Photo	MOM Config	Lynq_ME_EmployeePhoto	PhotoData
Analytics (OLE)	MOM Data	LYNQ_ME_Activity	Various Fields

SQL Views in LYNQ that read personal data from ERP

The views listed below will help you identify which SQL views contain personal data for inbound data mapping purposes. Inbound data mapping transforms data from the integrated ERP application to LYNQ. You will need to consider any customised views added by LYNQ or your organisation, if required.

Personal Data	Database Name	View Name	ERP Table	ERP Field
Name	ERP Database	Lynq_ME_EmployeeView	BomEmployee	Name
First Name	ERP Database	Lynq_ME_EmployeeView	BomEmployee	Name
Last Name	ERP Database	Lynq_ME_EmployeeView	BomEmployee	Name
Identification Number	ERP Database	Lynq_ME_EmployeeView	BomEmployee	Code

Screens in LYNQ that expose personal data

The menus listed below will help you identify where personal data is revealed within LYNQ's user interface. You will need to consider any custom columns added by your organisation, if required.

Main Menu	Sub Menu	Personal Data
APS Company Settings	User Access	User Name
Resource Management	Seat Maintenance (Seats)	Name
	Employee Maintenance	Display Name
		First Name
		Last Name
		Employee ID
		Employee ID (ERP)
		Workbench ID
		Email Address
		Login
		Photo
		IP Address
Resource Maintenance	Employee	Employee ID
		Employee Name
		Employee Photo
Data Collection	Workbench	Employee Name
		Employee Photo
		Employee Performance Data
	Timesheet Entry	Employee ID
		Employee Name
	Factory Automation	Employee Name
Tracking	Dashboard	Employee ID
		Employee Name
		Employee Performance Data
	Employee Status	Employee Name
		Employee Performance Data
	Job Status (List)	Customer Name (possibly)
	Job Status (Sub Jobs)	Customer Name (possibly)
	Job Card (Summary)	Employee Name
		Customer Name (possibly)
	Job Card (By Task)	Customer Name (possibly)
	Job Card (By Operation)	Customer Name (possibly)
	Job Card (By Materials)	Customer Name (possibly)
	Job Card (Sub Jobs)	Customer Name (possibly)
	Job Card (Schedule)	Customer Name (possibly)
	Job Card (Transactions)	Employee Name

	Employee Performance (Dashboard)	Employee ID
		Employee Name
		Employee Photo
		Employee Performance Data
	Employee Performance (Summary)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Performance (Detail)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Performance (Audit)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Performance (Adjustments)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Performance (Alerts)	Employee ID
		Employee Name
	Employee Performance (Issues)	Employee ID
		Employee Name
	Employee Performance (Attachments)	Employee ID
		Employee Name
	Management Reports (Availability)	Employee ID
		Employee Name
		Employee Performance Data
	Management Reports (Adjustments)	Employee Name
		Employee Performance Data
	Management Reports (Details)	Employee ID
		Employee Name
		Employee Performance Data
	Management Reports (Pivot)	Employee ID
		Employee Name
		Employee Performance Data
Continuous Improvements	Loss Management (Dashboard)	Employee ID
		Employee Name
		Employee Performance Data
	Loss Management (Availability)	Employee ID
		Employee Name
		Employee Performance Data
	Loss Management (Quality)	Employee ID
		Employee Name
		Employee Performance Data

Performance Analysis	Availability (Dashboard)	Employee ID
		Employee Name
		Employee Performance Data
	Availability (Details)	Employee ID
		Employee Name
		Employee Performance Data
	Performance (Dashboard)	Employee ID
		Employee Name
		Employee Performance Data
	Performance (Details)	Employee ID
		Employee Name
		Employee Performance Data
	Quality (Dashboard)	Employee ID
		Employee Name
		Employee Performance Data
	Quality (Details)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Analysis (Dashboard)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Analysis (By Employee)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Analysis (By Period)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Analysis (By Diversion)	Employee ID
		Employee Name
		Employee Performance Data
	Employee Analysis (Availability	Employee ID
		Employee Name
		Employee Performance Data
	Product Analysis	Employee Performance Data
Alerts & Issues	Alert Maintenance	Employee ID
		Employee Name
Document Library	Attachments (Employees)	Employee ID
		Employee Name
Issue Log	New Issues	
	All Issues	
Message Centre	All Statuses	Employee Name
System Insights	Transaction Log	Employee ID

[redacted]		Employee Name
		Employee Performance Data
	Sync Message Log	Employee ID
		Employee Performance Data
	Events	Employee Name
		Employee Performance Data

Other locations where personal data may be stored

Other than the databases and tables included in this document, personal data may also be found in documents, spreadsheets, email messages, and other types of files. It is easy to extract and transfer personal data from LYNQ using features such as:

- Export to excel
- Sending messages to recipients via email
- Sending alerts to recipients via email
- Extracting employee data using viewexporter.exe residing in the LYNQ mom website folder
- Using webhooks to pass data to third party applications
- Integration with custom business applications such as Power Apps and SharePoint

Personal data will/may also be stored outside of the database in these types of files:

- Database backup files (SQL or other formats)
- Default attachment location for document library files (see LYNQ api Global Settings)
- Log files
    - APS logs in Windows User Profile folders
        - 4.2020_server-log.txt
        - 4.2020_gui-log.txt

Other ways personal data may be viewed

Some features in LYNQ may be configured in such a way that personal data external to LYNQ may be viewed within the LYNQ user interface. This may apply to features such as:

- Bookmarks
- Webhooks
- URI Convertor

External data must be adequately protected under the GDPR.

Classifying personal data

- Personal Data would need to be classified outside of LYNQ.

Exporting data subject's personal data

- Personal Data may be exported from the LYNQ interface or by using database management tools.

Deleting data subject's personal data

- Personal data such as a user account or employee account can be deleted from the Seat Maintenance screens. Note: Transactional data is kept for historical purposes. Contact LYNQ for assistance to delete or anonymise the subjects data.

Managing data subject requests

- Data subject requests must be managed outside of LYNQ.

Providing detailed notice of processing activities

- The Bookmarks feature may be used to direct a user to a web based Privacy Policy.

Detect and respond to data breaches

The GDPR obligates you to report and notify the relevant supervisory authority and affected data subjects of personal data breaches. When LYNQ is installed within your organisations own premise, it will be your responsibility to monitor, detect and report data breaches within the time periods defined by the GDPR.

Discover, identify and classify personal data

This document is reviewed and updated in line with new software releases to ensure any changes made to the storage of personal data are correctly reflected in this document. Should this document not provide sufficient information to support your organisations GDPR compliance, SQL Server provides multiple out of the box solutions that can be implemented to discover personal data.

SQL Server tools you can use to discover personal data

- SSMS – Vulnerability assessment
- Querying sys.columns to identify column names which potentially contain personal information, you can also consider using Full text search to expand your search

Once personal information is located and gaps in policies of data governance are identified during the discovery phase, now it's time to implement mechanisms to minimise risks from unauthorised access to data or data loss.

SQL Server tools you can use during the manage phase:

- SQL Server authentication, there are two modes: Windows authentication mode and mixed mode. Windows authentication is often referred to as integrated security because this SQL Server security model is tightly integrated with Windows, this is the best practice.
- Create roles to define object level permissions, granting permissions to roles rather than users simplifies security administration. Permissions assigned to roles are inherited by all members of the role, and users can be added or removed to a role to include them in a permission set.
- Use server-level roles for managing server-level access and security, and database roles for managing database level access.
- Azure SQL Database firewall, at logical instance and database level. This way only authorised connections have access to the database, and align with the GDPR requirements.
- Dynamic data masking, to limit sensitive information exposure by masking the data to non-privileged users or applications.
- Row level security, to restrict access according to specific user entitlements.