Xeelo GDPR | Functionalities

NAME OF FUNCTIONALITY	DESCRIPTION
GDPR Legal Entity (Configuration)	Setup the legal entities that will be working with the system, including departments, coordinators, data sources, data incident types and personalized external web forms.
GDPR Assessments (Operations)	This function allows you to send out and manage the responses to various questionnaires, which can be from out databank, or created specifically by you (see below). It is used to perform readiness assessments, GAP analysis, Audit/Risk reviews & Data Privacy Impact Assessments. It allows to select departments/individuals who should answer Question Groups/Catalogs, you can track response rates, and review answers, store the history of responses as they evolve over time and easily repeat and re-launch identical or slightly modified Assessments.
GDPR Question (Configuration)	Setup Questions to be used in GDPR Assessments, these can be answered as either free text, or as a combo-box predefined list – which makes aggregation and review against expected responses much easier.
GDPR Question Group (Configuration)	Build Assessments/questionnaires by combining Questions into Question Groups – these are then used to quickly build assessments, you can either build a "CORE" Group and then add extra questions directly in the assessment, or create multiple variants in this section for easy re-use. The assessments function lets you easily combine multiple Question Groups into one assessment.
GDPR Register of Processing (Operations)	This provides the heart of managing personal data flows across the organization. It allows you to store information about each process which involves personal data (at a minimum these should be listed), attach process documentation, map relations to data sources, data subjects, data categories, list internal and external data processors, review GDPR considerations relevant to the process (Special categories of personal data, lawfulness of processing, data minimization, privacy by design, accuracy of the data, limitation, deletion & restriction of processing, obligations to inform & notify and data portability), perform a DPIA screening and automatically trigger a DPIA assessment.
GDPR Entity (Configuration)	Manage list of key external partners involved with GDPR, such as auditors, accountants, marketing agencies etc. (eg. Data Processors, sub-processors etc.)
GDPR Data Subject (Configuration)	Define the Data subjects at the level of granularity that you want to map within Xeelo GDPR (e.g. Customers/Suppliers or Customers B2B, Customers B2C etc.)
GDPR Data Category (Configuration)	Define the Data Categories & granularity that your organization works with and wants to map (e.g. Contact Data or Street Address, City, Post code)
GDPR Data Source (Configuration)	Create a list of data sources to be used in the Xeelo GDPR application, such as databases, ERP applications, physical storage locations as well as attach key attributes to each for easier searching & reporting.
GDPR Data Source entity (Configuration)	Combine the Data Subjects/Data Categories and map to Data Sources (eg. SAP) or subsets of Data Sources (SAP S&D Module) at the level you wish to track personal data. Then define for this combination core attributes for GDPR – Legal base for storing, data classification, retention period, transfer to 3rd countries, automated decision making. This is used in the Process Register to pre-load critical GDPR values based on a data source, but can always be manually expanded in each process.
GDPR Risk (Operations)	Manage the risks identified related to personal data, including required actions for risk resolution, mitigation or improvement.

	GDPR requires a risk assessment to be performed from the view of the data subject (not the organizational risks that may already be captured under ISO or other programs) we also include a detailed evaluation section specific to GDPR to enable a risk rating methodology to be systematically introduced in the organization, including Impact on Data Protection Objectives, Threat Type, Risk Severity, Risk Likelihood and Risk response. This includes mapping of the risks to Processes, Audits, Departments or Data Sources, as well as establishing review dates & individual tasks.
GDPR Audit (Operations)	Manage Data Privacy Audits, including tracking of findings, acceptance of audit findings, solution of findings or creation of risks in the Risk Register (above). Using the auditing features of Xeelo™ you can easily see all changes to audit issues/findings and who is involved in any decision making. This function also allows you to easily repeat audits, to ensure regular review & ongoing compliance with GDPR.
GDPR Training run (Operations)	Manage internal & 3rd party knowledge & acceptance of your organizations data privacy policies. This function allows you to easily assign departments/individuals to attend training sessions, or read organizational documents, and tracks compliance via attendance sign-off, or quizzes which can test the required knowledge level. It also allows for the managed distribution of document groups & confirmation of receipt via individual tasks being created for each nominated person. Although intended primarily for internal staff, it can be extended to include key contractors & 3rd party staff.
GDPR Training (Configuration)	Setup pre-defined trainings, training descriptions & reading materials as well as proof of understanding evaluations including pre-defined quizzes. This allows you to easily re-use a training type for new employees or during projects.
GDPR Document (Operations)	Allows you to store documents that are key to GDPR compliance such as data processor agreements, or supervisory authority notifications. It also allows you to assign these documents for review to departments or individuals, to ensure they have been formally reviewed. You can also setup automated review dates, when the documents will trigger new individual tasks for individuals to ensure they don't expire.
GDPR Article (Operations)	Provides an overview of all GDPR Articles (in as many languages as you like), can also be used to store Frequently Asked Questions and other key information that you want your staff to have access to read and review but does not require formal acceptance.
GDPR Legal Consent run (Operations)	This function allows you to obtain legal consent outside the scope of contractual arrangements from the employees and contractors of the organization. It allows you to specify the type of legal consent you would like (what will happen to their data), how long the consent is provided for (it cannot be indefinite anymore) and which individuals should provide consent (either internal staff or external contractors where you can provide an email to send the consent to). The system will track the consent being provided, monitor the expiration dates of the consent to allow automated resending to gather new consent (extensions) and also generate unique hash confirmation links for the external recipients to track their acceptance.
GDPR Legal Consent (configuration)	This allows you to predefine and format the subject & text of the legal consent emails that will be sent using the Legal consent function.
GDPR Incident (Operations)	This function allows you to report incidents that could result in personal data loss, or have resulted in personal data loss, it establishes links to related systems & departments, and allows you to determine the type of incident that has occurred (setup in Legal Entity Configuration). It then allows you to load predefined Action Steps that need to be taken for each incident type (setup in Legal Entity Configuration) and adjust the

	action steps necessary as needed before assigning them to individuals in the organization to resolve. It also includes an Incident Assessment section to describe the measures taken and impact assessment, as well as load all the impacted data subjects/data categories based on the data source to further help manage the impact. After all the actions are completed a final result can be documented and a report generated in PDF that can be shared as required with the supervisory authority or individuals impacted. Incidents in this function can also be automatically triggered by integrating with the Office365 Protection Services & Azure Protection Services features provided by Microsoft, to ensure Monitoring does not end with a lost email to a system administrator.
GDPR External Request (Operations)	This function supports Chapter III – Rights of the data subject in GDPR (articles 12-23). It allows you to generate a legal entity specific webform (that can be integrated into any existing website) to capture individual requests, and then manage the response to these requests. This includes automated confirmation via a hashed link of the email sending the request, to improve identity confirmation, and all relevant time stamps and actions taken to demonstrate compliance with GDPR. You can assign actions to each individual data source owner that is relevant for the request, and track progress. Once the request is finalized, you can send a tracked response to the requestor. If integrated with the Xeelo™ platform, the selection of individual data sources can trigger automated actions (depending on setup) – such as data searches or changes to individual system setup for the requestor.
GDPR Reference Definitions (Configuration)	Allows you the customize in as many languages as you like all the system components that appear in various areas, such as priority tags, drop down lists, incident response levels etc.
Tasks (for each Operational Area)	Tasks provides each user an individual area, where any individual task assigned to them, from the Operations functions listed above, can be managed, responded to or redirected/rejected to the coordinator. (eg. Work on risk mitigation tasks, respond to DPIA questions, manage data breach activities, read training manuals and answer quizzes etc.)
Audit History & Proof of Changes	Xeelo™ Platform is unique in that it fully audits not just Changes(C), Updates(U) & Deletions(D), but also keeps a full audit trail of all Read(R) activity (full & secure CRUD implementation that has been audited as part of Sarbanes & Oxley reviews without findings). This allows you to always prove the activities of all users in the system, and when combined with Master Data Management can ensure that you always know who is working with individual's personal data across the organization.
User Access & Roles Management	Create new users and assign roles and organizational responsibilities (eg. administrator, data privacy officer, business user, incident manager, training manager, audit manager).
Monitoring & Alerts	Easily setup automated reminders for tasks/activities, or automated escalations if tasks remain open too long. This functionality also allows you to automatically re-open unresolved risks for review 6-12months in the future, or re-assess DPIA's annually.
Notifications & Emails	For each stage of a task/activity decide who should receive emails about progress, automatically respond to new subject data requests and combined with Monitoring & Alerts ensure you have automated deadline extensions (e.g. 30 day response time extended upto 90 days)
Exports & Reports	Generate PDF reports for meeting GDPR requirements (Art. 30 and 35) as well as Supervisory authority notices (e.g. 3rd country data processing notification). Easily export all data in the system to Excel or Data cube for use with BI systems, to allow further processing & analysis.

Imports	Provides the ability to import data from standard data sources such as .CSV files, to simplify initial preparation of the Xeelo GDPR environment for managing GDPR activities.
Relations	Available from within each object/function above, this allows the real-time generation of a visual data map, that helps show relationships between objects at both a high level and for each individual item – allowing easy management across the organization for a DPO.
Dashboard	Provides an aggregated overview of the entire Xeelo GDPR module, with key KPI's such as open risks, open incidents, incomplete trainings etc. With the possibility to drill down into each area and perform further analysis. This is provided within Xeelo or through a Microsoft PowerBI report or Excel Report – for those with sufficient access to see the data.

Note: This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.