MyCompliance Cloud

MetaPrivacy Module

KEY TERMINOLOGY

MetaPrivacy Roles - There are four main roles available within the MetaPrivacy tool:

1. **Data Protection Officer (DPO)** will be the person(s) within the organisation who will have full administrative access to the site, which will enable them to deliver privacy assessments, policies and eLearning to employees, customise assessments and view reporting.

2. **Reviewers** will review the *Privacy Assessments* and based on the user's response, will provide further information if required.

3. **Data Champions** will be assigned Privacy Assessments. A separate Privacy Assessment can be completed for each Personal Data Processing Activity they undertake. If required, Champions can have elevated permissions to access the registers to create and update their own records only.

4. **Program Owners** will be assigned to individual programs so that they can assume responsibility of its completion. The program owner will also have visibility over completed assessments, created processing activities and any assigned risks/task within the program. Program owners will not be able to see other programs they are not the owner of.

Organisational Structure - Organisational Structure allows the creation of an internal structure of the business, which makes it easier to segregate the specific roles and responsibilities of staff. The primary purpose of the organisational structure is to allow for Privacy Assessments to be targeted to users and will be seen within Programs.

Programs

Programs allows for segregation of processes and the targeting of Privacy Assessments, GDPR eLearning and Privacy Policies to employees and 3rd parties. Programs also allow for visibility of related privacy Risks a Tasks. Dependent on the size and structure of your organization, several independent programs can be created to allow for more granular reporting and customised assessments on separate areas of the business. For example, organisations may want to separate programs by directorate, geographical location or department.

Privacy Assessments

Privacy Assessments can be delivered to employees to understand how they are processing personal data in their business areas. Questions can be customised to suit organisational requirements. Completion of assessments can create multiple records across one or several different registers.

Registers

Processing Activities

A Personal Data Processing Activity is an activity or task that is completed as part of a Business Process. For example, 'CV Collection' would be a Personal Data Processing Activity that is part of the 'Recruitment' Business Process alongside several other Processing Activities.

Business Process v Personal Data Processing Activity Example:

Data Record

Data subjects are individuals whose personal data is being collected, held, or processed. A Data Record is defined by the Type of Data Subject and their region of residency, and finally who controls the personal data to be processed. The Data Record is utilised across all the Processing Activities via a Processing Event, this allows data can be tracked through its lifecycle and visualised with lineage maps.

Business Process

A Business Process is a collection of related, structured processing activities or tasks that produce a specific service or product. For example, 'Recruitment' would be a Business Process that takes place within a Human Resources department.

Business Area

The Business Area register allows for organisational departments, business units/areas to be added as register records which can be displayed in Privacy Assessments. This allows for business areas to be linked to other register records (such as processing activities and processing events), which can then be filtered and reported on.

Business System

The Business System register defines all the internal business systems in your enterprise at a high level. A business system can be a software solution or a collection of technical or physical components called Assets. (See Asset Register). A business System is defined to be external, to be in a location and the data it holds, by a sum of its assets. A business System by itself cannot define these.

Asset

The Asset register defines all the technical or physical assets in the enterprise where the data operations are managed solely by the internal organisation, even if the service is owned and run by a third party as a service. In some cases the Asset could be seen as the 'child' of a Business System

Data

The Data register defines all the individual data elements in your enterprise. These elements are common across all the processing activities. It is used as an integral part in forming the definition of a 'Data Record', the processing event is used to hold the relationships to create this definition. A specific role of the Data Register is to hold the organisations classification of the data.

Third Party

Business/organisations that manage or supply external business systems/applications are regarded as Third Party Entries in the system, rather than similar Legal Party Entities who manage data processing under contract. Even though both can be regarded as Data Processors from a regulatory perspective.

Legal Entity (Legal Party)

Legal Party or registered businesses are responsible or active in activities involving the processing of personal data

Legal Parties can be either Internal or External.

- o **Internal Legal Parties** can identify the different parts of your organisation, which can represent both regional and global entities.
- o **External Legal Parties** identify business which support your data processing and are typically data joint controller, external Controller, Processors and Sub processors.
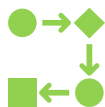
Processing Event

Processing Event is a defined action which stated the resources used in the processing of personal data within a named Processing Activity. The types of possible processing events are Storage (planned), Collection, Source, Processing, Access & Transfer

Please see below an overview of the different processing events types available.

Event	Description	Flow
Collection	Data collected from Data Subjects Directly	IN
Source	Data sourced from Assets or other legal parties	IN
Processing	Use, creating or management of Personal Data	CREATE
Storage	All data needs to be stored to be processed.	STORE
Access	Data that is accessed/viewed as part of a process but remains within internal systems	OUT
Transfer	Data is moved/copied to another system or third party.	OUT

Evidence/Controls

Data Protection and security regulations promote appropriate use of technical and organisation controls for use by controllers and processors when processing personal data. The type of control deployed by an organisation depends on the type and conditions of processing (Who, where, why) and the sensitivity and criticality of the data used.

Risk Register

The risk register allows for risks can be created and linked against multiple records and registers.

Task Register (Risk Mitigation Activities)

The task register allows for risks can be created and linked against multiple records and registers.

RuleBase

The RuleBase logic can be used to automate processing data flows using simple rule-based scenarios. A predetermined rule can result in either a risk, task or email being actioned.