Record of Processing Activity Guidance

Document Control

Policy Owner	PPCR – Data Privacy and Compliance Team
Responsible Person's Job Title	Data Privacy and Compliance Team Leader – XXXXX
Accountable Person's Job Title	Head of Data Privacy and Compliance – XXXXX
Consultation	N/A
Informed	DPC Team, Key Stakeholders
Review Schedule	Yearly
Last Approval date	
Next Review date	
Version Number	V1.0

Version Control (Change History)

Version	Reason for Change	Author (Full Name, Role Title)	Date
v1.0	Original document created and approved	XXXXX, Data Privacy and Compliance Practitioner	
v0.0			

Distribution List

Date	Method of Distribution	Roles

Contents

Key messages

- **The Data Privacy and Compliance (DPC) team are responsible for ensuring Record of Processing Activity (ROPA) is maintained and kept up to date.**
- **The DPC team will maintain strong relationships with the relevant Data and Information Managers and Stewards to ensure the ROPA is known among their business areas.**
- **All staff to ensure compliance with the UK GDPR and DPA 2018 ROPA requirements are met and maintained.**

Purpose

This document offers guidance to all TPR staff in how to complete a ROPA entry and maintain the ROPA to a high standard.

Scope

This document is intended for all TPR staff who are tasked with managing their business areas ROPA entries and how the DPC will support them.

The ROPA

The accountability principle requires us to demonstrate that TPR processes personal data in line with the UK GDPR and DPA 2018. Along with our privacy notices, DPIAs, internal policies and procedures the ROPA is key to ensuring TPR's compliance. Article 30, states that an organisation shall:

"…maintain a record of processing activities under its responsibility."

Further information and guidance from the ICO can be found here, What is documentation? | ICO.

TPR's ROPA can be found here, Data Privacy & Compliance - Records of Processing Activity - All Items.

Team Responsibilities

What is expected of the DPC team and key stakeholders.

DPC Team

- Monitor and review entries
- Engage with teams Data and Information Managers and Stewards to ensure ROPA is accurate and up to date at time of engagement

Data and Information Managers and Stewards

- To support DPC team create any missing entries for their team
- Review team related entries

Entries

You can find step by step guidance on what is required for each ROPA entry in Annex A. When submitting a new entry, you do not need to know everything from the beginning. However, the following fields are required to save and submit a new item.

- Directorate
- Purpose of Processing
- Categories of individuals

For guidance on how to complete an entry, please refer to Annex B.

When a new entry is first created, an automated email will be sent to the DPA inbox (DPA@tpr.gov.uk) and member of the DPC team will be allocated to review the entry.

Review/Sign-off

When submitting an entry, the DPC team will be notified. A review will be conducted by a member of the DPC team who will confirm any outstanding questions they may have before sending off.

Related policies

- Appropriate Policy Document - TPR Corporate Policy.docx
- Safeguards TPR Corporate Policy.docx

Annex A

ROPA Question	Guidance
ROPA Reference	Unique identifier, created automatically, assigned to this processing activity to ensure it can be tracked, reviewed, and audited effectively.
Directorate	The directorate within TPR that is responsible for overseeing the processing activity.
Department	The department carrying out or accountable for the processing of personal data.
Team	The team directly responsible for managing and executing the processing activity.
Data and Information Owner & Deputy	The senior individual accountable for the data set, with a named deputy who assumes responsibility in their absence. An update list can be found on the register,
Process Owner	The individual responsible for ensuring the processing activity is performed in compliance with policies, procedures, and data protection legislation. Likely to be Data and Information Manager
Business Function	A description of the business area or function that the processing supports (e.g. HR, Finance, Customer Services).
Purpose of Processing	Clear explanation of why the personal data is collected and how it is used to meet organisational or legal objectives.
Categories of individuals	Types of data subjects whose personal data is processed (e.g. employees, customers, suppliers, service users).
Categories of Personal Data	Description of the types of personal data processed (e.g. contact details, employment information, financial data, special category data).

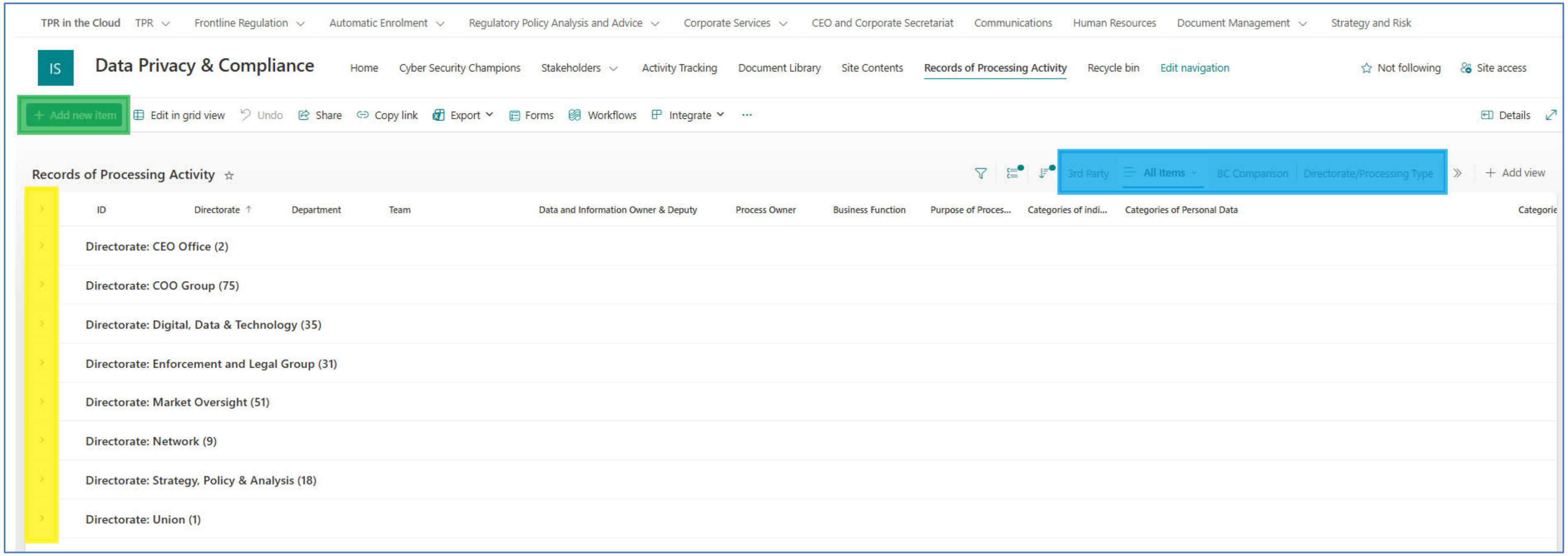
Categories of recipients	Details of internal teams or external organisations that receive or have access to the personal data.
Article 6 Lawful Basis	The lawful basis under UK GDPR Article 6 relied upon for processing personal data (e.g. contract, legal obligation, public task). Chose the most appropriate option(s)
Article 9 Lawful Basis	Where applicable, the additional condition under Article 9 for processing special category data (e.g. employment law obligations, public health). Chose the most appropriate option(s)
6(1)(a) Consent or 9(2)(a) Explicit Consent Record (if applicable)	Details of how consent is obtained, recorded, managed, and withdrawn where consent is relied upon.
Article 6(1)(f) Legitimate interests for the processing (if applicable)	Explanation of the legitimate interest pursued and why the processing is necessary and proportionate.
Has a record of legitimate interests assessment been completed?	Confirmation that a Legitimate Interests Assessment (LIA) has been completed and documented where applicable.
What is the Data Protection Act 2018 Schedule 1 condition for processing?	Relevant condition under Schedule 1 permitting the processing of special category data where required. Review alongside Appropriate Policy Document - TPR Corporate Policy.docx to ensure correct condition is used for processing special category and criminal offence data.
What is the Data Protection Act 2018 Schedule 8 condition for processing?	Applicable law enforcement processing condition under Schedule 8, if processing is for law enforcement purposes. Review alongside Safeguards TPR Corporate Policy.docx to ensure correct condition is used for law enforcement purposes when processing special category and criminal offence data

What is the source of the personal data?	Description of where the data originates (e.g. directly from individuals, third parties, public sources).
What rights are available to individuals?	Summary of applicable data subject rights, such as access, rectification, erasure, restriction, portability, and objection.
How long is the personal data retained for?	Defined retention period based on legal, regulatory, or business requirements.
General description of technical and organisational security measures (if possible)	Overview of safeguards in place, such as access controls, encryption, training, and policies to protect personal data.
Is there any automated decision-making included in the processing?	Statement confirming whether automated decision-making or profiling is used and, if so, how it operates.
What system is the personal data kept?	Details of the systems, applications, or platforms where personal data is stored and processed.
Link to contract with processor	Reference or link to the contract governing processing by third-party processors.
Contract Data Relationship	Clarification of roles (e.g. controller, joint controller, processor) in relation to the data processing. Chose the most appropriate option.
Do we transfer the personal data to third countries or international organisations?	Confirmation of whether personal data is transferred outside the UK.
What safeguards are there for exceptional transfers of personal data to third countries or international organisations (if applicable)	Description of safeguards such as adequacy decisions, SCCs, or other approved mechanisms.
Link to Data Protection Impact Assessment	Reference or link to the DPIA where one has been completed. This can be provided by the DPC team.
Link to retention and erasure policy document	Reference or link to the organisation's retention and disposal policy.

Is personal data retained and erased in accordance with the policy document?	Confirmation that retention and deletion practices follow the approved policy.
Reasons for not adhering to policy document (if applicable)	Explanation of any justified deviations from the retention policy.
Assurance review date	The date on which the processing activity was last reviewed for compliance and accuracy.
Inherent Risk impact score	Assessment rating of the potential impact on individuals if risks materialise, see appendix C – Risk Assessment and GDPR
Inherent Risk Likelihood Score	Assessment rating of the likelihood of risks occurring in the absence of controls, see appendix C – Risk Assessment and GDPR.
Reviewed by	Name and role of the individual who conducted or approved the review.
Next scheduled review	Planned date for the next review to ensure the record remains accurate and up to date.
Business Critical Process	Choos Yes or No
BC Service ID	If yes, to the above, please enter the BC Service ID. This can be obtained from the BC Team
Link to Data Sharing Agreement	Identify any DSA here: Data - Data Sharing Agreements (signed records) - All Documents.

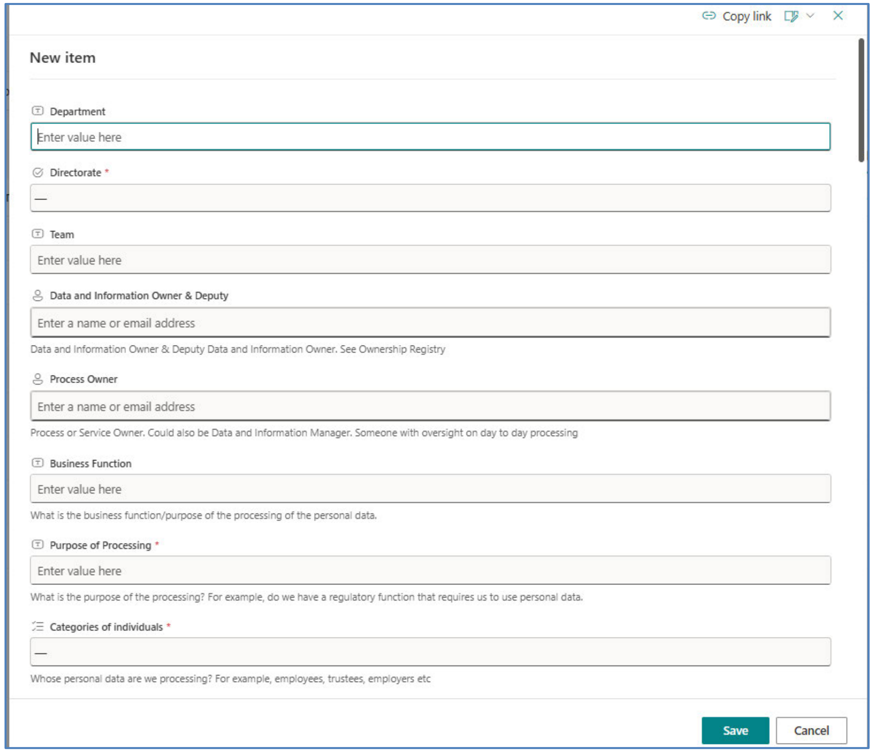
Annex B

The initial screen on the ROPA should look like the below. There are a variety of pre-set views you can select, highlighted blue. Entries are organised by directorate and then by department, highlighted yellow. You can add a new entry by clicking on the '+ Add new item' button, highlighted green.



Document Classification: Official

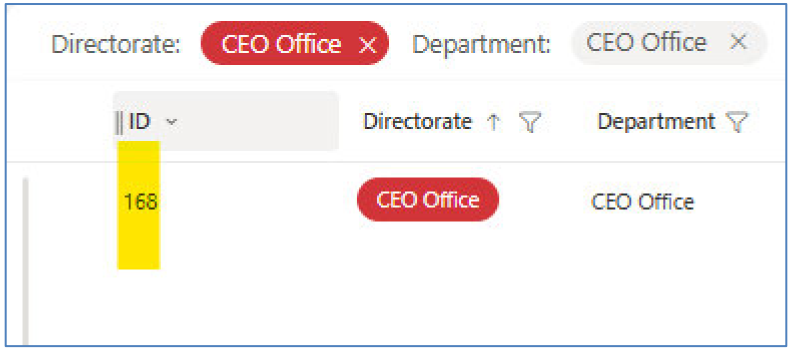
When you click on '+ Add new item' button, a list of all the columns will appear as seen below. See Annex A for what every column should be populated with. There are 3 required columns to submit a new item for the ROPA. These are:



1. Directorate
2. Purpose of Processing
3. Categories of individuals

For a ROPA entry, not all the information might be known when creating an entry and this is fine as the ROPA is a live document subject to changes as and when required.

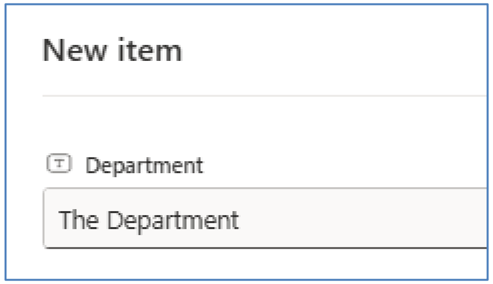
All new entries will be given a new ID reference, highlighted yellow below. These references should be used in DPIAs.



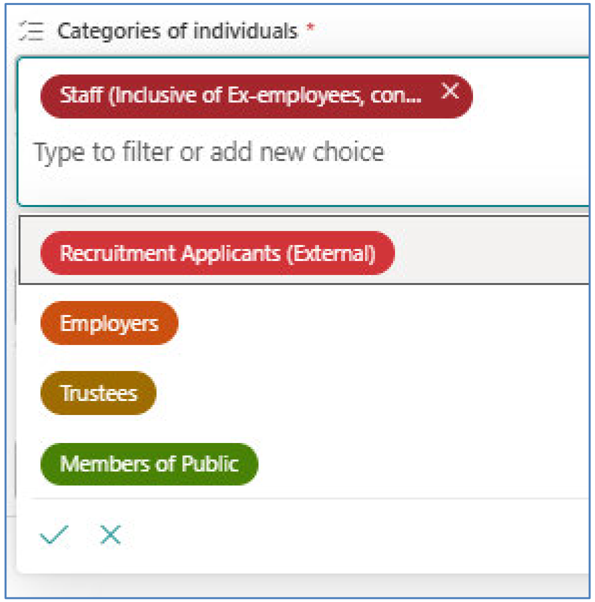
Document Classification: Official - Sensitive

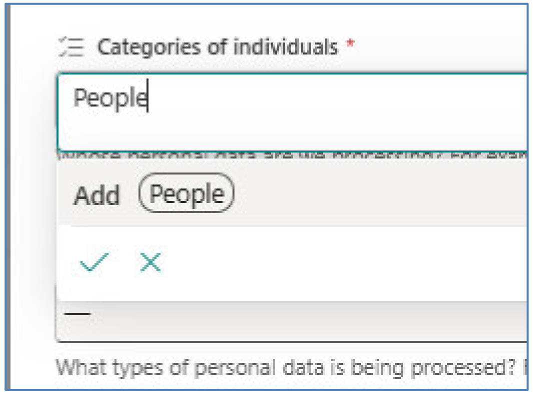
When going through the '+ Add new item' button route, there are a variety of columns settings that require different actions. For example:

- Lines of texts – Allows you to input what wording you like.

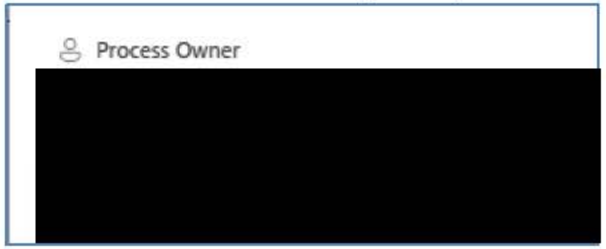


- Choice – Allows you to choose a pre-inputted choice or add a new one. When adding a new one, this will them become a pre-inputted choice for future entries. Some of 'choice' columns will allow you to input multiple entries others may not.

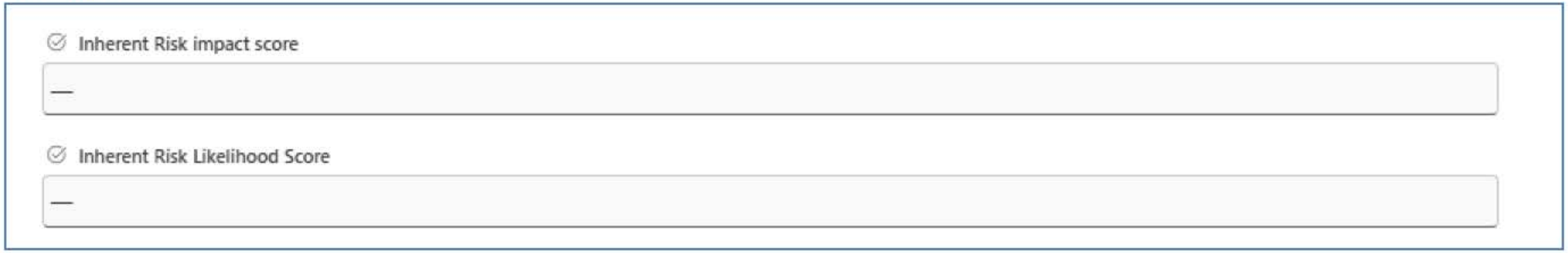




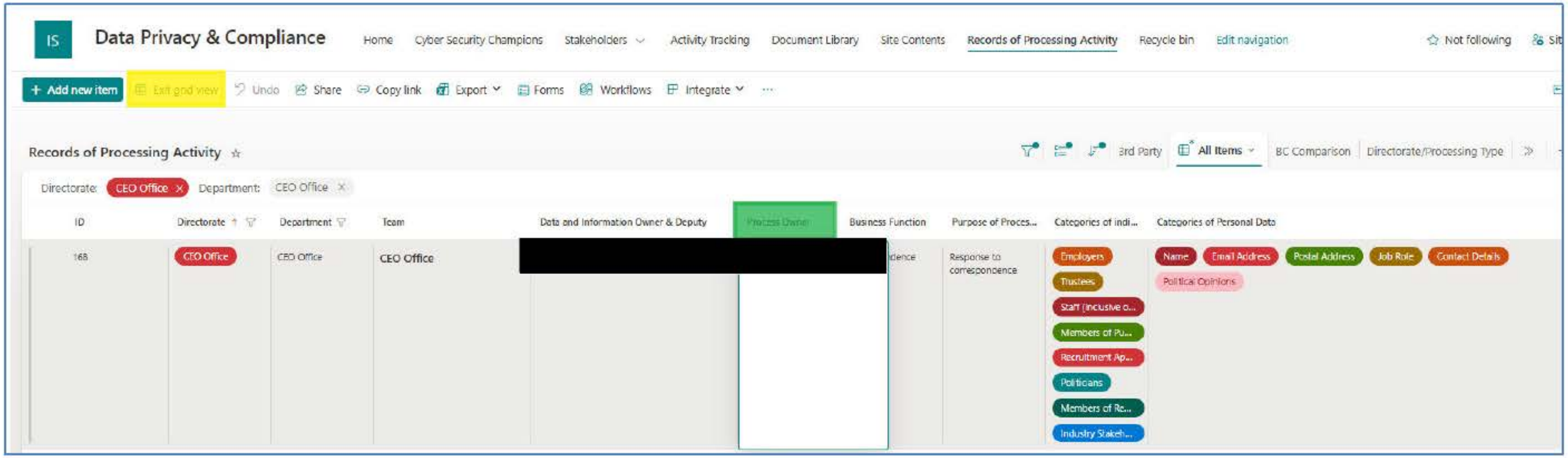
- Person – This should allow you to pick a staff member from the active directory.



- Risk Scores – The risk score should be identified using the risk metrics on contained in our DPIAs, see appendix C – Risk Assessment and GDPR

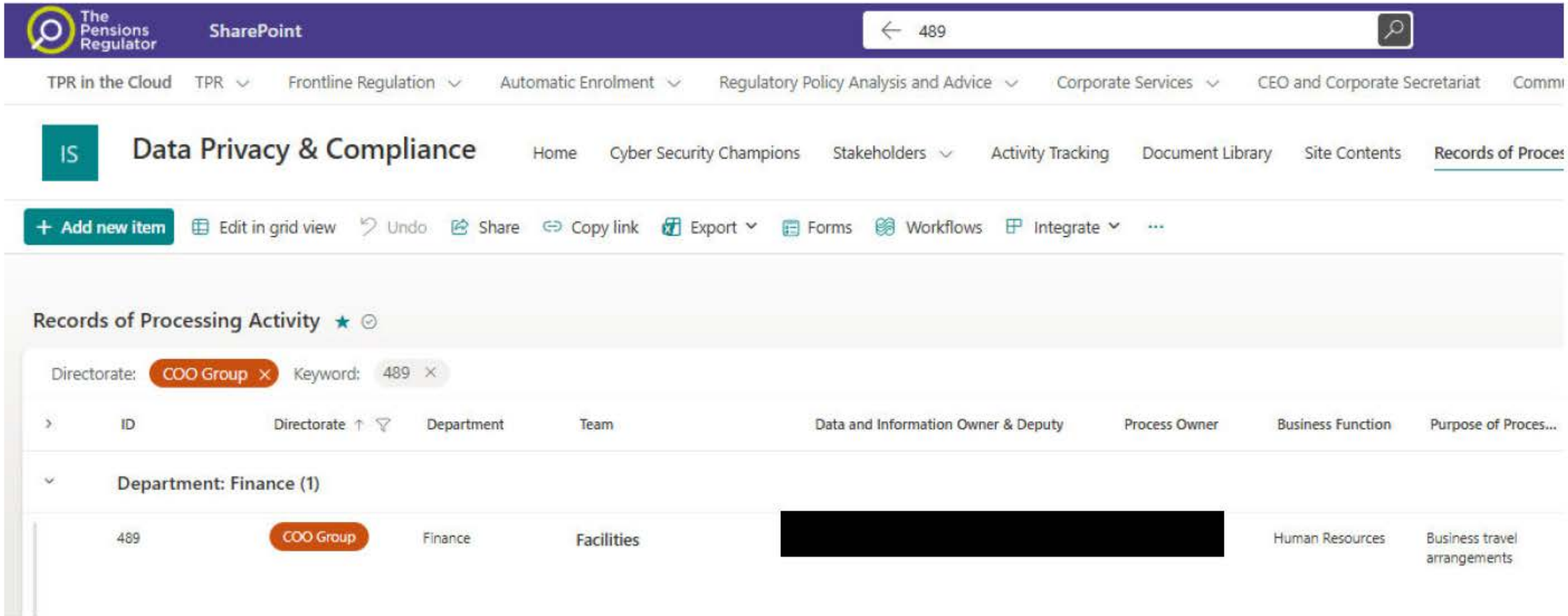


You can also edit entries in the grid view. You can do this by pressing the 'Edit in gird view', highlighted in yellow. Here you can edit columns for a specific entry as you please. The column you select will pop out for you to edit, highlighted in green in for the 'Process Owner' column. You can also copy and paste column entries into others. However, I would warn that sometimes the functionality for this can break your editing session. Make sure you press the 'Exit grid view' to save your changes.



Document Classification: Official

You can find entries through following the layout of directorates and then departments. It is also possible to find specific entries if you have the ID reference or an identifier like the Business Function. See below



Document Classification: Official - Sensitive