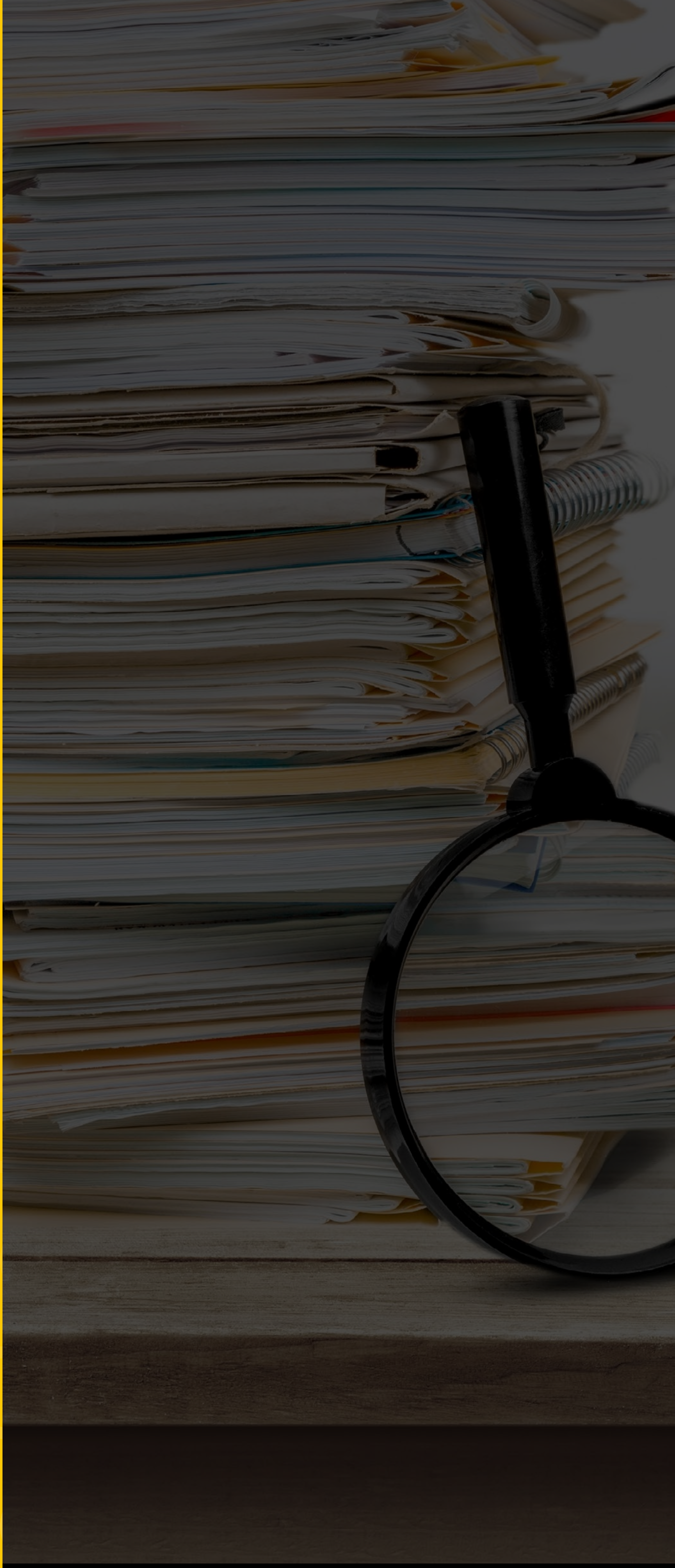
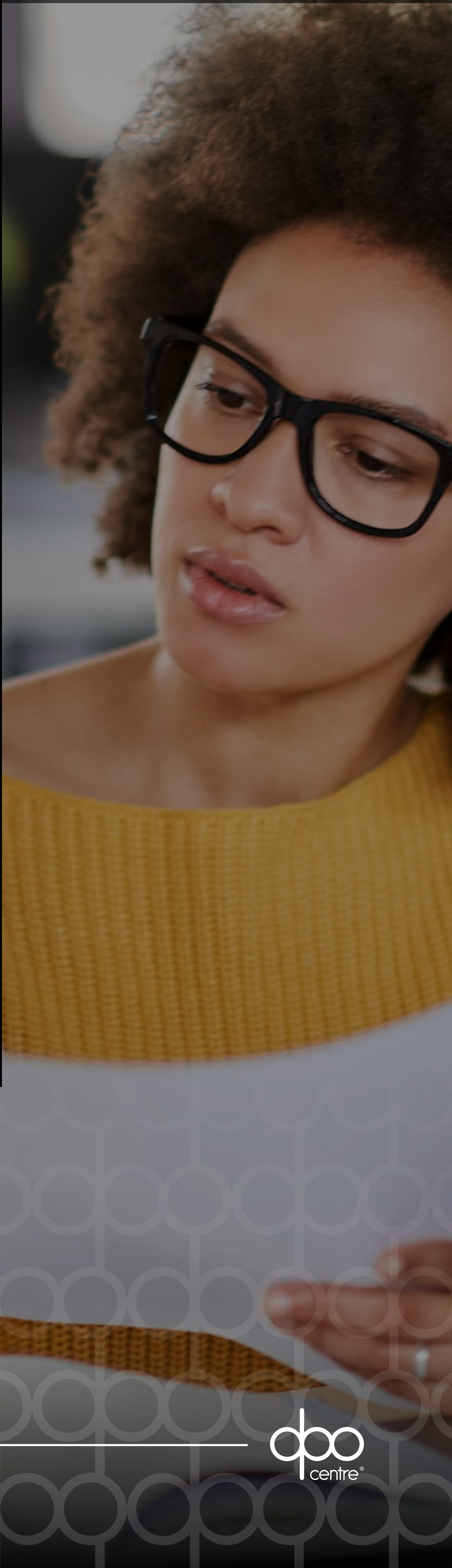
GUIDE TO BUILDING A RECORDS OF PROCESSING ACTIVITIES (RoPA)



www.dpocentre.com

dpo centre®

CONTENTS



1. ABOUT THE DPO CENTRE

The DPO Centre is a specialist data protection and compliance consultancy, providing data protection related services to over 600 clients from a wide variety of sectors, ranging from commercial, financial services, tech, health, education, and 3rd sector organisations.

Formed in July 2017, The DPO Centre has a large team of permanently employed Data Protection Officers (DPOs) located throughout the UK. Every member of this team is an experienced DPO who is knowledgeable and highly adaptable, so can deliver the exact level of support required and in the precise manner you require it.

The DPO Centre is based in London and Dublin and has a network of offices across Europe.

Further information on the company, staff and our services can be found on our website.

BRISTOW & SUTOR
Cera
Clinisupplies
egress
Hughes The Electrical Experts
Inivata
NSPCC
optos
PHIN
SlimFast
VenatoRx PHARMACEUTICALS
WSC WEST SUFFOLK COLLEGE

2. INTRODUCTION

Since coming into force in 2018, the European General Data Protection Regulation ('GDPR') and the Data Protection Act 2018 ('DPA') (and since the 1st of January 2021, the UK GDPR ('GDPR')), have required organisations to do more than ever before in terms of their data protection and information security practices. An important aspect of this has been the demand for accountability, which is one of the seven data protection principles outlined in Article 5, with which all organisations under the GDPR must comply. This principle states that organisations must take responsibility for complying with the rest of the GDPR but, crucially, they must also be able to **demonstrate** their compliance. Organisations are expected to demonstrate their compliance in a number of ways, these include:

- Implementing clear data handling procedures
- Producing and adhering to privacy policies
- Undertaking all-staff training on data protection and information governance
- Conducting Data Protection Impact Assessments (DPIAs), when required
- Signing Controller-Processor contracts and data sharing agreements

Being able to demonstrate compliance requires organisations to be more transparent than ever before about their processing of personal data. Transparency is also a key data protection principle which is closely linked to the rights that the GDPR gives to individuals, particularly the right of access and the right to be informed.

A key part of complying with the demands for accountability and transparency for most organisations is building a Records of Processing Activities ('RoPA'). Depending on the size of the organisation and the processing activities it undertakes, these documents can be very large and complex. They can also be very time-consuming to create as there are many steps involved, including understanding all processes and data; risk appraising; and identifying any Data Processors, data sharing and international transfers.

This guide aims to assist you in building and maintaining your organisation's RoPA. It will introduce you to what a RoPA must include and the steps you should take to gather this information and record it correctly. It is important to note that this is a general guide not tailored to your specific organisation or sector, and the examples given throughout are not exhaustive. Therefore, if you are unsure on anything you should seek further advice from your Data Protection Officer ('DPO') or from a specialist such as The DPO Centre.

3. WHAT IS A RECORDS OF PROCESSING ACTIVITIES (RoPA)?

A RoPA, as the name suggests, is a document in which an organisation's processing activities are recorded (an example for both a Data Controller and Data Processor can be found in Appendix A). At its most basic level, this involves recording the 'who', 'what', 'why' and 'how' of processing:

- Whose personal data are you processing?
- What types of personal data are you processing?
- For what purpose are you processing personal data?
- How are you processing the data / what processing activity are you undertaking?

A processing activity is any activity that is performed on personal data e.g. collection, recording, structuring, storage, adaptation or alteration, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. As such, they can be extremely big documents and may appear daunting to create. However, they are essential for most companies (see Section 3.1) in order to fulfil transparency requirements and demonstrate compliance with the GDPR pursuant to Article 5(2) – the Accountability Principle. The Information Commissioner's Office ('ICO'), or another relevant supervisory body, can request to see your organisation's RoPA. Therefore, it is essential that it is accurate and kept up to date.

A list of example processing activities, categorised by business department, can be found in Appendix B.

4. WHEN AND WHY DO YOU NEED A RoPA?

RoPAs are governed by Article 30 GDPR. Paragraphs 1 and 2 stipulate that every Controller and every Processor - or their Representative if established outside of the UK/EU - must maintain a RoPA. However, paragraph 5 gives some exceptions to this rule, stating that the requirement to maintain a RoPA does not apply to organisations employing fewer than 250 persons unless:

- **The processing it carries out is likely to result in a risk to the rights and freedoms of data subjects**
  Determining whether this applies will involve undertaking risk assessments to understand the nature, scope, context, and purposes of processing and the likelihood and severity of the risks to data subjects.

- **The processing includes special categories of personal data or personal data relating to criminal convictions and offences**
  Special category data types are listed in Article 9(1) GDPR and include: racial or ethnic origin, political opinions, religious beliefs, and health data. Personal data relating to criminal convictions and offences are outlined in Article 10 GDPR.

- **The processing is not occasional**
  This will only apply if processing plays a subordinate role in the activity and occurs for a very short time or once. For example, informing clients of a change of address after relocating. If some processing takes place on a structured basis, as in most companies, processing will be classed as more than occasional.

In reality, these limits mean that very few organisations, even those employing less than 250 people, are exempt from the requirement to have a RoPA. Therefore, it is most likely that your organisation will need one.

4.1 IF YOU ARE NOT REQUIRED TO HAVE A RoPA, WE STILL SUGGEST YOU DO!

As already mentioned, most organisations will be required to have a RoPA to fulfil their obligations under Article 30 GDPR. However, outside of complying with the law, there are other benefits of having a RoPA as outlined below:

1. **Responding to Data Subject Access Requests ('DSARs')**
   Having a clear record of how the personal data in question is being processed will enable staff to find it more easily and facilitate a prompt and accurate response to the request which will enable you to uphold individuals' rights.

2. **Risk identification**
   Understanding how each data set is handled will allow for future risks to be identified early on and then steps taken to mitigate them. This will support good practice in data governance.

3. **Demonstrating compliance**
   Even if not required to have a RoPA by law, all organisations have to comply with the transparency and accountability principles and having a RoPA will contribute to demonstrating that you are complying with them.

The additional merits of having a RoPA, other than complying with Article 30, mean that we recommend all organisations, regardless of size, create and maintain one.

5. CREATING YOUR RoPA

Once you have determined whether you are required to have a RoPA, or whether you would benefit from having one, you need to begin the creation process.

A RoPA should be in writing, either on paper or in electronic format. This can be as sophisticated or as unsophisticated as you wish. Whilst there are compliance tools in the market to produce RoPAs, or "Article 30 Records", such as OneTrust's Privacy Platform, building a RoPA does not necessarily need that level of investment. However, the more you invest in tools, the more features you will have accessible to you in terms of automated data mapping and linkages to other tools (such as vendor assessments, Data Protection Impact Assessments etc). In most instances, a simple Spreadsheet, (like the one at Appendix A) will be sufficient. The key issue for compliance is the content of your RoPA, not how much you have invested in completing it.

Creating a RoPA will not be just one individual's responsibility, whether that be the DPO or, if your organisation does not have a DPO, the designated RoPA Creator. A collaborative approach between them and various managers or owners responsible for processing data will need to be undertaken. Adequate time and resources should be allocated to the RoPA Creator and the business areas to provide the salient information needed to complete the RoPA.

5.1 WHAT INFORMATION SHOULD BE INCLUDED?

Article 30 prescribes the key information that your RoPA should include. It is important to note that this will vary depending on whether you are a Data Controller or a Data Processor, so you need to be clear on which category you fall into. Note that for some processing activities your organisation may be a Controller, and for others it may be a Processor. If this is the case, you will need to have a different section for each within your RoPA e.g. two different Excel tabs. The same applies for if you are a Joint Controller for any processing activities.

5.1.1 DATA CONTROLLERS

If you are a Data Controller or a Data Controller's UK Representative, as a minimum your RoPA must include:

- Your name and contact details and, where applicable, the name and contact details of the Joint Controller, the Controller's UK Representative, and the DPO
- The purposes of the processing e.g. payroll
- A description of the categories of data subjects e.g. employees, and the categories of personal data being processed e.g. name; DOB; email address; NI number; passport number
- The categories of recipients to whom the personal data has been or will be disclosed e.g. payroll provider
- Details of any transfers to third countries or international organisations, including information about the transfer mechanism in place e.g. adequacy, standard contractual clauses ('SCCs') etc.
- The retention schedules for each dataset
- A general description of the technical and organisational security measures in place e.g. encryption, access controls

5. CREATING YOUR RoPA CONT.

***5.1.2* DATA PROCESSORS**

If you are a Data Processor, or a Data Processor's UK Representative, as a minimum your RoPA must include:

- The name and contact details of the Processor or Processors, and of each Controller on behalf of which the Processor is acting, and, where applicable, the name and contact details of the Controller's or the Processor's UK Representative, and DPO
- The categories of processing carried out on behalf of each Controller
- Details of any transfers to third countries or international organisations, including information about the transfer mechanisms in place
- A general description of the technical and organisational security measures in place

Please note that this is the minimum information required. However, it may be useful to document additional information within your RoPA, as outlined in section 5.1.3.

***5.1.3* OTHER INFORMATION YOU COULD INCLUDE IN YOUR ROPA**

- Information required for privacy notices:
  - The lawful basis for processing
  - Where applicable, the legitimate interests being relied upon
  - Individuals' rights
  - The existence of automated decision making
  - The source of the personal data
- Where applicable, records of consent
- Controller-Processor contracts
- The location of the personal data
- Data Protection Impact Assessment reports
- Records of personal data breaches
- Information required for processing special category data or criminal conviction and offence data under the DPA 2018:
  - The condition for processing
  - The lawful basis for processing
  - Retention and erasure policy

Although not essential, this information is useful to have within your RoPA as it will help to inform your Privacy Notice.

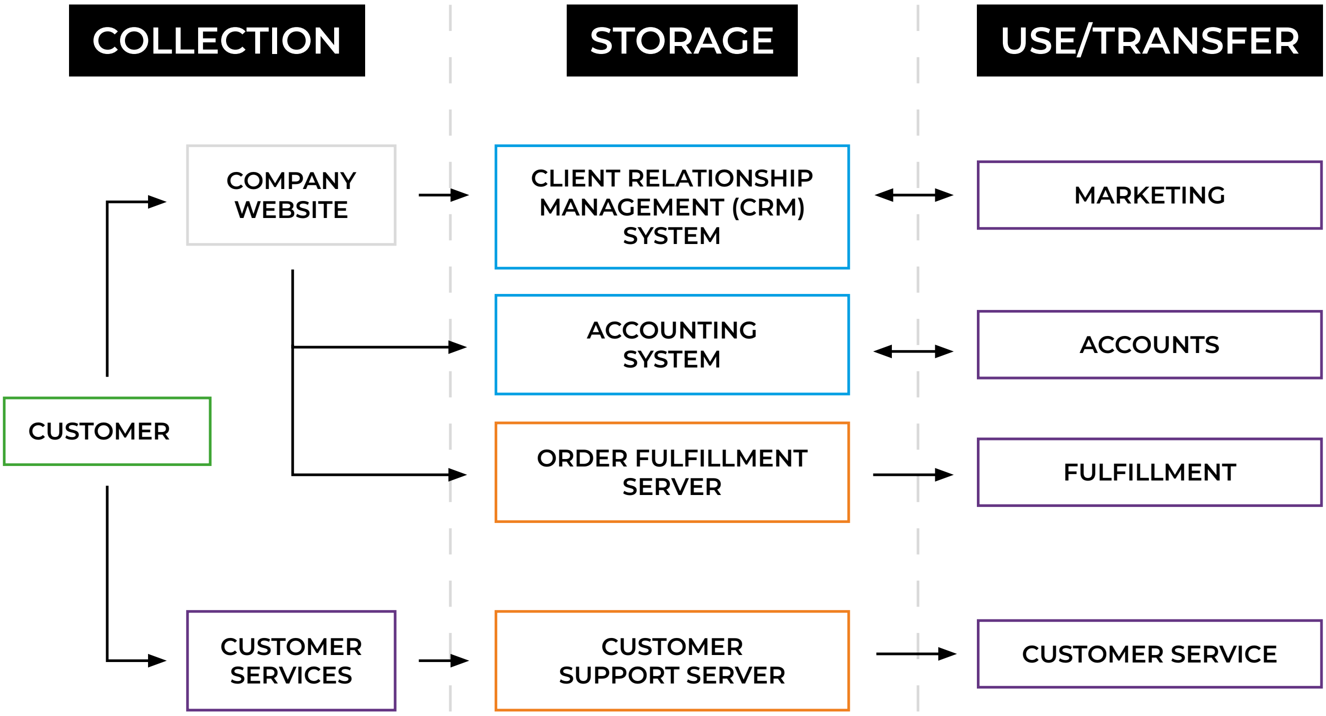
Furthermore, keeping records of your Data Processor Agreements, DPIAs and breaches in one place is worthwhile because it will make it easier for you to demonstrate compliance with the GDPR principles, particularly the Accountability principle.

5. CREATING YOUR RoPA CONT.

5.2 HOW TO BUILD YOUR ROPA

Beginning to create a RoPA can seem daunting due to the amount of information that you have to gather, which most likely will be in a wide variety of places and managed by lots of different departments. However, here we outline some key steps that may help you when creating your RoPA.

Step 1 – Data mapping
It is essential that before creating a RoPA, you first understand what personal data your organisation processes and where. Data maps show the flow of data through your organisation. Information in a data map includes where you source the data from, where it is held, what processes it is involved in, and where and how it is transferred. They will also help you to identify the processes for which your organisation is the Data Controller, Data Processor or Joint Controller. This will then determine what information you need to gather for each process when you begin. Data maps can be produced by individuals within each department who are likely to know best what their department does with the personal data they receive. Once you have this information, it will be much easier to ensure your RoPA is accurate and comprehensive.



🟩 Data Subject
🟪 Company Department
🟧 Electronic Data Store
🟦 Third Party Processor

Fig 1. Data map example for a B2C sales company

5. CREATING YOUR RoPA CONT.

Step 2 – Data collection: Questionnaires
If you have departments which have some level of pre-existing data protection knowledge, you may encourage them to do some preliminary work in identifying their processes and capturing some of the salient information you would be looking to capture as part of their data collection session. You may in fact wish to share a copy of Appendix B from this white paper with them, which lists a range of example processing activities for each business function.

If you would like to add some structure to the preliminary work, you may wish to utilise a Process Discovery Questionnaire (our example can be found at Appendix C). Whilst we do not necessarily expect that service leads, process owners etc. will complete these in their entirety or 100% correctly, an attempt at capturing some of the required information for a RoPA will be of help to the RoPA Creator.

The questionnaire we have provided is in two parts. Part 1 is to help the RoPA Creator understand the service and Part 2 is to understand each of the key processes. In a Human Resources context, we'd expect the Director of HR (or similar) to fill out Part 1 for their service and then multiple Part 2's for their respective processes, i.e. Payroll, Grievances, Sickness Management, Disciplinaries etc. It is then the role of the RoPA Creator to transpose the questionnaire findings, highlight any errors, compliance risks or areas which need further investigation or scrutiny, in the respective service meetings.

Step 3 – Data collection: Meet with key business functions
Meeting directly with members of your organisation's key business functions will enable you to fill in any gaps left by the questionnaires and better understand how departments within your organisation process data. In order to build the RoPA, the RoPA Creator will require oversight of all business areas which process personal data.

It is recommended that meetings are scheduled in turn with the key heads of service, heads of department, directorates etc. When identifying the relevant departments to arrange meetings with, it is important that you ensure that you do not focus solely on your 'customer' or main line of business processes, it is critical that you include your business's support service processes (i.e. Human Resources, Finance etc.) as these services process personal data too (in some instances, this will be sensitive special category data).

Step 4 – Data collection: Review policies, procedures, contracts, and agreements
Policy and procedure documents may contain some of the information that you need to include in your RoPA, such as retention schedules. They can also be compared against actual data processing practices to see if policies and procedures are being followed in practice, indicating where improvements may need to be made.

For transparency and accountability purposes, it may be expedient to include a link to, or document, where any relevant data sharing agreements, Controller-Processor agreements, and DPIAs can be found.

5. CREATING YOUR RoPA CONT.

Step 5 - Documentation
Once you have completed the data collection phase, you need to put all this data into one document – your RoPA. As already mentioned, this can be in paper or electronic form, but it is recommended that you store your RoPA electronically because this way it can be easily added to or amended. An example of a RoPA in an electronic form can be found in Appendix A.

The processes you document in your RoPA should be split up according to whether you are the Data Controller, Data Processor, or Joint Controller for that process. These should all be on different pages/tabs/tables to make it clear what role your organisation plays in each process.

The ICO states that when documenting your processing activities, it must be done in a 'granular and meaningful way'. This means that you must document the information required (as listed in section 5.1) for each and every process; you cannot merely have a general list of categories of personal data or types of data subjects whose data you process.

In order to consolidate these requirements in a ready-usable format, we have produced two templates at Appendix A (one for instances where you are acting as a Data Controller and the other for you as a Data Processor).

5. CREATING YOUR RoPA CONT.

5.3 COMPLETING THE ROPA TEMPLATE

As indicated in the, Creating your RoPA, section, there does not need to be a significant degree of technological sophistication to your RoPA. The value of the RoPA is dictated by the quality and the accuracy of the information contained within. You need to ensure that the information it contains reflects the requirements of the legislation.

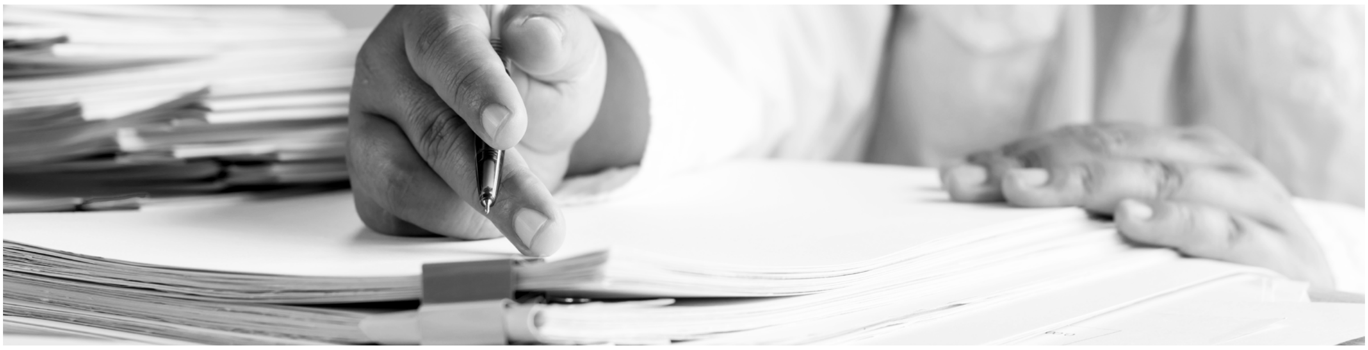
5.3.1 HOW DETAILED OR GRANULAR SHOULD YOUR ROPA BE?

You need to ensure that your RoPA details all of your personal data processing activities. There are no specific rules around how granular or detailed your RoPA necessarily needs to be. Some Controllers or Processors may prefer to drill down into specific lower-level functions, i.e. from a Human Resources perspective you may see separate RoPA entries for sickness at work, grievances, disciplinary hearing, performance management etc. whereas some other authors may classify this under the same umbrella as 'staff administration'. The minimised approach is advocated by the ICO on their website. It should, however, be noted that whilst you can flex your degree of granularity in terms of listing processes, the actual content that you need to record for each process should not alter from the requirements of Article 30 of the GDPR (see Section 5.1.1 and 5.1.2).

Ultimately, the decision regarding the level of detail is up to you. There are advantages to both approaches. In terms of a more detailed approach, it allows the author to risk appraise and identify remedial activity for each individual aspect of the department's processing activity whilst completing RoPA entries for each. This level of insight may be lost if individual processes are amalgamated into a broader category of 'staff administration'. Similarly, a higher level of detail could present you with more ready-made information to translate into your Privacy Policies. However, it must be noted that the 'detailed' approach comes at the expense of time and resources which often the RoPA Creator (potentially the DPO) and the departments may not necessarily have. The aggregated approach would obviously demand less time and resources to complete, but you need to rationalise whether this would give you the level of detail and the opportunity to remediate and risk assess that you will necessarily need.

If your desire is to achieve the minimal standard, we would draw your attention to the example aggregation cited by the ICO as a baseline that you should not fall below. If you work in other jurisdictions than just the United Kingdom, we also suggest that your refer to the respective supervisory authorities for any guidance or any local requirements which apply to creating your RoPA.

5. CREATING YOUR RoPA CONT.



5.4 DO I NEED TO SHARE MY ROPA OR PUBLISH IT ON MY WEBSITE?

There is no legal requirement to publish your RoPA anywhere. However, you must be able to make it available for inspection at the request of the ICO, or another supervisory authority. Therefore, whilst it should be stored in a secure place, it needs to be easily accessible to those authorised to do so.

Although you do not have to publish your RoPA, you must still pay overall attention to the data subjects' right to be informed. The right to be informed relates to the principle of transparency and is about being open and honest with data subjects about what you do with their data. As such, if you are complying with the principle of transparency and respecting data subjects' right to be informed, it is likely that a significant amount of the information that is in your RoPA will already be published in your Privacy Notice. Therefore, you may feel that there is no harm in publishing your RoPA. It must be noted, however, that if you do so, you may wish to redact some of the information, for example, regarding the security measures you use to protect the data, as this may risk the security of any information you hold.

A final point to note is that if your organisation is a public authority and subject to the Freedom of Information Act 2000, you may be compelled to disclose your RoPA if you receive a request for it.

TOP TIPS FOR CREATING YOUR ROPA

1 *Undertake data mapping before you start to create your RoPA*

2 *Delegate responsibility to Process Owners for documenting their processes*

3 *Ensure your RoPA is stored securely and backed-up to prevent loss*

6. MAINTAINING YOUR RoPA

The RoPA is only a snapshot in time from when it was created. Businesses, processes, and data processing activities constantly change, improve, and evolve. It is the responsibility of the RoPA Creator and the Process Owners to ensure that when changes are made, the RoPA is amended to reflect that change. Making amends to your RoPA should be a key component of your change control processes, along with other Data Protection considerations such as Data Protection by Design and Default, Data Protection Impact Assessments, amending Privacy Policies etc. Failure to reflect any changes in your RoPA could ultimately lead to non-compliance with the requirements of Article 30, the right to inform and the principle of accountability. It is important that your RoPA Creator and Process Owners set aside time on a regular basis to ensure that your RoPA is reviewed and kept up to date.

TOP TIPS FOR KEEPING YOUR ROPA UP TO DATE:

1 *Ensure RoPAs are a consideration in your business change control procedures*

2 *Diarise annual check-ins with Process Owners to review their RoPA entries*

3 *Have RoPAs as a standing item on any Data Protection or Information Governance steering group meetings*

4 *Delegate responsibility of RoPA reviews to Process Owners*

7. GLOSSARY OF TERMS

Records of Processing Activities (RoPA)	A document which lists all of the processing activities that each department within an organisation undertakes, with details on what is done with personal data and how it is protected
Data Controller	The organisation that determines the purposes and means of the processing of personal data
Data Processor	The organisation that carries out processing of personal data on behalf, and under the instruction, of the Data Controller
Joint Controllers	Two or more organisations that jointly participate in the determination of the purposes and means of processing
Data Protection Impact Assessments (DPIAs)	An assessment of the likelihood and severity of various risks to the rights and freedoms of individuals. These assessments help to identify these risks and then plan steps to mitigate them
Process Discovery Questionnaire	A questionnaire used to collect preliminary information required for a RoPA, to be completed by individuals within each organisation department
Process Owner	The individual who is assigned responsibility for a certain data process e.g. Payroll
Processing Activity	Any activity that is performed on personal data e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

APPENDIX A: RECORDS OF PROCESSING ACTIVITIES (RoPA) EXAMPLE TEMPLATES:

Data Controller example template:

Company Name	**General**		**Processing Activity**		**Dataset**			**Legality**		**Transfer of data**	
Department	Process Name/ Identifier	System(s) used	Description of processing activity	Purpose of processing activity	Categories of data subject	Categories of personal data	Special category data	Lawful basis for processing	Condition of processing special category data	Recipients of data within the UK	Reason(s) and purpose(s) or transfer
This should be a description of your department/ division	*This will be a short 1-6 word summary description of your process*	*If you use any systems such as Sage, Salesforce, any internal CRM systems or Databases*	*This should be a longer description of the process and what its purpose is*	*This will help to establish the legal basis for undertaking this activity. A brief description will suffice*	*You should break down your data subjects into categories, examples include: employees, clients, customers*	*What data do you capture about these data subjects?*	*Does the process utilise any special category data as defined in Article 9 GDPR?*	*What is your lawful basis for conducting this processing? Article 6 GDPR*	*What condition for processing under Article 9 GDPR are you relying on?*	*Is there anyone who receives the data located within the UK? It may be a company entity, a partner, contractor, or Processor*	*Why do you transfer this data?*
Example: HR	Payroll	Pay Dashboard	Processing payroll for employees	Paying employee wages	UK employees	Name; DOB; NI number; Internal IS; Location data	N/A	Performance of a contract	N/A	N/A	N/A

Transfer of data cont.					**Retention**	**Security**		**Document control**		
Recipients of data within the EU	Reason(s) and purpose(s) for transfer	Recipients of data outside of the EU and UK (inc. international organisations)	Reason(s) and purpose(s) for transfer	Certification or mechanism permitting international transfer	Retention period	Encryption	Access rights	Date of entry	Date last modified	Name and contact details of process owner
Is there anyone located in the EU that receives the data? It may be a company entity overseas, a partner company, contractor working on your behalf etc.	*Why do you transfer this data?*	*Is there anyone outside of the UK and EU that receives the data? It may be a company entity overseas, a partner company, contractor working on your behalf etc.*	*Why do you transfer this data?*	*What mechanism do you have in place for international transfers? E.g., adequacy decision, SCCs*	*Has a retention period for the data associated with the process been determined or suggested?*	*Are you aware if the data is encrypted where it is stored? What other technical measures are in place to protect the data? e.g. penetration testing, firewalls, anti-virus software*	*Who within your organisation has access to this data?*			*Who within your organisation has lead responsibility for this process?*
N/A	N/A	External payroll provider - XX	Process payment of employee wages	Standard Contractual Clauses	7 years	MFA; Encrypted servers	CFO; Finance manager			

APPENDIX A: RECORDS OF PROCESSING ACTIVITIES (RoPA) EXAMPLE TEMPLATE CONT.

Data Processor example template:

General				**Processing Activity**		**Dataset**			**Legality**		**Transfer of data**
Controller	Controller's contact details	Service(s) provided to Controller	System(s) used	Description of processing activity	Purpose of processing activity	Categories of data subject	Categories of personal data	Special category data	Lawful basis for processing	Condition of processing special category data	Recipients of data within the UK
The name of the company for whom you act as a Processor	*Name of key contact; number; email; address*	*What service(s) do you provide to them?*	*If you use any systems such as Sage, Salesforce, any CRM systems or databases*	*This should be a longer description of the process and its purpose*	*This will help to establish the legal basis for undertaking this activity. A brief description will suffice.*	*You should break down your data subjects into categories, examples include: employees, clients, customers*	*What data do you capture about these data subjects?*	*Does the process utilise any special category data as defined in Article 9 GDPR*	*What is your lawful basis for conducting this processing? Article 6 GDPR*	*What condition for processing under Article 9 GDPR are you relying on?*	*Is there anyone overseas who received the data? It may be a company entity overseas, is a partner company, contractor working on your behalf etc.?*
Example:		Payroll processing	Payroll Dashboard	Processing payroll for employees	Paying employee wages	Controller's UK employees	Name; DOB; NI number; Internal ID; Location data	N/A	Performance of a contract	N/A	Controller

Transfer of data cont.						**Retention**	**Security**		**Document control**		
Reason(s) and purpose(s) or transfer	Recipients of data within the EU	Reason(s) and purpose(s) for transfer	Recipients of data outside of the EU (inc. international organisations)	Reason(s) and purpose(s) for transfer	Certification or mechanism permitting international transfer	Retention period	Encryption	Access rights	Date of entry	Date last modified	Name and contact details of process owner
Why do you transfer this data?	*Is there anyone overseas who received the data? It may be a company entity overseas, a partner company, contractor working on your behalf etc.*	*Why do you transfer this data?*	*Is there anyone outside of the EU who received the data? It may be a company entity overseas, a partner company, contractor working on your behalf etc.*	*Why do you transfer this data?*	*What mechanism do you have in place for international transfers? E.g., adequacy decision, Standard contractual clauses*	*Has a retention period for the data associated with this process been determined or suggested?*	*Are you aware if the data is encrypted where it is stored?*	*Who within your organisation has access to this data?*			*Who within your organisation has lead responsibility for this process?*
Service delivery - processing employee wages	N/A	N/A	N/A	N/A	Standard Contractual Clauses	7 years	MFA; encrypted servers	Account manager			

APPENDIX B: PROCESSING ACTIVITIES EXAMPLE LIST

1. HR

1.1 BENEFITS

□ Deliver employee benefits program

□ Manage and administer benefits

□ Manage employee referral programs

1.2 ACCOUNTS

□ Administer payroll

1.3 RECRUITMENT

□ Manage applicant information

□ Screen and select candidates

□ Test and interview candidates

□ Draw up and make offer

□ Archive and retain records of non-hires

□ Manage employee onboarding, development, and training

□ Obtain candidate background information

1.4 STAFF COMMUNICATIONS

□ Manage employee communication

□ Manage employee relations

1.5 GENERAL

□ Develop and manage human resources planning, policies, and strategies

□ Develop and manage time and attendance systems

□ Manage and maintain employee data

□ Manage leave of absence

□ Manage promotion and demotion process

1.6 POLICIES

□ Manage employee grievances

□ Manage retirement

1.7 TRAINING

□ Develop employee career plans and career paths

□ Develop, conduct, and manage employee and/or management training programs

□ Develop and train employees

□ Evaluate and review performance program

□ Manage employee development and performance

□ Manage examinations and certifications

APPENDIX B: PROCESSING ACTIVITIES EXAMPLE LIST CONT.

2. PROJECT MANAGEMENT

□ Certify and validate suppliers

□ Collaborate demand with customers

□ Create/Distribute purchase orders

□ Expedite orders and satisfy inquiries

□ Manage contracts

□ Manage physical finished goods inventory

□ Manage repair/refurbishment and return to customer/stock

□ Manage suppliers

□ Manage transportation fleet

□ Manage warehouse transfers

□ Negotiate and establish contracts

□ Prepare/Analyse procurement and vendor performance

□ Process and audit carrier invoices and documents

□ Procure materials and services

□ Select suppliers and develop/maintain contracts

□ Solicit/Track vendor quotes

□ Support inventory and production processes

□ Track carrier delivery performance

□ Track third-party logistics storage and shipping performance

3. SERVICES

□ Archive records and update systems

□ Deliver service to customer

□ Solicit feedback from customer on service delivery satisfaction

□ Evaluate performance of existing products/services against market opportunities

□ Manage product and service master data

□ Review and approve data access requests

□ Train employees on appropriate regulatory requirements

APPENDIX B: PROCESSING ACTIVITIES EXAMPLE LIST CONT.

4. BUSINESS DEVELOPMENT

□ Maintain customer/product master files

□ Monitor and respond to social media activity

□ Perform customer and market intelligence analysis

□ Build engagement and relationship with members

□ Conduct customer and market research

□ Collect and maintain account information

□ Manage customer relationships

□ Perform sales calls

□ Manage customer master data

□ Record contact and address details

□ Terminate involved party information

□ Identify/receive leads/opportunities

□ Validate and qualify leads/opportunities

□ Solicit feedback from customer on service delivery satisfaction

5. ACCOUNTS / PAYROLL

□ Analyse and report paid and unpaid leave

□ Approve reimbursements and advances

□ Invoice customer

□ Maintain and administer applicable deductions

□ Maintain and administer employee earnings information

□ Manage corporate credit cards

□ Manage pay

□ Manage personnel accounts

□ Monitor changes in tax status of employees

□ Monitor regular, overtime, and other hours

□ Perform revenue accounting

□ Process and distribute payments

□ Process expense reimbursements

□ Process payroll

□ Process reimbursements and advances

□ Produce and distribute employee annual tax statements

□ Receive/Deposit customer payments

□ Resolve customer billing inquiries

APPENDIX B: PROCESSING ACTIVITIES EXAMPLE LIST CONT.

6. IT

□ Conduct and analyse IT compliance assessments

□ Develop and manage IT security, privacy, and data protection

□ Execute IT continuity and recovery action

□ Manage IT user authentication mechanisms

□ Manage IT user authorisation

□ Manage IT user directory

□ Operate IT user support

□ Resolve IT issues/requests

□ Respond to IT information security and network breaches

□ Review and monitor IT physical environment security controls

□ Review and monitor application security controls

□ Archive records and update systems

7. SALES, PRODUCTS AND SERVICES

7.1 SALES

□ Accept and validate sales orders

□ Administer key account details

□ Analyse customer service data and identify improvement opportunities

□ Analyse problems, requests, and inquiries

7.2 CLIENT/THIRD PARTY INFORMATION

□ Collect and maintain account information

□ Collect and merge internal and third-party customer information

7.3 CLIENT RELATIONS

□ Evaluate customer service operations and customer satisfaction

□ Gather and solicit post-sale customer feedback on products and services

□ Analyse customer complaints and response/redressal

□ Manage Customer Service

□ Measure customer satisfaction

□ Provide feedback and insights to appropriate teams

□ Resolve customer problems, queries and complaints

□ Solicit and process customer feedback

APPENDIX C: PROCESSING DISCOVERY QUESTIONNAIRE

Part 1: Understanding your service

Name of Department:	Provide the name of your Department. This will be the title in which your RoPA entries will be recorded against.
Head of Department/ Service:	Provide the details of the Head of Service/Senior Manager
Summary of Department's purpose:	Brief description of the departments purpose – i.e. "To manage the employment relationship between the company and the employee".
List of Department processes:	Each department processes should be listed. For example, in an HR department, processes would include: Recruitment, Appraisals, Grievances, Sickness Management etc. These should be listed individually. 1. 2. 3. 4.
What Systems are in use:	Briefly detail any systems which are in use within your department – i.e. Cascade for HR.
Do you use any 3rd parties to deliver your services? If so, list them:	Briefly detail any 3rd parties which are used by your department – i.e. JobTrain for Recruitment, Sage for Payroll etc. These will be expanded in more detail in the "Understanding your processes" section.

APPENDIX C: PROCESSING DISCOVERY QUESTIONNAIRE CONT.

Part 2: Understanding your processes *(Copy and paste as many of these as you require)*

Process ID:	The process ID may reflect the numbers you have used in Part 1 – List of Department processes
Name of Processing Activity/Function:	Brief headline title of the process
Description:	Short description of the process – i.e. "To investigate complaints made by service users"
Whose Data is being processed?	Detail the categories of the individuals whose data is being processed – i.e. employees, customers, commissioners, partner agencies, potential employees etc.
What Data do you process?	List the data being processed – i.e. name, address, telephone number, email address, national insurance number
Do you process any of the following 'special categories' of data? · Personal data revealing racial or ethnic origin; · Personal data revealing political opinions; · Personal data revealing religious or philosophical beliefs; · Personal data revealing trade union membership; · genetic data; · Biometric data (where used for identification purposes); · Data concerning health; · Data concerning a person's sex life; · Data concerning a person's sexual orientation; or · Data concerning criminal convictions or offences.	If any of the data listed above falls within the categories on the left, then it should be identified here

APPENDIX C: PROCESSING DISCOVERY QUESTIONNAIRE CONT.

Why do you process this data? I.e. what is your legal justification for doing this?	Choose one of the below – if you are unsure, choose which you feel fits best. This will be reviewed by the DPO/RoPA Creator prior to inclusion within the RoPA. (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). (d) Vital interests: the processing is necessary to protect someone's life. (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)
In respect of the 'special categories' of data, why do you process this data? I.e. what is your legal justification for doing this?	Choose one of the below – if you are unsure, choose which you feel fit best. This will be reviewed by the DPO prior to inclusion within the RoPA. (a) Explicit consent (b) Employment, social security, and social protection (if authorised by law) (c) Vital interests (d) Not-for-profit bodies (e) Made public by the data subject (f) Legal claims or judicial acts (g) Reasons of substantial public interest (with a basis in law) (h) Health or social care (with a basis in law) (i) Public health (with a basis in law) (j) Archiving, research and statistics (with a basis in law)
Are there any external 3rd parties you share this data with? If so, why do you share information with them?	Detail if you use any 3rd parties (i.e. Data Processors) to support the delivery of this process – i.e. do you use any systems or tools to deliver the process? do you use any other companies or outsourced agencies (i.e. printers, advertisers etc.)?

APPENDIX C: PROCESSING DISCOVERY QUESTIONNAIRE CONT.

How long do you retain records relating to this process?	Detail the length of time you keep records supporting this area. If you have never deleted anything, specify ‘never destroyed’.
What is your justification for keeping these records for this length?	Explain the reasons why you keep these records for this length. This might be because the law requires you to, there may be some applicable guidance from a regulatory body or there might be an operational necessity.
What security measures do you have in place and who can access such records?	Detail what security measures you have in place. This may be physical controls for hard copy records (such as filing cabinets, archive facilities etc.). For electronic records, detail your access controls (i.e. who has access, whether this is governed by permissions, where it is stored etc.).

HOW CAN THE DPO CENTRE HELP?

The DPO Centre assists with one-off projects, such as data protection audits, building RoPAs, responses to DSARs and conducting DPIAs. The DPO Centre also provides ongoing support and guidance as your designated DPO, taking ownership of the day-today responsibility for the role, or as your EU or UK Representative required under Article 27 of the GDPR.

DPO services are provided on a 'fractional' basis, so based on the precise level of resource required to meet your evolving needs.

The DPO Centre is based in London and Dublin, and has a network of offices across Europe.

To find out more about our service visit:

🌐 website

✉ hello@dpocentre.com

☎ +44 (0)203 797 1289

Version 1.0

London
The DPO Centre Ltd
50 Liverpool Street
London
EC2M 7PR United Kingdom

Dublin
The DPO Centre Europe Ltd
Alexandra House
3 Ballsbridge Park
D04 C7H2 Ireland

Amsterdam
The DPO Center B.V
Vijzelstraat 68-78
Amsterdam
1017 HL The Netherlands

www.dpocentre.com
☎ +44 (0) 203 797 1289
✉ hello@dpocentre.com
in Join us on LinkedIn