RECORD OF PROCESSING ACTIVITIES PRACTICE NOTE

Version: V2.0 **Date: 10th June 2022**

What is a ROPA?

The record of processing activities (ROPA) is a record of an organisation's administration and business activities that involve the processing of personal data. A copy of your organisation's ROPA must be made available, upon request, to the Information Commissioner's Office (ICO) or to a supervisory authority in an EU Member State via your EU Representative.

Article 4 of the UK General Data Protection Regulation ('UK GDPR') defines 'processing' as *''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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction''.*

Why do we need a ROPA?

The ROPA is a legal requirement under Article 30 of the UK GDPR. It represents the key element of the accountability principle as defined in Article 5.2 of the UK GDPR. Documenting your processing activities helps you ensure, and demonstrate compliance, with the UK GDPR.

Who needs a ROPA?

Organisations with 250 or more employees must document their processing activities. There is a limited exemption for small and medium-sized organisations. If you have fewer than 250 employees, you only need to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or,
- includes special categories of data as referred to in Article 9(1), or personal data relating to criminal convictions and offences referred to in Article 10.

However, notwithstanding that an exemption could be claimed, it is good practice to document all your processing activities regardless of the size of your organisation.

Controllers and processors each have their own documentation obligations where no exemption is claimed. As a **controller**, you must focus on each function of your business, one at a time, to accurately record all of your processing activities. Each business function is likely to have several different purposes for processing personal data, each purpose will involve several different categories of individuals, and in turn those categories of individuals will have their own categories of personal data and so on.

As a **processor**, you can still apply the 'broad to narrow' approach. You must start with the controller that you are processing personal data for, as there may be several different categories of processing you carry out for each controller, requiring different security measures to be applied and different mechanisms for international data transfers, and so on.

What is documentation?

Most organisations are required to maintain a record of their processing activities; this is called **documentation**. The checklists at Appendix 1 will assist you in determining what documentation is required and what documentation that is considered 'Best Practice'.

Documenting what personal data you hold, the reason why i.e. the purpose, the length of time the data is retained, and who the data is shared with, will enable your organisation can manage data effectively and comply with the UK GDPR.

Equally, documenting your processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the UK GDPR.

What do we need to document under Article 30 of the UK GDPR?

You must document the following information:

- the name and contact details of your organisation (and where applicable, of other controllers, your representative, and your data protection officer).
- the purposes of your processing.
- a description of the categories of individuals and categories of personal data.
- the categories of recipients of personal data.
- details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- retention schedules.
- a description of your technical and organisational security measures.

Should we document anything else?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the UK GDPR and the UK's Data Protection Act 2018 (DPA 2018). Such documentation may include:

- information required for privacy notices, such as:
    - the lawful basis for the processing
    - the legitimate interests for the processing
    - individuals' rights
    - the existence of automated decision-making, including profiling
    - the source of the personal data;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports;
- records of personal data breaches;

- information required for processing special category personal data or criminal offence data under the DPA 2018, covering:
    - the condition for processing in Schedule 1 of the DPA 2018;
    - the lawful basis for the processing in the UK GDPR; and
    - your record retention and deletion (RR&D) policy.

What about processing special category data and criminal offence data?

The UK GDPR defines special category (SC) personal data as:

- 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**; and
- data concerning a person's **sexual orientation**.

However, you can only process SC data if you can meet one of the specific conditions in Article 9.2 of the UK GDPR:

(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)

Five of the conditions for processing SC data are set out in Article 9 of the UK GDPR. The other five require authorisation or a basis in UK law, which means you need to meet additional conditions set out in Schedule 1, DPA 2018. For some of the conditions, you also need to justify why you cannot give individuals a choice and get explicit consent for your processing.

If you are relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1, Schedule 1, DPA 2018, and if you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2, Schedule 1, DPA 2018 (see Appendix 3).

The processing of criminal offence (CO) data equally needs to be aligned to a condition set out in Schedule 1, DPA 2018.

Where is the meaning of 'public interest'?

The public interest covers a wide range of values and principles relating to the public good, or what is in the best interests of society. It needs to be real and of substance. Given the inherent risks of SC data, it is not enough to make a vague or generic public interest argument. You should be able to make specific arguments about the wider benefits of your processing.

You may also need to consider how the risks associated with SC data affect your other obligations – in particular, obligations around data minimisation, security, transparency, appointing a DPO, conducting DPIA and rights related to automated decision-making.

Where do I start?

The best way to start is by conducting an audit or a data-mapping exercise, to identify what personal data is processed by your organisation and where it is stored. The information must be documented in writing in a granular and meaningful way.

You can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of your organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts, and agreements.

1. Devise a questionnaire. You should devise a questionnaire and distribute it to areas of your organisation where you have identified as processing personal data. You should be able to answer these questions about each personal data processing activity:
    - why do you use personal data?
    - who do you hold information about?
    - what information do you hold about them?
    - who do you share it with?
    - how long do you hold it for?
    - how do you keep it safe?
2. Meet with key functions of your organisation. You should meet with key functions of your organisation e.g. Human Resources, Marketing, Customer Support, etc. This will help you gain a better understanding of how certain parts of your organisation use data. Furthermore, other departments hold specific information about processing activities, such as the IT department holds information about the technical security measures, while the Legal department keep track of any data-sharing agreements.
3. Review policies, procedures, contracts, and agreements. You should locate and review policies, procedures, contracts and agreements as relevant information can be found in existing documentation such as why do you use personal data. Such policies, procedures, contracts, and agreements include, but are not limited to:
    - privacy policies
    - data protection policies
    - data retention policies
    - data security policies
    - system use procedures

- data processor contracts
- data sharing agreements
- joint controller agreements

Once the data-mapping exercise is complete, you will be in a good position to begin documenting your organisation's processing activities i.e. create your ROPA.

What should we document first?

It is recommended that you start with the broadest piece of information about a specific processing activity and then narrow it down to the scope, as you document each requirement.

The recording of information about your processing activities should be done in a granular and consistent way because different conditions may apply to different aspects of the processing activity i.e. separate retention periods for different categories of data.

Adopting this approach helps you to create a comprehensive ROPA in which you document the different types of information in a granular way. Examples of how to document your findings can be found at Appendix 2.

How do we create a ROPA?

Your processing activities should be documented in writing, pursuant to Article 30 (3).

Paper documentation i.e. tables created in Word, would be considered adequate for very small organisations whose processing activities rarely change.

Due to the ongoing need to add, remove, and amend information relevant to your processing activities, it is recommended that you create your ROPA in an electronic format i.e. Excel.

The ICO has made available two basic templates to help document your processing activities:

Documentation template for controllers

Documentation template for processors

It should be noted that if you choose different formats to the ones provided by the ICO, then your information must be listed in a meaningful way. A generic list of pieces of information with no meaningful links between them will not meet the UK GDPR's documentation requirements.

For consistency, drop-down lists should be added to the ICO's templates as follows:

Column D - Categories of individuals	Column E - Categories of personal data
Blank	Blank
Suppliers	Contact details
Employees	Financial details
Emergency contacts	Lifestyle information
Customers	Location
Clients...	IP address...

The data values in the drop-down lists [above] are indicative of the categories of individuals and personal data that could be included in your ROPA. The drop-down lists that you choose to use should accurately reflect the relevant categories of individuals and personal data that are most common to in your organisation.

The use of drop-down lists prevents other data values from being recorded in cells containing the drop-down lists. Accordingly, the use of drop-down lists in Columns D&E should be given due consideration at the start of the ROPA creation exercise, and not applied, if doing so, presents difficulties to staff who are required to document their departmental processing activities in your organisation's RoPA.

Column L – Article 6 Lawful basis …	Column M – Article 9 condition …
Blank Art. 6.1(a) Consent Art. 6.1(b) Contract Art. 6.1(c) Legal obligation Art. 6.1(d) Vital interests Art. 6.1(e) Public task or official function Art. 6.1(d) Legitimate interests	Blank Art. 9.2(a) Explicit consent Art. 9.2(b) Employment, social security and social protection Art. 9.2(c) Vital interests Art. 9.2(d) Not-for-profit bodies Art. 9.2(e) Made public by the data subject Art. 9.2(f) Legal claims or judicial acts Art. 9.2(g) Substantial public interest Art. 9.2(h) Health or social care Art. 9.2(i) Public health Art. 9.2(j) Archiving, research, and statistics

NB: Legal references e.g. Art 9.1(a) etc. can be discounted subject to the preference of the organisation, leaving just the headings purely in a text format.

The data values shown above are fixed and will not change unless the legislation changes.

What else do I need to do?

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2, Schedule 1, DPA 2018 (see Appendix 3).

The condition applied under Part 2 should be entered into Column Z of the ROPA template for controllers produced by the ICO. A drop-down list containing the 23 substantial public interest conditions can be used for this purpose as the data values are fixed and will not change unless the legislation changes. The conditions can be drawn from the table at Appendix 3.

It should be noted that Part 4, Schedule 1, DPA 2018 requires a controller to have an appropriate policy document (APD) in place when processing SC or CO data in reliance on a condition in Part 1, 2 or 3 of Schedule 1, DPA 2018.

What if we have an existing documentation method?

Organisations are often subject to several other regulations that have their own documentation obligations, particularly in sectors such as insurance and finance. If your organisation is subject to such regulatory requirements, you may already have an established data governance framework in place that supports your existing documentation procedures; it may even overlap with the UK GDPR's record-keeping requirements. If so, the UK GDPR does not prohibit you from combining and embedding the documentation of your processing activities with your existing record-keeping practices. But you should be careful to ensure you can deliver all the requirements of Article 30, if necessary, by adjusting your data governance framework to account for them.

Should we update the ROPA regularly?

Your ROPA must represent the current situation of your data processing activities and therefore, be updated regularly. Fundamentally, this makes the ROPA a living document that needs to be updated when necessary. In doing so, you should conduct regular reviews of the information you process to ensure your documentation remains accurate and up to date.

Shaun Beresford

Head of Data Privacy

Appendix:

1 Checklists.
2 Substantial public interest conditions.
3 Documenting your findings

Much of the information contained in this Practice Note has been drawn from information that is publicly available on the ICO's website and other open-source locations.

Appendix 1 – Checklists

Documentation of processing activities - requirements

☐	If we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the UK GDPR.
☐	If we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the UK GDPR.
☐	If we process special category or criminal conviction and offence data, we document:
☐	the condition for processing we rely on in the Schedule 1 of the DPA 2018
☐	the lawful basis for our processing; and
☐	whether we retain and erase the personal data in accordance with our policy document where required in.
☐	We document our processing activities in writing.
☐	We document our processing activities in a granular way with meaningful links between the different pieces of information.
☐	We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice

When preparing to document our processing activities we:

☐	do information audits to find out what personal data our organisation holds;
☐	distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and
☐	review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

☐	information required for privacy notices;
☐	records of consent;
☐	controller-processor contracts;
☐	the location of personal data;
☐	Data Protection Impact Assessment reports; and
☐	records of personal data breaches.
☐	we document our processing activities in electronic form so we can add, remove, and amend information easily.

Appendix 2 – Documenting your findings

What do controllers have to document?	What do processors have to document?
Your organisation's name and contact details.	Your organisation's name and contact details.
The name and contact details of your data protection officer – a person designated to assist with UK GDPR compliance under Article 37.	The name and contact details of your data protection officer – a person designated to assist with UK GDPR compliance under Article 37.
If applicable, the name and contact details of any joint controllers – any other organisations that decide jointly with you why and how personal data is processed.	The name and contact details of each controller on whose behalf you are acting – the organisation that decides why and how the personal data is processed.
If applicable, the name and contact details of your EU representative – another organisation that represents you if you monitor or offer services in the EU.	If applicable, the name and contact details of your representative – another organisation that represents you if you offer services to people in the EU.
The purposes of the processing – why you use personal data, e.g. customer management, marketing, recruitment.	If applicable, the name and contact details of each controller's representative – another organisation that represents the controller if they monitor or offer services to people in the EU.
The categories of individuals – the different types of people whose personal data is processed, e.g. employees, customers, members.	The categories of processing you carry out on behalf of each controller – the types of things you do with the personal data, e.g. marketing, payroll processing, IT services.
The categories of personal data you process – the different types of information you process about people, e.g. contact details, financial information, health data.	If applicable, the name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the UK.
The categories of recipients of personal data – anyone you share personal data with, e.g. suppliers, credit reference agencies, government departments.	If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the UK GDPR.
If applicable, the name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the UK.	If possible, a general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.

What do controllers have to document?	What do processors have to document?
If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the UK GDPR.	
If possible, the retention schedules for the different categories of personal data – how long you will keep the data for. This may be set by internal policies or based on industry guidelines, for instance.	
If possible, a general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.	

Much of the information contained in this Practice Note has been drawn from information that is publicly available on the ICO's website and other open-source locations.

Appendix 3 – Substantial public interest conditions

Conditions set out in Sections 1-4, Part 1, Schedule 1, DPA 2018:

1. Employment, social security and social protection
2. Health or social care purposes
3. Public health
4. Research etc.

Substantial public interest conditions: paragraphs 6 to 28, Part 2 Schedule 1, DPA 2018:

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
8. Equality of opportunity or treatment
9. Racial and ethnic diversity at senior levels
10. Preventing or detecting unlawful acts
11. Protecting the public
12. Regulatory requirements
13. Journalism, academia, art and literature
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
16. Support for individuals with a particular disability or medical condition
17. Counselling
18. Safeguarding of children and individuals at risk
19. Safeguarding of economic well-being of certain individuals
20. Insurance
21. Occupational pensions
22. Political parties
23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport

You should identify which of these conditions appears to most closely reflect your purpose.

Schedule 1, DPA 2018: https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted

Much of the information contained in this Practice Note has been drawn from information that is publicly available on the ICO's website and other open-source locations.