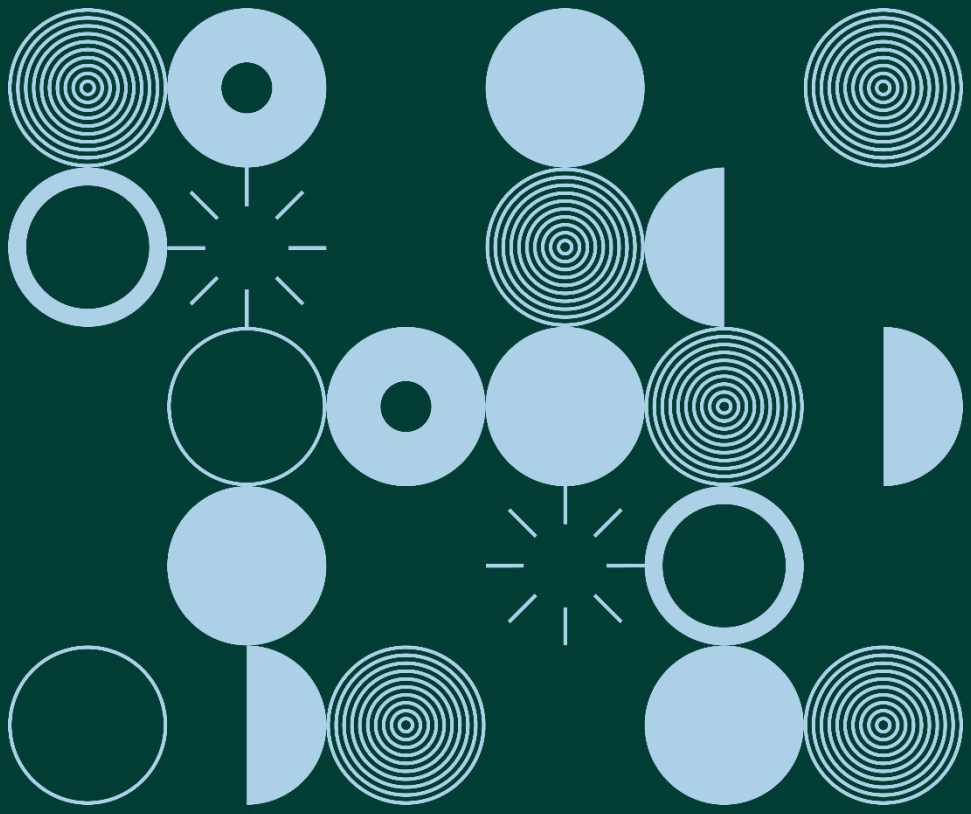
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Records of Processing Activities (RoPA) under Article 30 GDPR

April 2023



Contents

INTRODUCTION

Article 30 of the General Data Protection Regulation (**GDPR**) requires Data Controllers to maintain a Record of Processing Activities (**RoPA**) under their responsibility. The GDPR also requires Data Processors to maintain a record of all categories of processing activities carried out on behalf of each Data Controller they work with. Article 30 GDPR prescribes the information the records must contain and states that controllers and processors must be in a position to provide such records to the Data Protection Commission (**DPC**) on request. The Records of Processing Activities (RoPA), as a measure to demonstrate compliance, is one of the means by which Data Controllers demonstrate and implement the principle of accountability as set out in Article 5(2) GDPR. A well drafted RoPA will demonstrate to the DPC that a Data Controller is aware of, and has considered the purpose of, all processing activities taking place within the organisation. The RoPA should also demonstrate that the Data Controller has considered the implications of the processing of the personal data, the specific and limited personal data required for each activity, and the particularities of managing the security and retention of the personal data to be processed.

By way of other legislation on Records of Processing Activities, Article 24 of the Law Enforcement Directive (LED) and Section 81 of the Data Protection Act 2018 also require the maintenance of records of processing activities carried out under the LED, and prescribe the specific information such records must contain.

Article 57 GDPR details the 'tasks' to be performed by the DPC in relation to the GDPR. These tasks include creating awareness with data controllers and processors of their obligations. The DPC is also tasked with monitoring and enforcing the application of the GDPR. It was with these obligations in mind that in early 2022 the DPC conducted a 'sweep' of the Records of Processing Activities of thirty organisation, across both the public and private sectors, to identify common issues arising and possible shortcomings in respect of the drafting and maintenance of RoPAs held by organisations. As part of the sweep, the DPC requested that organisations of various sizes, in both the public and private sector, send their RoPA to the DPC for review[1]. As a result of the sweep, the findings made on examination of the RoPAs and the analysis of those findings, the DPC

[1] Or alternatively, to explain why they do not maintain records. Some organisations were exempt, as they have less than 250 employees, the processing they carry out is not likely to result in a risk to the rights and freedoms of data subjects, the processing is occasional, or the processing does not include 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. There is no exemption under LED.

has drafted the below guidance. This guidance has been drafted to assist organisations in complying with their Article 30 obligations. Particular emphasis is placed on the positive practices identified over the course of the sweep.

Shortcomings which were identified have also been highlighted, to assist organisations as to 'What Not to Do'.

Article 30 – What is required?

Article 30 of the GDPR places an obligation on controllers and processors to have in place within their organisations a detailed record which accurately identifies the activities the organisation carries out which use personal data. Failure to identify all relevant processing activities may result in personal data being processed in a way that is not in compliance with the GDPR. It may also mean that appropriate technical and organisational measures to protect the personal data being controlled or processed by an organisation are not put in place.

- Article 30(1) GDPR provides that all organisations that process personal data, either as a data controller or as their representative, **shall maintain a record** of the processing activities under its responsibility. Article 30(1) prescribes that this record must contain **all** of the following:
  a) The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the Data Protection Officer (DPO);

  b) The purposes of the processing;
     - Why the organisation is using the personal data in question, for example, for the purposes of payroll management.

  c) A description of the categories of data subjects and of the categories of personal data;
     - For example, both employees and clients of an organisation are examples of categories of data subjects .
     - Categories of personal data include contact details, previous employment history, and the health records of employees.

  d) The categories of recipients to whom the personal data have been, or will be disclosed, including recipients in third countries or international organisations;
     - By way of example, this would include an external HR company subcontracted to deal with an internal HR matter.
  e) Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or

international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

- This would include the transfer of information to an international organisation such as an international NGO or to a processor based outside of the European Economic Area (EEA).

f) Where possible, the envisaged time limits for erasure of the different categories of data;

- This is likely to be organisation dependant and may be set by statute, internal policies, industry guidelines or a combination of all three.

g) Where possible, a general description of the technical and organisational security measures referred to in Article 32(1);

- This may include, for example, the encryption of records, access controls and staff training.

- Article 30(2) GDPR details the records of processing which must be maintained by data processors or their representatives. This includes that a processor's representative must maintain a record of all categories of processing activities carried out on behalf of a controller, containing;

a) 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, of the controller's or the processor's representative, and the data protection officer;

b) The categories of processing carried out on behalf of each controller;

c) Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

Where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

- Article 30(3) GDPR requires the controller to maintain the records prescribed by Article 30 'in writing, including in electronic form'.

- Article 30(4) GDPR requires the controller to make the record available to the supervisory authority (the DPC) on request.

Exemptions to Article 30: Small and Medium Enterprises

- Article 30(5) GDPR provides for certain circumstances where the obligations set out in Article 30(1)-30(4) GDPR do not apply. A derogation, or exemption, to the obligations applies in circumstances where an organisation employs fewer than 250 persons. However this derogation does not apply to processing which constitutes **any** of the following:

    a) Processing that is likely to result in a risk (and not just a high risk) to the rights and freedoms of data subjects. By way of example, this would include the processing of mortgage applications, the use of artificial intelligence, and the tracking of an individual's location.

    b) Processing that is not occasional, such as HR or pay related processing for employees or

    c) Processing that includes special categories of data or personal data relating to criminal convictions and offences. This would include Garda vetting, trade union membership, or biometric data processing.

- The occurrence of any one of these forms of processing triggers the obligation to maintain a Record of Processing Activities, **however this obligation is only in respect of the particular type of processing that does not fall within the scope of the derogation**. For further information on the applicability of Article 30 GDPR, the DPC refers Data Controllers and Processors to the Article 29 Working Party position paper on Article 30(5) which has been endorsed by the European Data Protection Board. This position paper is available here.

Record of Processing Activities: 'Dos and Don'ts'

'Dos' for Organisations

Break down the RoPA with reference to the different functions within the organisation

RoPAs should be **clearly broken down** and detailed according to the different business units or functions within an organisation, such as HR, finance or marketing. This helps ensure that no processing activities are accidentally omitted when completing the RoPA. It is suggested that this can be achieved by creating separate tables or spreadsheets for each business unit within an overall RoPA document or system.

- It is advised that a data mapping exercise should be done by organisations to clarify what data organisations hold and where. Relevant units across the organisation should be involved in this process to again ensure that nothing is omitted.

    - For example, controllers could start with a common business function such as HR. This business function is likely to have several different purposes for processing, with each purpose involving different categories of individuals (for example employees, contractors and interns) and with each individual having several categories of personal data (such as health and safety information, sick leave, payroll details).

    - It is recommended that processors start with each controller they are processing data for, and then the breakdown of the different categories of personal data they are processing for each controller.

By way of example of good practice, although the DPC is not saying a RoPA should be done in this matter, in the sweep conducted by the DPC it found that some organisations include every business area of the organisation in the RoPA to ensure accuracy and to ensure that no unit or function is omitted. This was the case even if some business areas conducted no processing of personal data. By way of a further example of good practice, although not suitable for every organisation, the DPC found that some organisations appear to find it beneficial to break the RoPA down by various different business locations, where more than one office or branch of the organisation exists.

Use the RoPA as a tool to demonstrate compliance with the Accountability principle as set out in Article 5 GDPR

RoPAs should ensure to include granular and meaningful information. This means that RoPAs should go into specific detail for each category of data subject, category of personal data or processing activity.

- For example, retention periods are likely to differ depending on the category of data in question and the RoPA should reflect the retention period for each specific category.

Include relevant extra information as appropriate

The DPC identified in the sweep that many organisations include in their RoPA helpful extra information not explicitly listed in Article 30, for example:

- The Article 6 legal basis for processing
- The Article 9 basis for the processing of special category data
- Whether a breach has occurred in respect of a particular processing activity
- The transfer mechanism relied upon when listing third country transfers, and
- Risk ratings the organisation may have assigned to each processing activity.

While including this information is helpful, the specific prescribed information as set out in Article 30 should never be overlooked.

It is advised that organisations specifically state which information has been prescribed by Article 30, and which information has been included as a 'helpful extra'. This is to assist if different business areas and employees are inputting into the RoPA so that it will be obvious to a new reader which information is mandatory, and which information has been added to the RoPA as an additional extra. It is strongly advised that the prescribed information as detailed in Article 30 should not be buried or difficult to find in the RoPA document, or in any other document that an organisation may be using to satisfy the Article 30 requirements. For further information on this, see point three of the 'Don'ts' list below.

Gain buy-in across the organisation

The RoPA is an obligation which the data controller as a whole should be responsible for. It is recommended that the responsibility for completing the RoPA should not rest solely with the DPO. If it is solely an organisation's DPO preparing and maintaining the RoPA there is the potential processing activities may be missed, or that the RoPA will become a tick box compliance exercise. The DPC would suggest that the process can be led by the DPO with different areas of the organisation feeding into the process. There are different ways organisations can successfully gain buy-in from different areas of their organisation when completing the RoPA. The following are a number of suggestions of how to do so:

- An organisation could internally set specific RoPA review dates, and request all sections of the organisation participate in the review. It may be helpful to be strategic in scheduling this review date at a time where there is likely to be capacity within the organisation to give the task of reviewing the RoPA due attention, for example, not in a busy period such as the run up to Christmas.

- The DPC found that some organisations find it helpful to include definitions, or guidance and explanation sections in the RoPA document which can be used for reference, for example setting out typical examples of processing activities, categories or recipients, for that particular organisation. This helps members of the organisation who may not work closely with data protection issues to accurately provide the information required for the RoPA.

- Organisations should specifically set out the process owners- that is, who within each business function is responsible for maintaining the information required by Article 30 and who is responsible for centrally collating the document.

- Drop down menus can be used to ensure that a uniform, cohesive RoPA document is maintained. However free text fields should also be included for each processing activity to record nuanced information that may only be relevant to one particular processing activity.

Maintain a living document

The RoPA should be a living, dynamic, document, which is continuously updated to reflect the current position of the organisation at all times with regard to their processing of personal data. To achieve this the following steps are recommended;

- Regular reviews of the RoPA and any necessary updates should be carried out.

- To this end, it is likely an electronic (rather than paper based) RoPA will be more suitable for the majority of organisations, so that it can be edited and saved easily.

- As part of employee training, business units should be aware that new products or services that require the processing of personal data should be added to the RoPA as they are rolled out.

- It is recommended that processing activities no longer taking place are marked as such or removed from the live RoPA. However, maintenance of an archive of

obsolete processing activities should be kept for accountability purposes if removal is the preferred option within the organisation.

'Don'ts' for Organisations

Neglect to update the RoPA

As stated in the 'Dos' section above, the RoPA should be maintained as a living and dynamic document. The DPC found that in the course of the sweep conducted some organisations found it challenging to provide a copy of their RoPA within the ten day period requested by the DPC. Some organisations did not meet the deadline given. As stated above, the RoPA should be maintained sufficiently such that it is 'ready to go' at any time.

- The obligation under Article 30 is to 'maintain' a record of processing and 'make the record available to the supervisory authority on request'; therefore, the DPC advises that ten days should be sufficient notice for any organisation in all circumstances.

- Organisations should note that the DPC may carry out similar compliance sweeps in the future. The DPC may also request the RoPA from a controller as part of other regulatory activities being carried out, including but not limited to, breach notification management, complaint handling, Inquiries and investigations.

- Failure to have such documentation to hand could be considered as non-compliance with the GDPR.
    - ➢ It should be noted that providing the DPC with RoPA templates or a 'sample' of the RoPA is not sufficient, as the requirement under Article 30 is to make the actual RoPA maintained available to the supervisory authority on request.

- RoPAs should not refer to out of date or expired information, for example referring to the Privacy Shield as the mechanism for the transfer of personal data to the US.

Don't cut corners with detail and granularity

The DPC identified as part of its sweep that some organisations' RoPAs are not adequately detailed or granular. By way of examples drawn from RoPAs received:

- In response to the requirement to list 'categories of personal data' the DPC received responses to this category which stated 'personal data', 'personally identifiable

information' and 'responses to questions'. These responses are unequivocally not sufficient in terms of describing what information is actually collected by an organisation and needed to be significantly further particularised.

- In response to the requirement to list 'technical and organisational security measures' an organisation stated 'measures are in place that ensure appropriate security' or 'appropriate security'. Again this detail is insufficient. The GDPR states that where possible, a general description of the technical and organisational security measures in place in an organisation should be included. The DPC has noticed a trend that technical and organisational security measures are often not described in detail in many organisations' RoPAs. It is recommended that organisations should give a general description of what technical and organisational measures are in place in their RoPA.

Don't maintain RoPA that is not self-explanatory

In order to be fit for purpose, the RoPA provided to the DPC needs to be a complete, self-contained document clearly listing all information as required by Article 30. RoPAs must be self-explanatory.

Recital 82 GDPR states:

> ...in order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

The following practices should be avoided:

- Hyperlinking documents into the RoPA, as a response to a requirement to list information, that are not accessible when clicked on. For example, hyperlinking a retention schedule which when clicked on is not available to the DPC as it is stored on an internal company drive. Stating 'in accordance with the retention policy' or 'solicitors' retention schedule' but not elaborating on what these documents actually stipulate in terms of retention periods.
    - This makes the RoPA deficient and or unfit for purpose as the DPC cannot rely on the RoPA to gain insight into the processing activities of the particular organisation where such information is unavailable.

- Rather than having a complete RoPA document, hyperlinking or referring to a number of different documents or sources to satisfy the Article 30 requirements. The RoPA should not be prohibitively confusing as this goes against the purpose of the document to assist the DPC in carrying out its functions.
    - If there is no base RoPA document and a piecemeal approach is taken, there is also the risk that processing activities may be overlooked. The RoPA should not just be a 'catch all' document that refers to other documents; all processing activities should be recorded in sufficient detail.

- The DPC should not have difficulty accessing the prescribed information set out in Article 30 GDPR; it should not be left wondering if it has exhausted all available sources of information and should not have to try to reconcile discrepancies between various pieces of information set out in different locations. No personal data should be kept by an organisation 'just in case'. For example, one organisation indicated in their RoPA that they processed the passport information of staff for use in their organisational structure chart, as passport information was used by the HR function.

- Using acronyms that are undefined, which may be common terms within the organisation in question but which do not have an obvious meaning to the DPC. As stated, drafters should be mindful that the DPC as an external reader needs to be able to fully comprehend the document.

- If an organisation is unable to document its RoPA it calls into question its understanding of the purposes for which personal data is processed and retained by the organisation, and the ways in which such data is processed.

RoPAs for Smaller Organisations

As set out above, smaller organisations may not be required to maintain a full RoPA due to the size of the organisation. However, most organisations will need to record processing activities such as HR and payroll functions. For small organisations it may be that a simple spreadsheet is sufficient to maintain the RoPA. For larger or more complex organisations, the data controller may opt to use a relational database or one of the many RoPA tools available from third party data protection service providers. Whatever method used, the RoPA should be a standalone record that the DPC can request and view in a readable format. If an organisation is using software to record its RoPA a report should be able to be easily generated if it is asked for.

The maintenance of a RoPA by a small organisation should not be a burdensome exercise. Having a RoPA will allow a small organisation to map and understand all of the personal data it is processing and for what reasons. A RoPA, as well as being a compliance and risk management tool, will assist a data controller in identifying personal data processing that may not be necessary, and may help in demonstrating to data subjects a commitment to best practice data protection policies and procedures.

Records of Processing Activities Examples

The above guidance, and the examples given, have been informed by the RoPAs provided to the DPC in its RoPA sweep conducted in early 2022.

A number of examples of poor RoPA practice were received amongst the records. One organisation that responded to the sweep provided the DPC with several Data Protection Impact Assessments (DPIAs), claiming that these documents met the requirements of Article 30 of the GDPR. The DPC does not agree with this argument. The RoPA is a standalone record, a compliance tool that the DPC should be able to rely on to provide an accurate view of data processing taking place within an organisation. The accountability obligation lies with the organisation concerned and the information required under Article 30 should be presented to the supervisory authority in a manner that facilitates a demonstration of compliance and assists the supervisory authority in the performance of its functions, as required under Article 31. Expecting the DPC to review a large number of separate documents in order to try to find the information required under Article 30 is not acceptable. In addition, not every processing activity would have, or require, a DPIA.

The DPC received many good examples of detail in respect of Article 30(1)(b) and (c); the purposes for processing and personal data categories requirements. One organisation utilised a relational database system to group processing activities by business units and teams. The organisation was able to present the information as and when required in a spreadsheet format. While it is impractical to provide a full example of a RoPA within this guidance, below, at Approach A and Approach B, are two possible layouts using a spreadsheet programme. Approach C is a RoPA that would not be of sufficient detail. Table A is a table of the information required, with examples of suggested detail and examples of insufficient detail.

Guidance: Records of Processing Activities (RoPA) under Article 30 GDPR

Approach A: An example of a well completed RoPA

A Company Record of Processing Activities

Data Controller: A Company Ltd
123 A Street
Dublin
info@acompany.ii
DPO: David P Other

GREEN COLUMNS ARE **MANDATORY**

BLUE COLUMNS ARE AS **APPLICABLE**

Reference	Processing Activity	Sub Processing Activity	Process Owner	Purpose of Processing	Categories of Data Subject	Categories of Personal Data	Data Accessed by	Joint Controller	3rd Country transfer	International Organisation Transfer	Safeguards for transfer	Retention	Technical and Organisational Security Measures	Legal Basis	Legislation	Risk Register Reference	Notes
1.1	Staff Payroll	Reconcile Hours Worked	HR	Pay Calculation and Working Time requirements	Staff	Name Staff number Clocking hours	HR	NA	No	NA	NA	7 Years (Financial Records)	Password protected system Encrypted archive after 1 year	6(1)(b) Contract 6(1)(c) Legal Obligation	Working Time Act, 1997	NA	Electronic clocking system Accessed by DS and their line manager for day-to-day admin (See Process 15)
1.2	Staff Payroll	Staff Pay	HR	Issue Staff Pay	Staff	Name Staff Number Address PPSN Bank Details Length of Service Sick status Deductions	HR	NA	No	NA	NA	7 Years (Financial Records)	Password protected system Encrypted archive after 1 year	6(1)(b) Contract		NA	
1.3	Staff Payroll	Staff Pay	Accounts	Instruct Bank to Pay Staff	Staff	Name Address Bank account details	Accounts HR ABC Bank	NA	No	NA	NA	7 Years (Financial Records)	End-to-end encryption	6(1)(b) Contract		6.6	Low risk of bank compromise of personal data

Guidance: Records of Processing Activities (RoPA) under Article 30 GDPR

Approach B: An example of a well completed RoPA

Data Controller: A Company Ltd
123 A Street
Dublin
info@acompany.ii
DPO: David P Other

A Company Record of Processing Activities

Reference	Business function	Purpose of Processing	Categories of DS	Personal Data	Recipient	Third Country / International Organisation Transfer	Safeguards	Retention	Technical and Organisational Security Measures	Lawful Basis
1.1	HR	Personal file	Staff	Contact details	NA	NA	NA	X years post employment	Encrypted storage Password-protected HR system	Article 6(1)(b) Contract
1.2	HR	Personal file	Staff	Pay details	NA	NA	NA	X years post employment	Encrypted storage Password-protected HR system	Article 6(1)(b) Contract
1.3	HR	Personal file	Staff	Annual leave details	NA	NA	NA	X years post employment	Encrypted storage Password-protected HR system	Article 6(1)(b) Contract
1.4	HR	Personal file	Staff	Sick leave	NA	NA	NA	X years post employment	Encrypted storage Password-protected HR system	Article 6(1)(b) Contract
1.5	HR	Personal file	Staff	Performance review	NA	NA	NA	X years post employment	Encrypted storage Password-protected HR system	Article 6(1)(b) Contract
2.1	HR	Payroll	Staff	Contact details	Revenue	NA	NA	X years post employment	Encrypted storage Encrypted transfer	Article 6(1)(c) Legal Obligation
2.2	HR	Payroll	Staff	Bank details	Revenue	NA	NA	X years post employment	Encrypted storage Encrypted transfer	Article 6(1)(c) Legal Obligation
2.3	HR	Payroll	Staff	PPSN	Revenue	NA	NA	X years post employment	Encrypted storage Encrypted transfer	Article 6(1)(c) Legal Obligation
2.4	HR	Payroll	Staff	Pension information	Revenue	NA	NA	X years post employment	Encrypted storage Encrypted transfer	Article 6(1)(c) Legal Obligation
3.1	IT	Systems login creation to ensure access	Joiners Staff	Name	NA	NA	NA	1 month	Password protection Limited admin level staff with access	Article 6(1)(f) Legitimate interests
3.2	IT	Systems login creation to ensure access	Joiners Staff	Staff number	NA	NA	NA	1 month	Password protection Limited admin level staff with access	Article 6(1)(f) Legitimate interests
3.3	IT	Systems login creation to ensure access	Joiners Staff	Staff location	NA	NA	NA	1 month	Password protection Limited admin level staff with access	Article 6(1)(f) Legitimate interests
3.4	IT	Systems login creation to ensure access	Joiners Staff	Staff email	NA	NA	NA	1 month	Password protection Limited admin level staff with access	Article 6(1)(f) Legitimate interests
3.5	IT	Systems login creation to ensure access	Joiners Staff	Start date	NA	NA	NA	1 month	Password protection Limited admin level staff with access	Article 6(1)(f) Legitimate interests

Guidance: Records of Processing Activities (RoPA) under Article 30 GDPR

Approach C: An example of a RoPA with insufficient detail

Data Controller: A Company Ltd
123 A Street
Dublin
info@acompany.ii
DPO: David P Other

A School Record of Processing Activities

Reference	Processing Activity	Process Owner	Purpose of Processing	Categories of Data Subject	Categories of Personal Data	Data accessed by	Joint Controller	3rd Country transfer	International Organisation Transfer	Safeguards for transfer	Retention	Technical and Organisational Security Measures	Legal Basis	Notes
1	Student Registration	A School	Student Registration	Student / Parent / Guardian	Personal Data	School / ETB / DoE	NA	Yes		Processor Agreement	As per DoE		Legal Obligation	Processed by xzy Company USA
2	HR	A School	HR Purposes	Staff / Volunteers	Personal Data Special Category Data	Head	NA	No	NA	NA	As per retention policy		Legal Obligation Legitimate Interests	
3	TUSLA Report	A School	Mandatory Report	All	Personal Data Special Category	TUSLA	Yes	No	NA	NA	As per DoE and DoH		Legal Obligation Legitimate Interests	
4	Permission Slips	A School	Trip and sports permission	Student	Personal Data	School	NA	No	NA	NA	ETB policy		Legitimate Interest	

Guidance: Records of Processing Activities (RoPA) under Article 30 GDPR

Requirement	Requirement Type	Example A	Example B	Insufficient Example	Recommendation
Name and contact details of the controller	Required	Example company Building, Road, Town, County, Eircode 045 XXX XXX info@examplecompany.ie	Example company Town, County, Eircode 045 XXX XXX info@examplecompany.ie	John.doe@examplecompany.ie	Full contact details of the controller to be supplied. Personal emails are not recommended due to personnel changes.
Name and contact details of the joint controllers	If relevant		NA		
Name and contact details of the controller's representative	If relevant		NA		
Name and contact details of the Data Protection Officer	Required	John Doe dpo@examplecompany.ie 045 XXX XXX	External DPO company dpo@examplecompany.ie ExampleCompanyDPO@externalcompany.ie	John.doe@externalcompany.ie	Full contact details of the DPO to be supplied. If an external DPO is used, clarity to be provided and full details supplied
Purposes of processing	Required	HR—Payroll	Protected Disclosures Receipt and Investigation	HR	Purpose of processing should be granular enough so that only the personal data required are processed
Description of the categories of data subjects	Required	Temporary staff Permanent staff	Discloser of information Any persons named in disclosure Witnesses Any other person identified during investigation	All	Separation of different categories of staff, or different types of service user, customers, potential customers etc. is recommended where relevant to different processing activity types. Categories of data subject may include identifying where the processing of vulnerable person's data is to take place
Description of categories of personal data	Required	Name, employee number, PPSN, location, hours worked, remuneration, employee bank details, leave information, deductions	Name, employee ID, personal contact details, work contact details Additional categories of personal data may be required dependent on the nature of the disclosure. These will be recorded in the disclosure record.	Personal data	The actual data processed should be recorded
Categories of recipients to whom the personal data have been or will be disclosed	Required	Revenue, employee bank, Dept. of Social Protection (as required)	On a case-by-case basis: The Protected Disclosures Commissioner An Garda Síochána or other relevant law enforcement authorities if offences are discovered Legal advisors Anonymised report required to be published annually	Internal	The data controller should be in a position to know and to demonstrate to whom personal data will be shared
Time limits for erasure of the different categories of data	If possible		7 years post completion, archived securely after 1 year	As per retention policy	Where available, specifics should be included
General description of the technical and organisational measures referred to in Article 32(1)	If possible		Secure reporting system pursuant to the Protected Disclosures (Amendment) Amendment Act 2022 Systems uses 2 factor authorisation Only trained and designated personnel have access to the PD system	GDPR compliant	This is an opportunity to demonstrate the measures taken to ensure the security of personal data processing carried out
Where personal data may be disclosed or otherwise transferred to a third country or an international organisation			NA		
Categories of recipients to whom the personal data have been or will be disclosed in other country/organisation	Required	NA	NA		
The name of the country or international organisation	Required	NA	NA		
The documentation of suitable safeguards in the case of Article 49(1) transfers	If relevant	NA	NA		
Lawful basis	Recommended	Article 6(1)(b) and (c) Article 9(2)(b)	Article 6(1)(c) Protected Disclosures Act 2014 Protected Disclosures (Amendment) Act 2022	Article 6	
For all entries on the RoPA, should the data controller wish to link to other governance documents in order to better demonstrate compliance, or to provide clarity, the links should work outside the data controllers IT environment or the additional documentation must be supplied to the DPC at the same time as the RoPA, if requested.					