information commissioner
Barrantagh Fysseree

A closer look at

Records of processing activities

Important

This document is part of a series, produced purely for guidance, and does not constitute legal advice or legal analysis.

Legal advice, if required, should be sought from a Manx advocate.

All organisations that process data must comply with the Isle of Man data protection legislation and need to be aware that the EU General Data Protection Regulation may also apply directly to them.

Overview

"data protection legislation" means the Data Protection (Application of GDPR) Order 2018 and the "GDPR and Implementing Regulations 2018" ("Implementing Regulations")

"Applied GDPR" means the Annex to the Data Protection (Application of GDPR) Order 2018 and reference to an "Article" is to an Article in the "Applied GDPR"

Reference to a "Regulation" is to a Regulation in the Implementing Regulations.

Article 30 requires that records of processing activity are created and maintained. This obligation applies to **controllers and processors**.

The provisions are set out in full in Annex A.

"Records of processing activities" is not a new concept, but has existed in the Island and across Europe (in the various guises of the 'register entry') since the inception of data protection legislation.

However, the Applied GDPR mandatory requirement to create and maintain written "records of processing activities" now rests with the controllers and processors.

Controllers and processors required to maintain records of processing activity, must make them available to a supervisory authority on request.

Article 58(1) allows the supervisory authority to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information required for the performance of its tasks. This includes the provision of records of processing activities.

The Commissioner may impose an administrative fine of up to £1,000,000 for failure to provide access in violation of Article 58(1).

Whilst there is a narrow exception from the obligation to maintain "records of processing activities", other obligations in the Applied GDPR still require demonstrable compliance with the data protection legislation and evidence of review.

Records of processing activities

Controllers **and processors** must, unless an exception applies, maintain records of processing activities. The exception from the Article 30 obligation is set out on page 7, together with a worked example on page 8.

Article 30 specifies that records of processing activities must contain the following information:

(a) the name and contact details of the controller or processor (and, if applicable, the joint controller/processor, the controller/processor's representative and the data protection officer);

(b) the purposes of the processing;

(c) a description of the categories of data subjects, personal data and recipients;

(d) details of overseas transfers and the suitable safeguards for the transfers;

(e) the envisaged time limits for erasure of the different categories of data;

(f) a general description of the technical and organisational security measures.

However, Article 30, and the need for records of processing activities, should not be considered in isolation from other responsibilities and obligations where a detailed knowledge of the processing activities is required.

Even if a controller or processor believes itself to be exempt from the Article 30 requirement to maintain 'records of processing activities', the information is interconnected and interwoven with that required for compliance with other obligations under the Applied GDPR.

Article 24, for example, requires that measures including appropriate data protection policies, "shall be reviewed and updated where necessary" and Article 32 requires the regular testing, assessing and evaluation of the effectiveness of the technical and organisational measures for ensuring the security of the processing. It seems almost inevitable, therefore, that records of the processing are kept in some form.

It is difficult to see how other obligations can be achieved, evidenced or regularly reviewed, without some form of record about the processing being created and maintained.

Records of processing activities

This information is also required for compliance with other obligations set out in the GDPR and include:

1. providing transparency information to data subjects
2. integrity and confidentiality (establishing the relevant technical and organisational measures including security measures for personal data and the implementation of data protection policies)
3. accountability for compliance with the principles
4. undertaking data protection impact assessments
5. ensuring data protection by design and by default
6. demonstrating compliance to a supervisory authority
7. reporting data breaches

All the obligations listed above apply to controllers and the obligations set out in points 2, 4, & 7 above also apply to processors.

The following page illustrates the broad types of information required for the obligations under the Applied GDPR, including records of processing activities, and also indicates the inter-dependency between knowing the details of processing activities and establishing the appropriate security measures.

There is no single way to generate records of processing activity and the means by which records are generated will, to a great extent, depend upon the detail and knowledge of the processing activities and the level of compliance with the existing law.

Examples of where to start could include:

- A data flow analysis, which should generate most, if not all, of the information required for records of processing activities.
- Alternatively, if you have, for example, reviewed and updated the transparency information provided to individuals, a subset of that information could feed into the record of processing activities.

Information required for GDPR compliance

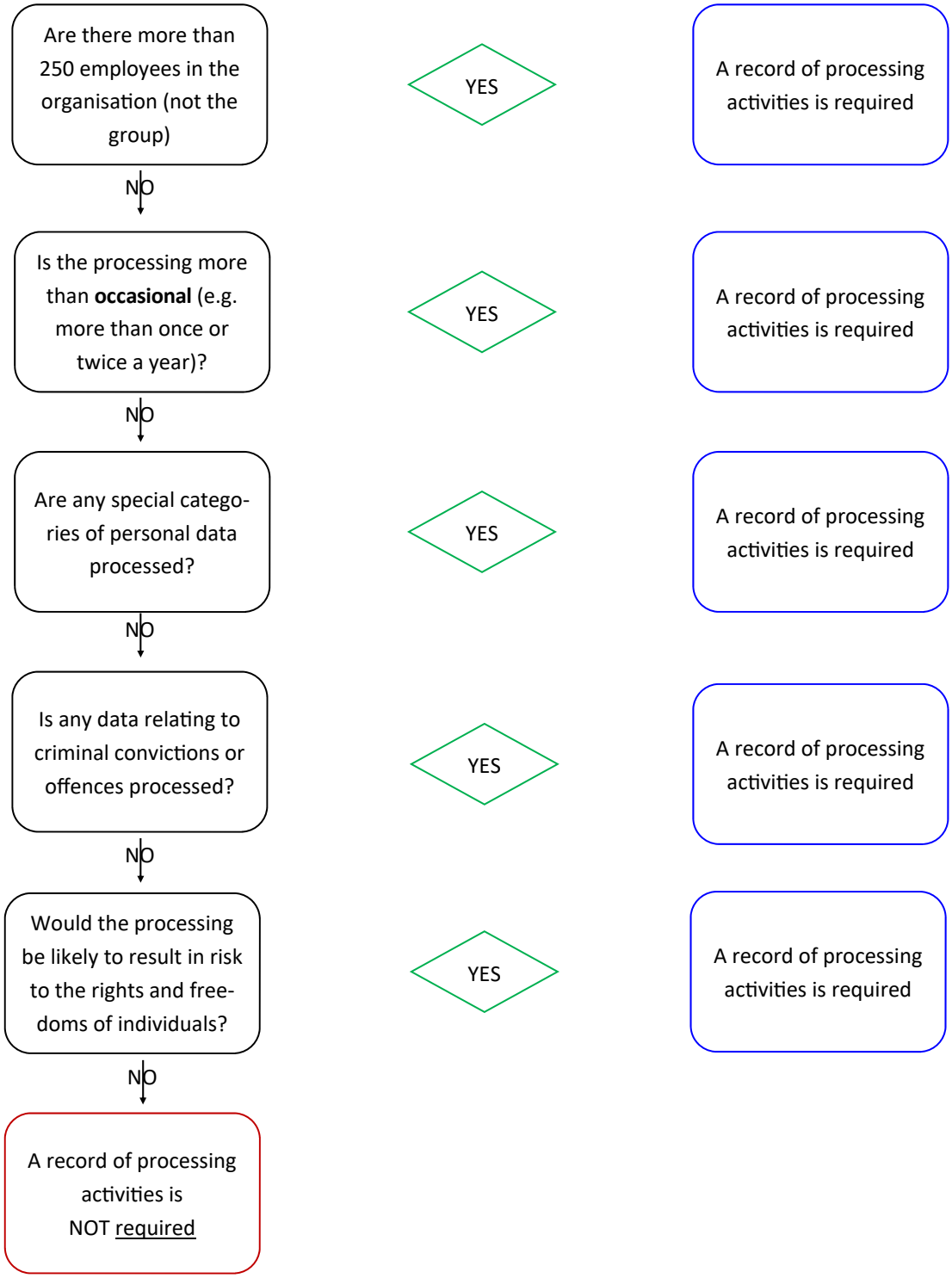
The information required for compliance with the Applied GDPR can be broadly grouped as follows:

Group 1	Technical and organisational measures
Group 2	Purposes for processing, details of data subject, categories of personal data, details of overseas transfers and retention periods
Group 3	Data protection officer
Group 4	Conditions for processing
Group 5	Recipients and transfers of personal data

The following matrix indicates where the information Groups identified above are required or used in relation to the Applied GDPR obligations or duties.

	Group 1	**Group 2**	**Group 3**	**Group 4**	**Group 5**
Integrity and confidentiality (Article 5, 24, 32)					
Providing transparency information to data subjects (Article 12-14)					
Undertaking data protection impact assessments (Article 35)					
Demonstrating compliance to a supervisory authority (Article 24, 30, 31, 33, 42, 58)					
Accountability for compliance with the principles (Article 5)					
Records of processing activity (Article 30)					
Reporting data breaches (Article 32, 33, 34)					
Ensuring data protection by design and by default (Article 25)					

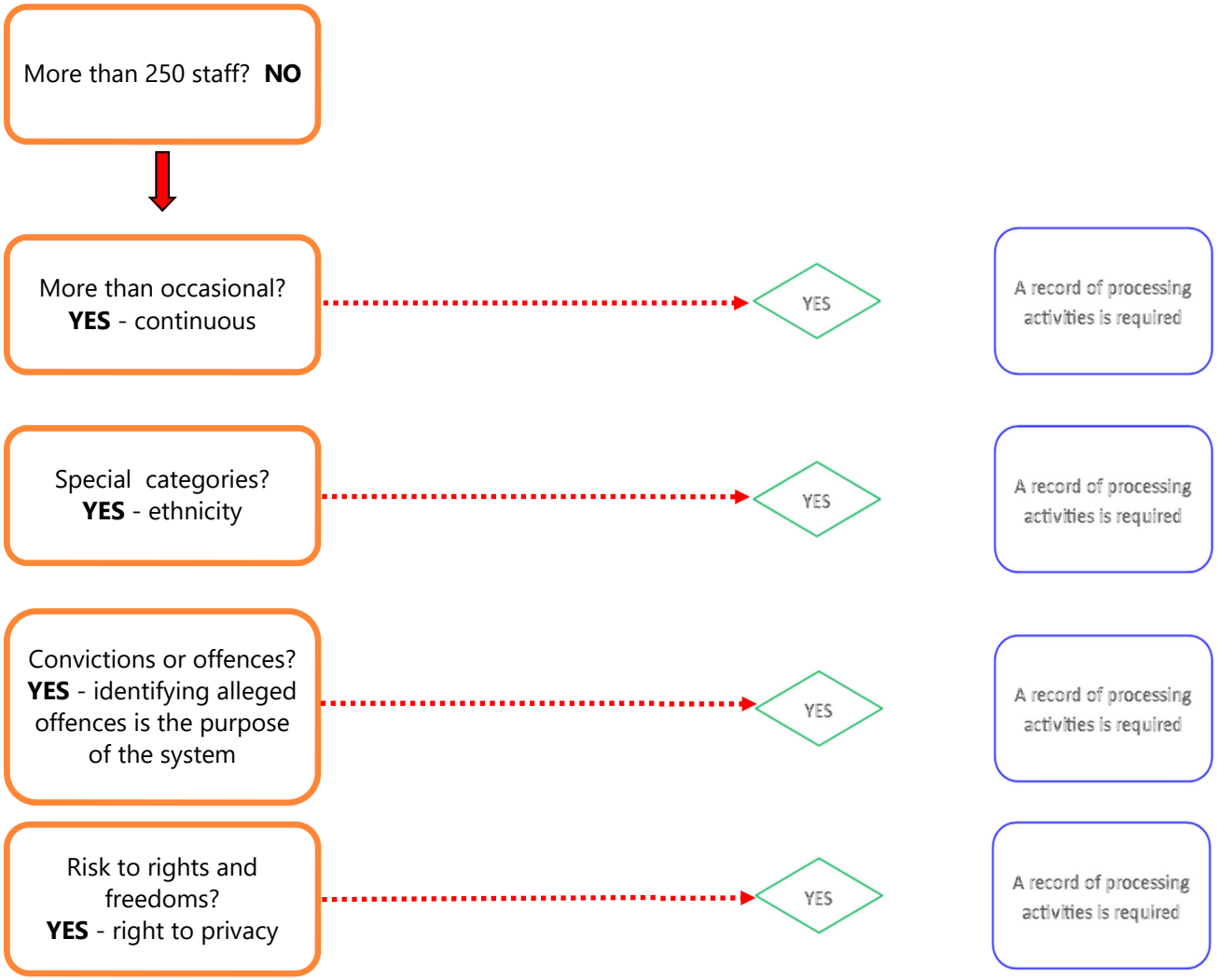
Exceptions to the requirement for Article 30 'record of processing activities'



Worked example of assessing the requirement for Article 30 'records of processing activities'

We have taken **the routine use of surveillance equipment (CCTV) by a shop** as an example of whether the controller requires records of processing activities.

In most cases, CCTV will be used to monitor customers (and staff) inside the shop and in the immediate vicinity. The processing of personal data will be for crime prevention and detection purposes.



In any event, the information will be required to give transparency information to individuals.

ANNEX A

Article 30

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

   (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

   (b) the purposes of the processing;

   (c) a description of the categories of data subjects and of the categories of personal data;

   (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

   (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;

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

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

2. Each processor and, where applicable, the processor's representative shall 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;

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

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation 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, the processing is not occasional, or the processing 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.

information commissioner
Barrantagh Fysseree