Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit
IGDC • DHCW

Expectations Guidance Document

1.5-Records of Processing and Information Assets

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the 'Records of Processing and Information Assets' section of the Welsh Information Governance Toolkit (WIGTK).

Article 30 of the UK GDPR states that 'Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.'

The ICO expects organisations to have a ROPA that contains all the relevant requirements set out in Article 30.

Creating and maintaining a ROPA will help your organisation understand what information is held, where it is and what you do with it. It will also help to demonstrate how you are processing data and that it is done so in line with the accountability principle.

The organisation's processing won't be lawful without a valid lawful basis. It is extremely important that you can justify your reasons and have a record of this decision.

Minimum Expectations

Record of Processing Activities
To be compliant with Article 30 of the UK GDPR, your ROPA should include 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)"

The requirements for ROPA are set out within the Records of processing and lawful basis section of the ICO's Accountability Framework.

You will be required to upload a copy or extract of your ROPA if you have ticked that your organisation has one.

Asset Register
It is important that your organisation knows what information it holds, so that assets can be managed appropriately. The organisation can do this by implementing and maintaining an asset register. The asset register should hold details about all hardware, software and information assets within your organisation.

As a minimum, your asset register should include:

- asset owners name
- asset location
- retention periods
- security measures deployed

The organisation should review the asset register and risk assess assets periodically to make sure it remains accurate and up to date for your organisation.

Further information about asset registers can be found on the ICO's website, using the following links: Data mapping and recording | ICO and Asset management | ICO

Consent – HB/Trust/SHA and Prison Healthcare only
If your organisation uses consent as a lawful basis for processing, you should keep evidence of what the individuals were told, when they consented and how the consent was informed.

You must be able to demonstrate that consent is freely given and meets the following conditions outlined under Article 7 of the UK GDPR:

> "1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
>
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
>
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

Your record of consent should show what an individual has consented to, including what they were told and when and how they consented.

Consent should always require a positive opt-in; and no pre-ticked boxes should be used.

Your organisation should also record whether the individual in question has provided their own consent, and if not, who provided the consent on their behalf, such as a parent or guardian.

The record of consent should be thorough and easy for the relevant staff to access, review and apply withdrawal of consent if required.

The ICO expects the organisation to review records of previously gathered consent. This includes having a procedure to review consent to check that the relationship, the processing, and the purposes have not changed and to record any changes. As well as a procedure to refresh consent at appropriate intervals.

The requirements for consent are set out within the Records of processing and lawful basis section of the ICO's Accountability Framework.

Legitimate Interests - HB/Trusts/SHAs and Prison Healthcare only
If your organisation relies on Legitimate Interests as a lawful basis for processing, a Legitimate Interests Assessment (LIA) must be completed prior to starting the processing.

The LIA should identify the legitimate interest, the benefits of the processing and whether it is necessary.

A 'balancing test' should then be conducted to show how your organisation determines that its legitimate interests override the individuals', and considers the following issues:

- Not using people's data in intrusive ways or in ways which could cause harm, unless there is a very good reason.
- Protecting the interests of vulnerable groups such as people with learning disabilities or children.
- Whether you could introduce safeguards to reduce any potentially negative impact.
- Whether you can offer an opt-out.
- Whether you require a DPIA.

The outcome of the assessment and final decision should be clearly documented, and the LIA should be regularly reviewed and updated if any changes affect the outcome.

Privacy Information - HB/Trusts/SHAs, Prison Healthcare and Third Party Contractors only

To be transparent with customers about their data, we need to provide them with information at the first chance possible which details how we process their data and what lawful basis we rely upon to do so. This information is typically contained within a privacy notice.

The organisation should be able to demonstrate that all processing on your ROPA is covered by the privacy information.

The ICO expects the organisation to have procedures in place to regularly review the privacy information provided to data subjects, to make sure that it is accurate, up to date and effective.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Consent

If your organisation uses consent as a lawful basis for processing, you should keep evidence of what the individuals were told, when they consented and how the consent was informed.

You must be able to demonstrate that consent is freely given and meets the following conditions outlined under Article 7 of the UK GDPR:

> "1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
>
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
>
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
>
> 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

Your record of consent should show what an individual has consented to, including what they were told and when and how they consented.

Consent should always require a positive opt-in; and no pre-ticked boxes should be used.

Your organisation should also record whether the individual in question has provided their own consent, and if not, who provided the consent on their behalf, such as a parent or guardian.

The record of consent should be thorough and easy for the relevant staff to access, review and apply withdrawal of consent if required.

The ICO expects the organisation to review records of previously gathered consent. This includes having a procedure to review consent to check that the relationship, the processing, and the purposes have not changed and to record any changes. As well as a procedure to refresh consent at appropriate intervals.

The requirements for consent are set out within the Records of processing and lawful basis section of the ICO's Accountability Framework.

Legitimate Interests – General Practices, Community Pharmacies, Optometrists, Dentistry, Third Party Contractors and urgent and Emergency Care only

If your organisation relies on Legitimate Interests as a lawful basis for processing, a Legitimate Interests Assessment (LIA) must be completed prior to starting the processing.

The LIA should identify the legitimate interest, the benefits of the processing and whether it is necessary.

A 'balancing test' should then be conducted to show how your organisation determines that its legitimate interests override the individuals', and considers the following issues:

- Not using people's data in intrusive ways or in ways which could cause harm, unless there is a very good reason.
- Protecting the interests of vulnerable groups such as people with learning disabilities or children.
- Whether you could introduce safeguards to reduce any potentially negative impact.
- Whether you can offer an opt-out.
- Whether you require a DPIA.

The outcome of the assessment and final decision should be clearly documented, and the LIA should be regularly reviewed and updated if any changes affect the outcome.

Privacy Information – General Practices, Community Pharmacies, Optometrists, Dentistry and Urgent and Emergency Care only

To be transparent with customers about their data, we need to provide them with information at the first chance possible which details how we process their data and what lawful basis we rely upon to do so. This information is typically contained within a privacy notice.

The organisation should be able to demonstrate that all processing on your ROPA is covered by the privacy information.

The ICO expects the organisation to have procedures in place to regularly review the privacy information provided to data subjects, to make sure that it is accurate, up to date and effective.