TYFU CYMRU
GROW WALES

12 Steps to GDPR compliance

ANNA BEZODIS
TRAINING AND CONSULTANCY

Cronfa Amaethyddol Ewrop ar gyfer Datblygu Gwledig:
Ewrop yn Buddsoddi mewn Ardaloedd Gwledig
European Agricultural Fund for Rural Development:
Europe Investing in Rural Areas

Llywodraeth Cymru
Welsh Government

This document has been developed by Anna Bezodis Training and Consultancy for information purposes only and does not constitute legal advice or opinion as to the current laws, regulations, or guidelines of any jurisdiction. While every effort has been made to ensure the accuracy and completeness of the information provided, Anna Bezodis Training and Consultancy will not be held liable for any damages, however suffered, flowing from the direct or indirect use of, or reliance upon, that information. This document is protected by copyright, and unless otherwise stated no part them may be reproduced or used for any purpose other than private personal use, without the prior written consent of Anna Bezodis Training and Consultancy.

TyfuCymru has received funding through the Welsh Government Rural Communities – Rural Development Programme 2014-2020, which is funded by the European Agricultural Fund for Rural Development and the Welsh Government.

TyfuCymru
Lantra Wales, Royal Welsh Showground,
Builth Wells LD2 3WY
T:+44 (0)1982 552646
E: tyfucymru@lantra.co.uk
W: www.tyfucymru.co.uk

TyfuCymru is led by Lantra Wales
which is a company registered in
England and Wales.
Registered no: 2823181
Charity no: 1022991
VAT no: 585 3815 08

Introduction

If you collect or receive personal data and you have overall **control** over why you need that data and how it should be used, you will be deemed to be a **data controller**. Or if you **process** personal data on behalf of a data controller, you will be classed as a **data processor**. In either case, you and those within your organisation need to work to the rules that are set out in the UK GDPR legislation, to be legally compliant.

What is classed as ‘personal data’?

Personal data includes information like:

- a person’s name or contact details (this person is known as the ‘data subject’)
- an identification number, for example a person’s National Insurance or passport number
- location data, for example a person’s home address or mobile phone GPS data
- an online identifier, for example a person’s IP or email address.

Personal data that is considered to be more sensitive is also covered by the UK GDPR, and is referred to as ‘special category data’. Special category data specifically includes:

- genetic data relating to genetic characteristics which give unique information about a person’s physiology or health
- biometric data for the purpose of identifying a person, including facial images and fingerprints
- data concerning a person’s physical or mental health, and the provision of health care services
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- sex life or sexual orientation.

(Source: https://www.which.co.uk/consumer-rights/advice/what-counts-as-personal-data-a4T2s2Y2ffXd#what-is-personal-data)

Here is a 12-step task list to help you comply with the UK GDPR:

STEP 1

Register with the Information Commissioner's Office (ICO) and pay a registration fee, unless you are exempt from doing so. If you are unsure whether you need to register, the ICO have a handy self assessment quiz to help you determine your status.

STEP 2

You will need to audit and document the data that you hold.

Documentation templates can be downloaded from here!

Questions to be asked may include:

- **Who** are our data subjects? Who has access to personal or special category data?
- **Where** do we keep personal data? Where/who do we transfer personal data to?
- **Why** are we processing personal data (what is the purpose)? Why do we share it with third parties?
- **What** mechanisms do we have in place to safeguard personal data? What lawful basis/bases are we relying upon to process data?
- **How** is data being processed? How long should it be kept?

(Source: https://www.which.co.uk/consumer-rights/advice/what-counts-as-personal-data-a4T2s2Y2ffXd#what-is-personal-data)

STEP 3

From the data audit carried out in STEP 2, identify any areas of risk, and put security measures in place to manage those risks.

Cronfa Amaethyddol Ewrop ar gyfer Datblygu Gwledig: Ewrop yn Buddsoddi mewn Ardaloedd Gwledig
European Agricultural Fund for Rural Development: Europe Investing in Rural Areas
Llywodraeth Cymru
Welsh Government

The law requires that you have a level of security that is ‘appropriate’ to the risks presented by your data processing.

On the documentation templates there are columns to complete (see second tab of spreadsheet for helpful examples!).

STEP 4

Understand when a Data Protection Impact Assessment (DPIA) is required. A DPIA is a process to help you identify and minimise the data protection risks of a project, and you must do a DPIA before you begin any type of data processing that is likely to result in a high risk to individuals.

For further information on this, and to access a sample DPIA document, please follow this link!

STEP 5

Create/update your data protection policy (which might also be referred to as your ‘privacy policy’) and ensure it reflects any changes you have made in line with the UK GDPR.

Useful guidance notes on how to create a data protection policy can be found here!

It is not essential that you have one, BUT you do need to let people know what you are going to do with their personal data (using a privacy notice – See STEP 6).

STEP 6

When processing personal data, you must tell people what you are doing with it. They have the right to know key information such as why you need it, what you’ll do with it and who you’re going to share it with. You should provide this information in a clear, open and honest way.

It’s best to have this written down in a document called a privacy notice.

A privacy notice template can be downloaded from here!

STEP 7

Do you rely on having a person’s consent to process their personal data? Consent is only one of the lawful bases that you can rely on, so you won’t always need consent but there are some instances where it will be the best option.

If you are relying on consent, review how you will seek, record and manage it.

Under the UK GDPR, for consent to be valid it has to be freely given, specific about what the person is consenting to, clear, opt-in (you can’t use pre-ticked boxes or rely on default ‘opt-out’ consent), properly documented and easily withdrawn.

You may need to seek fresh UK GDPR compliant consent if your existing consents don’t meet the standard required, or are poorly documented.

Click here for a handy checklist to ensure that your method of asking for, recording and managing consent is compliant.

STEP 8

Does your organisation need a data protection officer (DPO)?

The ICO have a 5 minute self-assessment quiz to help you determine whether or not you need to legally appoint a DPO.

STEP 9

Consider how you can comply with processing data in line with an individual’s rights – e.g. responding to a request to delete data, or to transfer data in line with the new right of data portability.

STEP 10

Be prepared for a personal data breach! We can all make mistakes, so make sure you identify procedures that you can put in place to detect breaches as quickly as possible. You might need to report a breach to the ICO, so it’s really important that everyone in your organisation knows how to recognise and highlight any breaches that occur.

The ICO have checklists available on how to prepare for and respond to a data breach, which can be found here!

STEP 11

Update your procedures for dealing with any Subject Access Requests (‘SAR’).

STEP 12

Train staff, volunteers and/or temps to ensure they know to adhere to your systems/processes. Provide checklists and/or guidance documents that may help with compliance on a day-to-day basis.

Cronfa Amaethyddol Ewrop ar gyfer Datblygu Gwledig:
Ewrop yn Buddsoddi mewn Ardaloedd Gwledig
European Agricultural Fund for Rural Development:
Europe Investing in Rural Areas
Llywodraeth Cymru
Welsh Government

Task List Summary

○ Register with the Information Commissioner’s Office

○ Carry out a data audit

○ Identify risks (and document them)

○ Understand when Data Protection Impact Assessments are required

○ Create/update your data protection policy

○ Review/update privacy notices

○ Review how you will seek, record and manage consent

○ Determine whether you need to legally appoint a Data Protection Officer

○ Consider how you can ensure you are processing data in line with an individual’s rights

○ Identify procedures to prepare for and respond to a data breach

○ Update your procedures for [dealing with a Subject Access Request]

○ Provide training and checklists/guidance notes to help your staff or volunteersprocess data in a compliant way

Cronfa Amaethyddol Ewrop ar gyfer Datblygu Gwledig:
Ewrop yn Buddsoddi mewn Ardaloedd Gwledig
European Agricultural Fund for Rural Development:
Europe Investing in Rural Areas
Llywodraeth Cymru
Welsh Government