Act Now GDPR Policy Pack

User Guide

GDPR compliance is a complex task requiring, amongst other things, a set of policies, procedures and notices. This can be daunting especially for organisations starting on this journey.

We have applied our information governance knowledge and experience to create a policy pack containing essential documentation templates to help you meet the requirements of GDPR as well as the Data Protection Act 2018.

You will need to adapt the templates to fit your organisation's circumstances and requirements. Text highlighted in yellow indicate areas that are most likely to require review and amendment. Before doing so please read the guidance notes and blog posts listed in the Appendix.

In some templates, reference is made to a Data Protection Lead as opposed to a Data Protection Officer (DPO). This is because, in the case of those organisations who do not by law have to nominate a DPO (businesses and third sector organisations which are not engaged in large scale monitoring or processing of Special Category data), if they name someone as a DPO they then take on the legal obligations set out in Articles 38 and 39 of GDPR. For this reason we use the neutral term DP Lead. If your organisation has appointed a DPO, please amend the documents accordingly.

Contents

- Data Protection Policy - To give you an overarching framework for the governance of personal data processing
- Special Category Data Processing - To assist in compliance with the requirements of Schedule 1 (Part 4) of the Data Protection Act 2018
- CCTV - A basic policy providing a high-level description of governance and controls on the use of CCTV
- Information Security - A basic policy providing a high-level description of governance and controls in the area of information security

These policy templates will require you, at the very least, to insert the organisation name and relevant contact details, replace the Act Now headers and confirm the various role details. In most cases you will also have to edit the templates to reflect your organisation's approach and controls.

3. Template procedure documents:

- Data breach reporting
- Data Protection Impact Assessment template
- Data Subject rights request templates

The Data Protection Impact Assessment(DPIA) template is adapted from the Information Commissioner's Office (ICO) template, with some clarification of language, the addition of document control and a tracker for recording responsibility and progress against actions identified in the DPIA. This can be omitted if you track these separately in a risk register or issues log.

The Data Subject rights response templates provide a starting point in addressing the potentially vast range of permutations in dealing with requests. The Subject Access Request response template addresses the types of contextual information to which applicants are entitled under Article 15 of GDPR, in addition to access to their data. However, you may already address much of this context in your privacy notices.

A combined set of trackers and logs (Excel workbook "Data Protection trackers template.xls)

The tracker spreadsheets include:

- Information Asset Register
- Record of Processing Activity (Article 30)
- Record of Special Category Data processing
- Data Subject Rights request tracker

- Information security incident log
- Personal data breach log
- Data protection advice log

The above documents are inter-related and contain cross references, particularly across the various tracker logs.

Not all information security incidents will be personal data breaches according to the definition in Article 4 of GDPR. For that reason, we have two separate sheets in the tracker logs: A basic Information Security Incident log to capture incidents and near misses and, where these are identified as personal data breaches, they can also be recorded in more detail (including decisions on whether or not to report to the ICO and Data Subjects) on the Personal Data Breach log.

While the Information Asset Register(IAR) is not a requirement of GDPR, many organisations find it a vital tool in providing visibility of information assets. There are also clear links between the IAR and the record of processing activities required under Article 30 of GDPR. We recognise that a single information asset may be used in more than one processing activity and that a single processing activity may involve more than one information asset. For that reason, our templates for both the Information Asset Register and the Article 30 Record of Processing Activity contain columns for cross-referencing between them.

Feedback

Data protection law is complex and open to interpretation. The Act Now GDPR Policy Pack is designed to provide you with general templates which can be used as the foundation upon which you can design your own organisation specific policies and procedures based on your own data processing activities. This policy pack is not a comprehensive solution for GDPR compliance and it is not intended to replace your own independent legal advice.

We know there is always scope for improvement. Please feel free to send us your comments and suggestions.

Act Now Training

www.actnow.org.uk

info@actnow.org.uk

01924 451054

Appendix

List of Useful Guidance Notes and Act Now Blog Posts

TOPIC	URL
Privacy Notices	A29WP Guidelines on Transparency: https://tinyurl.com/y8h4xckq Act Now Blog post: https://tinyurl.com/y9bzel4m
CCTV	Act Now blog post: http://tinyurl.com/yaxgdg7h
Information Security	ICO Guide: https://tinyurl.com/y8az28o5 Act Now Blog Post: https://tinyurl.com/hcghlfj
Breach Reporting	A29WP Guidelines on Breach Notification: https://tinyurl.com/y8h4xckq ICO Guidance on Personal Data Breaches: https://tinyurl.com/yaf8xdnu
DPIAs	A29WP Guidelines on Data Protection Impact Assessments https://tinyurl.com/y8h4xckq Act Now Blog post: http://tinyurl.com/yd2l249s
Article 30 Records	ICO Guidance on Article 30 records: https://tinyurl.com/y9754wxu
Subject Access	Act Now Blog post: https://tinyurl.com/zlf44g9
Data Portability	Act Now Blog post: https://tinyurl.com/y7z3hr9u