Strategic Perspectives | Cybersecurity Policy Report

Data Protection Audit — What You Need To Know

By Monica Mastropasqua of Clarkslegal

A data protection audit is the process of auditing all of your data protection processes and procedures to understand your current levels of compliance and identify any areas for improvement. This will include a review of any information your business holds relating to its employees and staff, its clients and customers, suppliers, prospective purchasers and suppliers, and even any individual contacts within your network.

The audit can be conducted internally or by appointing a data protection solicitor to undertake the review on the organisations' behalf If engaging with a solicitor, following a data protection audit, they can also provide you a comprehensive plan to ensure compliance with data protection laws. Our expert lawyers are ready to assist all businesses and have expertise in drafting General Data Protection Regulations ("GDPR") compliant contracts, employment agreements, and other commercial documents that involve sensitive or special category data.

Why conduct a data protection audit?

The primary purpose of an audit is to assess whether an organisation has effective policies and procedures in place for managing personal data and if these practices are being correctly implemented. Adhering to these standards ensures that organisations handle personal data responsibly and comply with relevant law and guidance,

However, most businesses undertake a data protection audit in order to in order to mitigate the potential impact of a data breach by understanding the data their data flow, the types of data they collect, and whether adequate security measures are in place. The guidelines are outlined in the GDPR and the UK Data Protection Act (DPA), and they state that non-compliance with GDPR regulations can result in hefty fines, reaching up to £17.5 million or four percent of global annual turnover, whichever is greater. Conducting a data protection audit can prevent compulsory and mandatory audit by the Information Commissioner's Office ('**ICO**').

Conducting a Data Protection Compliance Audit step by step

Under GDPR, businesses that control or process data must continuously demonstrate compliance. Performing a data protection audit indicates your commitment to meeting these obligations and proactively addressing any potential breaches.

The following are the relevant steps to conduct a Data Protection Compliance Audit:

Planning and Preparation

First, it is crucial to secure board-level support for GDPR compliance. The board must understand both the benefits and challenges of the GDPR to effectively allocate resources. They need to be educated on data protection risks and the advantages of GDPR compliance.

Once top-level understanding and support are in place, the next step is to plan and prepare for the audit. This step will clarify the audit's purpose, the areas to be examined, the financial resources available, and the schedule for completion.

Next, specific roles should be assigned, including designating a Data Protection Officer ('**DPO**'), to ensure responsibilities are clearly defined and managed effectively. Additionally, all relevant stakeholders, including employees, should be informed about the upcoming audit. This communication helps manage expectations, facilitates cooperation, and ensures everyone involved understands their roles and responsibilities during the audit process.

Data Inventory

Understanding the nature of the data your organisation collects is vital for recognising risks in handling, storage, and transfer of the same. Establishing a thorough inventory of your data is key to formulating an effective GDPR compliant plan.

We would advise a business starts by cataloguing the various types of data you manage, including information related to customers, employees, and suppliers. Then, map the lifecycle of each data set within your business operations. This mapping should track the data's path through every physical and virtual location it inhabits. This approach helps identify all data storage areas, ensuring nothing is missed.

After completing the data mapping, share the inventory with relevant departments and stakeholders. This step ensures that all data types and their locations are accurately identified and acknowledged, promoting a unified approach to data protection throughout the organisation.

Risk Assessment

Once a business is clear on its data inventory, the next crucial step is to evaluate the risks associated with potential data breaches and compare them to GDPR requirements. This assessment should include all third parties, including customers and suppliers, involved in your data handling.

To perform a thorough risk evaluation, there are 3 key questions:

1. What are the existing compliance gaps?
2. Which areas are at risk of non-compliance in the future?
3. What immediate steps are necessary to improve GDPR compliance?

By considering and formulating responses to the above questions, you can pinpoint areas where your organisation is vulnerable, prioritise risk mitigation actions and align your practices with GDPR standards. Including third parties in this risk assessment ensures a comprehensive understanding of your data handling environment and uncovers potential compliance issues arising from external partnerships.

Policy and Procedure Review

After identifying all actual and potential compliance gaps, you may want to develop a detailed roadmap to support your GDPR implementation plan. This will outline necessary process changes and system updates to meet GDPR requirements.

This could include ensuring your data protection policies and privacy notices are GDPR-compliant, verifying that consent-based data processing meets regulations, and reviewing and updating contracts with employees, customers, and suppliers to properly address personal data processing.

You may also want to create a strategy for managing data subject access requests ('**DSARs**') within the statutory time limit of one month and establish procedures for determining when a Data Protection Impact Assessment (DPIA) is needed.

Technical and Organisational Measures

Your organisation must have a comprehensive information security policy to outline guidance on protecting personal data. Basic security measures should be in place to avoid data leaks or cyber threats, as well as using encryption to protect sensitive information.

Finally, the organisation must develop strong procedures to detect, report, and investigate any personal data breaches.

Experienced auditors

If you choose to engage our experienced team of solicitors to perform the audit, we will provide a comprehensive report. This report will include an assurance rating for each scope area, details of any non-conformities, associated risks, and recommendations to mitigate these risks. Additionally, we will provide an action plan outlining how, when, and by whom these recommendations will be implemented.

Our skilled team of GDPR auditors possesses deep expertise in data protection regulations and industry best practices. We offer detailed, objective audits customized to meet your business needs, ensuring full GDPR compliance while protecting your organisation's reputation and financial health.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Monica Mastropasqua
Clarkslegal
5th Floor
Thames Tower
Station Road
Reading RG1 1LX
UNITED KINGDOM
URL: www.clarkslegal.com

(c) Mondaq Ltd, 2024 - Tel. +44 (0)20 8544 8300 - http://www.mondaq.com