A Guide to Data Privacy and Protection

RelianceCyber

Contents

A Guide to Data Privacy and Protection

Introduction

Data privacy considerations are a part of everyday life, both for organisations and private individuals. Stories of breaches exposing the personal data of thousands or even millions of individuals are far from uncommon, and businesses are under constant scrutiny with regards to the volumes of data they process, why they process this data and how they keep it safe.

Organisations must face up to an increasingly strict regulatory landscape, which has created compliance requirements that have fundamentally impacted operations across any business function that handles personal data.

Not only are these regulations far-reaching, but they are also constantly changing, meaning businesses are always trying to hit moving targets to ensure they meet their global data privacy compliance obligations.

If an organisation processes personal data – be that of customers, prospects or employees – it will need to have a program in place to manage it. This is particularly important given the current working environment where, with more remote workers than ever, collaboration tools encourage sharing information in the cloud, leading to data potentially being accessed by people who shouldn't or stored in places that create a security risk.

What is data privacy and protection management?

Data privacy and protection management is a broad discipline which ranges from understanding where data is stored and why it is being processed, to assessing compliance with global regulations (such as the UK/EU General Data Protection Regulation - GDPR), to overseeing fundamental process, policy and technical upgrades to make sure that data is properly managed in keeping with local and global legislation and guidance.

The Information Commissioner's Office (ICO), the UK's data protection watchdog, has been extremely active in responding to complaints from data subjects and breaches of personal data failing to meet their obligations under the GDPR.

British Airways (£20M), Marriott Hotels (£18.4M) Interserve Group (£4.4M) and, as recently as April 2023, TikTok (£12.7M) have all been served large penalties after breaching data privacy regulations – and the ICO has made it clear that it will pursue companies that do not have an active data privacy management program in place.

In response to the fine given to construction group Interserve in October 2022, John Edwards, the Information Commissioner, described "*complacency*" within organisations as the biggest cyber threat. "*If your business doesn't regularly monitor for suspicious activity in its systems and fails to act on warnings or doesn't update software and fails to provide training to staff, you can expect a similar fine from my office*".

This is a powerful message concerning regulators' expectations around protecting personal data, and a clear warning for those who fail to take manging this data seriously.

Unlocking the key to data protection: Essential data privacy and protection services

Data discovery and Data Loss Prevention

Data Loss Prevention (DLP) is a set of tools and processes to help ensure sensitive information is not misused, lost or accessed by unauthorised parties. DLP can help solve major pain points for organisations around the data they hold, namely: protecting and managing personal information; protecting intellectual property; and increasing visibility of company data.

This, in particular, will identify and help address issues created by collaboration tools in the modern working environment, where data is often shared in the cloud with individuals that should not have access to it (both in and outside organisations) or stored insecurely leading to the risk of a breach.

DLP can help an organisation understand the size of this data footprint, the risks it creates and how to take back control.

Organisations are often not aware of the volume and types of data that are being gathered, and for what purpose. This is further complicated by the fact that the definition of processing in the GDPR is so broad. Getting to grips with these questions is vital to designing measures that work to protect the data being held and maintain data privacy compliance.

Securing your data assets: Top DLP services every organisation must utilise

Data discovery and mapping - The first step in protecting and managing personal data held by a business is understanding what data is being collected, how much is being collected and where it is being stored. This can be achieved through a data discovery exercise, and the creation of a data map, which will help you both answer the questions posed above and see exactly where your data sits.

DLP analysis and consulting - A DLP investigation can help an organisation better understand the data it holds and provide recommendations to better protect it. These assessments include analysis of policies, processes, and technology implemented to guard against inappropriate data disclosures, and recommendations to close any gaps.

Implementation of DLP tools and solutions - Once an organisation has determined that it has gaps in its DLP protections, it may choose to implement an appropriate DLP tool. This implementation has to be carried out carefully and methodically, not only from the perspective of configuring the technology, but also in ensuring that a business has the right processes, procedures and controls to help any DLP tool work successfully.

Exploring the role of assessments in managing data protection compliance

Data privacy and protection regulations such as the GDPR provide key principles and rules around processing personal data that businesses must follow to remain compliant. Conducting a review of internal processes and controls against the requirements of the GDPR and other applicable laws will help an organisation identify areas for improvement and assess its overall compliance with those regulations.

Data privacy rules are ever changing and will vary from jurisdiction to jurisdiction. For global businesses, this can create a challenge to stay on top of all the regulations that apply to thier operations – as well as considering any privacy-related standards that can help promote good data protection hygiene.operations – as well as considering any privacy-related standards that can help promote good data protection hygiene.

Book Your Free Consultation

Planning for success - Essential Considerations for an assessment

Gap analysis and compliance reviews - A gap analysis will help an organisation understand exactly where they have potential issues and where to focus effort and resource in improving its overall compliance. This will involve analysis of an organisation's compliance with a range of standards specific to its requirements, from the GDPR and similar regulations (e.g., the California Consumer Privacy Act, Dubai International Finance Centre's data protection law, and Brazil's LGPD), to industry-specific laws, such as the US Health Insurance Portability and Accountability Act (HIPPA). The results of this analysis can help improve your compliance with existing privacy and data protection laws, meet the challenge of expanding into new jurisdictions and sectors, or anticipate improvements ahead of regulatory changes.

Compliance mapping across different privacy frameworks - The production of a global data protection framework can help consolidate multiple privacy-related regulations that an organisation needs to comply with into a single set of controls. This ensures an organisation can be confident that it is compliant with global laws and industry best practice, wherever it operates, and makes it substantially easier to demonstrate compliance with a number of different standards and prioritise areas of improvement.

Planning for success - Essential Considerations for an assessment

Data protection health check - If you are unsure where to focus your efforts and/or require a rapid assessment of your data protection compliance, a light-touch health check can give insight into the strength of your privacy program. This will also highlight areas for further investigation and improvement to help allocate time and resource to the most pressing issues.

Technical security reviews - As part of an organisation's data protection measures, there is an obligation to ensure that data is processed securely using appropriate technical and organisational means. Whether the level of security and technical measures are sufficient to protect the data an organisation holds, and whether it should invest in any specific data privacy compliance software to manage its obligations, can be established by a thorough review of its information security environment and controls.

Assessing specific areas of data protection compliance - Data protection regulations demand that organisations are compliant in a range of areas – and you may therefore recognise that you have blind spots in only certain ones. This could mean there are concerns specifically about data transfers or cookie compliance, and you need a bespoke assessment focused solely on these areas.

Understanding the role of a Data Protection Officer

The Data Protection Officer (DPO), as described in the GDPR, is responsible for ensuring that an organisation processes personal data in compliance with the applicable data protection rules. The DPO role requires a broad level of experience and expertise, and not all organisations have the resources to appoint an individual to the position full-time – whether they are obligated to have one or not.

It is possible to outsource some of the responsibility of managing data protection obligations, either through appointing a virtual DPO or through engaging a third-party expert to support existing or new DPOs in building robust data privacy and protection programs and roadmaps.

Book Your Free Consultation

Ensuring Data Protection Without a Full-Time DPO

Virtual DPO services - A virtual DPO service allows you to rely on the experience of a data privacy expert who will work with you to oversee your data privacy program and help maintain levels of regulatory compliance within your organisation, as well as help respond to issues with regards to personal data you hold.

Data privacy and protection program development - Managing data privacy requirements presents a large number of considerations – from assessing risks to the organisation, to establishing proper processes and procedures to protect data (including privacy by design and default), to auditing and monitoring overall compliance. An organisation might consider external support to build these key components and develop a roadmap of activities to help meet its data privacy objectives and needs.

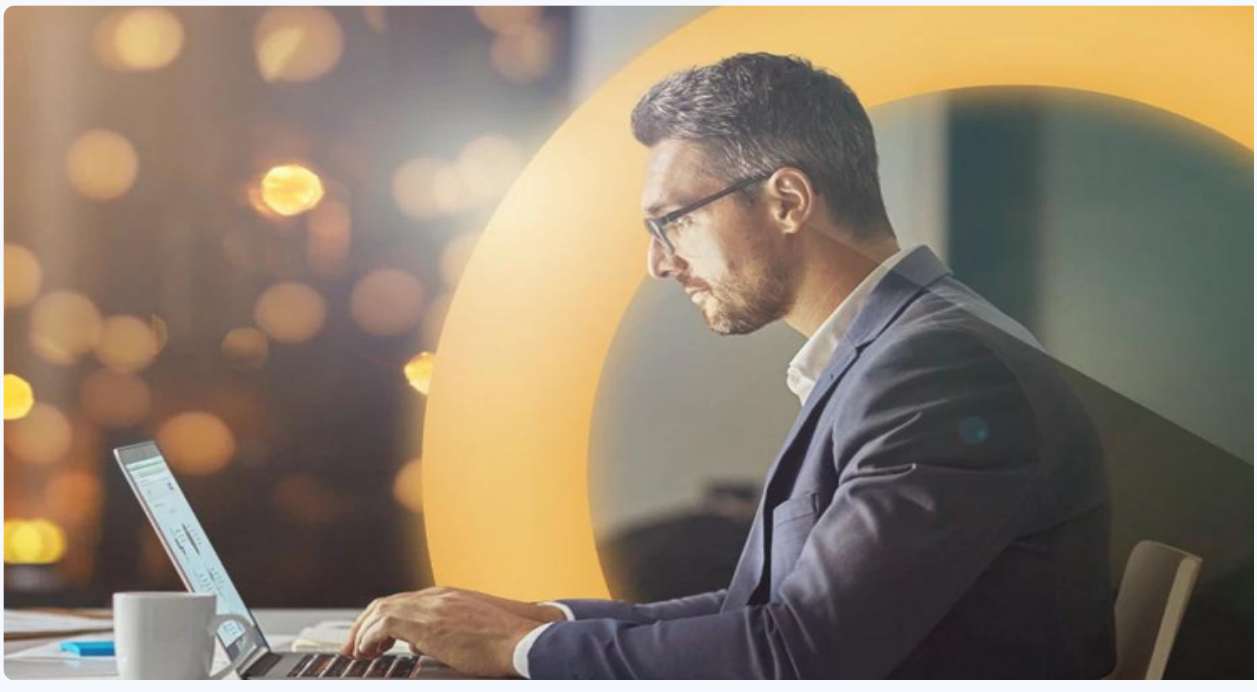
Data protection breach support - A personal data breach can unearth critical deficiencies in an organisation's data privacy and protection controls, and pressure to fix any issues quickly. Data Protection Agencies, such as the ICO, will want to see affected organisations work to close any gaps in compliance, and will often reduce regulatory fines when they see progress being made. You may wish to consider external expertise to help identify and analyse deficiencies that resulted in a breach (as well as any other potential issues) and help ensure that your organisation responds to a breach with positive and rapid improvements.

Data privacy and protection management is an important consideration for any business that handles personal data. With evolving regulatory requirements and an increasingly digital landscape, it is essential to take proactive steps to protect personal data, by implementing a robust data privacy program to safeguard against potential data breaches.

Our cyber security consultancy services help businesses understand their current data privacy and protection posture and identify areas for improvement.

About Reliance Cyber

At Reliance Cyber, we believe in truly partnering with our customers. We work with organisations in many different sectors, to defend them against advanced cyber threats including up to nation-state-level. We develop a real, in-depth understanding of the risks an organisation faces and develop bespoke solutions. Our industry-leading cyber security expertise and experience enable organisations to focus on the things that they do best.



Get a free Data Privacy & Protection Consultation with one of our cyber consultancy team today

Book Your Free Consultation