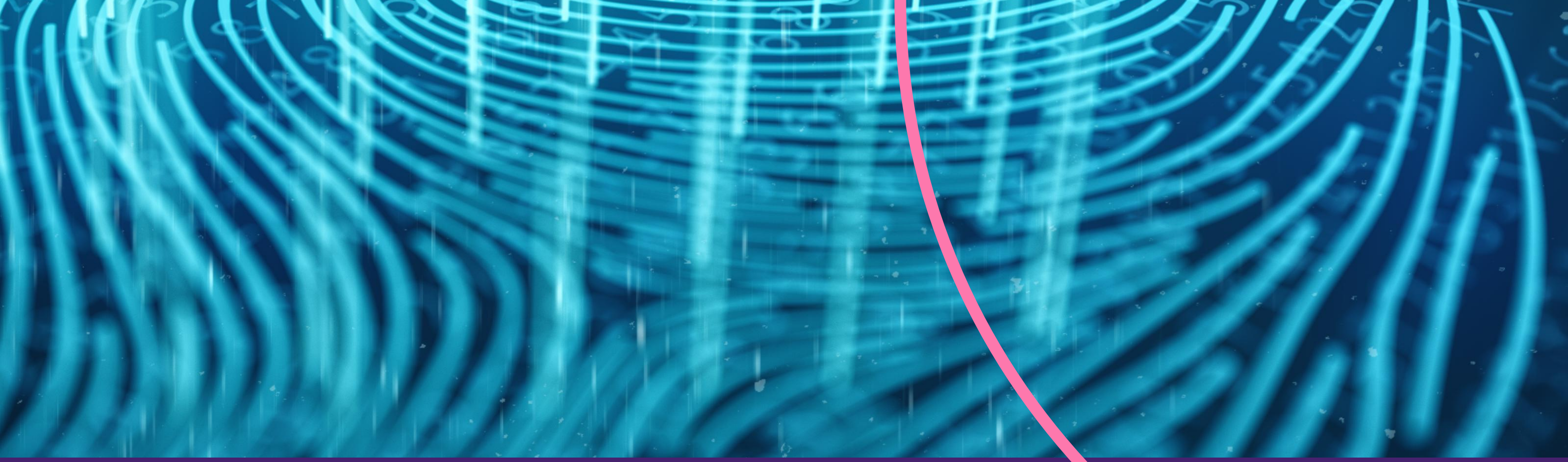


Achieving Effective Data Privacy Compliance

How to achieve greater profitability and competitive advantage through strong data protection.

The sensitive data a company holds on its employees, partners, customers and prospects is the life blood of its ability to trade and compete in a global market. Consistently ensuring the right information is shared with the right parties at the right time can make the difference between failure and success.

In the current trading conditions faced by virtually every company, finding a competitive edge and trading as efficiently as possible is literally an existential challenge and a fundamental component to any digital transformation initiative companies need to adopt.

Furthermore, never has there been greater public awareness and concern over what personal information is held by companies and how it is exploited. Regulations such as The General Data Protection Regulation (GDPR) and the UK's equally draconian equivalent - The Data Protection Act 2018 - mean that companies can be fatally damaged by the reputational and financial consequences of inappropriately storing, sharing or processing personal data.

This means the companies who manage and leverage sensitive information effectively will thrive, whilst those that don't will ultimately fail. This has been brought into even starker relief during the current trading environment, when many employees are required to work remotely, and supply chains are having to operate in different ways than they have in the past.

cloud business

espyder

Effective Data Privacy Compliance and what's required to achieve it

As with many best practices, it is useful to think of managing data privacy compliance in terms of a maturity model.

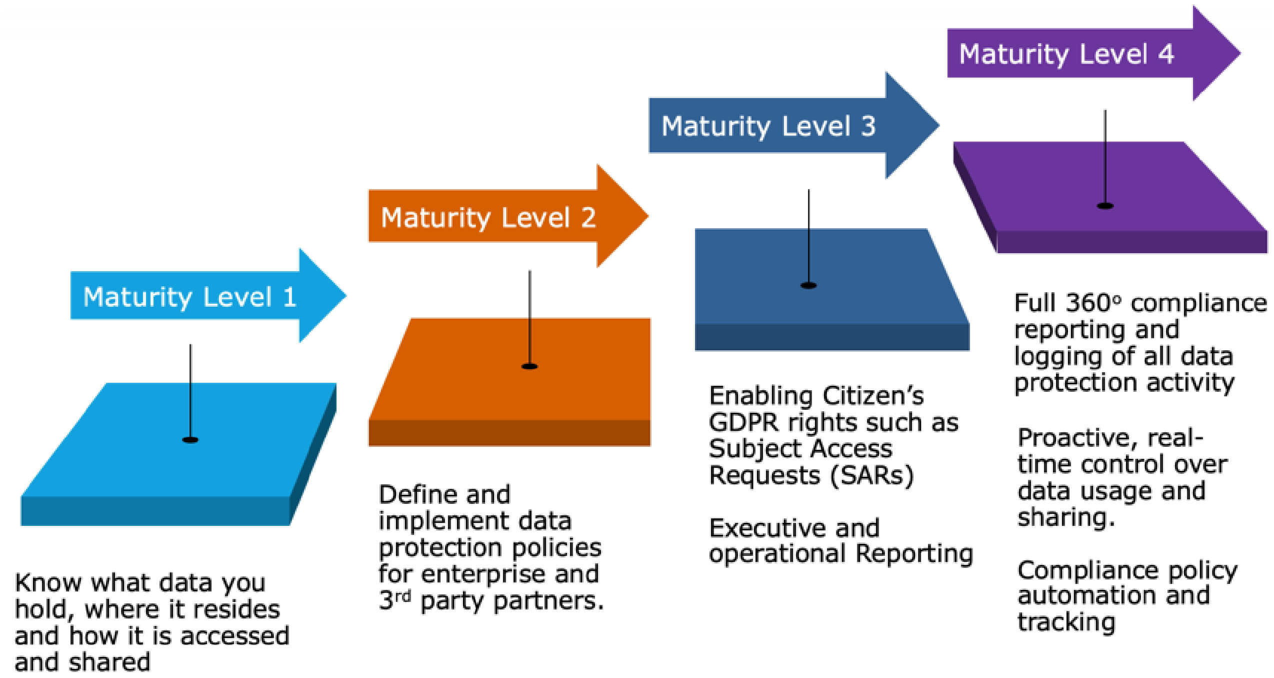

Maturity Level 1
Know what data you hold, where it resides and how it is accessed and shared
Maturity Level 2
Define and implement data protection policies for enterprise and 3rd party partners.
Maturity Level 3
Enabling Citizen's GDPR rights such as Subject Access Requests (SARs)
Executive and operational Reporting
Maturity Level 4
Full 360° compliance reporting and logging of all data protection activity
Proactive, real-time control over data usage and sharing.
Compliance policy automation and tracking

Figure 1: Data Privacy Compliance Maturity Model.

The basic questions the Data Protection Officer must have the answers to are:

1. What data do we hold and for what purpose?
2. Do we have the consent of the individuals to hold their data and for the purposes we use it?
3. Have we documented our data protection and processing policies as required by law?
4. Do we operate effectively in line with those policies?
5. Can we support the rights of our employees, customers and prospects to access their data and request its amendment, or removal from our systems, as appropriate?
6. Where are we in our maturity journey? The ultimate goal being fully automated, real-time controls over data processing, sharing and compliance management.

The **General Data Protection Regulation** was adopted in April 2016 and companies had 2 years before it became enforced in May 2018. European Regulators stated that companies should have effective controls and policies in place by May 2018. This meant companies should have appointed a DPO, audited what data they store and who it is shared with. Ensure consent has been gained from the individuals whose data the organisation holds and document their compliance policies and operational practices. In reality, many organisations have struggled to identify what data they hold and where it resides. One off data audits are costly, time consuming and quickly became redundant as data storage and sharing continued to evolve in their companies.

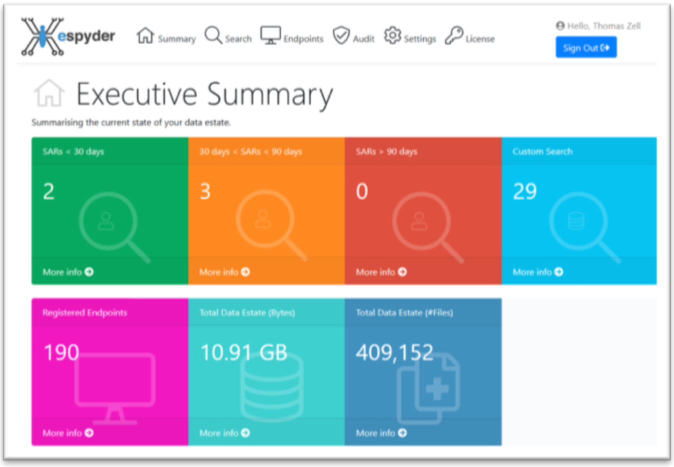
Another major challenge companies typically struggle to overcome is that managing and reviewing data is often a resource intensive and manual exercise that relies heavily on IT, even though the DPO and other business managers are often the stakeholders who ask the questions and need the answers regarding data privacy and compliance. As an example, processing a Data Subject Access Request (DSAR) from an employee or customer can cost thousands of pounds and take longer than the 30-day legal deadline mandated by the GDPR.

Conclusion

Ensuring your company knows where its data resides and that it is shared appropriately provides significant competitive advantages over companies that struggle to achieve that obligation.

Managing how data is leveraged appropriately will ensure greater business agility which is critical in today's business environment. Automating your data privacy compliance as much as possible will help drive revenue generation activity, lower operational costs and ultimately increase company profits.

Cloud Business assist its customers achieve their Data Privacy Compliance by offering its Data Discovery and Compliance Reporting Service in collaboration with eSpyder.



Executive Summary

Summarising the current state of your data estate.

SARs < 30 days
2
More info

30 days < SARs < 90 days
3
More info

SARs > 90 days
0
More info

Custom Search
29
More info

Registered Endpoints
190
More info

Total Data Estate (Bytes)
10.91 GB
More info

Total Data Estate (#Files)
409,152
More info

GDPR Compliance Platform

Do you know where all your organisation's PII is? Could remote workers have exported data onto a personal laptop to review or manage it? Or might a disgruntled ex-employee demand a DSAR knowing that this will result in a costly and protracted process to identify their PII?

The financial consequences of these scenarios are just as compelling as the much publicised <€20 million fines the regulators can levy, and for many organisations much more likely.

That's why Cloud Business and our technology partner eSpyder have developed a GDPR Compliance Platform to support Data Processing Officers (DPOs) and ensure company compliance with GDPR regulations and global data privacy legislation.

espyder

Our service includes:

- **Data discovery & review**
- **GDPR compliance assessment & implementation**
- **Monthly data discovery & reporting**

Our GDPR assessment and data discovery service also ensures your DPO can respond to Data Subject Access Requests (DSARs) quickly and easily, tracking progress and reducing the cost of compliance.

Based on the industry leading eSpyder Enterprise PII identification engine, eSpyder is able to rapidly identify Personal Identifiable Information across a customers estate no matter if on servers, clients, visible or hidden, remote or on premise.

To explore our GDPR service in more depth, contact the Cloud Business team:

08456 808538
hello@cloudbusiness.com
www.cloudbusiness.com

cloud business