

oysterims*

Information governance specialists
Consulting | Software | Service

The CEO's guide to data protection and privacy



Why data protection and privacy matters



Data protection and privacy either matters...or it matters a great deal. Whilst for some organisations data protection and privacy is merely an essential component of a regulatory compliance framework, for others it is a cornerstone of the organisation's raison d'être for whom a privacy breach would mean more than just a large fine under GDPR – it would threaten the very existence of the organisation itself.

As a CEO or senior executive, you probably already know which of these types of organisation you are and the extent of your legal requirements under GDPR.

And knowing these things helps you to understand where privacy should be ranked on your organisation's risk register. If not, then here's a clue – it's usually very high. In fact, we work with several clients where data protection and privacy is now #1 on the corporate risk register.

Remember that at the very least an executive-backed privacy programme shows a real level of respect towards both your customers and your staff and shows them that you care about the data that they have trusted you with.



What do you need to know?

Whichever type of organisation you are, there are certain things you need to know. At the very least you need to know the goals of your organisation's privacy programme and be aware of the agreed scope and the approach being taken to achieve those goals.

One approach is to run with the risk "uninsured" and take any sanction that might come your way on the chin. Obviously this is a high-risk way to deal with compliance and again it depends on your appetite for that risk. More realistically, you might want to know the minimum level of activity suitable for an organisation like yours to comply

with relevant legislation and reduce risk levels. However, most of our clients choose to put in place a structured data protection and privacy programme that is tailored to the size and type of organisation and the level of exposure to personal data.

It usually starts with a short, sharp, "Where are we now?" privacy status review which determines the level of risk and what the current programme looks like. This is usually followed by an audit or data mapping exercise and the development of an ongoing programme of work under the guidance of the Data Protection Officer (DPO) function.

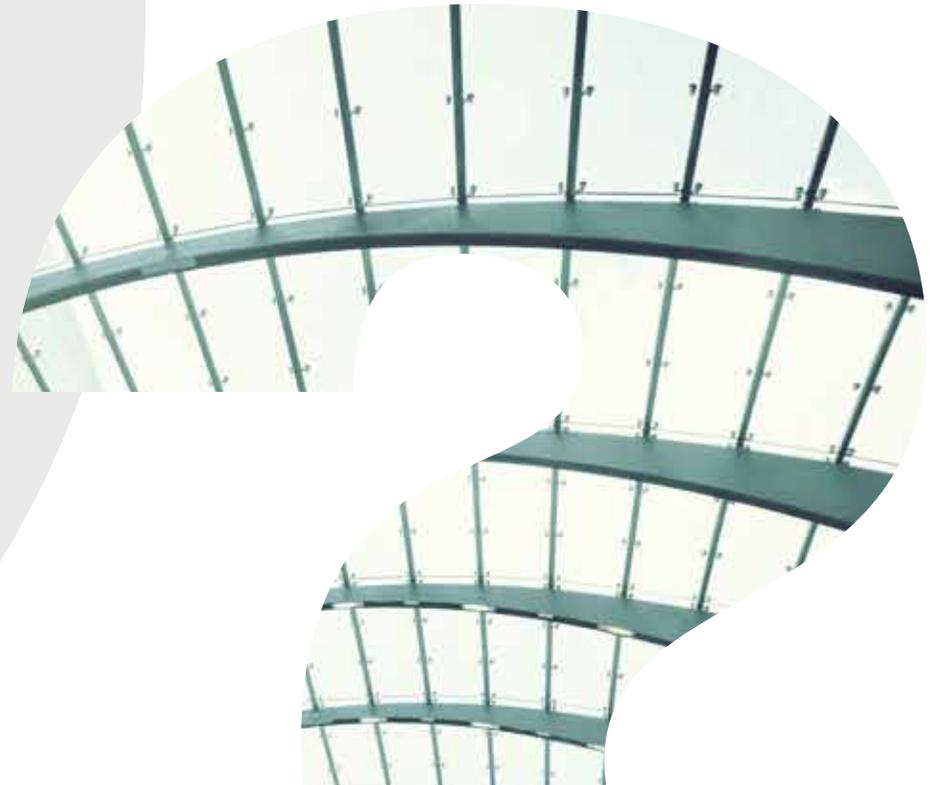
It usually starts with a short, sharp, "Where are we now?" privacy status review...

Where do you stand?

To get started, try asking yourself a few simple questions:

- Who in your senior leadership team is responsible for privacy and data protection?
- How effective is your Data Protection Officer (DPO) function?
- How successful has your GDPR programme been and how has your approach to GDPR changed in the light of the developments since the regulation was introduced in May 2018?
- Do you know what good looks like for a privacy and data protection programme for your organisation?
- What would the Regulator want to see from your organisation if they chose to review you?
- How are you making sure that what has emerged as the biggest risk area, employee malpractice or ignorance, is being dealt with appropriately?

*Ask yourself
a few simple
questions...*



Data privacy by numbers

Since the GDPR became law, in the UK alone –

33,089

complaints raised with the UK's Information Commissioner's Office. ¹

32,000

organisations have appointed a DPO. ³

11,600

breach notifications reported to the Information Commissioner's Office. ¹

78%

of organisations make privacy a board level concern. ²

56%

of organisations say they are less than fully compliant with the law. ³

48%

of organisations say the DPO is more than just a compliance obligation. ²

What next?

Oyster IMS have several offerings that can help you:

- Maturity model assessments – short, sharp engagements to understand your baseline position and produce action plans for change
- Data and information audits – deep dive engagements to diagnose specific issues and build out a full change programme
- Programme delivery – management of privacy projects and programmes including the Oyster IMS Data Protection Officer as a Managed Service (DPOaMS) offering to fully support your organisation's privacy and data protection initiatives

If you would like to find out more about these services and how other organisations similar to yours are managing their data protection and privacy programmes, then please get in touch.



Consulting



Risk & readiness assessments

Short, sharp engagements to produce action plans for change

Software



File analytics

Data mining tools to understand and manage structured and unstructured data.

Service



Implementation & delivery

World-class delivery teams offering traditional and agile approaches.



Data & information audits

Deep dive engagements to develop whole change programmes.



Document & records management

Best-of-breed software solutions delivering practical information governance.



Software & solution support

Full-service solution support and system administration services.



Programme oversight & delivery

Ongoing management of projects and programmes.



Privacy management

Tools to operationalise privacy programmes and manage ongoing change.



On-premise/ hosted managed services

Infrastructure provision to support your organisational strategy

oyster_{ims}*

Oyster Information Management Solutions
The Loom, 14 Gower's Walk, London E1 8PY
+44 (0)207 199 0620

✉ info@oyster-ims.com

🌐 www.oyster-ims.com

in bit.ly/oysterims

🐦 [@oysterims](https://twitter.com/oysterims)