

**oyster** ims\*

**Preparing for GDPR**

A brief guide to Risk and Readiness

BUSINESS WHITE PAPER



*IT IS ESSENTIAL TO CUSTOMISE YOUR APPROACH TO GDPR TO SUIT YOUR OWN ORGANISATION'S CIRCUMSTANCES*

## What will GDPR mean?

The upcoming GDPR creates a number of issues and concerns around the existence and usage of personally identifiable information (PII). In order to be ready for the new regulations you first need to get an understanding of what information you have, where it is stored, how you use it and whether it is shared with or transferred to any third parties.

## Where do you start?

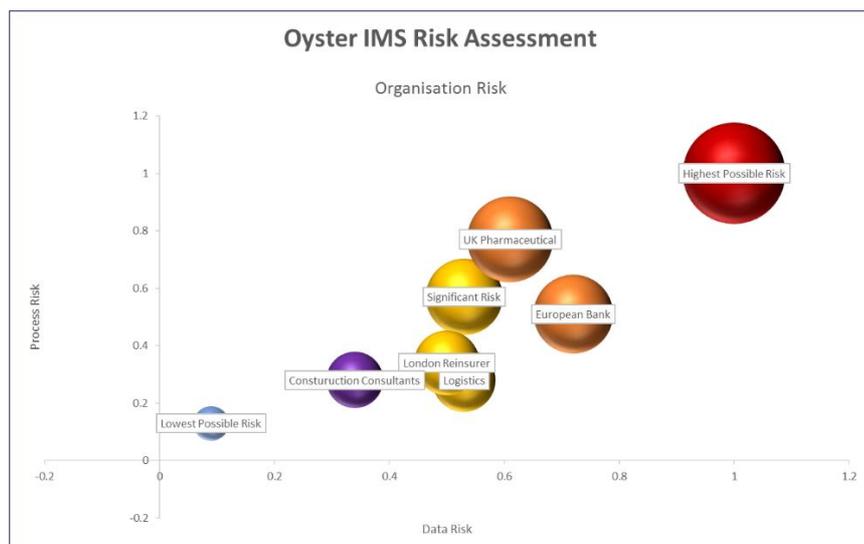
In order to get an accurate picture, you should carry out a traditional audit/information gathering exercise to establish your GDPR standing in respect of risk and readiness.

## Step 1: A High Level Risk Profile

Undertake an assessment exercise including interviews with stakeholders, workshops and questionnaires as appropriate, to capture the following:

- **Type of Personal Data Processed**
- **Volume of Personal Data Processed**
- **Size of organisation**
- **Complexity of data processing and supporting systems**
- **Complexity of organisation**

This information is used to generate an objective and specific risk measurement for the organisation which can be compared to other organisations and industries as shown below:

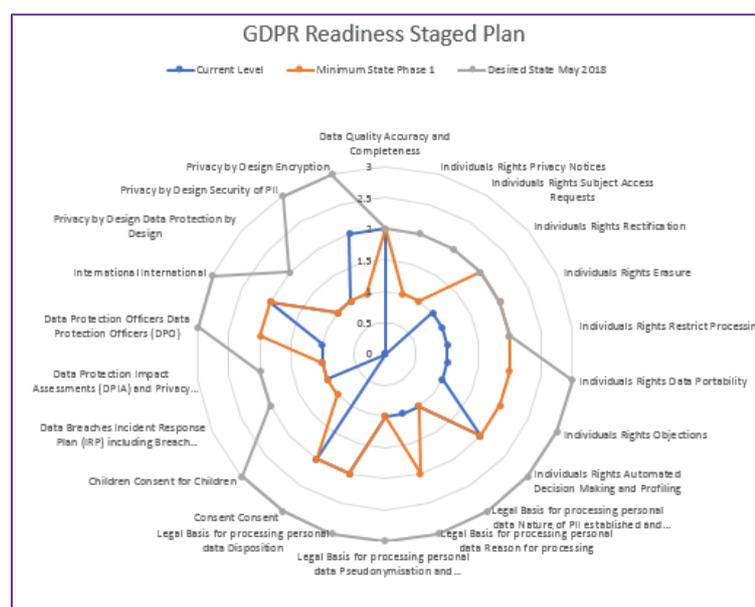


## Step 2: A Readiness Assessment

An assessment of readiness will comprise a detailed evaluation of the organisation's maturity and current capabilities via interviews, workshops and a review of relevant policies, procedures and systems currently in place. Outputs of this process can include:

- Detailed four-level readiness rating against each of the 29 data protection sub-principles
- Professional assessment of the required level of readiness in each area by the time the GDPR comes into force in May 2018
- Action Plan with detailed activities to ensure compliance with the Regulation and a set of interim tasks to deal with any immediate issues

Principle	Sub-Principle	Current	Minimum State	Desired State May
Data Quality	Accuracy and Completeness	2	2	2
Individuals Rights	Privacy Notices	0	1	2
	Subject Access Requests	0	1	2
	Rectification	1	2	2
	Erasure	1	2	2
	Restrict Processing	1	2	2
	Data Portability	1	2	3
	Objections	1	2	3
	Automated Decision Making and Profiling	2	2	3
Legal Basis for processing personal data	Nature of PII established and minimisation	1	1	3
	Reason for processing	1	2	3
	Pseudonymisation and Anonymization	1	1	3
	Disposition	2	2	3
Consent	Consent	2	2	3



## Benefits of the Assessment

The Oyster IMS Risk and Readiness Assessment gives a really good grasp of the current state and allows organisations to bring a level of control over personal data as well as ensuring compliance and reducing risk.

Carrying out this process will demonstrate to regulators that organisations are proactive in taking data privacy seriously. The ensuing actions will also reduce potential liabilities in the case of a breach.

Having taken control of personal data and ensured the systems are properly managed, organisations will reduce the likelihood of a breach – especially of the accidental type – and lessen the potential impact through an understanding of what personal data was at risk or had been affected.

*“As a leading insurer at Lloyd’s, we take our data protection obligations very seriously. Oyster IMS have provided the expertise and efficient methodology to ensure that we can continue to operate in a compliant way under the GDPR regulations”*

**Head of Information Governance and Privacy**

## About Oyster IMS

Oyster IMS offers specialist records and information governance consultancy to a variety of organisations across a multitude of sectors. We provide expert advice on information strategy, policy and process development, data protection and e-Discovery. We also assist with requirements gathering, business case development, product selection and ROI calculation. In most cases, Oyster IMS provides consultants with professional qualifications in the areas to be reviewed. Our data privacy consultants have qualifications from the International Association of Privacy Professionals (IAPP).

*For more information contact:*

*Oyster IMS, The Loom, 14 Gower’s Walk, London, E1 8PY*

*Phone: +44 (0)207 199 0620*

*info@oyster-ims.com*

*Twitter: @OysterIMS*