GDPR Services

Market Analysis
Abstract
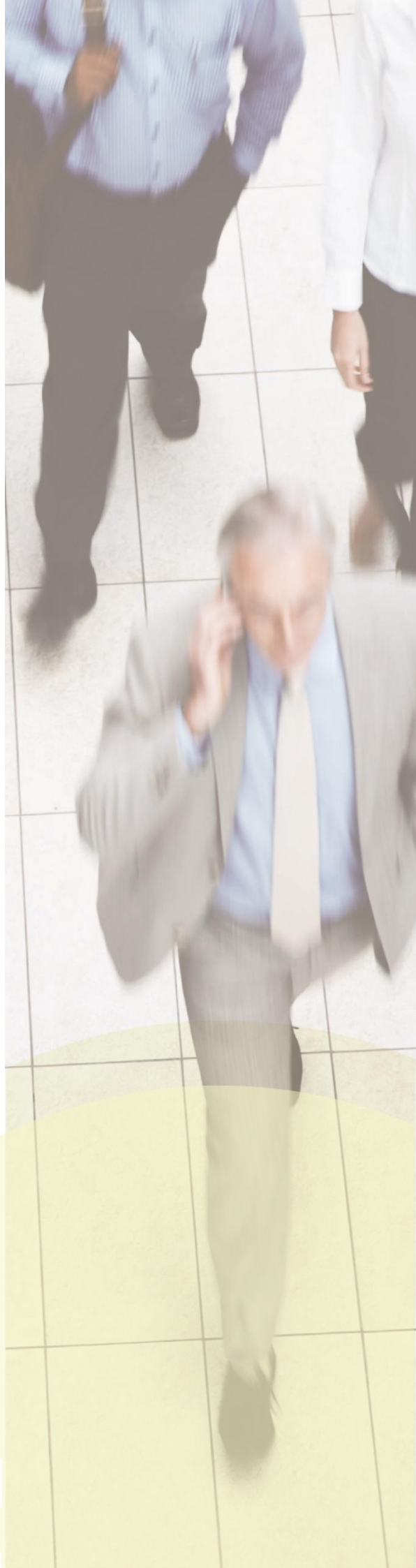
Who Is This Report For?

NelsonHall's "GDPR Services" report is a comprehensive market assessment report designed for:

- Sourcing managers investigating sourcing developments within the GDPR outsourcing market

- Vendor marketing, sales and business managers developing strategies to target ITO service opportunities within GDPR compliance

- Financial analysts and investors specializing in the IT services sector, including IT security services.

Scope of the Report

The report analyzes the worldwide market for GDPR services and addresses the following questions:

- What is the market size and projected growth for the global GDPR services market by geography?

- What is the profile of activity in the global GDPR services market by industry sector?

- What are the top drivers for adoption of GDPR services?

- What are the benefits currently achieved by users of GDPR services?

- What factors are inhibiting user adoption of GDPR services?

- What pricing mechanisms are typically used within GDPR services and how is this changing?

- Who are the leading GDPR services vendors globally and by geography?

- What combination of services is typically provided within GDPR services contracts and what new services are being added?

- What is the current pattern of delivery location used for GDPR services and how is this changing?

- What services are delivered from onshore and which from offshore?

- What are the challenges and success factors within GDPR services?

Key Findings & Highlights

NelsonHall's market analysis of the GDPR services market consists of 53 pages.

The EU's General Data Protection Regulation (GDPR) is a regulation adopted on April 8th, 2016 and will be put into force on May 25th, 2018. The regulation is the result of four years of preparation and debate by the EU Parliament, with an aim to bring data protection up to date as the previous legislation, the 1995 EU Data Protection Directive (Directive 95/46/EC) being terribly outdated.

GDPR has stricter controls and definitions on:

- The data that GDPR applies to
- When organizations can process personal data
- The definition of consent
- The control a data subject has over its data
- Obligations for controllers and processors.

The regulation imposes higher fines for non-compliance, the fines are divided into two categories:

- Fines of up to €20 million or 4% of worldwide annual turnover for the preceding financial year whichever is greater for serious cases such as large breaches
- Fines of €10m or 2% of worldwide annual turnover in less serious cases such as procedural failures.

While organizations should be undergoing action to meet the requirements of GDPR to avoid these hefty fines, there are a number of other benefits that arise in working towards this level compliance:

- GDPR can be seen as a chance to review the company's data handling processes, restructuring them not only to meet compliance but also to identify potential efficiency gains or new business opportunities/revenue streams
- Increasing the level of security of personal data through encryption or pseudonymization will build trust with users, as breaches of the organization's cybersecurity are less likely to impact them
- In performing a review of IT processes, organizations will be able to identify and eliminate 'shadow IT' and build proper processes that are known to the organization
- By being shown to work with the supervisory authorities and trying to protect personal data, organizations will presumably have less reputational damage if they have a personal data breach
- Greater cybersecurity intelligence and mindshare from training and from forcibly raising the profile of cybersecurity to the C-level (see DPO)
- It is a chance to improve IT systems and processes behind the scenes, e.g., through the implementation of customer identity and access management (CIAM) and by moving away from old-style backup systems.

Contents

Report Length

53 pages, consisting of 8 chapters

Report Author

Mike Smart

mike.smart@nelson-hall.com

Vendors Researched

Atos, Capgemini, DXC Technology, IBM, Infosys, LTI, Secureworks, Sopra Steria, TCS