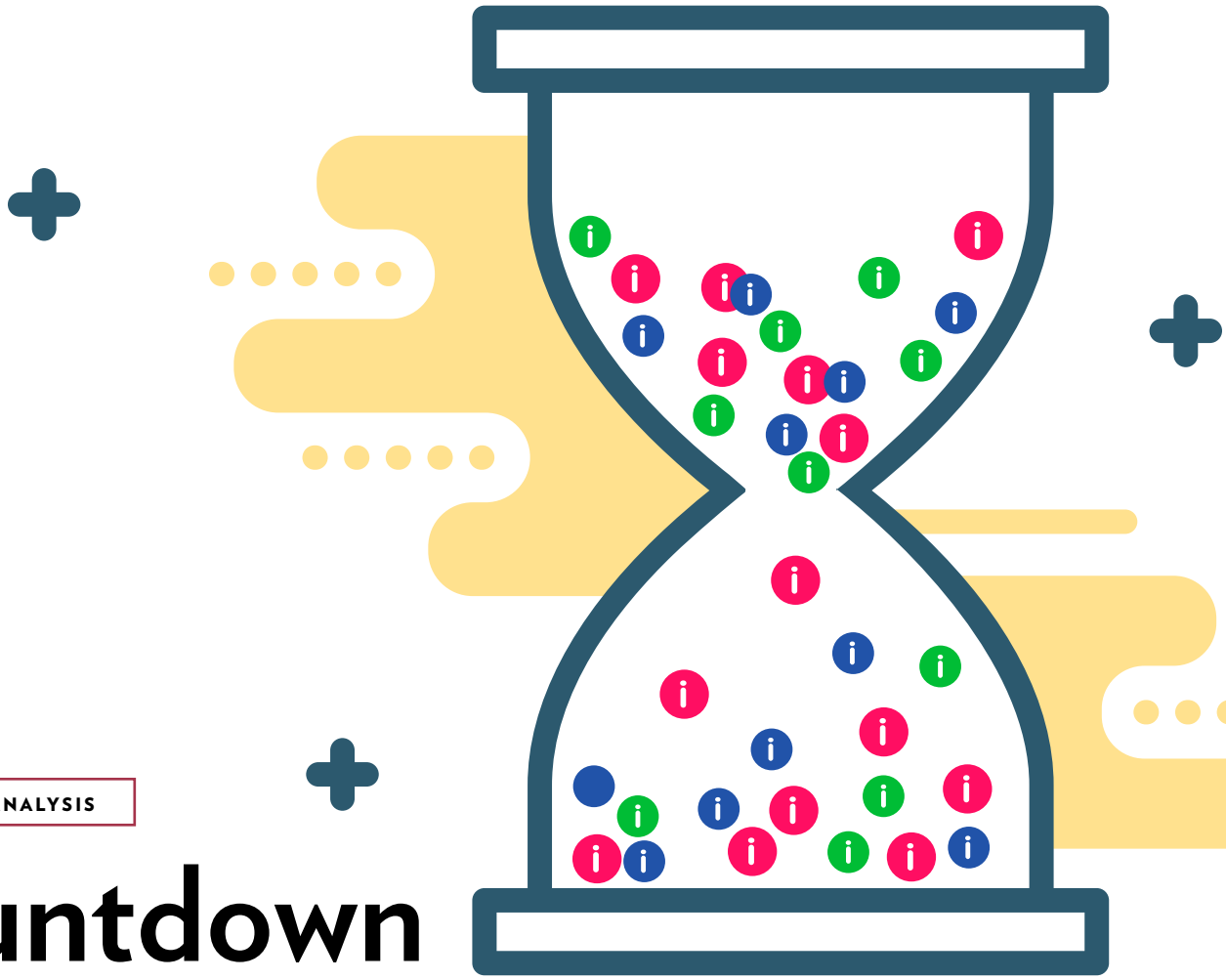
July 2017

Briefing

SMARTER LEGAL BUSINESS MANAGEMENT

Seize the play

Carol Sawdye, global chief operating officer of the PwC network, on why you might need to take a risk or two to win at this game



INDUSTRY ANALYSIS

Countdown with confidence

Ian Raine, director of product management at iManage, reminds us that there's just under a year to go until EU citizens have new rights over what we do with their data

The European Union's General Data Protection Regulation (GDPR) – which takes effect on 25 May 2018 – is officially less than a year away. This is the final countdown, and as the clock ticks on toward the enforcement date, the question remains: will professional services firms in the UK be able to meet GDPR's numerous requirements and ensure compliance?

This will be no small undertaking. Four years in the making, the new rules represent the most important change in data privacy regulation for 20 years. The definitions of "personal data" and "sensitive personal data" have been significantly widened, and the requirements around how that data is processed and stored have expanded.

Meanwhile, the territorial scope of the regulation has increased – GDPR applies not just to all EU member states, including the UK (for now at least), but also to non-EU companies that process personal data of individuals in the EU. The penalties for non-compliance have also mushroomed: organisations in breach of GDPR can be fined up to 4% of annual global turnover, or £20m (whichever is the greater).

To better understand the potential impact of GDPR and how best to reduce exposure, all firms in the UK now need to ask themselves: are we storing or processing personal data/sensitive personal data – and critically, is this data adequately protected?

In many cases companies will need a revised information governance strategy in order to respond with an unqualified 'yes'.

Change of governance

When we talk about information governance, we're referring to the ability to manage, secure and

For more information, visit: www.imanage.com

Firms will need to notify the authorities of any data-protection breaches within 72 hours of becoming aware that one has resulted in unauthorised loss.

govern critical information at every step of a professional engagement – from inception to closure, and beyond, including disposal when policy rules permit.

Information governance starts with a comprehensive document management or work product management system that can capture and organise sensitive information embedded in email and other communications streams, as well as the firm's documents.

Many of the GDPR's requirements centre on the idea of security and privacy by design, which means firms should look for a work product management system that provides support for multi-factor authentication – requiring the user to have more than a password to get access. The system should also offer matter or project-level security, enabling restriction of access to team members only. And it should provide encryption at rest and in motion, so data isn't easily compromised in the event of a breach.

Speaking of the cyber threat, under GDPR firms will need to notify the authorities of any data-protection breaches within 72 hours of becoming aware that one has resulted in unauthorised loss, amendment, or disclosure of data. If there's a high risk to the data protection rights of any affected clients, prospects or employees, firms will also need to communicate the breach promptly to the data subject individually.

In order to best address this aspect of GDPR, firms will want a system with the ability to detect an intrusion quickly through behaviour analytics to limit or minimise the data loss. Correct data access audit trails, which can provide a method for identifying the scope of a data breach, are also desirable. Without these types of features to help identify what specifically has been breached, firms will need to inform all potentially affected parties, which could dramatically – negatively – affect a firm's reputation.

Rights moves

A separate point is that data subjects have new and expanded rights under the GDPR, including the "right to access" (to obtain confirmation from the data controller as to whether or not personal data is being processed, and to receive a copy, free of charge, in a portable electronic format) and the "right to be forgotten." Also known as data erasure, the latter entitles the data subject to have the controller erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

To satisfy these, companies should look for a system that offers the ability to track all personal data mapped to each client and engagement, as well as enterprise-grade search across different repositories. These capabilities can ensure compliance with data access requests and help to discover data for return, erasure and portability.

Finally, a comprehensive information governance strategy should also apply to any cloud service providers (CSPs) firms engage. To ensure GDPR compliance, firms should carefully evaluate any CSP against its ability to meet GDPR requirements, and ensure contracts with the CSP contain the appropriate language.

It's critical for all UK firms to start planning now for how they will respond to these extensive requirements. With a robust information governance strategy, firms can start implementing the controls and protections needed to achieve strong security for their client, prospect, and employee personal data, ensuring a worry-free countdown to GDPR compliance.