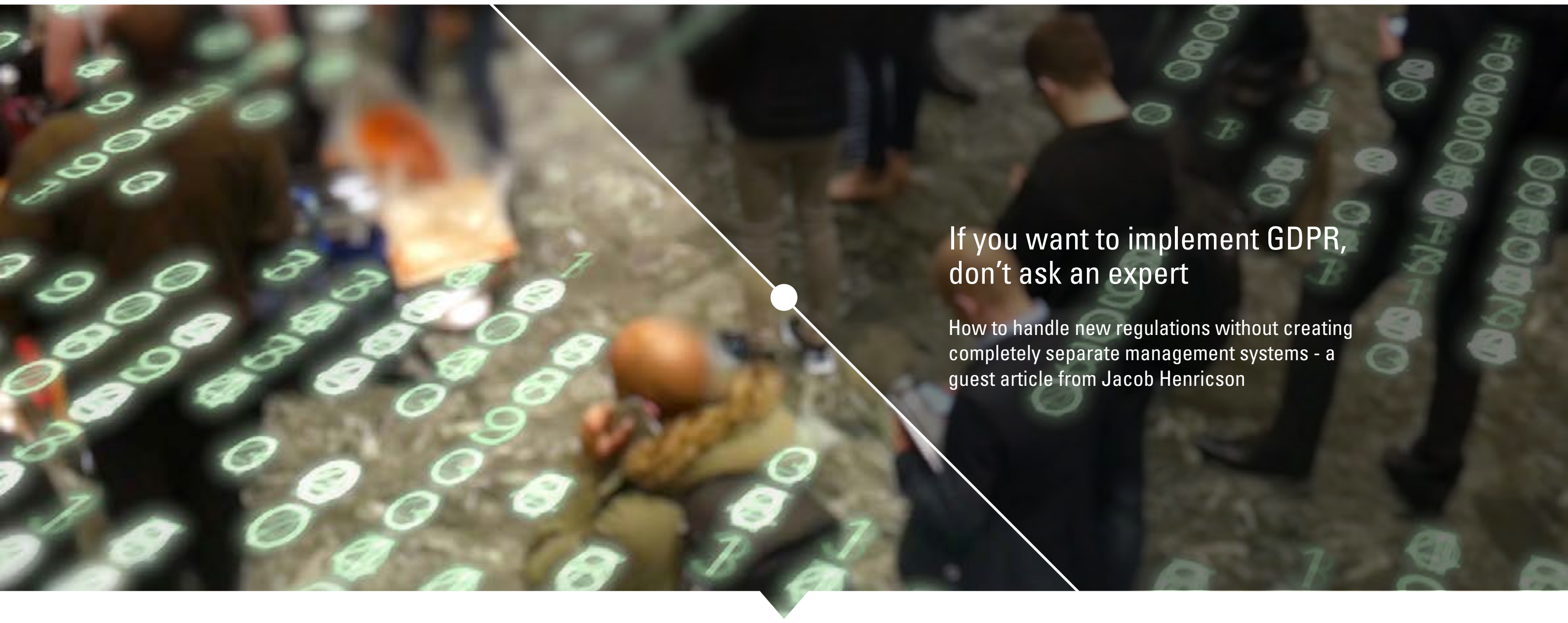
human resourcefulness
globally delivered
a:connect



If you want to implement GDPR, don't ask an expert

How to handle new regulations without creating completely separate management systems - a guest article from Jacob Henricson

On 27th April this year, the European Parliament voted to adapt the new General Data Protection Regulation (GDPR). As the first EU data protective directive for more than 20 years, it aims to 'strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market.'[1] After the law is adopted, there is a two-year 'grace period' for adoption, but organizations should, of course, start the work as soon as possible.

The arguably most publicized change is that violations by companies can lead to huge sanctions: 4 percent of annual turnover or €20 million ('whichever is higher'). It remains to be seen whether this option will be exercised, and to what extent, but it has certainly received some attention. Other changes include the need to report incidents within 72 hours, a requirement for organizations in the scope to appoint a Data Protection Officer (DPO), and a general strengthening of the rights of citizens over their own information.

The GDPR joins a long line of compliance requirements that have been hitting organizations for the past decades. For a few years, I was Head of Compliance for a Fortune 500 company and saw the increase firsthand. It seemed that every other week we were asked by customers, governments or international organizations to comply with rules in new areas: security, privacy, occupational health and safety (OHS), conflict minerals, and environment and corporate social responsibility, along with many other national and international requirements that put a lot of stress on the organization.

Every time a previously unknown requirement popped up from a customer, we looked within our organization; most often, there was an expert somewhere. The experts were then called into the headquarters to set up a compliance response to the new requirements. But over time, we found that we could not give the expert the lead on the integration. Why not?

The plus sides are obvious: the expert is knowledgeable and often very committed, but the problem with experts is that they have – by definition – narrow expertise. If you are an OHS or security expert, it is very rare that you have any wider experience of management. The typical response, then, is to treat each new requirement as something fundamentally new. That leads to the creation of tailored responses that do not integrate with already existing solutions. All of a sudden, you have one management system for security, another for privacy, and yet another for conflict minerals. In the worst-case scenario, you have one of each in each country you operate in. You can forget about scale and skill then.

[1] http://europa.eu/rapid/press-release_MEMO-15-6385_en.html

Most compliance regimes have a lot in common. For example, they all require some sort of demonstrable management commitment, documentation, policies, etc. Within IT jurisdiction controls – like change and patch management – are requirements of many different standards.

That means that a lot of work can be done on a common level to address several different compliance requirements. Once those elements have been addressed, it is possible to address unique aspects of different legislations or standards. That is where the experts come in.

For example, to address the GDPR, companies need to know where in their IT environment they have personally identifiable information (PII). Privacy risk assessment workshops need to be set up and conducted efficiently. An expert can help with that. But the requirement to report to authorities within 72 hours is not so clear-cut. For most, if not all, organizations, this requirement will need to be carefully integrated with other reporting procedures, such as the whistleblower and the IT incident reporting procedures. The person leading that effort cannot be (just) a privacy expert, they have to be someone who understands the complexities and challenges of general management.

So, what should you do to address the GDPR without creating a completely separate management system?

1. Put the ownership of implementation with someone who has an overview and understands the challenges of day-to-day management. This is not a role; it is a person. It is someone with the intellectual faculties to be able to tackle complex issues, the experience to know what works, and the diplomatic skills to negotiate a 'good-enough' solution that fits all needs without costing a fortune.

2. Make sure s/he has the expert support s/he needs, but retains ownership of the process.

3. Have as few controls as possible, and let the people who are normally in charge of the processes work out how to make them as effective and efficient as possible.

4. Follow up qualitatively, as well as quantitatively, to ensure that the controls are meeting their objectives.

5. Let senior executives do the actual follow up as often as possible. It will help them understand the integration of different requirements under their responsibility and immediately address problems that are discovered.