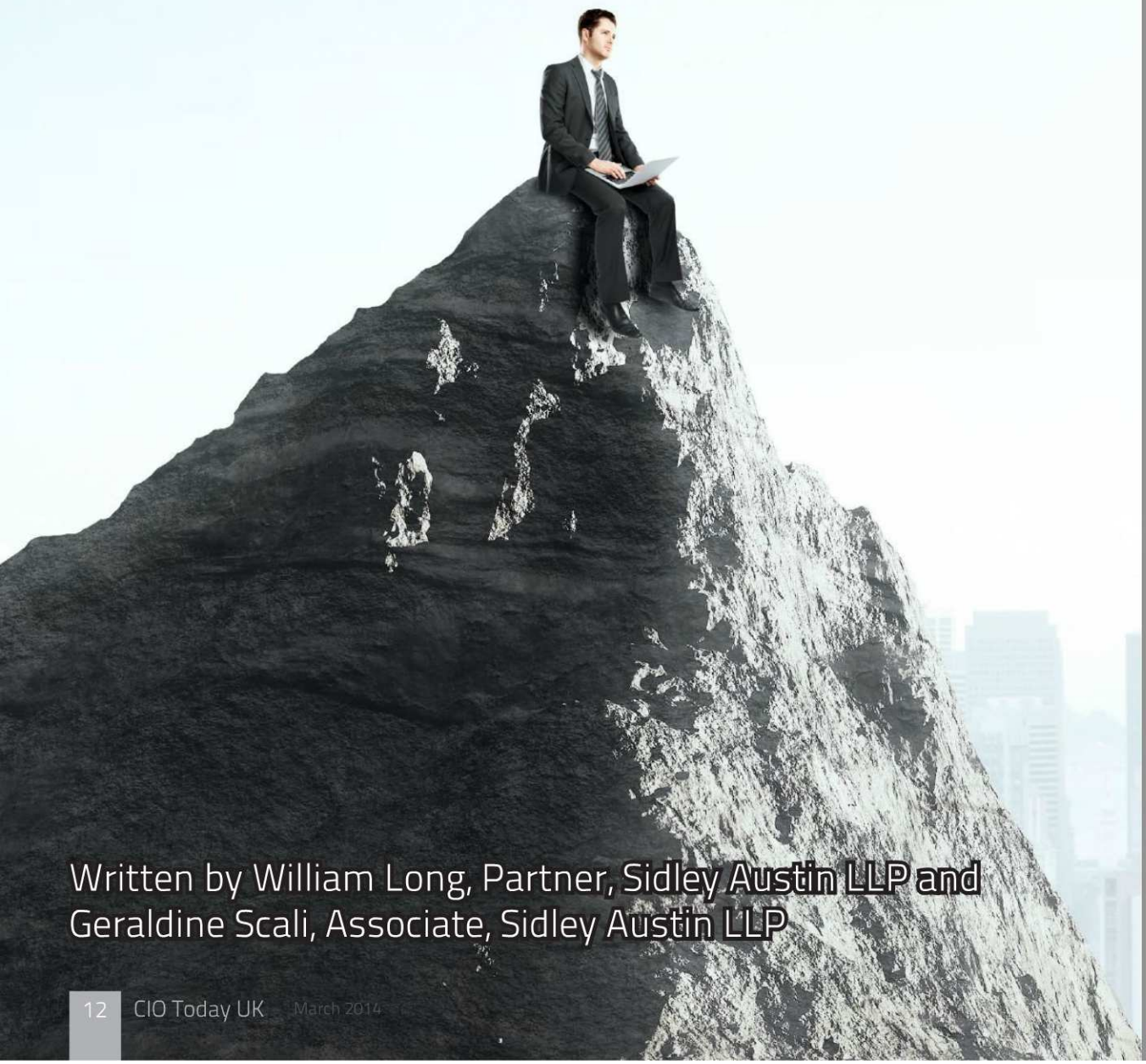
CIOs

and the changing legal landscape



Written by William Long, Partner, Sidley Austin LLP and Geraldine Scali, Associate, Sidley Austin LLP

The European Commission wishes to ensure a competitive and growing share of the global digital economy. It is, therefore, working on a number of key proposals that will directly impact CIOs and information security departments throughout this current digital decade.

European Cloud Computing Strategy

The European Cloud Computing Strategy, "Unleashing the Potential of Cloud Computing in Europe", aims promote the rapid adoption of cloud computing in all sectors of the economy in order to boost European productivity. This strategy will impact cloud providers who will consequently have to adapt their services to comply with new standards and modify their terms and conditions. Simultaneously, cloud customers will need to further assess how providers meet their data protection and information security obligations.

EU Cyber Security Strategy

The European Commission has recently published the EU Cyber Security Strategy of the European Union and a proposal for a Network and Information Security Directive (the so called "NIS Directive"). The NIS Directive proposes to extend to certain types of companies the obligation to assess the risks they face and adopt appropriate measures to ensure network and infrastructure security. Some companies will also have to report to the competent authorities any incidents seriously compromising their networks and information systems. Companies would also have to report issues significantly affecting the continuity of critical services and supply of goods including among others key internet companies, the banking, energy, and health sector. The NIS Directive also encourages the use of security standards.

As a result of these developments, organisations, through their CIOs and IT departments, should consider assessing their companies' security in light of the standards currently being developed at a European level. Organisations falling under the scope of the NIS Directive will also need to assess the risks they face, have procedures in place to report significant security breaches and implement new procedures in order to comply with these proposed obligations.

Proposed EU Data Protection Regulation

Two years ago, a proposal for an EU regulation on Data Protection was published by the European Commission (the "Regulation"). The Regulation once adopted will replace the current European data protection regime. The major changes

announced under the proposed Regulation are summarised below.

Scope – The proposed Regulation will apply not only to European businesses but also to those outside the EU where the processing activities relate to the offering of goods and services to EU citizens or the monitoring of such individuals.

Fines - Fines of up to 5% of a company's worldwide annual turnover or €100 million, whichever is the highest, for non-compliance with the Regulation.

Security and notification of security breaches – Under the proposed Regulation organisations will have to report security breaches "without undue delay". In addition, there will be an obligation to have security policies containing a number of elements including a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans and ensuring the ongoing effectiveness, confidentiality, integrity, availability and resilience of systems. Security breach procedures and policies should therefore be reviewed to ensure compliance with the new obligations under the proposed Regulation.

Data Protection Officers – Organisations may have to appoint a data protection officer ("DPO") with expert knowledge. One proposed test under the Regulation of when a DPO must be appointed is if the organisation processes personal data on more than 5,000 individuals in a consecutive twelve month period or sensitive data such as health data.

Accountability and Privacy by Design – Organisations will also have to adopt all reasonable steps to implement the necessary compliance procedures and policies to protect personal data and review these procedures and policies every two years. Organisations will also need to implement privacy by design throughout the lifecycle of processing from collection of data to its deletion. In addition, businesses will need to keep detailed documentation of data being processed and carry out a privacy impact assessment where processing presents specific risks, such as use of health data, or where the data involves more than 5,000 individuals, with the assessment being reviewed every two years.

Over the next 18 months European legislation which imposes significant new requirements in relation to cybersecurity and data protection may be adopted. As a result, CIOs and their organisations should start considering these new requirements now and assessing how they may impact their businesses.