CMS
law·tax·future

Advising the Board on **Data Risk**

Reports looking at the full range of commercial risk

Risk, Resilience and Reputation

Directors' risk report

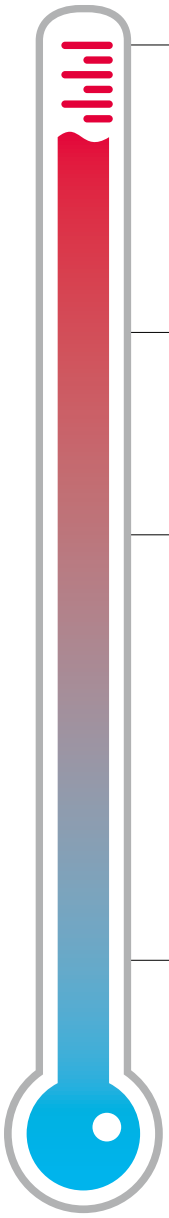
Data can be one of an organisation's most valuable assets but it can also result in significant exposure if not managed properly. Within a data ecosystem, many things can potentially go wrong – data can be lost, corrupted, not secured properly, misused or "overused", excessive, inaccurate or kept for too long. Even for businesses that undertook a comprehensive General Data Protection Regulation (GDPR) implementation programme, managing data effectively is an ongoing exercise. The value of data assets and the high price of non-compliance means that data risk management has become a headline board level issue.

In the lead up to the GDPR, directors had an important role in properly understanding, prioritising and implementing the changes needed to ensure compliance and their buy-in was often key to the success of those initiatives. With GDPR becoming more entrenched, directors will be even more focused on ensuring ongoing compliance and achieving commercial success through a sustainable data strategy.

The GDPR introduced a new accountability principle, requiring organisations to be able to demonstrate that they comply with the data protection principles. Central to this is having a robust data governance framework of effective policies, procedures and personnel. For certain organisations it is mandatory to appoint a data protection officer (DPO), who has specific responsibilities under the GDPR and will report directly to the board. Even if a DPO is not appointed, an organisation must allocate sufficient staff and resources to discharge its obligations under the GDPR.

The position regarding directors' liability (and on criminal liability generally) under data protection laws varies between EU member states. In the UK, directors can be liable for criminal acts of the company under the Data Protection Act 2018.

Stakeholder risk thermometer



HIGH RISK

Customers / Consumers / Employees

— The individuals whose rights are infringed will be directly impacted, and this will have knock-on effects for business reputation. If HR data is involved, employees and consultants will be affected.

Board

— If directors or other officers are complicit in an infringement of data laws, they could face serious individual criminal penalties.

Suppliers

— In addition to data controllers (who decide why and how personal data will be used) processors (who process data on behalf of a controller) can be directly liable for certain data protection breaches. Data processing agreements will seek to allocate liability between customer and supplier. The supply chain may be targeted by malicious actors.

Shareholders

— Data breaches and other high profile actions or complaints can have a significant negative impact on share price.

LOW RISK

Consequences of breaching data laws

Organisations breaching data protection laws may face a range of serious consequences including:

— Regulatory investigations and audits
— Regulatory notices
— Administrative fines of up to the higher of €20m or 4% of global annual turnover
— Complaints and compensation claims from affected individuals

The impact to the business may strike right at the bottom line in further ways, such as:

— Reputational damage
— Business disruption
— Contractual risk

In-house legal perspective

Janet Cursi
Group Data Protection Officer
SSE plc

What have been the significant concerns on your radar in terms of compliance with the GDPR?

Along with many companies, we had two major challenges to GDPR compliance. The first was legacy databases. We ran a cross group project to audit all databases that held personal data to ensure data retained was in accordance with business unit retention polices. As we are a multi-faceted company the retention polices vary, with each business being accountable to demonstrate their need for data. Subject Access and Right to Erasure requests have been at a high volume since GDPR, but these are easier to comply with due to the clean-up work done before.

The second challenge was the number of data processing contracts we had; these all needed to be remediated to comply with the specific provisions of GDPR. A combination of in-house resource and assistance from external solicitors was essential in light of the volume.

How do you go about building a compliance culture from within?

Having the support of the directors was a key component. In the six years leading up to GDPR implementation, I attended directors' meetings and other senior stakeholder meetings to raise awareness of what was coming. The directors understood that the requirements for a robust and well-resourced data protection function was aligned with SSE's core principles and likely to promote the success of the Company. As DPO, I now report directly to the directors.

At grass roots level, I appointed full-time business-related Data Protection Specialists with a dotted reporting line to the DPO. This team are familiar with SSE business procedures and we have trained them on GDPR requirements. These DP Specialists carry out statutory GDPR tasks etc (SARS etc) and investigate personal data incidents. They are also first point of contact in monitoring compliance and awareness raising.

The combination of having dedicated specialists in the team liaising with the DPO central team alongside the buy-in of directors has brought about a significant change in culture from pre-GDPR which we continue to build on.

The laws relating to data

Data protection

The GDPR is the key law regulating data protection in the EU. It extends to countries in the EEA. The GDPR was intended to harmonise data protection laws across the EU, but individual member states still have some discretion to legislate national measures in specific areas, such as enforcement and the requirements for DPOs. As a consequence, local law requirements will still need checking.

ePrivacy

Alongside data protection laws sit the ePrivacy laws concerned with confidentiality of communications, direct marketing and the rules regarding tracking and monitoring. The ePrivacy Directive is the primary current EU legislation, and this has been transposed at a member state level by various local laws. This is in the process of being overhauled and is likely to be replaced with an EU-wide regulation.

Sector-specific laws and regulations

Additional sector-specific laws and regulations or codes of conduct may apply, for instance, to:

- Communications services providers
- Relevant digital service providers (RDSPs) and other organisations covered by the Directive on security of network and information systems (NIS Directive)
- Public sector organisations
- Users of health data
- Regulated industries, such as financial services

Areas of risk

Fines

There are two tiers of administrative fines under the GDPR:

1. The most serious contraventions (especially those relating to individuals' rights) attract fines of up to €20m or 4% of global turnover in the preceding financial year, whichever is higher.
2. Others attract fines of up to €10m or 2% of global turnover in the preceding financial year, whichever is higher.

There is a list of aggravating and mitigating factors that are taken into account when setting fines.

Regulatory enforcement

Fines are not the only enforcement action that can be taken. The UK Information Commissioner's Office (ICO) has the power to issue various types of notices which, for instance, permit the regulator:

- to carry out dawn raids and audits, enter premises, be directed to documents and equipment, examine them, be given copies and explanations, observe processing and interview staff, or
- to require an organisation to stop infringing processing activities which, if core to the business, could be extremely disruptive and costly.

Compensation claims

Under the GDPR, affected persons can make compensation claims for breaches of the GDPR. Claims can now be brought against both controllers and processors, including collective class actions, which was not previously possible in many member states.

Director liability

In the UK, directors may be liable for the criminal offences of the company where these were committed with their "consent, connivance or neglect". However, the company will generally be the primary target of enforcement measures and there are no separate provisions making directors individually liable for non-criminal breaches of the legislation.

Reputational damage

If consumer or shareholder confidence is shaken by issues related to data risk, this can have a significant financial impact in terms of loss of business or reduction in share price.

An often cited high profile example is the 2015 cyber attack against TalkTalk in which 150,000 customers' banking details were hacked. According to the UK Information Commissioner, TalkTalk's *"failure to implement the most basic cybersecurity*

measures allowed hackers to penetrate systems with ease". The company later reported in its financial results that the incident cost it £60m and 95,000 customers.

Business disruption

Business operations may be disrupted if access to data is compromised or data cannot be used compliantly.

The 2017 WannaCry cyber attack caused mass disruption worldwide. In the UK, the NHS was hit particularly hard, with the hack causing over 19,000 appointments to be cancelled and 200,000 computers to lock out users with messages demanding ransom payments in Bitcoin. The initial response, subsequent clean up and upgrades to its IT systems apparently cost the NHS over £90m. The NHS's vulnerability was partly blamed on its use of outdated IT systems.

Contractual risk

Infringing data protection laws or breaching information security requirements can also put an organisation in breach of its contracts with customers, clients, suppliers or other relevant business partners.

Data risk: market snapshot

Below are some trends emerging in the post-GDPR world related to data risk:

Regulator focus

- **Spammers beware** – Senders of nuisance calls, texts and emails continue to be under the regulation spotlight.
- **Ad tech and big tech** – Complaints concerning transparency, invalid consent (or other legal bases) and using data for purposes incompatible with those for which it was collected ("overuse"). For example, the French National Commission on Informatics and Liberty (CNIL) €50m fine against Google Inc (which Google is currently appealing) and Privacy International's complaints against data brokers, credit reference agencies and ad tech companies.
- **Political marketing** – For similar issues to those mentioned above (e.g. Canadian data services company AggregateIQ) and for unsolicited marketing (e.g. leave.EU).
- **Data breach reporting** – The number of personal data breaches reported to regulators and to affected individuals has significantly increased (primarily as a result of the new mandatory breach reporting regime).
- **Non-EU businesses** – Organisations established outside the EU may still be within the reach of EU regulators if they direct goods or services at individuals, or monitor their behaviour, in the EU.

Increased consumer awareness

- **Data subject requests** – Many businesses have experienced an increase in the number of requests to exercise data subject rights, spurred by greater consumer awareness, and the prohibition under the GDPR in charging a fee in most circumstances (and in some cases misunderstanding) of the relevant regulatory requirements.
- **Complaints and consumer rights groups** – Consumer groups are gaining traction in bringing complaints to regulators on behalf of groups of individuals for the purported infringement of their data protection rights.

Marketing database shrinkage

- **The big pre-GDPR "re-consent" debacle** – Many businesses lost a huge proportion of their marketing databases by attempting to re-consent when this may not have even been required. Some saw this as an opportunity to cleanse redundant data whilst others may look to seek recourse for negligent advice.

Supply chain

- The Dutch regulator recently undertook an exploratory investigation to assess whether 30 large organisations complied with the GDPR across a broad spread of sectors. As part of this investigation the Dutch regulator requested various organisations' data processing agreements and details relating to the processing activities, retention periods and security. Supply chains can also be targets in cyber breaches and hence the Dutch regulator also requested the various private organisations to provide the agreements in place with the third parties that process personal data on their behalf.

ePrivacy uncertainty

— Even though the new ePrivacy Regulation was intended to be applicable from the same date as the GDPR, the final text is still to be agreed. This is a particular area of uncertainty for businesses that use cookies-driven technologies and undertake direct marketing (including in a B2B context).
— The definition of "consent" will likely be aligned with the GDPR, which would mean a major change for businesses used to a lesser standard of "implied" or "deemed" consent in certain jurisdictions.
— We are seeing changes already in how cookie consent is obtained for non-essential cookies, such as advertising tracking cookies, with users being given more choices upfront about which types of cookies they wish to accept. As a result, this is presenting significant challenges for the traditional operating models of website operators and third party advertisers.
— The European Data Protection Supervisor (EDPS) has issued guidance on the interplay between ePrivacy laws and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. This provides some insight at least into how the equivalent provisions of the new ePrivacy Regulation may be interpreted by the regulators once eventually finalised.
— Not complying with the new ePrivacy Regulation will expose organisations to similarly high levels of fines to those under the GDPR.

Brexit uncertainty

— Brexit contingency planning has been high on the agenda in many boardroom discussions to ensure that data can still flow between the EU and the UK, particularly in the event of a "No Deal Brexit".
— The ICO has issued detailed guidance on what to do when the UK becomes a "third country" for the purposes of international data transfers under the GDPR. For many EU businesses, this may mean putting in place European Commission-approved standard contractual clauses to enable personal data to be exported to the UK compliantly within the GDPR requirements.
— The US Department of Commerce has also issued guidance on the updates that need to be made to the EU-US Privacy Shield certifications to ensure that organisations that rely on that regime can continue to receive personal data from the UK.
— Not complying with the international data transfer requirements of the GDPR exposes organisations to the highest tier of fines (being up to the greater of €20m or 4% of the total worldwide annual turnover of the preceding financial year).

The expert's perspective

Lucy Russell
Cyber Innovation Underwriter
AmTrust

It is hard to overestimate the importance of data in business today. Companies store huge amounts of data, much of which is highly sensitive. This brings great risk to companies and their customers in a world where data breaches are ever more common and cyber security threats are increasing in magnitude. Companies must endeavour to keep data safe and take steps to minimise the potential loss of data in the event of a breach.

Over the past year (since the GDPR came into effect), the cyber market has seen growing recognition from companies of the value of cyber insurance as part of a data security program. Cyber insurers provide cover for first party losses arising from a breach, regulatory fines, penalties issued following a breach and third party claims resulting from a breach. Whilst insurers require that companies take steps to protect data (by means of segregation, back-ups and encryption for example), a cyber policy can protect the company against losses. Insurers collaborate with technology companies to provide companies with the tools to protect themselves from a data breach (by education and training, vulnerability assessments and intrusion detection). Increasing emphasis on pre-breach action means that insurers are helping Boards protect themselves from a data breach rather than simply waiting for something to go wrong.

Having a strategy around data is essential. Boards need to know what data they have, where it is stored, how long the company must retain it for and how to protect it.

Boards should allow for the possibility that something may go wrong (whether due to human error, system failure or malicious attack) and consider putting a cyber policy in place to respond in those situations.

Summary: practical risk management for directors

1. **Ethics** – Consider what kind of business you want to be and ensure your data strategy is driven by strong ethical considerations.

2. **Accountability** – Simply complying with the data protection principles is not enough; you must be able to evidence this, so retain documentation and ensure that staff have been trained – regulators will hone in on this.

3. **Data use** – Ensure your business is communicating clearly about what it is doing with people's data and ensure that data is processed lawfully, fairly and never "overused".

4. **Security** – Invest in order to ensure appropriate levels of security and have a robust breach response plan ready to go and test this regularly.

5. **3rd party data** – Only use trusted suppliers who can guarantee that data is GDPR-compliant and fit for use. Ensure robust instruction terms, retain control over processing the personal data and managing the relationship with the individual and undertake due diligence and ongoing audits of third party processors.

6. **M&A targets** – If acquiring a business for its data or data-driven technology, undertake sufficient due diligence to ensure it complies with GDPR standards – if not, this could significantly affect value and provide exposure to non-compliance liabilities.

7. **Data Protection Officer** – Appointing a DPO is not always mandatory but, particularly for data-driven businesses, an experienced DPO can be an integral part of good governance, engaging with the business to drive the right behaviours and ensuring a robust data protection compliance culture.

Authors

Katherine Eyres
Privacy Counsel
T +44 20 7367 2539
E katherine.eyres@cms-cmno.com

Emma Burnett
Partner
T +44 20 7367 3565
E emma.burnett@cms-cmno.com

Loretta Pugh
Partner
T +44 20 7367 2730
E loretta.pugh@cms-cmno.com

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

1905-0094628-5