

Regulation and Legislation

- Directors must ensure that they know and understand all legislation and sector regulation relating to information risk, and that their knowledge remains up to date.
- Directors are personally accountable, and can be held personally liable, for non-compliance.
- The tide is running towards an ever greater focus on the control of information.

This Guide is intended to serve as a general guide to directors and is not intended to serve as legal advice. Legal opinion should be sought on a case-by-case basis as required.

Directors' Accountability and Liability

Information risk is one of the many risks for which the Board is accountable, and hence the normal requirements, regulations and penalties apply. However, regulators, legislators and the public in general have become increasingly concerned to ensure the proper protection of information and the accountability of the individuals who direct organisational behaviour. Directors need to understand the nature of their obligations, which may vary from country to country, and to take care that they are discharging those obligations fully.

The consequences, both for the organisation and for directors personally, can be severe. For the organisation, disregarding relevant provisions can result in:

Regulatory penalties	Regulators can impose fines, sanctions, or additional monitoring, and in extreme cases withdraw a licence to operate within the sector.
Claims for compensation	Perhaps for breach of confidentiality or for not being able to resist claims due to a failure of records management.
Reputational damage	Publicity relating to a breach of key legislation or an irregularity in fundamental controls can damage the brand and lead to a crippling loss of confidence.

Under, for example, section 1121 of the Companies Act 2006 or the Criminal Justice and Immigration Act 2008, individual directors can be held liable for offences committed by their organisation. For the director, disregarding relevant provisions can result in:

Fines	In some circumstances, unlimited fines can be imposed.
Civil claims	For example, for negligence, a breach of duty or a breach of trust.
Criminal penalties	In serious cases, a culpable director can be charged with a criminal offence (which might entail extradition) and possibly sentenced to imprisonment.

There has been a significant growth in the UK of litigation against directors. Directors cannot rely on Directors and Officers Liability Insurance to provide them with complete protection from such penalties. And, even if charges against a director are unsuccessful, defending claims can still be highly disruptive and very costly.

Directors' Responsibilities

A director's responsibilities fall into two classes. The first is to ensure that the organisation retains and protects all the records it might need to meet its obligations. These can include legal and regulatory obligations (e.g. under money laundering regulations, the Companies Act, Health and Safety, tax regulations), the obligation to manage operational risk (e.g. ensuring that copies of contracts are retained for the duration of the contract) and to fulfil business needs.

The second class is to ensure that confidential information is not disclosed without appropriate authority. This can be driven by legal, regulatory or sectoral requirements (e.g. the Data Protection Act 1998, the Financial Services and Markets Act 2000, the Official Secrets Act), by common law duties of confidentiality (e.g., in banking, health services) or by contractual terms (e.g., confidentiality provisions within contracts).

Directors should ensure, at a minimum, that their organisation implements a records management programme that provides for the identification, capture, protection and proper disposal of key documents. Directors should also ensure they seek competent legal advice whenever appropriate. The standard of care required by directors is an objective and retrospective test. Directors cannot hide behind incompetent advice if they knew, or should have known or suspected, that such advice was wrong or incomplete.

Legislation

There is a vast range of relevant statutes and laws. These include:

- The **Companies Act 1985** and its 2006 replacement. Relevant sections cover, for example, culpability for destroying company documents and providing false information. Documents are defined as information recorded in any form.

- The **Data Protection Act 1998** (DPA). In particular, the DPA lays out eight principles regarding the way in which data should be retained and handled.
- The **Computer Misuse Act 1990** (CMA) and revisions.
- The **Regulation of Investigatory Powers Act 2000** (RIPA).

There are also many other acts and sector-specific legislation which, though they might not mention record keeping per se, do imply it. Defences under such acts might not be available unless the organisation can provide evidence, in the form of reliable protected records, to show that senior management conformed to legal and regulatory duties.

Organisations operating or trading outside the UK or having dealings with foreign organisations will also need to pay attention to EU and foreign laws. Many other countries, both within the EU and beyond, have equivalents to the UK's DPA. America (e.g. Sarbanes Oxley Act 2002; individual state legislation dealing with data loss disclosure) is recognised as a more litigious country than the UK and directors need to take extra care. Other countries with relevant legislation include Australia, Canada, Hong Kong, Singapore, Dubai, UAE, France, Germany, Switzerland, South Africa, Gibraltar, Jersey, and many more.

Some regulators, follow a "principles-based" approach. This requires compliance not only with the letter but also the spirit of relevant regulation. Even if an issue does not result in a breach of a specific rule, the regulator may still censure the organisation, and, in extremis, its directors, for failing to apply the spirit of the rule.

