STILL GOT ANALOGUE LIGHTS ON YOUR TREE? THE CHRISTMAS TREE AS A MODEL FOR CORPORATE DIGITISATION

Hardly any other topic interests today's markets as much as digitisation, hardly any other topic will change companies so fundamentally in the medium term and hardly any other topic is so complex. Introducing digital governance is a good way to identify and mitigate digital risks within your company. Take a look at the Christmas tree for inspiration in setting up such a framework.

Topics

- Digital Governance: digitisation compliance
- Selection of suitable digitisation officer
- Implementation of functional control and monitoring processes

Author Profile

Dr. Gunnar Sachs, *Maître en droit (Paris)* is partner in the Düsseldorf office of Clifford Chance.

He is an expert lawyer for Intellectual Property and he is a member of our global sector group Telecommunications Media & Technology.

He focuses on the requirements of **enterprise digitisation** and the development and implementation of customized **digital governance organisations**.

I. LOST IN DIGITALISATION?

Originally conceived by highly specialised IT experts, digitisation has long since spread far beyond the information sector and now has a global impact across all geographical and sectoral boundaries, from primary production through the entire industrial and services sector to the waste management, tourism and leisure industries. It raises not only macroeconomic and micro-economic questions, but also a plethora of technical, legal and philosophical issues. Entire economies focus their foreign investments on high-tech sectors in other countries, companies around the world are developing digital strategies, and lawyers and philosophers are discussing previously inconceivable responsibilities for digital products now made by entities other than humans. Digitisation will shape companies to an even greater extent than recent developments in compliance and data protection.

But have companies learnt from the initial problems they had and continue to have in implementing new compliance and data protection processes? Far from it. As they put digitisation into practice, companies are courting chaos similar to that seen at the beginning of the compliance and data protection movements. This is exacerbated by the fact that, unlike in the compliance and data protection context, the key topics associated with digitisation often fall within the remit of many different functions within a company rather than being handled centrally.

Although the trend towards digitisation has occupied the business world for some time, so far most companies have taken a rather uncoordinated approach to the challenges involved. When it comes to digital transformation concepts, people often forget the bigger picture. Too few digital strategies are managed centrally, and it is even rarer for constructive processes to be implemented across a company to reflect the relevant commercial and legal

requirements. In many cases, the different business units or divisions working on digitisation issues are unaware of one another. This means opportunities are missed and risks arise. As a result, many companies miss out on protection for new digital developments, make themselves vulnerable to cyber attacks and data leakage, mess up their digital contract management, fail to keep a record of digital processes, risk handling data in a legally unsafe manner, overlook relevant sanctions and export control regulations and expose themselves to antitrust complaints, thus creating liability risks and the like.

To compete in a digital environment, companies are primarily investing in developing new digital products and replacing analogue business operations with digitalised ones. Since most market participants do not have the knowledge or staff to launch such products and processes, or at best have insufficient know-how and staff resources for this task, digital expertise and developments are often bought externally along with all the associated risks, or entire projects are contracted out to external providers. In the race for digital leadership, many companies are focussing solely on new technical developments and ignoring the fact that their digital transformation involves numerous new risks and responsibilities, and that failure to observe these may jeopardise not only the new products and processes but also their company's very existence. Those who don't ensure their companies are adequately protected against such risks are exposing not only themselves but also their companies to considerable liability risks and potential fines.

II. DIGITAL GOVERNANCE

One key challenge – and opportunity – of corporate digitisation is not only to produce a digital strategy fit for the future but also to set up digital governance. Digital governance is the framework for implementing and monitoring a company's digital transformation. It is based on the company's digital strategy, covers all the legal and commercial requirements to be met when implementing such a strategy and involves not only a network of qualified staff, but also corporate processes tailored to ensure both the successful implementation of the digital strategy and the appropriate management of its inherent risks. Digital governance therefore enables companies to take a holistic, systematic and responsible approach to their digital transformation. They can then identify the risks associated with their digital transformation, assess these risks against the applicable legal and commercial requirements and ensure they have the necessary staff structure and processes to adequately tackle them.

Anyone unsure how to cope with the complexity of the challenges of digitisation would be well advised at Christmas time to take a look at a tree decorated with fairy lights. Like the tight knit web of fairy lights, good digital governance depends first of all on close interaction between a network of decision-makers from all of the business areas involved in the digital strategy, with the degree of network interaction dictating the degree of "enlightenment".

A digital officer should function as a central switchboard. The greatest challenge facing such digital officers – also known as chief digital officers (CDOs), chief digital information officers (CDIOs) or chief digital disruption officers (CDDOs) – is not only to keep abreast of the digital strategy and continually evolving technological developments of his or her own company, as well as of competitor companies, but also to act as a personal interface for all business areas responsible for digitisation issues and for the company's business deal-

ings with other companies. In this role, digital officers ideally need to know everyone responsible for digital transformation both internally and in competitors' and business partners' companies, as well as having a sound knowledge of the different approaches to this topic.

However, as technology advances, this becomes more difficult. In times when central components of digitisation such as software or processors have often been developed by combining and continually optimising a number of individual innovations, transparency as to the rights to and those involved in digital developments, as well as the relevant legal provisions, is often very difficult to achieve. To meet these challenges the digital officer should either be a member of the company's management or have a direct reporting line to management, data protection, compliance and IT security officers. From this position, digital officers can coordinate the company's digital transformation inter alia by:

- scouting out external markets and competitors to find out about new, disruptive technologies and the associated opportunities and risks, and – if the benefits outweigh the risks – helping make these accessible to their own companies
- setting up and managing a company-wide network comprising all staff involved in the digital transformation.

Reporting lines between digital and data protection officers are advisable simply because, to a large extent, digital transformation by definition involves electronic data often made up of personal data on clients, employees or business partners of the company.

In light of this, the choice of digital officer is likely to vary from one company to the next. While data protection and compliance officers often have a legal background, IT experts, product engineers, economists or other people who are particularly familiar with the digital strategy may also be suitable for the role. At the end of the day, digitisation is linked to key responsibilities in all these roles and a good digital officer needs interdisciplinary knowledge and close connections to the other functions. This is underscored by the fact that corporate digitisation affects various technical, commercial and legal topics.

To be as well prepared as possible for all relevant issues, digital officers need to be able to rely not only on their own expertise but also on digital governance tailored to the requirements of their company. Ideally, good digital governance should cover all issues connected to a company's digital strategy, offer both economically viable and legally sound answers, protect the company from the aforementioned legal risks and improve the quality of digital products. Effective digital governance can – depending on the digital strategy – include processes for IP and data protection, for cyber security, for avoiding the risks associated with IT outsourcing and for the legally watertight use of social media, big data sets or sanction and export control regulations for technological products. It gives companies more legal certainty and reduces their risks in dealing with all manner of relevant digital topics such as investments in third-party technology, awarding development projects and procuring external know-how, generating monopoly-like databases, IT security issues in the increasingly sophisticated Internet of Things, finance technologies and digital currencies, programmed contracts and electronic contract management, the digitisation of supply chains and merchandising systems, export restrictions on

digital products and special requirements in strictly regulated fields such as digital health.

III. CONCLUSION

In essence, digital governance is similar to the corporate governance and compliance already set up at most companies. It is aimed both at compliance with the legal requirements for digital transformation and adherence to recognised technical and ethical standards. In terms of physical resources, digital governance involves the development and implementation of appropriate corporate policies, and in terms of human resources, the introduction of management and control structures with appropriate specialists. It therefore facilitates responsible, specialised, legally adequate digital transformation aimed at long-term corporate success. As a result, digital governance serves to protect not only companies themselves, but also their managers, owners, shareholders, staff, clients and business partners.

And to return to the metaphor of a Christmas tree with fairy lights: in the same way as the rest of the lights continue to work if individual connections fail, sound digital governance keeps the business going even if individual divisions or whole areas stop working and prevents "the lights going out" in all branches due to individual errors, as they would have done in the days when one Christmas light failing meant that they all did.

With this in mind, a very Merry Christmas and a successful new digital year to you!

AUTHOR

Dr. Gunnar Sachs, Maître en droit (Paris)
Expert lawyer for Intellectual Property
Partner, Düsseldorf

T +49 211 4355-5460
E gunnar.sachs
@cliffordchance.com