COLLYER BRISTOW

GDPR DATA PRIVACY

# ESG AND DATA PROTECTION

**Investors and the wider public are increasingly gravitating towards businesses that prioritise Environmental, Social, and Governance (ESG) credentials. Discussions around ESG investing commonly focus on factors such as minimising carbon emissions and broadening the diversity of staff and board members. Critical though these undoubtedly are, it is important not to overlook the role of data protection in the context of ESG initiatives.**

Facebook, for example, has learnt this the hard way: in the wake of the Cambridge Analytica scandal, where a political data consultancy firm was accused of harvesting the personal data of over 80 million users, the tech giant's stock lost a fifth of its value and several ESG funds reconsidered their ties with the company. Following the allegations published in the *Wall Street Journal* last month, Facebook's practices have again come under intense scrutiny from ESG-focused investors.

Irrespective of whether or not a business operates a global social media network, it is inevitable that its data privacy practices will come increasingly under the ESG spotlight. It is predicted that a staggering 175 trillion gigabytes of new data will be created around the world in just four years' time, with data protection pushed to the top of the corporate risk agenda following the post-pandemic shift to cloud computing and hybrid working.

Data protection most obviously falls within the Governance ('G') arm of ESG concerns, given the accelerating global implementation of laws concerning personal data processing, most notably spearheaded by the European Union's General Data Protection Regulation (GDPR). A company's failure to comply with these not only flags to ESG-conscious investors that its executives are worryingly complacent as regards current regulatory and cultural trends, but can result also in receiving steep fines. Contraventions of the UK's version of the GDPR, for example, can result in eye-watering penalties of up to the greater of 4% of worldwide turnover or £17.5 million. Any sanction of this nature is likely to be accompanied by a requirement for immediate remedial action, which may entail a considerable operational cost and hinder the company's ability to rely on — and reduce the value of — its existing data sets. Coupled with the probable reputational damage to the company, this in turn could result in an investment making a loss or a reduced profit. Furthermore, with data breaches generating headlines more frequently than ever before, ESG investment firms are paying closer attention to the effectiveness of measures implemented by businesses to protect their information security.

If the way in which a business uses information about individuals affects their privacy or the functioning of a democratic society, then this should also be taken into account as part of the Social ('S') element of ESG criteria. By way of illustration, if an organisation deploys artificial intelligence or some kind of automated decision-making process that has real-life consequences for living individuals (such as to determine whether to award a loan or to detect potential fraud by benefit claimants), then it should be able to detect and prevent any inherent bias in this process on the basis of protected characteristics such as race, ethnic origin, gender, marital status, and sexual orientation.Any such technologies should be deployed only after a careful impact assessment and individuals whose personal data is handled in this way must understand how the process works and how it can affect them. Given that matters of human rights and freedoms often inform ESG investment decisions, it is worth remembering that the European Convention of Human Rights enshrines the right to respect for an individual's private life.

Albeit not immediately apparent, there are also environmental ('E') factors at play in a business's data protection practices. A key principle of the GDPR, for instance, is data minimisation. In other words, a business must ensure that the personal data over which it has control is relevant and limited only to what it needs for its operations. It would be a contravention of this principle, for example, for a business to obtain superfluous information about its staff's health conditions that are not relevant to their jobs. Storing and processing excess data in this way necessitates larger data centres and server farms, increasing energy consumption. With recent research indicating that information technology of this kind could account for up to 3.9% of global greenhouse gas emissions, adherence to the data minimisation principle is not merely a question of regulatory compliance, but also of energy efficiency.

Public awareness of data privacy concerns is now at an all-time high. The most recent annual report from the Information Commissioner, the UK's privacy watchdog, states that 77% of those it surveyed in early 2021 agreed that protecting their personal information is important to them. The trend of data protection metrics constituting key ESG criteria for investors, therefore, can only continue upwards.

**RAJ SHAH**
**Senior Associate**
**Commercial Services**
+44 20 7468 7341
+44 7779 447021
raj.shah@collyerbristow.com