COMPLIANCE TO PRIVACY POLICY FOR DIRECTORS

*William Fawcett

Introduction

No doubt you have recently been hearing about the GDPR and receiving notices from various companies, asking you to agree to their new data privacy rules. That is becausethe European Union's General Data Protection Rule (see also Director Today, July 2018 "Demystifying GDPR") came into effect on May 25th. While the law obviously applies to European organizations specifically, it bears an impact on Indian and other non-EU companies as well.

That's because many Indian companies do business in more than one country. Organizations that are based outside of the European Union but run operating entities in Europe, or who have clients in the European Union are required to comply with more than one set of laws. In this case, that means updating their privacy policies based on the new European regulation.

One might suppose that such companies could simply choose to confine these updates to their European entities, leaving the overseas side alone. But it would make no sense to compartmentalize one's policies in this way. For one thing, it would add needless complication: why maintain two policies when one will do? For another, there's nothing to be gained from it. Third and most importantly, it's probably not even possible. According to the NACD, "digital commerce per se has no geographic boundaries." No matter where you're located, if ever you collect online data from a European subject, you're accountable to uphold the GDPR.

Unlike other vague and ineffectual measures, the GDPR contains specific requirements and penalties that can result in large fines, *as well as personal criminal liability for board members*.

Which is why it's critical that corporate directors take a leadership position to understand and to move their organizations into compliance with the new law's requirements because where the GDPR is concerned, what you don't know can hurt you.

Why does the GDPR matter?

The GDPR demands higher standards for the security and privacy of consumer and employee data. It matters because people's security and privacy matter.

For the corporate director, it matters because the GDPR focuses the cybersecurity issue personally and directly upon board members. This is true for Outside directors as well. If a company is cited under the GDPR, there is almost no way to deflect this focus or to avoid responsibility by board members. (see also "Cyberattack: The Risk to Corporate Directors" by this same author.)

How real is the risk for this type of data?

Consider this: when the International Association of Privacy Professionals studied ten thousand reports by "large, publicly traded companies," it found "that losing customers' or employees' personally identifiable information was the most common information-related risk cited." According to the new law, that's no longer acceptable.

Which organizations does the GDPR affect?

If you collect data from individuals (consumers or employees) within the European Union, the GDPR applies to you.

What happens if I don't comply?

Your organization may face intensive reputational damage stemming from the fallout following a breach; regulatory penalties as high as €20 million or 4 percent of your total annual worldwide revenue; and civil litigation brought by any "person who has suffered material or nonmaterial damage" due to your noncompliance.

In July, the U.K. Information Commissioner's Office levied a £500,000 fine on Facebook after it found the company broke data protection laws in its dealings with Cambridge Analytica. As reported by Ad Age, the regulator "could have levied a much higher and potentially more painful penalty under new European Union rules in place since May 25 [the GDPR], where violations could lead to fines of as much as 4 percent of a company's global annual sales. In 2017, Facebook generated $40 billion in ad sales. But the law only applies to violations committed on or as of that date and not retro-actively. That's why the ICO's intended fine is capped at the maximum of 500,000 pounds, or $664,000, that it could levy under previous privacy rules."

What should I do first?

First off, do your homework. Fair warning, getting to know the law will require some effort on your part, because the GDPR isn't short. It consists of "99 articles organized into 10 chapters." That said, the NACD has lightened the burden a little by pointing out the sections that are specifically relevant to corporate directors. Focus on chapters 1-4, which cover "General provisions," "Principles," the "Rights of the data subject," and "Controller and [/or] processor."

Are there specific actions I can take?

Yes. Here are ten tips to get you started:

1. Create educational opportunities to help your board understand the GDPR. For example, you could invite a GDPR expert to give a presentation.
2. Form a committee to learn about data privacy and GDPR compliance and report back to your board.
3. Require board leaders to familiarize themselves with how data is

CONTINUED ON p: 48

Communicating the company's performance story is an important part of the board's responsibilities. Explaining strategy and the business model, providing relevant metrics and long term vision are key elements of building trust through communication with investors and other stakeholders. Rebuilding trust in business is an attribute which is earned and built over time and a measure of whether investors want to do business with the company and put their capital at risk. As custodians for investors and major stakeholders, boards are responsible towards protecting their investment as well as societal interests. An integrated report can be instrumental in providing stakeholders with the information that builds long term trust a

The IIRC ran a three-year pilot programme for investors and over 100 businesses from around the world to experiment with and trial the integrated reporting concepts before launching the framework in 2013.Black Sun LLC did a survey of the pilot programme participants on the impacts and benefits of integrated reporting. The observations below reflect the internal benefits of alignment, embedding sustainability into business and positive relationship building with investors.

Integrated Reporting is increasingly being used by Boards to drive good corporate governance which is about the 'how of business' that drives responsible business behaviours and processes and ultimately results in transparency and accountability towards key shareholders.

Vrushali Gaudleads advocacy and outreach for the International Integrated Reporting Council (IIRC) in India.

CONTINUATION OF p:46

COMPLIANCE TO PRIVACY POLICY FOR DIRECTORS

*William Fawcett

processed; it's specifically important for them to understand whatever mechanism you use to obtain consent.

4. If you don't have such a mechanism in place, establish one. Obtaining consent is crucial when collecting data from consumers as well as employees; for example, you must get a prospective team member's permission before collecting diversity-related information when adding them to your board, your executive team, and your general workforce.
5. Inquire into your data retention policies: make sure you're not holding onto data for too long.
6. Find out what steps your management team takes to ensure the accuracy and currency of the information that your company collects.
7. Confirm that any long-term data you store for research is anonymized, so that it's not personally identifiable.
8. Review the strength of your company's cyber security and educate yourself on best practices.
9. Review your protocol for responding to a security breach and disclosing it, if necessary, to the public. The GDPR requires that you respond to a security incident within 72 hours. Translation: you must have systems in place to alert you to a breach immediately; many infamous breaches in the United States have taken weeks, even months, to detect.
10. Ensure that if you receive requests to delete an individual's data, you have the ability to locate it and expunge it from your records.

Are there questions I should be asking?

Begin by consulting the resources offered by the Institute of Directors. Additionally, your auditors and organizations similar to the Institute of Directors offer lists of questions that corporate directors can ask their management teams about GDPR compliance. The questions provided focus on GDPR readiness and exposure, personal data collection, data breaches, policies and programs related to the new law, and roles for GDPR compliance. We encourage you to look at the report for more information.

While GDPR compliance cannot be achieved overnight, it is possible and necessary. Considering the privacy and security of your employees and consumers, it's also a genuinely positive development. We wish you diligence and success as you set about bringing your policies up to date. ■

William Fawcett, F.IOD is an experienced outside director and chief executive officer with over 30 years of international experience. He is currently the Chairman of Haverford Bermuda Limited. An attorney qualified in the US, the UK and Bermuda.