Eight Ways Board Directors Should Be Preparing for the GDPR Right Now

The implementation of the General Data Protection Regulation on 25 May 2018 represents the biggest change in privacy legislation in a generation. By bringing the balance of power back to the individual, the legislation marks a paradigm shift in the way that organisations must process and protect customer information. Although ostensibly an EU directive, the borderless nature of global commerce means that the GDPR will act as a catalyst for global change in how we manage the rights of the individual. The penalties for infringement are severe, and the buck stops with the board.

Company Directors and Boards should be at the forefront of driving compliance with the GDPR. This paper highlights eight ways that directors should be preparing for the GDPR right now and examines how they can go further to embrace the opportunity to deliver outstanding customer value.

Diligent

BIG DATA: BIG PRIVACY CHALLENGE

When George Orwell devised the dystopian world of his novel *1984*, where every facet of human interaction is observed, analysed and controlled by an all-powerful "Big Brother", he never imagined that humanity would opt-in to such an existence. Yet this is the scenario that has become more of a reality over the last 20 years as individuals have voluntarily relinquished their personal information to organisations in return for the supply of goods and services. It's time for a shift in both the culture and the regulation of how we manage individual privacy.

Big data is the lifeblood of the digital economy. Analysing the trillions of online interactions that take place every day provides rich information to businesses aiming to deliver what people want, exactly when they want it. Customers hand over detailed levels of private information in exchange for highly personalised products and services. This insight is so supremely valuable that, as far back as 2006, data was described by Clive Humby of retail giant Tesco as "the new oil".[1] Unlike limited oil reserves, however, data increases in volume exponentially. Analysts at IDC have predicted that by 2025, the global datasphere will reach a trillion gigabytes, 10 times greater than that in existence in 2016, heralding "a new era of the Data Age".[2]

So the genie is out of the bottle. Your business needs big data and your customers have high expectations of the experience they will receive in return for handing over their information. But high-profile data breaches, identity theft and the constant incursions by cybercriminals intent on extracting and selling personal data have eroded the trust between individuals and businesses. So we have a paradox: big data must flow, but individual rights must be protected. This is the challenge that the GDPR sets out to overcome.

"What all of these measures are intended to do is to enhance the trust that individuals have in the digital economy, to protect individuals, but also to facilitate and enable the flow of data for appropriate purposes: commercial purposes, government purposes and law enforcement purposes."[3]

The UK's Information Commissioner, Elizabeth Denham

The GDPR is designed to make privacy regulations fit for purpose in the 21st century and it is the role of company directors and boards to promote compliance.

BUSINESS BEYOND BREXIT

The GDPR comes into force before the UK leaves the European Union in 2019, meaning that companies will need to comply in any case. Furthermore, any UK organisations that wish to trade with EU citizens must meet the regulation, so it is imperative that preparations are in hand.

In advance of Brexit, the UK has committed to incorporating the EU's data legislation into UK domestic law, aligning the UK's Data Protection rules with those of the EU at the point of exit and building a future framework that will allow data to flow.[4] What this means for UK businesses is that work done to meet the GDPR will not be wasted, but will stand them in good stead to meet post-Brexit regulations.

The UK published the Data Protection Bill in September 2017, repealing the 1998 Data Protection Act and updating national Data Protection in line with the GDPR. There are likely to be some domestic variations compared with the GDPR and directors should monitor developments to ensure that companies can comply with these as they are implemented.

EIGHT WAYS DIRECTORS AND BOARDS SHOULD BE PREPARING FOR THE GDPR RIGHT NOW

The impact of the GDPR must not be underestimated. Boards need to act now to ensure that they are able to demonstrate compliance by the May 2018 deadline.

PERSONNEL

1. Appoint a Data Controller

Appoint a data controller at the executive level who is responsible for data protection throughout the organisation and who is accountable to the board. Organisations that carry out large-scale monitoring of individual behaviour, such as tracking online activity to inform marketing activities, must officially designate a Data Protection Officer (DPO) under the terms of the GDPR. Check whether this requirement applies to your company.

2. Increase Employee Awareness

The GDPR will have an impact on most areas of the business so it's important that it is communicated effectively to staff. Ensure that there is a comprehensive education programme in place and fulfil any training requirements well in advance of implementation.

PROCESSES

3. Audit Existing Data Processes

Establish how and where your company's data is collected, stored and transferred. What are the current procedures for seeking and recording consent to hold and manipulate data? Is consent specific, informed and unambiguous in the way required by the GDPR? Conduct risk analysis to identify weaknesses in processes and act to mitigate any issues.

4. Document Data Processes

The requirement for accountability is a key obligation introduced by the GDPR when compared with previous legislation; you must be able to actively demonstrate how you are complying with the regulation. An essential part of this is documenting of the data procedures that are in place, so you need to ensure that robust systems exist to record and regularly review those procedures.

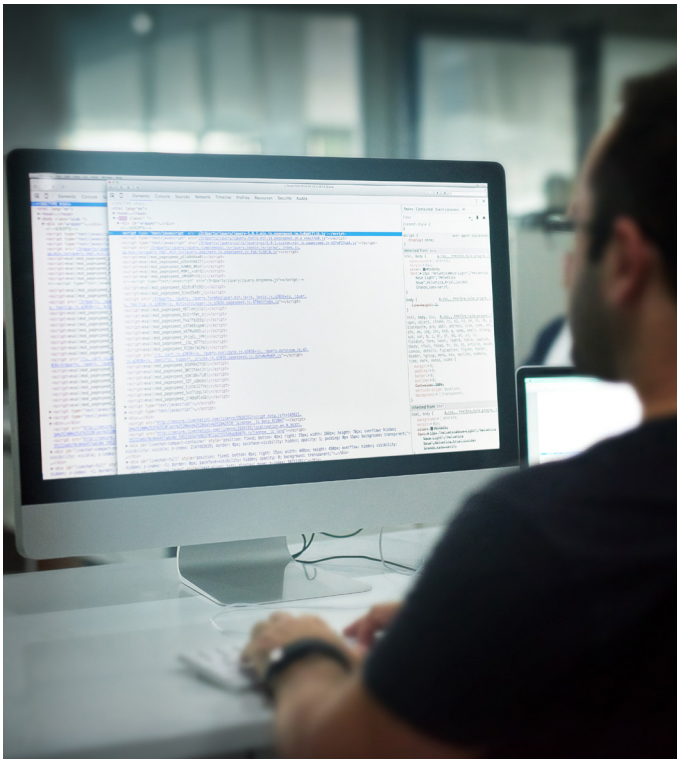
DUE DILIGENCE

5. Verify Third-Party Compliance

It is the responsibility of data controllers to ensure that all third parties they use to process, store and manage their data also meet the standards of the GDPR. Check that your marketing, payroll and cloud partners are able to clearly demonstrate that they are compliant data processors. You must be confident that you are able to audit their compliance independently if required.

6. Test Data Security and Breach Procedures

In recognition of today's threat-intensive online environment, the GDPR adopts a when, not if, approach to data breaches. Companies that suffer a data breach which constitutes a risk to individual privacy must inform the relevant national authority within 72 hours of the incident. Ensure that your IT security systems and procedures are robust and capable of identifying, neutralising and reporting any breach well within the reporting timeframe.



7. Assess Data Visibility

The GDPR introduces a data subject's "right to be forgotten". This means that you need to be able to track every instance of a data subject's records – online and offline – so that the information can be effectively deleted. Recent research from *Computing* magazine showed that only 9% of organisations were confident that their data management tools were effective and easy to manage[5], meaning those with less effective tools may struggle to honour the right to be forgotten. Verify that your company's data management tools and procedures are capable of meeting this requirement and upgrade them if necessary.

STRATEGIC PLANNING

8. Plan Strategically for Ongoing Compliance

Under the GDPR, building privacy into data management will be more than best practice, it will be a legal requirement. Ensure that as a board you are prepared to advise on future company strategy built around this central principle of privacy by design. Consider the benefits of appointing/recruiting a data specialist to the board.

PAYING THE PRICE FOR NON-COMPLIANCE

The penalties for breaching the GDPR are severe. Organisations face fines of up to €20 million or 4% of annual global turnover, whichever is greater. Aside from the financial implications, the reputational damage caused by non-compliance is bound to be harsh. Despite this, Julian David, chief executive of industry body TechUK, told the *Financial Times* in August of his concerns that organisations are not giving the GDPR the board attention it deserves: "Companies should have been doing this at board level for some time, but we have a feeling that some aren't".[6] This concern about lack of board involvement in GDPR preparations is echoed in research carried out by cloud company Calligo among IT Directors, which found that only 31% of organisations reported having governance sponsorship for GDPR compliance at board level.[7]

The legislation indicates that responsibility for compliance is shared through all levels of the organisation, but the requirement for the Data Protection Officer to report to the board implies that in practice ultimate responsibility lies at board level.

BEYOND COMPLIANCE: MAKING TRUST THE CORNERSTONE OF CUSTOMER ENGAGEMENT

In today's seamlessly connected world, the relationship between customers and businesses or public sector organisations has deepened beyond the fundamental supply of goods and services. Customers view organisations through a lens of their own personal values and expect the companies and authorities that they deal with to act with principles and ethics that reflect high levels of integrity. How organisations manage and protect the personal data with which they are entrusted is one way in which they can prove that the customer's well-being is at the heart of their business. This means being robustly clear about what information is being collected, how it will be used and the rights that the data subject has to change or erase that data. With ICO research indicating that 75% of consumers do not trust companies with their personal data,[8] the implementation of the GDPR offers a golden opportunity for boards to use regulation as a catalyst for business change and initiate a culture of customer respect that permeates the organisation and offers a competitive advantage. As the UK's Information Commissioner Elizabeth Denham commented: "It is a legal trend that we've seen in other parts of the world: a demand that the boardroom builds a culture of privacy that pervades an entire organisation. It's about moving away from seeing the law as a box-ticking exercise, and instead working on a framework that can be used to breed a company-wide culture of privacy, so it becomes the norm for generations to come".[9]

So beyond the technology and legal procedures made necessary by the legislation, boards should establish what is being done to develop a culture of customer privacy and data protection. Helping staff to work according to good data protection practice

"It is a legal trend that we've seen in other parts of the world: a demand that the boardroom builds a culture of privacy that pervades an entire organisation. It's about moving away from seeing the law as a box-ticking exercise, and instead working on a framework that can be used to breed a company-wide culture of privacy, so it becomes the norm for generations to come." [9]

The UK's Information Commissioner, Elizabeth Denham

also reduces the risk of inadvertent weakening of the procedures that are in place. Employees should be encouraged to feel that they have a valuable role to play in supporting customer privacy and building trust.

Marketing departments also need to know what they should do to ensure that the highly personalised and timely marketing enabled by big data also respects individual privacy rights. A survey by the Direct Marketing Association found, unsurprisingly, that gaining the right level of consent to carry out marketing activities was top of the list of concerns for marketers.[10] However, marketing departments should also consider how they can turn GDPR compliance into a competitive advantage that builds a reputation as a trusted partner.

When it comes down to it, respecting a customer's privacy is simply the logical extension of respecting the customer. It creates a virtuous circle of trust: the more people trust you, the more information they'll share, the more relevant and tailored your market offering can be and the more successful your business will become. And building successful organisations that deliver outstanding value is the guiding principle of every board.

1 "Data is the new oil" ANA marketing maestros Clive Humby, November 2006 http://ana.blogs.com/maestros/2006/11/data_is_the_new.html

2 "Data Age 2025: The evolution of data to life-critical" IDC sponsored by Seagate David Reinsel, John Gantz, John Rydning, April 2017, https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

3 EU Home affairs subcommittee briefing on The EU Data Protection Package, Elizabeth Denham, UK Information Commissioner, March 2017 http://www.parliamentlive.tv/Event/Index/125e1463-62ed-41bb-ab64-811d0f94bfee 10:44:22

4 "HM Government: The exchange and protection of personal data. A future partnership paper" HM Government, August 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

5 "Computing Research Paper: GDPR – Confidence versus reality" Computing Magazine, September 2017 https://www.carbonblack.com/wp-content/uploads/2017/09/Computing-Research-GDPR-Readiness-Whitepaper.pdf

6 "Tech sector struggles to prepare for new EU Data Protection laws" Aliya Ram, The Financial Times, August 2017 https://www.ft.com/content/5365c1fa-8369-11e7-94e2-c5b903247afd

7. "Majority of UK boards are neglecting GDPR while retail suffers breaches" Roi Perez, SC Magazine UK, July 2017 https://www.scmagazineuk.com/majority-of-uk-boards-neglecting-gdpr-while-retail-suffers-breaches/article/676291/

8. "Information Rights Research 2016" The Information Commissioner's Office https://ico.org.uk/about-the-ico/our-information/research-and-reports/information-rights-research/

9. "With one year to go, UK firms have no time to waste in preparing for the GDPR" Elizabeth Denham, City A.M. May 2016 http://www.cityam.com/265367/one-year-go-uk-firms-have-no-time-waste-preparing-gdpr

10. "Why GDPR training is a must for marketers" Rosemary Smith, The Institute of Direct and Digital Marketing May 2017 https://www.theidm.com/content-resources/blog/may-2017/why-gdpr-training-is-a-must-for-marketers

Diligent

Unleashing the value of information. Securely.

Diligent helps the world's leading organisations unleash the power of information and collaboration – securely – by equipping their boards and management teams to make better decisions. Over 4,700 clients in more than 70 countries rely on Diligent for immediate access to their most time-sensitive and confidential information, along with the tools to review, discuss and collaborate on it with key decision-makers. Diligent Boards expedites and simplifies how board materials are produced and delivered via iPad, Windows devices and browsers. At the same time, Diligent Boards delivers practical advantages like cutting production costs, supporting sustainability goals, and saving administrative and IT time for leaders around the world.

Join the Leaders. Get Diligent.

Download on the App Store · Get it from Microsoft · GET IT ON Google Play · AICPA SOC · ISO 27001 CERTIFIED BY BRIGHTLINE

For more information or to request a demo, please contact us by:

Tel: +44 (0)20 7605 7480
E-mail: info@diligent.com
Visit: diligent.com

WP0037_UKEN