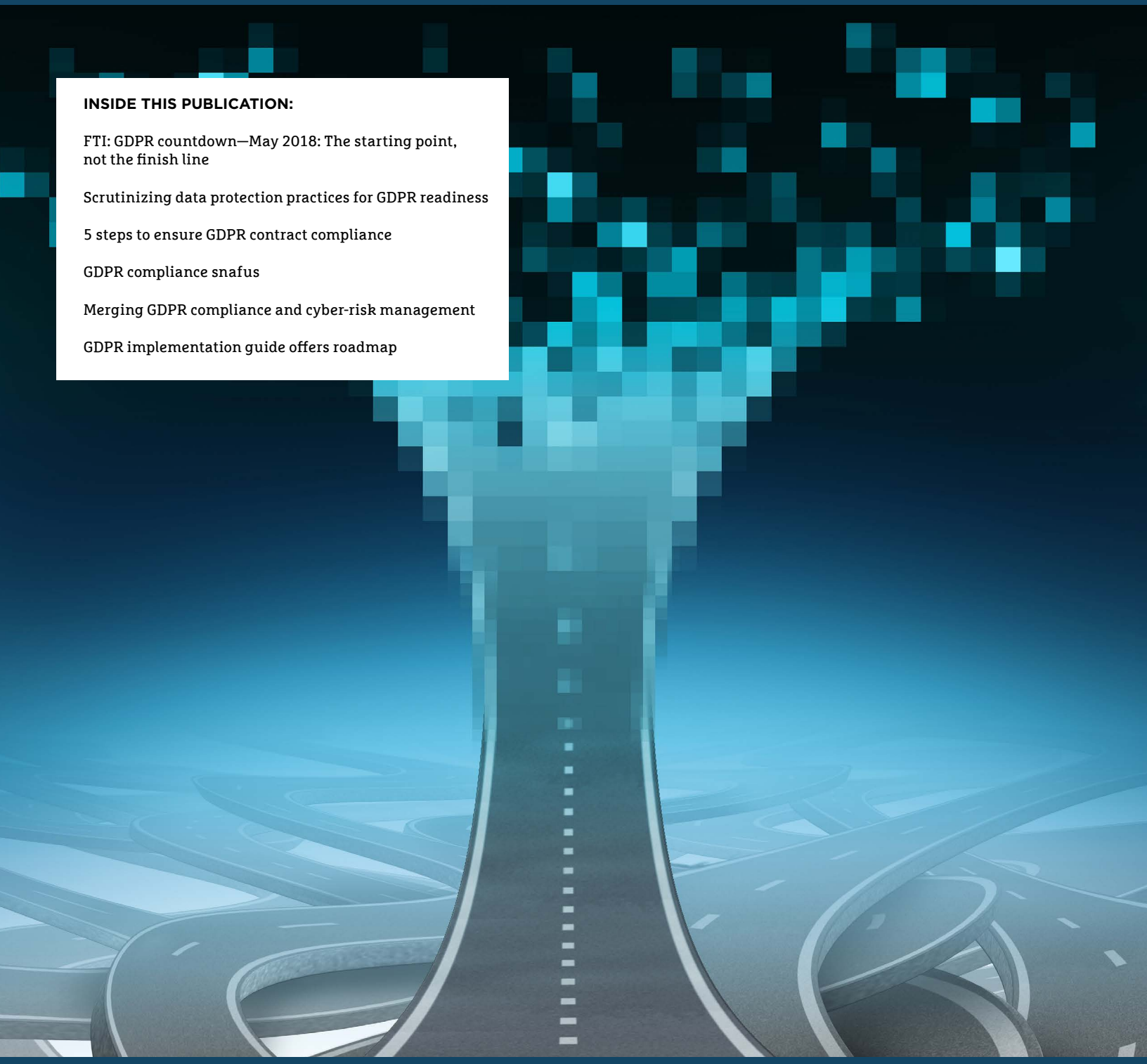
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

FTI: GDPR countdown—May 2018: The starting point, not the finish line

Scrutinizing data protection practices for GDPR readiness

5 steps to ensure GDPR contract compliance

GDPR compliance snafus

Merging GDPR compliance and cyber-risk management

GDPR implementation guide offers roadmap

Twists and turns in the road
Driving toward GDPR

An e-Book publication sponsored by FTI CONSULTING | TECHNOLOGY

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

FTI CONSULTING | TECHNOLOGY

FTI Technology solves data-related business challenges, with expertise in legal and regulatory matters. As data grows in size and complexity, we help organizations better govern, secure, find, analyze and rapidly make sense of information. Innovative technology, expert services and tenacious problem-solving provide our global clients with defensible and repeatable solutions. Organizations rely on us to root out fraud, maintain regulatory compliance, reduce legal and IT costs, protect sensitive materials, quickly find facts and harness organizational data to create business value. For more information, please visit www.ftitechnology.com.

Inside this e-Book

FTI: GDPR countdown—May 2018: The starting point, not the finish 4

Scrutinizing data protection practices for GDPR readiness 8

5 steps to ensure GDPR contract compliance 11

GDPR compliance snafus 13

FTI: GDPR countdown—May 2018: The starting point, not the finish 14

GDPR implementation guide offers roadmap 18

FTI CONSULTING

GDPR COUNTDOWN

May 2018: The starting point, not the finish line

Companies around the globe are impacted by the landmark EU legislation, the General Data Protection Regulation (GDPR) which comes into force on May 25, 2018. While there is tremendous focus on the steep fines, the risks associated with reputational damage due to the inappropriate management of personal data is much greater. Trust is the fuel behind the digital economy. Done right, GDPR will help companies to strengthen trust and transparency with its clients.

Cost of a data breach

£120m

-1.8%

A firm listed on the FTSE 100 becomes worse off by roughly £120 million in the wake of a breach, while share prices fall by an average of 1.8 per cent.[1]

Over 140 million Americans and UK residents were impacted as a result of the Equifax data breach in September 2017. Under the GDPR, the potential fine of 4% of global annual turnover would have meant about a $63 million USD fine. The event also resulted in the resignation of the CEO, CIO and CISO and subsequent criminal investigations for insider trading. The case for evolving data privacy and security from being a CIO/CISO technical issue to becoming a company wide and board room priority is clear.

The GDPR modernises and replaces the existing EU Data Protection Directive (95/46/EC), adopted in 1995. Under the GDPR, individuals across Europe will have enhanced rights, including the right to have their data deleted, as well as rights around data portability. The bar has also been raised around consent, which will need to be unambiguous, freely given, and an affirmative action.

One of the aims of the GDPR is to give control of personal data back to the individual, while simultaneously promoting greater corporate accountability and transparency. There is now increasing demand from consumers worldwide that organisations take stronger measures to secure and protect their personal data.

> *According to the International Association of Privacy Professionals (IAPP) at least 75,000 new data protection officers (DPOs) will be needed worldwide in response to this EU law.*[3]

According to a survey by the Information Commissioner's Office (ICO)[2] only one in four UK adults trust businesses with their data. This piece of legislation is already generating a lot of debate and discourse across the UK, Europe and beyond, at the c-suite and boardroom levels of many businesses. This is because of the potential for significant penalties and brand damage.

More importantly data protection issues are fast becoming reputation issues. Investors have started punishing companies for poor security; listed companies have lost millions of pounds with share prices dropping in the wake of data breaches. According to a study by Oxford Economics a firm listed on the FTSE 100 becomes worse off by roughly £120 million in the wake of a breach, while share prices fall by an average of 1.8 per cent.[1]

The legislation is complex and far-reaching, laying out specific mandates for any company doing business in Europe involving the personal data of consumers in 28 EU member states plus Norway, Liechtenstein and Iceland. This will also include the UK, which is likely to maintain compatible data protection laws to enable free data flows post-Brexit.

Information governance as a journey

Managing data compliance, risk and security is unlikely to be a simple issue to resolve. Compliance for the GDPR and better information governance is a journey for many corporations - one that involves ownership of aligning complex rules & obligations with the data itself.

Corporations are now taking stock of their data assets. There is greater realisation that many businesses sit at the centre of a complex ecosystem of information. This raises questions about data protection regulation throughout their data landscape, such as why and how they collect and process the personal data they do, the answers to which lay at the very core of their business.

Additionally, holding on to data for longer than you are legally allowed creates a multitude of issues beyond the GDPR. Corporations are now taking the opportunity to get rid of personal data they no longer need or use.

For many corporations, there are still as many – to use a phrase coined by former U.S. Secretary of Defence, Donald Rumsfeld – 'unknown unknowns' as there are 'known unknowns' when it comes to the GDPR with respect to the data they hold. Companies will need to take a risk-based approach, but also develop a strategy for dealing and mitigating the risk associated with these unknowns.

The scale of the task is not to be underestimated. According to the International Association of Privacy Professionals (IAPP) at least 75,000 new data protection officers (DPOs) will be needed worldwide in response to this EU law.[3]

Holistic approach needed

All companies handling the personal data of EU citizens will be accountable for complying with the GDPR, including data processors. Prior to this new regulation, data processors were only responsible for following data controller's instructions. Everyone along the data supply chain will now need to take a proactive role in the identification, management, security and governance of personal data.

This EU legislation will have a systemic effect on how we handle information relating to an individual. Companies will need to have clearly defined procedures and systems in place when a data breach occurs, and the company will need to notify supervisory authorities within 72 hours, and in some cases, also notify the impacted individuals without 'undue delay'.

GDPR Considerations

- **Data inventorying** also has the net effect of forcing an organisation to understand its core business processes, **why** they do **what** they do, and **where** they could be simplifying or eliminating unnecessary collection/steps and consequently reducing risks.
- The GDPR is not a box-ticking exercise; it is about a whole **cultural shift** within an organisation, well beyond 25 May 2018.
- The legislation has **extraterritorial reach**, which means any company around the globe, including those based in the US, that interact with EU personal data will be required to comply.
- **Personal data** under the GDPR is broader than Personally Identifiable Information (PII) and includes any information which directly or **indirectly** identifies an individual.
- **GDPR** it just one regulation. **NIS** cyber directive, Payment Service Directive **(PSD2)** and other regulatory requirements need to be considered in a broader framework for how and why data is collected and protected through its life.
- **Data protection** and **information governance** is everyone's issue, not just that of the IT department.

Compliance therefore needs a holistic and integrated approach. This involves many stakeholders, processes and technology, all of which need to talk to one another. IT, privacy, marketing, legal, business and security professionals and the board must get involved and take a proactive approach.

Executives must act less in silos and realise everyone has a vested interest to make data compliance work. There is also a recognised disconnect in businesses, between the requirements of data whether it be legal, regulatory or business value and how it is being managed, in reality.

Those companies who have brought the right stakeholders together to address data compliance regulations have reaped the benefits of a collaborative approach, working through the issues as a team.

> *When it comes to compliance, you need to ask the right questions about how and why you have the data you do, align it with the rules around it so that you can use it lawfully.*

Restraints and constraints with the GDPR

Many organisations have budget constraints when it comes to governing data and allocating resources for a large piece of legislation such as the GDPR. Budgets also vary greatly depending on the scope of compliance activities and also existing investments made in data privacy, security and information governance.

Some organisations are seeing this legislation as an opportunity to get board level support and funding towards critical digital transformation and data management initiatives. The GDPR enables companies to take a client-first approach, re-engaging with their clients, employees and other business associates about their preferences, personalisation and security, based on transparency and openness.

One of the other intents of the GDPR is to streamline and provide greater consistency in the enforcement of EU data protection regulation. Companies will still need to pay attention to applicable local data protection legislation which minimally apply the GDPR and may adopt even more stringent requirements. There are still a number of areas in the GDPR that leaves it up to member states to adopt their own national rules, such as those regarding the processing of personal data in an employment context.

The GDPR is just one of many regulations governing the privacy and security of customer data being implemented across the globe. The ePrivacy Regulation (EPR) and the NIS cyber directive are also upcoming legislation that need to be considered in the overall design of a GDPR compliance framework.

Many corporations are also considering the implications of moving data to the cloud. Some cloud-based service providers have enhanced retention, security and privacy controls built in. However, even with these controls in place, it is up to the company to ensure they understand the location of their cloud providers and where they host their data. It is crucial that the required organisational and technical controls are applied, and the appropriate provisions are declared in any applicable contracts to enforce these new obligations.

The role of the authorities such as the ICO which will implement the GDPR in the UK is also a factor when it comes to compliance. Dealing with the potential volume of inquiries may be an issue for the ICO. The amount of resources needed to investigate some cases could be vast. Some highly regulated industries such as financial services and pharma may have started compliance efforts early and therefore have an advantage over other industries such as retail and manufacturing who may have less maturity or budget in managing/protecting its personal data and may be particularly vulnerable to GDPR related threats.

Many firms are working on completing their assessments and are beginning their remediation efforts in order to comply with the 25th of May 2018 deadline. With limited time and resources, companies need to prioritise their compliance actions.

Focus on clients and customer personal data first and those areas of highest risk and impact in the event of breach. Understand the role of technology as an enabler, not the solution to GDPR compliance. Finally, if you do nothing else, bring awareness to your organisation about the GDPR and take some steps towards compliance. Doing nothing is the highest risk choice that you can make.

RESOURCES:
1. The Cyber-Value Connection, www.cgi-group.co.uk, 2017
2. Consumers taking action over mistrust of organisations handling personal data , www.ico.org.uk, 15 June 2016
3. Study: GDPR's global reach to require at least 75,000 DPOs worldwide, www.iapp.org, 9 Nov 2016

Lessons to be learnt

1 **Know your Approach:** Consider your risk profile, company size and industry to shape how you approach GDPR compliance. One size does NOT fit all.

2 **Cultivate Awareness:** Your executive stakeholders and board need to understand the specific risks and costs, and how it impacts your organisation.

3 **Process First, Technology as an Enabler:** Don't believe the hype, technology alone will not make you magically compliant. Get to know your business processes first, follow the data, and augment with technology where it is cost-effective. Technology without process context or purpose could result in wasted budget, resources, and organisational fatigue.

Sonia Cheng
Senior Director
Information Governance & Compliance Services
+44 (0)20 3727 1783
sonia.cheng@fticonsulting.com

Paul Prior
Managing Director
Performance Analytics
+353 879665296
paul.prior@fticonsulting.ie

FTI CONSULTING™

EXPERTS WITH IMPACT

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.


0123456789
0123456789
0123456789
0123456789
0123456789

Scrutinizing data protection practices for GDPR readiness

By May 2018, the EU's General Data Protection Regulation will take effect, and many companies are seriously underestimating the amount of compliance work this will require. **Steve Durbin** has more.

The Information Security Forum (ISF) considers the General Data Protection Regulation (GDPR) to be the most noteworthy shake-up of global privacy law in decades. Not only does it redefine the scope of EU data protection legislation, it forces organizations globally to comply with its requirements.

The regulation officially goes into effect in May of 2018 and will have an international reach, affecting any organization that handles the personal data of European Union residents, regardless of where it is processed. Many U.S.-based organizations will fall under the GDPR's purview. In fact, few organizations will be able to completely avoid the requirements.

The GDPR adds another layer of complexity to the issue of critical information asset management that so many organizations are already struggling with. The GDPR aims to establish the same data protection levels for all EU residents and will focus on how organizations handle personal data. Businesses face several challenges in preparing for the reform, including a widespread lack of awareness among internal stakeholders. The additional resources required to address the obligations are likely to increase compliance and data management costs while pulling attention and investment away from other important initiatives.

In the longer term, organizations will benefit from the uniformity introduced by the reform. If the GDPR means companies no longer have to circumnavigate the current array of often-contradictory national data protection laws, compliance costs and activities may decrease once past the initial implementation and transition period. There will also be worldwide benefits as countries in other regions dedicate more attention to the defense of mission-critical assets and personal data privacy.

The GDPR has the potential to serve as a healthy, scalable, and exportable system that sets an international benchmark for sustainable online commerce and communication. But first, companies need to understand the nuances of their obligations under GDPR and carefully examine and test their preparedness. The results of recent surveys (e.g., PwC, Veritas, and Compuware) about GDPR readiness indicate that organizations are overly optimistic about their compliance with major provisions of the pending regulation, particularly the requirement to report data breaches within 72 hours of awareness.

The consequences of non-compliance

Most countries, including all EU nations, have established supervisory authorities to oversee the use of personal data. These supervisory authorities are government-appointed bodies that have powers to inspect, enforce, and penalize the processing of person-

al data. In the United States, a number of authorities enforce data protection requirements under the sectoral approach, most notably the Federal Trade Commission, which has substantial regulatory powers.

Supervisory authorities are granted investigatory powers by the GDPR, allowing them to investigate any complaint they receive through a variety of measures, such as audits and reviews of certifications and codes of conduct. Complaints may be received not only from the data subjects themselves, but also from any organization or association that chooses to complain or has been chosen by a data subject to represent their interests. These complaints can be submitted to any supervisory authority, not just the authority with territorial responsibility.

If an organization is found to be infringing the requirements of the GDPR, supervisory authorities have a variety of corrective powers from which to choose. These include the ability to issue warnings and reprimands to controllers or processors, but also far more substantial powers. Authorities can compel an organization to process data in certain manners or cease processing altogether and can also force an organization to communicate data breaches to affected data subjects.

The time to prepare is now

No organization that operates on a global footprint of suppliers can afford not to prepare for changes that will result from new GDPR compliance rules. Falling out of compliance with data regulation can really hit you in the pocket. The checklist of rules requires extreme preparation and responsibility, all of which must be shouldered by the individual organization; relying heavily on government or regulators for help is imprudent.

The GDPR is putting data protection practices at the forefront of business agendas worldwide. For most organizations, the next year will certainly be a critical time for their data protection regimes as they begin to determine the applicability of the GDPR and the controls and capabilities they will need to manage their compliance and risk obligations. Because of the effort required to report data breaches, it is essential that organizations prepare in advance.

Executive management will be responsible for ensuring that an organization meets its legal obligations to implement the GDPR's requirements. A Data Protection Officer should be designated to act as a focal point for ongoing data protection activities. An organization's governance functions, including information security, legal, records management, and audit should ensure they are familiar with the requirements of the GDPR and have the necessary people, processes, and technical solutions in place to achieve compliance.

With reform on the horizon, organizations planning, or already doing business in Europe, should get an immediate handle on what data they are collecting on European individuals, where it is coming from, what it is being used for, where and how is it being stored, who is responsible for it, and who has access to it.

Optimally, an organization should complete GDPR preparations well before May 2018 in order to leave a good amount of time for requesting and responding to third-party (processor) assurances. These activities require resources with the expertise and time to assess contracts and data impacts, issue assurance requests, and process responses. Data protection, legal, and information security teams should plan for this task so that they are not overwhelmed with requests closer to the enforcement deadline.

The General Data Protection Regulation raises the stakes; players who want to stay at the table come next year must have their data management affairs in order. Those caught unprepared will be scrambling, vulnerable, and poorly positioned against better-organized competitors. ■

Steve Durbin is Managing Director of the Information Security Forum (ISF). His main areas of focus include strategy, information technology, cyber security and the emerging security threat landscape across both the corporate and personal environments. Previously, he was senior vice president at Gartner.

5 steps to ensure GDPR contract compliance

By May 2018, the EU's General Data Protection Regulation will take effect, and many are seriously underestimating the amount of compliance work this will require. **Mark Ross** reports.

The European Union's implementation date for the General Data Protection Regulation is fast approaching. May 25, 2018, will be here before we know it. Companies that interact with and/or process EU personal data should hopefully be well on their way to ensuring all data protection processes and procedures are GDPR compliant. If not, they could face steep fines and penalties (€20 million (U.S.$23M) or up to 4 percent of global annual turnover, whichever is greater) after GDPR takes effect.

One of the most involved—but important—tasks to ensure General Data Protection Regulation compliance is a comprehensive review of customer, supplier, inter-company, and data privacy agreements. For many companies, this can be a significant undertaking and requires careful attention to make sure these contracts follow internal corporate policies, are in line with overall corporate strategy, and meet GDPR and other regulatory requirements. If not, and the contracts govern relationships involving access to individuals' personal data, then they need to be remediated.

Below are five critical steps companies should take to review and amend contracts in advance of the GDPR implementation date that can serve as a checklist.

1. Review existing policies and procedures and perform a gap analysis. Before any customer or supplier contracts are reviewed or amended, companies should conduct a thorough review of existing data privacy compliance initiatives, policies, and procedures and flag anything that does not meet GDPR and other regulatory standards. Like other regulations (e.g., the Foreign Corrupt Practices Act), you should also verify that third-party suppliers that may handle your data are GDPR compliant or well on their way to compliance by May 2018. This "gap analysis" should also include ensuring data retention policies specify how long information is kept and that data maps exist that show where and how data is stored across the organization.

This review and gap analysis will ensure the organization's GDPR compliance processes are fully aligned with its strategic objectives, and it will help to determine best practices and internal policies to guide and facilitate compliance. It also reveals red flags, inconsistencies, and areas for remediation that can be addressed before any contracts are amended.

2. Develop a playbook for moving forward. After a company has undertaken a detailed GDPR gap analysis, they can turn to contract review and remediation. The first component should be the design of a comprehensive playbook to guide the end-to-end contract drafting and contract amendment process both for legacy contracts and contracting

on a going-forward basis. Many companies are both controllers and processors of data, and the playbook should consider the implications of this on the end-to-end contracting process. In addition to setting out the processes that need to be followed, the playbook should include a GDPR amendment template that includes new GDPR-compliant clauses together with guidance for contract negotiators on how to deal with likely pushbacks from counterparties.

The playbook will be used to redline and negotiate amendments or any counterparty templates received by the company. The creation of a playbook will help minimize the risks associated with GDPR non-compliance by standardizing the approach to contract remediation and setting out clearly the approved templates and clause language required.

3. Review and identify in-scope contracts. Once the above step is complete, a company can then turn to reviewing contracts. Depending on the size of the company, there could be a high volume of contracts to review and, if necessary, amend. Using an A.I./machine-learning contract review tool can greatly speed the process of identifying active and inactive agreements, abstracting relevant contract provisions and pinpointing contract types for GDPR compliance remediation. In this stage, companies will want to:

» Sort legacy customer and supplier contracts first by whether they are active or in-active. Only contracts that will continue beyond May 2018 should be further reviewed to identify if in-scope or out-of-scope for GDPR compliance purposes;
» Prioritize initially your highest risk, active, in-scope contracts for review and potential remediation; and
» Identify whether these contracts are compliant or non-compliant with GDPR. Unless terms have already been updated, these contracts will be non-compliant and require amendment. In addition, if under the terms of the contractual relationship data is being transferred outside of the European Union, an appropriate data transfer mechanism will need to be in place, such as the Standard Contractual Clauses.

4. Draft and send amendments. After the contract review is complete, organizations should draft amendments incorporating updated GDPR-compliant terms and send these out to the in-scope counterparties. Keep in mind that some counterparties may be unresponsive and require multiple follow-ups. Also, don't assume that all customers and vendors will be up-to-speed with the implications of GDPR. Some amendment negotiations will run extremely smoothly, and others may be more difficult and elongated. These eventualities and guidance for contract negotiators will be detailed in the playbook.

5. Finalize and execute contracts. With agreed-upon language in place, finalize and execute the amended contracts and upload or store them in your contract lifecycle management platform or repository with the key terms entered in a structured data format. This way companies will have an auditable "source of truth" if ever called upon to demonstrate GDPR compliance.

Now is the time to begin prepping for GDPR. Companies that have not yet started a comprehensive GDPR compliance review would be wise to start as soon as possible. This is an involved, time-consuming process that should not be left to the last minute. A rushed job, or one that does not follow a thoughtful, strategic path, could lead to costly gaps in compliance. ■

Rachita Maker and Patrick Won contributed to developing this article.

Mark Ross is global head of contracts, compliance and commercial services at Integreon; Rachita Maker is vice president of contracts, compliance and commercial services at Integreon; Patrick Won is manager of contracts, compliance and commercial services at Integreon.

GDPR compliance snafus

Any company with business ties to the EU should be aware this rule has teeth that can cut into bottom lines. **Jason Hart** reports.

How can U.S. businesses ensure they are compliant with the General Data Protection Regulation? For starters, they must focus on who is authorized to access sensitive data. The best approach is to use two-factor authentication, which requires an employee to have something more than just a code or password that can be guessed. Next, U.S. firms should adopt a multistep formal process to protect data, like their EU brethren. This should begin with gaining a thorough understanding of the rule and include a compliance audit conducted against the GDPR legal framework. Once there is a clear idea of readiness to meet requirements, they need to keep a record of efforts to comply—essentially a GDPR diary.

Data should be evaluated, including understanding how it's produced and protected. As part of this, businesses should complete a Privacy Impact Assessment and Data Protection Impact Assessment of security policies, evaluating data lifecycles from origination to destruction. Next is to assess and document other risks. Below are areas to focus upon:

» **Leverage ISO 27001:** This can begin to put a company on the road to GDPR compliance. By meeting specifications, the information security management system framework can take an organization part of the way for complying with important policies and procedures encompassing legal, physical, and technical controls of a company's information risk management processes. While this is not entirely sufficient, many companies already adhere to it, so it should be leveraged.

» **Classify data:** Understanding data and where it is stored is critical. Specifically, classifying it can help provide an overview of PII possessed by a company. Identifying what data you have and where it resides is not only vital to protecting the very information that can raise most GDPR compliance issues, it can assist in exposing vulnerabilities.

» **Control access:** Map out who has access to sensitive data, so you are able to gain the control you need to ensure it's protected and compliance measures are being met. This should include an internal examination of employees and those outside the firm.

» **Document compliance:** Companies need to keep a detailed record of compliance progress. Whether it's a data register or documentation road book, an organization should be able to show a record of efforts to comply to data protection authorities.

» **Consider consent:** Consent is important under GDPR and is defined as "any freely given, specific, informed, and unambiguous indication of his or her wishes by which the person, either by a statement or by a clear affirmative action, signifies agreement." Businesses should not rely on silence or opt-outs. Instead, a process such as box-ticking should be put in place for compliance purposes.

» **Plan for breaches:** Today, it's not a question of "if" you will be hacked, it's "when." Prepare and develop an action plan. Know that breaches must be reported to the relevant supervisory authority without delay and, "where feasible," no later than 72 hours after a data controller has become aware.

Firms need to start taking security seriously from the top down and start prepping before it's too late and they are faced with fines and a damaged reputation. ■

Jason Hart is VP and chief technology officer for data protection at Gemalto, a digital security provider.

Merging GDPR compliance & cyber-risk management

Many organizations today are elevating cyber-risk to the top of the corporate agenda in response to the impending EU General Data Protection Regulation, a new report reveals. **Neil Hodge** has more on the GDPR preparedness study.

In preparing for the impending implementation of the EU General Data Protection Regulation, many organizations today are elevating cyber-risk to the top of the corporate agenda, a new cyber-risk perception survey has found.

The survey, "GDPR Preparedness: An Indicator of Cyber Risk Management," conducted by insurance broker Marsh, found that organisations are using the process of complying with the EU General Data Protection Regulation (GDPR) as an opportunity to beef up their cyber-risk management and resilience.

Furthermore, the survey found that respondents who said their organisations either complied with, or were developing a plan to comply with, the GDPR were more than three times as likely to adopt some cyber-security measures—and more than four times as likely to adopt some cyber-resiliency

measures—as those who had not started planning.

The survey of over 1,300 executives worldwide also found that respondents with a higher level of GDPR readiness were more than 1.5 times as likely to purchase or strengthen their cyber-risk insurance to help offset the financial impact of a cyber-event.

Among respondents who said their organisation was subject to the GDPR, 65 percent viewed cyber-risk as a top-five risk management priority—little wonder given that one in four of them (23 percent) had been victims of a successful cyber-attack in the last year. Moreover, the threat of a cyber-attack leading to a data leak is significant, and fines for serious data breaches under the new regulation can rise to €20m or 4 percent of global turnover (whichever is greater). Thus, organisations need to equate GDPR compliance with good risk management.

Marsh believes that cyber-risk management is "both a cause and consequence of GDPR compliance." In fact, a key provision of the EU regulation, which comes into effect next May, states that the adoption of "appropriate technical and organisational measures" is essential if they want to ensure a "level of security appropriate to the risk."

Marsh states that "organisations with strong cyber-security measures have a jumpstart on compliance, since the GDPR strongly encourages certain practices, such as encryption." It added that several other cyber-security-related measures can positively impact general GDPR compliance—for example, although cyber-incident planning and cyber-insurance are not explicitly required under the regulation, they enable firms to quickly marshal the resources to meet the GDPR's 72-hour data breach notification guidance.

Other than having to notify regulators and data subjects of a breach within three days, the GDPR has few explicit requirements (though national regulators may provide additional guidance later). In fact, most are recommendations, rather than strict provisions, such as strongly encouraging encryption.

This principles-based approach puts the onus on organisations to determine "appropriate" controls based on their risks and, with no ready-made checklist, requires them to look more deeply at their business operations and review how they protect personal data, especially since the regulation's scope is extra-territorial. The GDPR applies to all organisations that collect or process data on EU residents, no matter where they are headquartered or operate. Any company that offers products or services in the European Union may be affected.

Because the GDPR compliance process requires organisations to implement measures that are appropriate to the potential threats they face, these forward-looking organisations have rigorously analysed their cyber-risk exposures and have put a dollar amount on potential losses.

Evidence suggests that organisations that are compliant or that are developing a GDPR plan are more likely to adopt cyber-risk management measures, irrespective of whether the regulation requires them to do so. For example, 56 percent of respondents in the Marsh survey have ensured that their work desktops and laptops are encrypted to prevent data losses, which is strongly encouraged—though not required—under the regulation.

The same number have conducted penetration testing and carried out improved vulnerability testing and patch management—again, without being forced to do so. Thirty-one percent have identified external legal, PR, and/or cyber-security experts to provide support during a cyber-incident—a precau-

Marsh reports that GDPR preparation is focusing executive attention on broader data protection and privacy issues and prompting related investments. Among respondents with a higher level of GDPR readiness, 78 percent reported an increase in cyber-risk management spending, including on cyber-insurance.

tion that the GDPR strongly implies that organisations should take.

Other cyber-risk management actions that organisations have carried out include conducting cyber-security gap assessments; providing enhanced phishing awareness for employees; requiring multifactor authentication for employees to have remote access to the company network; and developing cyber-response plans and scenario testing.

Marsh reports that GDPR preparation is focusing executive attention on broader data protection and privacy issues and prompting related investments. Among respondents with a higher level of GDPR readiness, 78 percent reported an increase in cyber-risk management spending, including on cyber-insurance.

Not many respondents to the Marsh survey, however, have made much progress toward full GDPR compliance. Just 8 percent of respondents said that their organisations were fully compliant. Over half (57 percent) said that their organisations were developing a compliance plan, while 11 percent had yet to start, and 24 percent did not know how far along in the process their organisations were.

Common factors. According to Marsh, organisations that have made the most progress in using GDPR compliance to review their cyber-security measures share three common characteristics.

Firstly, they understand that cyber-risk management is a shared responsibility that extends from the IT department to the executive suite. Regardless of size, Marsh said that many of these organisations have set up internal cross-functional taskforces or steering committees led by senior executives—sometimes including or reporting to the CEO.

Marsh said these organisations are using the GDPR compliance process to look comprehensively at how they collect, retain, use, and manage data across the enterprise. They are exploring new tools (such as the use of cloud services), are championing privacy rights and have made significant investments to ensure that any information they possess is secure. More broadly, they are re-examining their privacy and data protection practices to ensure that people, processes, and technology are properly aligned.

Secondly, they treat cyber-events as inevitable. Instead of focusing only on preventing cyber-attacks, these organisations look to respond to incidents more quickly and reduce the potential damages, viewing the GDPR's data breach notification requirement as an opportunity to develop stronger incident management protocols, for example, or encrypt their computer systems so that stolen data is rendered useless.

Thirdly, they take a quantitative and holistic approach. Because the GDPR compliance process requires organisations to implement measures that are appropriate to the potential threats they face, these forward-looking organisations have rigorously analysed their cyber-risk exposures—both internal and external—and have put a dollar amount on potential losses. As a result, they are not only investing in appropriate cyber-security defences, but they are strengthening cyber-incident response plans as well as other risk mitigation and resiliency measures. ■

WHAT IS THE EU GDPR

A look at the key points of the General Data Protection Regulation follows.

EU member states—including the United Kingdom (despite Brexit)—have had since May 2016 to prepare for the GDPR. The regulation comes into effect across the 27-nation bloc next May and its powers are sweeping: it affects all organisations gathering data on EU citizens anywhere in the world—not just European companies operating in the EU—and can raise fines up to €20m or 4 percent of global turnover (whichever is greater) for serious compliance failures.

Other key points regarding the regulation include:

- Organisations must gain explicit consent for the collection of specific categories of sensitive personal information.
- There are new restrictions on the profiling of data subjects.
- Organisations must maintain an inventory of where personal data exists and be able to demonstrate compliance with the regulation.
- There is a legal requirement for organisations to appoint a data protection officer when core activities include the large-scale processing of special categories of personal data and/or criminal conviction information, or the systemic monitoring of data subjects.
- Data privacy impact assessments will be required for certain new or changed products and services.
- If organisations have suffered a personal data breach, they are required to notify both the regulator and data subjects "without undue delay"—meaning within 72 hours.
- There are new and enhanced rights for data subjects, including the right to request access, correction, and deletion of personal data.
- Regulatory or enforcement action will be lead by a single regulator/authority.

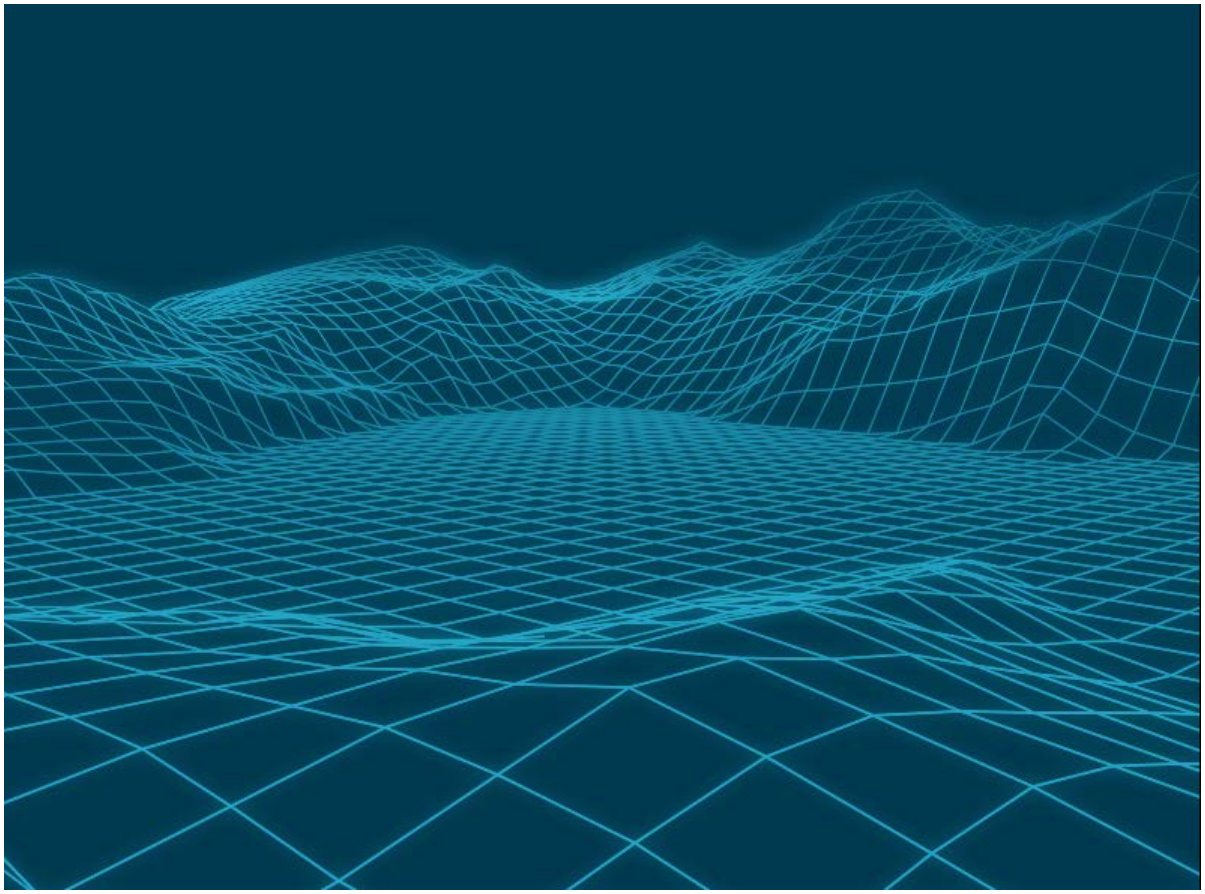
As the implementation deadline looms closer, several membership bodies have issued guidance in recent weeks to help organisations get to grips with the compliance requirements.

Working with law firm Baker & McKenzie, the Institute of Chartered Secretaries and Administrators (ICSA), an organisation that promotes better corporate governance practices, issued guidance to facilitate conversations between the board and those within organisations responsible for dealing with data to help them deal more effectively with the implications of the forthcoming GDPR.

Alongside an overview of the new legal landscape, the guidance highlights the strategic and practical considerations raised by GDPR. It includes a series of checklists that compliance professionals may find useful.

Meanwhile, the Information Security Forum (ISF), an organisation that champions IT security practices, has also issued its GDPR Implementation Guide, which includes best practice tips for compliance functions to prepare for the regulation coming into effect. The guide presents GDPR compliance in two phases: the first phase is to "prepare" by discovering personal data, determining its compliance status, and defining the scope of a GDPR compliance programme; while the second phase is to "implement" the GDPR requirements to demonstrate sufficient levels of compliance.

—Neil Hodge



GDPR implementation guide offers roadmap

Figuring out how to comply with the fast-approaching GDPR isn't easy, but this handy guide from the ISF will be a big help to compliance officers everywhere. **Bill Coffin** has more.

On May 25, 2018, the General Data Protection Requirement, one of the most far-reaching global privacy laws in decades, will take place. And as it does, it will place a huge responsibility upon any business that handles the personally identifiable information of any EU citizen, regardless of where that data is processed.

Backed by the European Parliament, the Council of the European Union, and the European Commission, the GDPR gives data subjects (i.e., customers, employees, and contractors) the right to demand to know what data a business has on them, to request that data be passed to a competitor, or demand that the data is deleted. For any business that gathers or

processes personal data, this law is huge; failure to comply with it could impose significant fines, civil penalties, and additional compliance costs totaling as much as four percent of annual turnover. Plus, European regulatory authorities retain the power to intervene operationally against companies not in compliance with the GDRP, including halting all information processing immediately. For some companies, this would mean essentially shutting down the entire operation.

The GDPR is a big enough regulation to affect a company's entire risk profile, if it is not handled appropriately. And the compliance needs here can be so extensive, and the time left in which to begin work is so short, that for many organizations, complying can be an overwhelming task. To that end, the Internet Security Forum (ISF) has released the GDPR Implementation Guide, a guidance document that provides a detailed roadmap for building an organizational effort for complying with GDPR.

"To get the most out of the GDPR Implementation Guide, an organization should consider its current data protection practices and how to improve those practices in line with GDPR requirements," says Steve Durbin, managing director of the ISF. "Utilizing the GDPR Implementation Guide, organizations can better prepare, implement, evaluate, and enhance their data protection activities."

According to Durbin, the GDPR is a unique compliance burden because there is no endpoint to it; every member of an organization's workforce has the opportunity to either comply with it or not as they gather personally identifiable information.

"If you haven't started on GDPR compliance yet, you need to," Durbin says. "The key thing to do is to map out the gaps. You need to have a roadmap, and you need to be able to demonstrate that you are at least making steps to achieve the end objective, and that will stand you in good stead. If you don't have any of that in place, you are in trouble. And you don't have very long to rectify the situation."

Durbin says that regulators are realistic about GDPR; they understand that not all organizations are going to be fully compliant by next May, but what they are looking for is intent. Has it bought into the fact that it needs to comply with GDPR? And is it taking reasonable steps to ensure compliance?

To that end, companies will need to provide a roadmap and demonstrate progress. Those that do not and that take a "head in the sand" approach to the new law, Durbin says, will be the ones that will garner the first big fines for non-compliance. "Nobody wants to be in that category," he says.

The ISF Implementation Guide breaks the GDPR compliance roadmap down into two main phases: Phase A (Preparation) and Phase B (implementation). Phase A needs top project management resources, Durbin says, because the data involved will not come in a nice, tidy package. It will require an extensive, enterprise-wide audit, and the time it will take will differ depending on any given organization's comfort with how it collects, stores, and manages data.

Phase B tends to cause organizations to ask themselves certain questions, Durbin says, such as "What process do we have in place? How do we manage data process impact assessment? How do we demonstrate lawful processing of data? How do we demonstrate that we can respond to subject access requests?" All of these are relatively new questions for organizations to ask regarding GDPR, and few organizations have ready answers.

The bottom line, Durbin says, is that the GDPR considers an individual's personally identifiable information to be almost sacrosanct. Supervisory authorities will have the power to make a difference in how that data is handled, and they will be looking early on for those organizations that can provide a roadmap to others by dint of their own compliance efforts.

"Nobody believes the GDPR can prevent data breaches, or that everybody will be able to tick the box on GDPR compliance on day one," Durbin says. "But the authorities are saying, 'this is the process, it's here to stay, we have teeth, and we will use them if you don't comply.' "

The GDPR Implementation Guide, as well as other GDPR-related materials, is available now to ISF member companies by way of the ISF Website. ■

GDPR IMPLEMENTATION

Below is a look at GDPR implementation at a glance from the ISF.

The ISF has prepared a handy guide for building a GDPR compliance program that consists of a preparation phase and an implementation phase.

But these will take as much time as an organization has to give them, so companies should begin their GDPR compliance work now.

Phase A – Preparation

- A.1 Discover personal data
- A.1.1 Define personal data
- A.1.2 Maintain records of personal data processing
- A.2 Determine compliance status
- A.2.1 Conduct data discovery exercise
- A.2.2 Perform GDPR requirements gap analysis
- A.3 Define GDPR implementation scope
- A.3.1 Identify key GDPR compliance activities
- A.3.2 Create GDPR compliance plan

Phase B—Implementation

- B.1 Satisfy role requirements
- B.1.1 Designate an appropriate data protection officer
- B.1.2 Assign roles and train staff
- B.2 Protect personal data
- B.2.1 Apply data protection by design and by default
- B.2.2 Apply appropriate security to data processing
- B.3 Manage data protection impact assessments (DPIAs)
- B.3.1 Identify when DPIAs need to be conducted
- B.3.2 Conduct DPIAs on specified personal data processing
- B.3.3 Determine how DPIA findings will be addressed
- B.4 Demonstrate lawful processing
- B.4.1 Determine legal basis for processing personal data
- B.4.2 Obtain and revalidate consent of data subjects
- B.4.3 Handle processing of special categories of personal data
- B.5 Uphold data subject rights
- B.5.1 Resolve requests for data subjects upholding their rights
- B.5.2 Demonstrate transparency of personal data processing
- B.5.3 Respond to subject access requests
- B.5.4 Support rectification of personal data
- B.5.5 Apply restrictions on personal data processing
- B.5.6 Handle objections to processing of personal data
- B.5.7 Enable personal data portability
- B.5.8 Erase personal data as requested by data subjects
- B.5.9 Investigate objections to automated decision making
- B.6 Meet data transfer requirements
- B.6.1 Establish process for managing personal data transfers
- B.6.2 Protect cross-border transfers of personal data
- B.7 Respond to personal data breaches
- B.7.1 Identify suspected data breaches
- B.7.2 Investigate personal data breaches
- B.7.3 Report personal data breaches to supervisory authorities and data subjects

Source: Internet Security Forum

FTI CONSULTING™ | TECHNOLOGY

Trusted Global Leaders in Data Privacy, Security and Information Governance

FTI GDPR PREPAREDNESS SERVICES INCLUDE:

- GDPR RISK ASSESSMENT
- GDPR-SPECIFIC TECHNICAL INVENTORY OF PERSONAL DATA SOURCES
- GDPR POLICY REFRESH
- TACTICAL AND STRATEGIC ROADMAPPING
- DATA REMEDIATION AND SYSTEM DECOMMISSIONING
- PROGRAM DESIGN AND PROJECT MANAGEMENT OFFICE SUPPORT

Learn more at: www.ftitechnology.com/gdpr