GENERAL DATA PROTECTION REGULATION (GDPR) REPORT

Implementation challenges and milestones for early adopters of the GDPR

JULY 2017

250
Participants

38.4%
From large organisations

41.6%
Are still planning for GDPR compliance

INTRODUCTION

IT Governance is pleased to release the results of its first General Data Protection Regulation (GDPR) survey. The report provides GDPR practitioners and senior management with useful insight into how organisations are progressing with GDPR compliance, the challenges they face and the measures they are adopting.

It should be noted that the research reflects the issues affecting progressive organisations that have already started working towards achieving GDPR compliance and does not reflect the average organisation. It should also be emphasised that IT Governance's clients have a higher level of awareness: since early 2016, IT Governance has continually worked to raise client awareness of the GDPR through free resources, webinars, blogs, training courses, books and other avenues, which has helped clients to initiate and manage GDPR compliance.

In the past year, large-scale research on GDPR awareness and compliance has shown that only 47% of organisations are fully aware of the GDPR (Source: SCMagazine UK).

ABOUT IT GOVERNANCE

IT Governance is a leading global provider of IT governance, risk management and compliance solutions, with a special focus on data protection, cyber resilience, the PCI DSS, ISO 27001 and cyber security.

We're well positioned to help organisations address the challenges of GDPR compliance with our comprehensive suite of information resources, training courses, toolkits and consultancy services.

Since May 2016, when the GDPR became law, IT Governance has trained over 500 data protection professionals on the GDPR through its Certified GDPR Foundation and Practitioner training courses.

More information is available at www.itgovernance.co.uk.

EXECUTIVE SUMMARY

66%
Say senior management have been briefed on the GDPR

38.4%
Have appointed a DPO to oversee GDPR compliance

52.8%
Rely on practitioners to achieve compliance with the GDPR

63%
Are planning to undertake GDPR training

With the GDPR set to impose fines of up to 4% of annual global revenue or €20 million – whichever is greater – organisations can no longer afford to ignore their responsibilities.

The GDPR, which will apply from May 2018, imposes a much stricter regulatory framework for the processing of personal data across the EU. To meet its requirements, organisations need to know what personal data they currently hold or process, understand the risks to that data, adapt their business processes and infrastructure, implement tools and compliance processes, and change the way they collaborate with suppliers. In some instances, those changes could be significant and work will need to start as a matter of urgency.

Organisations face a range of challenges, the primary one being a lack of competence and expertise to implement the measures necessary to secure data and to protect the rights of data subjects. Organisations increasingly have to rely on external support and training to address this knowledge and skills gap.

This report analyses data from more than 250 professionals worldwide, a large majority of whom are IT Governance clients and partners. The report identifies the level of awareness that organisations, employees and management have of the Regulation, the measures taken to manage compliance, and the key challenges faced in the process. The research data was collected between November 2016 and February 2017.

SURVEY PARTICIPANTS

BY COUNTRY

United Kingdom	65.9%
United States	4.5%
Australia	1.1%
South Africa	0.8%
France	1.5%
Germany	2.7%
Netherlands	2.7%
Other	20.8%

BY SIZE

Fewer than 10 employees	17.8%
10–50 employees	12.9%
51–100 employees	7.6%
101–200 employees	8.3%
201–500 employees	14.8%
501–1,000 employees	9.5%
More than 1,000 employees	29.1%

BY REVENUE

Less than £5m/€5,8m/$6.2m	40.2%
£5m–£50m/€29m–€58m/$31m–$62m	23.9%
£50m–£100m/€58m–€116m/$62m–$124m	8.0%
£100m–£500m/€116m–€582m/$124m–$620	10.5%
More than £500m/€582m/$620m	17.4%

BY PROJECT STAGE

Well advanced	8.5%
Started	35%
Still planning	41.5%
Not yet on our agenda	15%

BY JOB TITLE

Compliance/risk manager	10.6%
IT director	2.3%
IT manager	11%
ISMS manager	9.1%
Data protection officer (DPO)	12.1%
CISO	4.2%
Quality manager	0.8%
Project manager	1.5%
CEO/managing director	6.4%
Operations manager	2.7%
CIO	1.9%
Head of risk	0.8%
Business executive	3.0%
Marketing professional	3.4%
Consultant	13.6%
Other	16.6%

BY INDUSTRY

Technology	28.4%
Financial services	10.2%
Business services	10.2%
Government/local authority	9.5%
Telecommunications	2.3%
Manufacturing	5.3%
Engineering	0.8%
Legal	1.1%
Education	5.7%
Healthcare	5.7%
Charities and non-profits	3%
Energy and utilities	1.1%
Retail	2.7%
Other	14%

REPORT FINDINGS

FINDING 1

Forward-thinking senior management are aware of the importance of the GDPR

FINDING 2

Ensuring the right level of competence and expertise is one of the biggest GDPR challenges for implementers

FINDING 3

50% of companies have not yet allocated a GDPR staff awareness budget

FINDING 4

68% have not yet updated their processes to comply with data subject rights

FINDING 5

Nearly 40% have appointed a DPO to oversee GDPR compliance

FINDING 6

Almost half of those responsible for GDPR compliance lack a formal or relevant qualification

FINDING 7

Compliance practitioners are planning to undertake GDPR training

FINDING 8

Most organisations have implemented, or are implementing, a breach notification procedure and an incident response plan

FINDING 9

More than half of organisations rely on data protection practitioners for GDPR compliance, while 31.9% rely on lawyers

FINDING 10

Most organisations are assigning the role of DPO to an existing employee

FINDING 11

The typical budget for GDPR compliance is less than £5,000/€5.800/$6,200

FINDING 12

Organisations rely on building internal competence to assist GDPR compliance

FINDING 13

Respondents recognise that ISO 27001 improves information security compliance with the GDPR

FINDING 1

Forward-thinking senior management are aware of the importance of the GDPR

GDPR awareness is spreading beyond privacy professionals to the boardroom because of the Regulation's broad scope, its contractual and operational impact, and the significant risk management challenge it presents. Our results show that only 22.3% of organisations have not yet briefed their board or senior management on the importance of the GDPR.

SENIOR MANAGEMENT BRIEFED ON GDPR

FINDING 2

Ensuring the right level of competence and expertise is one of the biggest GDPR challenges for implementers

The GDPR imposes strict data security obligations on organisations. 61.1% of respondents ranked implementing the appropriate technical and organisational measures to secure data as the biggest compliance challenge.

Although the Regulation has been published and guidance issued, there is still uncertainty about what some of the provisions mean or how they should be applied. Just over 52.3% of respondents say they are having difficulty understanding the requirements of the Regulation.

Resource shortage is another common challenge for many organisations: 50.5% of respondents said they're struggling to obtain the right level of competence and expertise to implement their GDPR project. Recent findings show that the GDPR will create demand for at least 75,000 data protection officers (DPOs) worldwide, which could lead to competition for appropriately qualified staff and increasingly rewarding salaries to attract suitably skilled candidates. Given the current shortage of data protection professionals, this issue is only going to become more acute.

Other notable challenges include conducting data flow mapping (49.5%), data protection impact assessments (44%) and data audits (40.7%).

THE MAIN CHALLENGES IN ACHIEVING GDPR COMPLIANCE

61.1% Implementing the technical and organisational measures	**52.3%** Understanding the requirements of the Regulation	**50.5%** Ensuring the right level of competence and expertise	**49.5%** Mapping the flow of PII (personally identifiable information)	**44.0%** Conducting data protection impact assessments
40.7% Conducting a data audit	**38.4%** Assessing data privacy practices	**38.4%** Reviewing, updating and creating policies and procedures	**31.5%** Creating information notices for data subjects	**28.7%** Conducting risk assessments

FINDING 3

50% of companies have not yet allocated a GDPR staff awareness budget

The Regulation requires organisations to implement policies and procedures, and conduct regular staff awareness training to ensure employees are appropriately briefed and trained on their data protection responsibilities. 26.9% have taken the first steps towards GDPR compliance by briefing some or all employees on the GDPR.

Guidance from data protection authorities emphasises the importance of making staff aware of the GDPR, and for organisations to start factoring this into their compliance planning. Employees need to be educated on the privacy rights of individuals and the data security policies and procedures in their organisation.

Many respondents (41.5%) are only at the planning stage of their GDPR project and are not yet ready for staff awareness. A further 53.2% plan to undertake staff training in the future, but, worryingly, more than 50% of organisations have not yet allocated a budget for this activity.

9.3%
Have provided GDPR staff awareness to all employees

4.6%
Are not planning to deliver any GDPR staff awareness training

17.6%
Have provided GDPR staff awareness to some employees

27.2%
Are not aware of any plans to deliver staff awareness training

53.2%
Are planing to undertake GDPR staff awareness in the future

FINDING 3 (continued)

The survey suggests that the majority of respondents (71.3%) do not have a GDPR staff awareness budget or are unaware if such a budget is in place. Only 28.7% of the organisations have allocated a budget to help staff understand the compliance requirements of the GDPR.

Although briefing employees on the impact of the GDPR is a good start, it is not a substitute for building a training and awareness programme that ensures all employees understand the company's practices and procedures for processing personal data. Industry reports bring solid evidence that the lack of a staff awareness programme or poor staff awareness practices are major contributing factors to data breaches. Therefore, staff awareness should be a major concern, especially as most organisations do not have a budget in place yet.

ORGANISATIONS THAT ALLOCATED GDPR STAFF AWARENEESS BUDGET

FINDING 4

68% have not yet updated their processes to comply with data subject rights

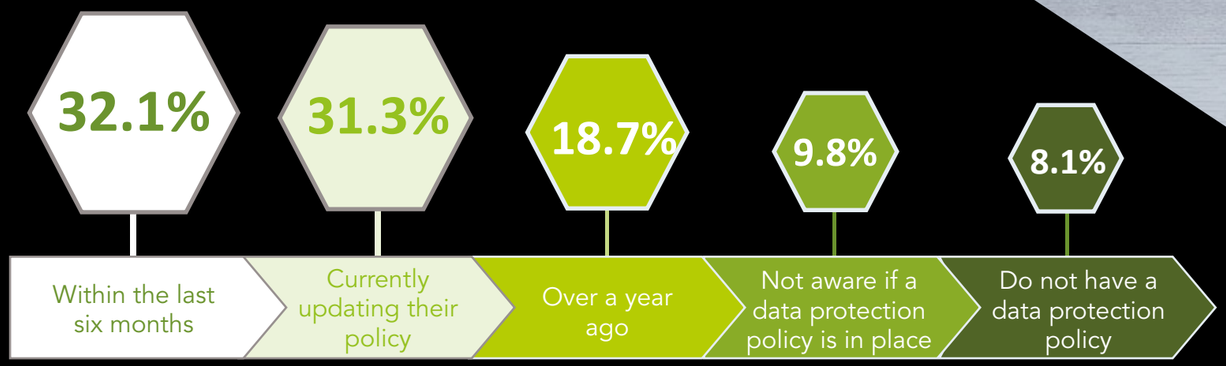
The Regulation extends the data rights of individuals, and requires organisations to develop clear policies and procedures, and to adopt appropriate technical and organisational measures to protect personal data.

More than half of the organisations that responded are either currently updating their data protection policy (31.3%) or have updated their policy in the last six months (32.1%).

68.1% of the respondents said that they have not yet updated their processes to comply with the new rights afforded to data subjects, such as the right to be forgotten and the right to data portability.

This finding should concern most organisations, as the lack of appropriate policies and procedures could lead to fines of up to 4% of annual revenue or €20 million (whichever is greater) and lawsuits from data subjects.

ORGANISATIONS LAST UPDATED THEIR DATA PROTECTION POLICY



FINDING 4 (continued)

While having appropriate policies and procedures plays a major part in GDPR compliance, 61.7% of respondents are focusing on conducting data protection impact assessments, and 58.3% are developing a risk management framework.

ORGANISATIONS HAVE PLANNED OR COMPLETED THE FOLLOWING:

FINDING 5

Nearly 40% have appointed a DPO to oversee GDPR compliance

The GDPR recognises the data protection officer (DPO) as a key player in facilitating compliance, with the appointment of a DPO being mandatory for all public authorities and many private organisations. Article 37 of the GDPR requires controllers and processors that handle large volumes of data to designate a DPO.

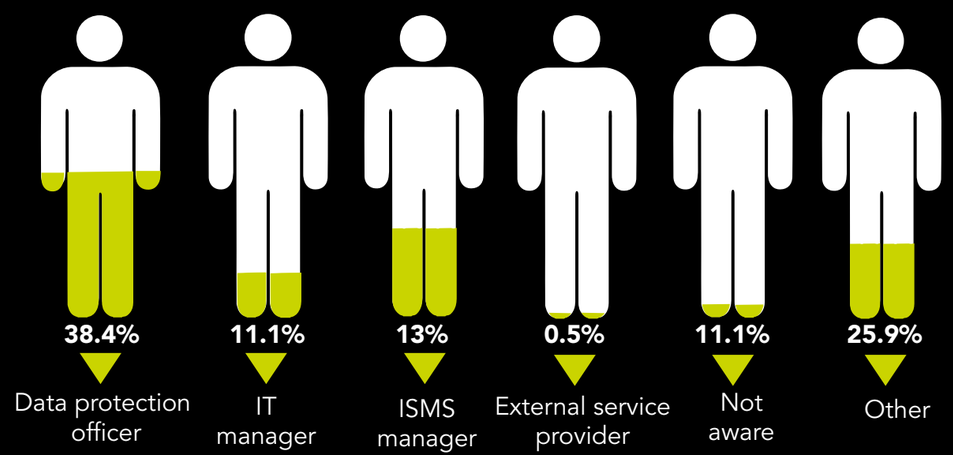
Even in cases where the GDPR does not specifically require the appointment of a DPO, the Article 29 Working Party (WP29) recommends appointing one as a matter of good practice and to demonstrate compliance.

A DPO should assist the controller or processor in monitoring compliance with the Regulation.

For nearly 40% of responding organisations, a DPO has been appointed to oversee GDPR compliance, particularly in organisations with more than 1,000 employees.

In a quarter of the organisations, either the IT manager (11.1%) or the ISMS manager (13.0%) will take responsibility for GDPR compliance.

JOB ROLES RESPONSIBLE FOR GDPR COMPLIANCE



FINDING 6

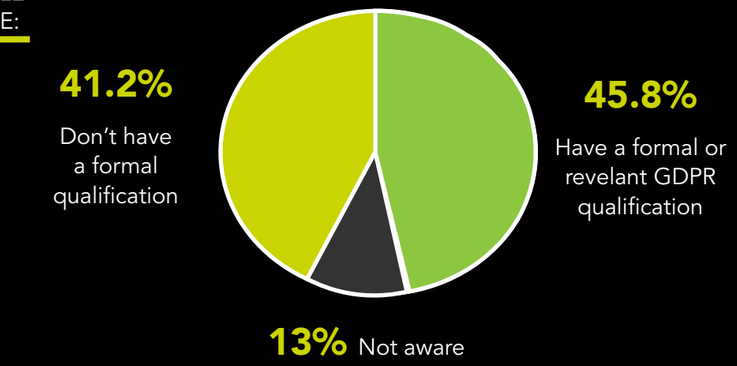
Almost half of those responsible for GDPR compliance lack a formal or relevant qualification

Nearly half of the respondents (41.2%) said that the person responsible for GDPR compliance in their organisation does not have a formal or relevant qualification, and a further 13% report that they aren't aware if the person responsible for GDPR compliance has any formal or relevant qualifications.

45.8% of the people responsible for GDPR compliance have a formal or relevant qualification (such as the Certified EU General Data Protection Regulation (GDPR) Practitioner qualification).

Considering the numerous challenges that organisations are experiencing with GDPR compliance and the demand for DPOs, organisations should prioritise training for the people involved in managing GDPR compliance to ensure a smooth transition.

EMPLOYEES RESPONSIBLE FOR GDPR COMPLIANCE:



FINDING 7

Compliance practitioners are planning to undertake GDPR training

Given the numerous challenges that organisations experience in becoming GDPR compliant, it's unsurprising to see that 63% of respondents are planning to undertake training to develop their GDPR knowledge and skills.

DPOs are particularly interested in gaining a practical understanding of the GDPR (16.9%), followed by compliance/risk managers (11.8%) and IT managers (10.3%).

PRACTITIONERS PLANNING TO UNDERTAKE GDPR TRAINING

FINDING 8

Most organisations have implemented, or are currently implementing, a breach notification procedure and an incident response plan

Requirements for breach notification are one of the major changes the GDPR has brought to data protection law. Data controllers will be required to report any personal data breaches to their supervisory authority and, in some cases, to notify the data subjects affected by the data breach.

With the GDPR mandating that organisations report any data breach to their supervisory authority within 72 hours of becoming aware of it, organisations need to implement the policies and procedures to act accordingly in the unfortunate event of a data breach.

Businesses should develop and update their breach notification procedure in order to effectively communicate a breach, and implement an incident response plan to detect and respond to breaches.

The survey shows the majority of responding organisations are well on the way to being compliant, with 33.1% already having a breach notification procedure in place, and 43.1% having started to take the necessary steps.

A large number of organisations already have an incident response plan in place (48.5%), while a further 35.3% of organisations are currently implementing an incident response plan.

ORGANISATIONS THAT HAVE IMPLEMENTED A BREACH NOTIFICATION PROCEDURE

ORGANISATIONS THAT HAVE IMPLEMENTED AN INCIDENT RESPONSE PLAN

FINDING 9

More than half of organisations rely on data protection practitioners for GDPR compliance

A large proportion of organisations are using data protection professionals to ensure compliance with the GDPR. Data protection professionals are considerably more popular (52.8%) than lawyers (31.9%), but there is considerable overlap: 73.9% of the respondents that are using lawyers are also planning to use practitioners to achieve GDPR compliance.

While the GDPR requires legal and regulatory knowledge, it is crucial that organisations implement the technical and operational controls required to avoid data breaches.

GDPR COMPLIANCE PROJECT SUPPORT AND ADVICE:

31.9%
Are using lawyers to comply with the GDPR

52.8%
Are relying on data protection practitioners to comply with the GDPR

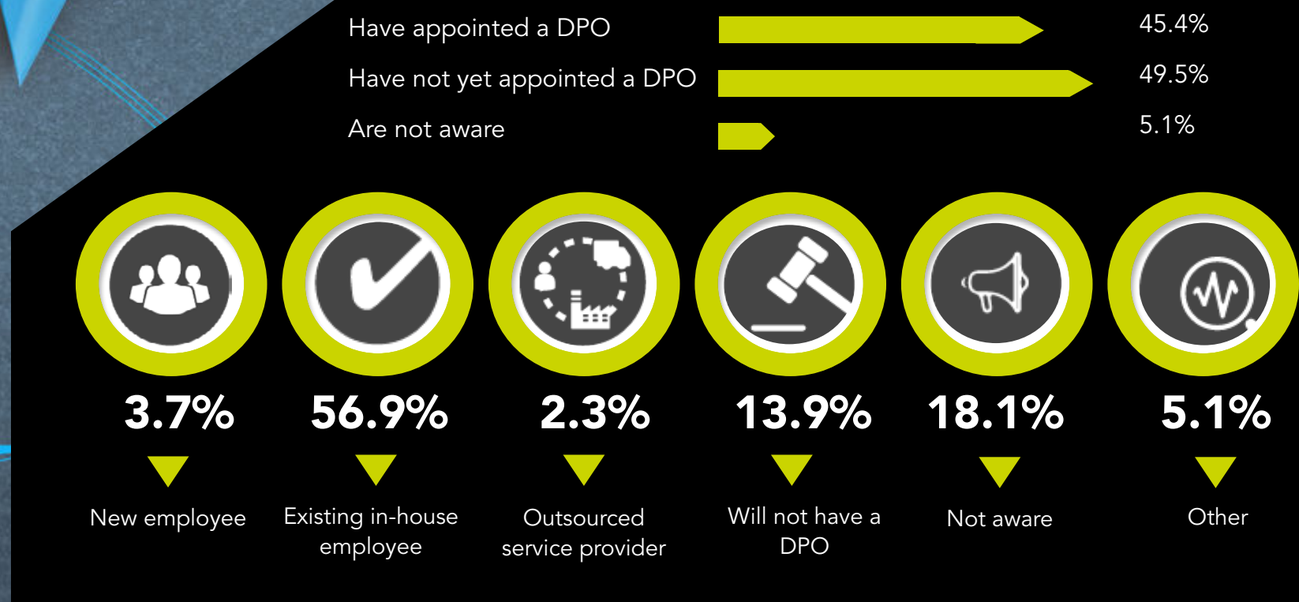
73.9%
Of those using lawyers are also planning to use practitioners

FINDING 10

Most organisations are assigning the role of DPO to an existing employee

Half of the respondents to the survey reported that they have not appointed a DPO, while 45.4% have already appointed one. 56.9% of organisations have designated, or will designate, an in-house employee to the role.

Very few organisations currently plan to outsource the DPO's responsibilities.



FINDING 11

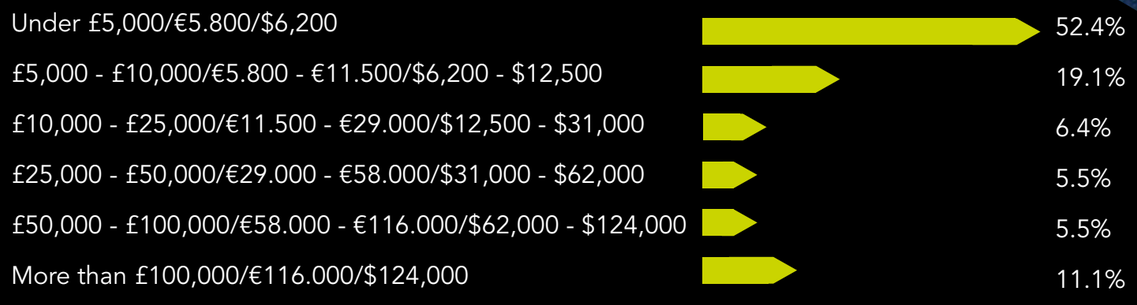
The typical budget for GDPR compliance is less than £5,000/€5.800/$6,200

56.1% of responding organisations said they had a budget of less than £5,000/€5.800/$6,200 to meet the GDPR's requirements. This means that compliance practitioners may find themselves in a difficult position, given that the scope of GDPR work could be significant, particularly if they need to rely on external support or solutions for their compliance programme.

Nearly all of the organisations with budgets of more than £100,000/€116.000/$124,000 are organisations with more than 1,000 employees (90.4%).

Similarly, organisations worldwide spend, on average, between £5,000/$6,500 and £20,000/$26,000 to implement and certify an ISO 27001-compliant information security management system (ISMS) (Source: ISO 27001 Global Report 2016).

ALLOCATED GDPR BUDGET



FINDING 12

Organisations rely on building internal competence to assist GDPR compliance

The survey shows that many organisations rely on training courses to assist GDPR compliance (46.4%), as well as staff awareness training tools and resources (42.8%), and purchasing documentation toolkits (26.3%). A significant number of organisations rely on consultants (28.4%) and GDPR gap analysis products (32.5%).

This point underlines the increased need for training so that data protection professionals can fulfil key duties. While consultancy services provide a structured approach that benefits from immediate expertise and guidance, most professionals find that training courses, such as the Certified EU General Data Protection Regulation (GDPR) Practitioner training course, provide a practical and comprehensive understanding of the Regulation.

FINDING 13

Respondents recognise that ISO 27001 improves information security compliance with the GDPR

The GDPR encourages the use of approved certifications and schemes to help organisations demonstrate they've taken "appropriate technical and organisational measures" to secure personal data.

Most survey respondents (56.7%) reported that they use the internationally recognised best-practice standard ISO/IEC 27001:2013. Through its risk-based approach to information security, ISO 27001 provides an effective means of demonstrating compliance with the information security requirements of the Regulation. The fact that it is also the default management system for protecting organisations against cyber crime doubles its benefit. While cyber crime is not directly addressed in the Regulation, it is an increasingly common cause of data breaches. The large proportion of participant organisations certified to ISO 27001 shows that the survey results do not necessarily represent the typical organisation.

32.5% of organisations are certified to the UK government's Cyber Essentials scheme, which provides a basic level of cyber security and helps prevent around 80% of cyber attacks.

The Payment Card Industry Data Security Standard (PCI DSS) is mandatory for all organisations worldwide that accept card payments. 26.8% of respondents reported being compliant with the PCI DSS.

DATA PROTECTION AND CYBER SECURITY CONTROLS IMPLEMENTED:

THE GDPR ONE-STOP SHOP

How can IT Governance help you get ready for GDPR compliance?

As a leading global authority on data protection, IT Governance can help your organisation address the challenges of GDPR compliance with a comprehensive suite of information resources, training courses, toolkits and consultancy services.

BOOKS

- EU GDPR: A Pocket Guide
- EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide

TOOLKITS

- EU GDPR Documentation Toolkit
- EU GDPR Compliance Gap Assessment Tool

TRAINING COURSES AND QUALIFICATIONS

- Certified EU GDPR Foundation training course
- Certified EU GDPR Practitioner training course
- Data Protection Impact Assessment (DPIA) Workshop
- GDPR Staff Awareness E-learning Course

CONSULTANCY SERVICES

- Data flow audit
- GDPR gap analysis
- Data protection impact assessment

IT Governance Ltd
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs, CB7 4EA
United Kingdom

T: + 44 (0)8450 701750
E: servicecentre@itgovernance.co.uk
W: www.itgovernance.co.uk

@ITGovernance /it-governance /ITGovernanceLtd