DO YOU NEED TO BE COMPLIANT WITH THE GENERAL DATA PROTECTION REGULATION (GDPR)?

Helping your organisation adhere to the Data Protection Act 2018 and GDPR

The General Data Protection Regulation (GDPR)—introduced in the UK with the Data Protection Act 2018—greatly improved the way in which businesses use, store, and manage personal data, increasing the protections and rights of European data subjects.

Why do I still need a GDPR consultant?

Compliance with GDPR isn't a one-time task; when it comes to data protection, ongoing compliance is just as significant as the initial work you put in. Not placing an importance on ensuring that data protection processes and policies are followed means that—over time—they become diluted and forgotten, ultimately placing the organisation in a non-compliant position. In this situation, should there be a breach and your organisation is not compliant, fines are likely to be significantly higher, which can impact both bottom line and reputation.

Why does my organisation need to comply with the GDPR?

Organisations that fail to comply may be fined by Supervisory Authorities—potentially up to €20 million or 4% of global annual turnover.

If you collect and store any form personal information, you must know how to comply with the legislation and remain compliant; it is a legal requirement that personal data is stored and processed securely and lawfully.

It's not just about keeping your business safe. Being compliant with the GDPR also helps you maintain a strong reputation within your industry by demonstrating legal compliance and an ongoing commitment to protecting the privacy of your clients, customers, employees and stakeholders.

Does my organisation store and collect personal data?

Personal data can fall into two categories, 'Personal Data' and 'Special Category Data' (sometimes known as 'sensitive personal data').

Personal Data is any information that can be used to directly identify an individual, or information that can be used to identify an individual in combination with other information. Examples include name and surname, personal email address and an individual's National Insurance number.

Special Category Data are considered to be more sensitive and likely to cause harm to the individual, and therefore can only processed in more limited and tightly controlled circumstances. Examples include information about an individual's sexuality, their political opinions, race and ethnicity, medical history and biometrics.

If the data you store sounds like any of these, you must adhere to the Data Protection Act 2018 and the GDPR.

How PGI can help

Every organisation will be at a different stage of compliance with the Data Protection Act 2018/GDPR, so our information assurance team can offer assistance in four key areas:

Scope of processing

Understanding what personal data your organisation holds and how it is used is the critical first step to ensuring that all processing is carried out lawfully and in accordance with the principles of the Data Protection Act 2018 and the GDPR.

Gap analysis

Once you know what data you hold and how it is processed, a gap analysis will inform where there are shortfalls in compliance and where efforts must be concentrated to meet the requirements of the legislation.

Implementation

This stage focuses on implementing control measures to ensure compliance with relevant data protection legislation. With PGI's support, your organisation can be assured that these control measures are pragmatic and provide the appropriate levels of assurance.

Continuous support

Our consultants provide ongoing support, such as expertise on how to improve security controls and reviewing any business changes and their impact to your compliance obligations.

WHY CHOOSE PGI

PGI is a UK-based risk mitigation consultancy with key services across risk analysis, cyber security, intelligence and training. We believe that cyber and information security don't need to be overly complicated, incomprehensible or vastly expensive.

A tailored approach
Not every business is the same, so we don't attempt to approach every project in the same way. We get to know your organisation, so we can provide appropriate advice.

Practical and affordable
Solutions are affordable because they are proportionate only to a client's needs, not a blanket approach.

Cross-sector experience
PGI are made up of personnel with backgrounds in security, law enforcement, intelligence, the military and academia and have implemented information security measures across a wide range of industries.

Global experience
PGI have worked with companies in more than 50 countries.

Vendor-neutral advice
PGI are vendor-neutral, so we will always act in your best interests when assessing your risks and offering a solution.

OTHER PGI SERVICES

Since 2013, PGI has been helping organisations of all sizes achieve compliance with a range of frameworks, including GDPR/The Data Protection Act, ISO 27001 and PCI DSS.

We also offer a wide range of cyber security services, including vulnerability assessments and penetration test to further support effective data protection.

Understanding the threats that your organisation and industry are up against will help you defend your data, infrastructure and reputation. Talk to our team to discuss your cyber and information security needs and how we can help.

+44 (0) 845 600 4403
sales@pgitl.com
www.pgitl.com

YOUR MAP TO COMPLIANCE WITH THE DATA PROTECTION ACT 2018 AND THE GDPR

1. SCOPE OF PROCESSING	2. GAP ANALYSIS	3. IMPLEMENTATION	4. CONTINUOUS SUPPORT
WHAT IS THIS SERVICE?			
To ensure that your organisation is operating in compliance with the Data Protection Act 2018 and the GDPR, you must first understand what personal data your business processes. PGI will help you to establish, document and justify the personal data processing activities that are performed by your organisation.	Gap analysis involves comparing what you are currently doing against what you must do to meet the requirements of the Data Protection Act and the GDPR.	This stage focuses on putting control measures in place to ensure compliance with relevant data protection legislation. PGI consultants can provide expertise in the appropriate implementation of controls.	Continuous improvement is all about maintaining your compliance with the Data Protection Act 2018 or the GDPR.
WHY IS IT IMPORTANT?			
Understanding what personal data your organisation holds and how it is used is the critical first step to ensuring that all processing is carried out lawfully and in accordance with the principles of the Data Protection Act 2018 and the GDPR.	It informs where there are shortfalls in compliance and where efforts must be concentrated to meet the requirements of the legislation.	Failure to implement the necessary controls could mean that the organisation is not compliant with data protection legislation. This in turn could result in data breaches and subsequent fines or penalties, as well as enormous reputational damage. In the event of a breach, organisations that do not comply with the relevant regulations are likely to be fined at a higher rate.	Organisations must take steps to maintain their compliance with data protection legislation and ensure the security of all personal data held. Failure to do so can increase the likelihood of data breaches and result in significant penalties and fines, as well as considerable reputational damage.
WHAT DOES YOUR ORGANISATION GET FROM THIS SERVICE?			
PGI can help you to define your processing activities by investigating your businesses operations and use of personal data. The PGI team will work with relevant process owners and stakeholders within your business to map the flow of personal data through your organisation and to identify the appropriate **lawful basis for processing**. You will be provided with documented records of all processing activities, their purpose and the personal data used. This activity can also be useful in improving efficiency by identifying unnecessary processing activities or where these activities can be consolidated, ensuring all processing remains lawful.	The gap analysis provides a view of where effort needs to be concentrated to ensure compliance, and which actions should be performed first. **This can facilitate effective project planning, resource forecasting and budgeting.** Once the gap analysis is complete, the consultant will provide a detailed Gap Analysis Report, comprising findings and prioritised recommendations. The consultant will also document in detail the evidence reviewed, which will help to streamline compliance reporting at a later stage.	With PGI's support, your organisation can be assured that control measures implemented are pragmatic, and provide the appropriate levels of assurance. As an example, PGI consultants can apply their expertise to develop data protection related policies, procedures and privacy notices, build registers of processing activities, and perform Data Protection Impact Assessments (DPIAs). PGI's wider team can also perform penetration tests and vulnerability assessments and advise on other best practice security standards, including ISO 27001, ISO 27701 and Cyber Essentials, all of which support effective data protection. In addition, PGI can provide data protection training and incident response capabilities if required.	Our consultants provide ongoing support, such as expertise on how to improve security controls and reviewing any business changes and their impact to your compliance obligations. PGI can also provide: • Regular security audits • Ongoing security documentation review and update • Penetration Testing • Vulnerability Assessment • Security awareness and education • Data protection advice on an ad-hoc basis as and when you need it. For example, this time can be used to review compliance, enquire about the implications of new processing activities, or review DPIAs.
HOW LONG WILL IT TAKE?			
This depends on the size of the organisation and the complexity of its processing activities. Approx. 1 – 8 days	This depends on the size of the organisation and the complexity of its processing activities. Approx. 3 – 6 days	This is heavily dependent on the organisation's current levels of compliance. Establishing a timescale can be very difficult, which is why PGI recommends performing a Gap Analysis. The findings of the Gap Analysis can be used in project planning and resource forecasting. Approx. 3 – 10 months	For all ongoing support, PGI will provide clear timescales, considering the size of the organisation and complexity of its operations.
WHY DO I NEED PGI'S HELP?			
Our consultants are equipped with a practical understanding of data protection legislation and its application. This means that PGI can provide reassurance that your processing activities are lawful, justified and appropriately documented.	PGI consultants' expertise in data protection legislation allow them to accurately assess your organisation's current levels of compliance and provide pragmatic recommendations. **With the help of PGI's consultants, a gap analysis can be performed more efficiently and effectively than by internal staff, who are likely to hold other responsibilities, and may not be as familiar with the requirements of the Data Protection Act and the GDPR.**	It may be the case that your organisation is best placed to perform much of the implementation. However, where necessary, **PGI consultants can provide support, and advise where specialist expertise is necessary or where your organisation lacks the appropriate resource.** Engaging with PGI allows an independent and unbiased view of the suitability of the controls being implemented.	PGI's expertise and experience can help you devise an effective continuous improvement programme that is appropriate for your organisation. PGI consultants provide you with specialist knowledge and resource capacity, enabling your workforce to concentrate on core operations.