*i*TGRC Asia

EU General Data Protection Regulation (GDPR)

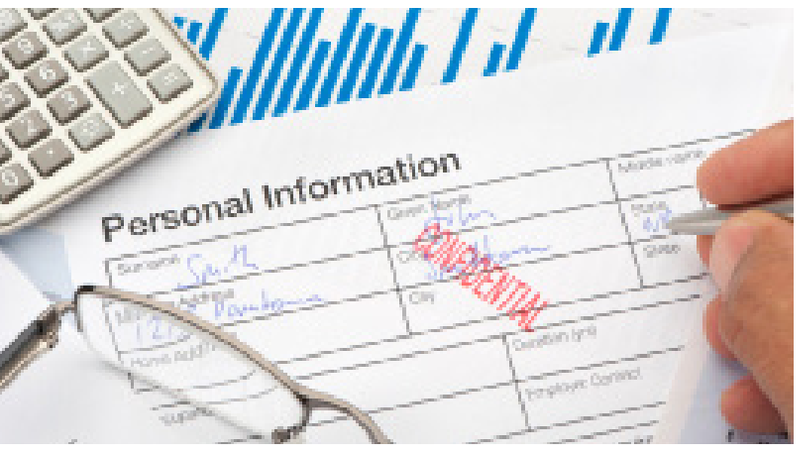
All-encompassing business solutions

Delivered in partnership with:

IT governance™

www.itgrc.asia

iTGRC Asia has partnered with IT Governance to help organisations interpret data privacy legislation and provide guidance on EU General Data Protection Regulation compliance.



Many organisations still believe that having a firewall or antivirus software is sufficient protection against a data breach, but research* has shown that more than 60% of the most disruptive security breaches have been caused by intentional misuse of systems by staff rather than inadvertent human error.

Cyber Security Breaches Survey 2016 – HMG.

The General Data Protection Regulation (GDPR)

Approved by the European Parliament in April 2016, the GDPR supersedes national laws, such as the UK's DPA, to unify data protection laws and facilitate the flow of personal data across the 28 EU member states.

The GDPR will come into effect on 25 May 2018, and organisations around the world that process the personally identifiable information of EU residents will be required to abide by a number of provisions or face fines of up to 4% of annual global turnover or €20 million – whichever is higher. Given its impact, organisations that process EU residents' data should pay careful attention to the following elements of the GDPR:

- Data must be processed lawfully, fairly and in a transparent manner.
- Personal data should be protected through pseudonymisation and encryption.
- Personal data can only be collected for defined purposes, and storage limitations will apply.
- Organisations have to meet new requirements to secure data subjects' consent.
- Data subjects have been granted extended rights.
- Organisations need to be able to demonstrate compliance.
- Data subjects can bring legal action against organisations in case of data breach.

The GPDR and ISO 27001

The GDPR encourages the adoption of certification schemes as a means of demonstrating compliance. Certification to ISO 27001 can help organisations achieve their compliance objectives, protect their data and create greater business efficiency.

ISO 27001 is the internationally recognised best-practice standard that lays out the requirements of an ISMS (information security management system) and provides a holistic approach to information security that encompasses people, processes and technology. Implementing an ISO 27001-compliant ISMS forms the backbone of an intelligent cyber security risk management strategy, and helps the organisation to avoid potential data breaches resulting from inadequate information security practices.

The Network and Information Security (NIS) Directive

First proposed in 2013 as a means of implementing the EU's Cybersecurity Strategy, the NIS Directive aims to achieve a high common level of network and information systems security across the EU by:

- Improving national cyber security capabilities.
- Increasing cooperation between EU member states.
- Requiring "operators of essential services and digital service providers" to take appropriate security measures and notify the relevant national authorities of serious incidents.

The NIS Directive was adopted by the European Parliament on 6 July 2016, and entered into force in August 2016. EU member states have until May 2018 to translate it into national laws, and a further six months to identify the "operators of essential services and digital service providers" it applies to.

Comply with the GDPR and NIS Directive by May 2018 to avoid the fines associated with a data breach

We can help your team develop and implement an effective and robust personal information management system (PIMS) to help you comply with the GDPR.

Comprehensive data protection solutions

We provide unique products and services that are essential for IT and information security teams to achieve strategic goals, protect and secure personal and sensitive data, and meet the GDPR's requirements.

	Awareness	Risk & impact assessments	PIMS implementation	Management documentation	Alignment with standards	Internal audit & compliance audit
Free resources	✔	✔	✔	✔	✔	-
Standards	✔	✔	✔	✔	✔	✔
Books & tools	✔	✔	✔	✔	✔	-
Training & e-learning	✔	✔	✔	✔	✔	✔
Technical testing	-	✔	✔	-	-	✔

Available products and services

We can offer an extensive range of products and services to help you meet your compliance requirements and give you peace of mind that your data is protected.

Consultancy services	Training and awareness	Standards, books and toolkits	Software and tools
Data Protection Health Check and Gap Analysis	Certified EU General Data Protection (GDPR) Foundation training course	EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide	vsRisk™ information security risk assessment tool
GDPR data flow audit & mapping	Certified EU General Data Protection (GDPR) Practitioner training course	EU General Data Protection Regulation Documentation Toolkit	Endpoint encryption tools (Cloud-based endpoint encryption)
Risk assessments and privacy impact assessments	Data Protection Staff Awareness E-Learning Course	EU GDPR – A Pocket Guide	Infrastructure, Network and Web Application penetration testing services
Development of policies and procedures	Data Protection Impact Assessment (DPIA) Workshop	EU GDPR Compliance Gap Assessment Tool	
PIMS implementation audit	In-house information security courses and workshops	ISO 27001:2013 – the internationally recognised best-practice standard for information security	

To purchase any of these packages, please get in contact >>

We can help organisations avoid the fines associated with breaches and reduce their total GDPR compliance expenditure.

Why has iTGRC Asia partnered with IT Governance to deliver GDPR solutions?

- This partnership brings together our extensive expertise and understanding of data protection best practice to ensure that all of our clients are able to achieve compliance with the GDPR.
- IT Governance is a global authority on ISO 27001, the international information security standard, which presents a recognised route to achieving compliance with the GDPR.
- We get access to cost-effective and customised advisory services that provide you with a tailored route to achieving compliance with data protection laws, scalable to your budget and needs.
- Together we can deliver insight and advice that is not available through off-the-shelf technical solutions.
- We can now support professional development: IT Governance's EU GDPR Foundation and Practitioner training courses are ISO 17024-accredited and qualify for 7 CPD/CPE credits.
- We get access to expertise in other internationally adopted standards, such as the PCI DSS, ISO 27001 and ISO 9001, meaning that we can offer our clients an integrated approach to GDPR compliance.
- IT Governance is an IBITGQ Accredited Training Organisation (ATO) and an official publisher of the IBITGQ study guides and courseware.

Why do thousands of organisations worldwide trust ISO 27001 for cyber security?

- ISO 27001 and its supporting body of good practice is specifically focused on helping organisations tackle cyber risk.
- An ISO 27001 ISMS is audited by an independent third party, giving your partners and clients confidence and peace of mind that their information is well protected.
- Certification to ISO 27001 eliminates repetitive third-party information security audits.
- Many governments and private-sector companies now require their suppliers to provide evidence that they have implemented ISO 27001 at tender and/or contract award stage.

IT Governance's credentials and corporate certificates:

Data Protection Brochure - v3

iTGRC Asia
Regus JTC Summit
8 Jurong Town Hall Road
Level #24-05, unit 2408 Singapore 609434

t: + 65 6818 0839
e: info@itgrc.asia
w: www.itgrc.asia

/company/itgrc-asia-pte-ltd/