

GDPR Services



Your challenge

The European General Data Protection Regulation (GDPR) replaces the existing Data Protection Directive and comes into force with immediate effect in May 2018. This Regulation applies to data controllers or data processors that keep or process any information about living people referred to as data subjects. If you are presently required to comply with the Data Protection Acts (DPA) then GDPR will also apply. The GDPR enhances the rights and principles already defined in the Directive and the DPA however it also introduces some more significant changes such as:

- A requirement to actively demonstrate compliance and document processing activities;
- Greater powers for supervisory authorities and increased reliefs available to data subjects. The Office of the Data Protection Commissioner (ODPC) will have the ability to issue fines for non-compliance for up to €10M or 2% of global turnover (whichever is the greater) for serious breaches and up to €20M or 4% of global turnover (whichever is the greater) for extremely serious breaches;
- Mandatory reporting of data privacy breaches to the appropriate supervisory authority;

- Introduction of ‘privacy by design’ as a concept when developing, designing, selecting and using applications, services and products that are based on the processing of personal data;

- Requirement to complete Privacy Impact Assessments (PIAs) for change activity where there is a “high risk to the rights and freedoms” of the data subject or where processing is likely to be carried out on a large scale.

The ODPC in Ireland has urged organisations to begin preparing for GDPR without delay and to carry out a review of all current and envisaged processing activity. This is complemented by guidance from other supervisory bodies such as the Information Commissioners Office (ICO) in the UK who have advised organisations to consider the following: information you hold; awareness and communication; rights of individuals; data subjects access requests; legal basis for processing; consent; processing of children’s data; data breach reporting; privacy by design and PIA’s; data transfers and appointment of Data Protection Officers (DPO’s).

Our Services

While GDPR suggests security technologies and approaches such as encryption and pseudonymization, it does not offer an exact check

list for technology solutions and technical processes that should be in place to protect personal data under your control.

Article 32 of the regulation states that there should be “appropriate technical and organisational measures to ensure a level of security appropriate to the risk”.

Integrity360 offers a number of services to ensure your technical security and organisational processes are appropriate for the protection of the personal data under your control. This will contribute greatly towards your GDPR programme.

Our services include:

- Personal Data Discovery
- Data Governance, Classification & Handling
- Documentation & Policy Review
- Third Party Risk Assessment
- ISO 27001:2013 Aligned ISMS Implementation
- Data Breach Process Development & Testing
- CIS Top 20 Framework Alignment
- NIST Framework Alignment & Assessment
- Cyber Risk Assessment
- Security Architecture Review
- Penetration Testing
- Managed Security Services
- Automated IT Testing
- Threat & Vulnerability Management
- Security Incident Programme Implementation
- Security Awareness Programme Development

How your business benefits

Engaging a security partner to assist with your GDPR preparations ensures that you get an unbiased, independent review of your current security posture from a team of experts in the information security field who can advise on the best approaches for your business depending on your size and level of risk.

Our security teams have a proven track record of delivering compliance programmes to our enterprise clients across all verticals and ensure that they make the best use of the people, processes and technologies already in place, in line with any regulation requirements.

Integrity360 at a glance

- Established in 2005, the company continues to be one of the fastest growing cybersecurity specialists in the UK and Ireland.
- Given its focus on cybersecurity the company prides itself in its understanding of the evolving threat landscape and on its wide-ranging service offering to aid its clients in combatting these threats.
- The company was founded with an emphasis on technical expertise and that philosophy remains today with over 100 people working in technical areas of the business.
- Provide consistently reliable business, information and cyber security risk services that add value to the bottom line.
- With a 24x7 Security Operations Centre (SOC) the company boasts a global security capability with a local presence and personalised service offering.
- The skills and experience in the company are some of the greatest in the industry and clients remain with Integrity360 because they can rely on and trust them to understand their needs and advise them accordingly.
- Clients can be found in all business verticals and include many large and well-known brands.
- The company’s process driven approach and emphasis on customer service gives clients confidence in their security offering and ability to execute on projects.
- Partnering with many of the industry leading security technologies, the company can