Tiedata
Computing Solutions for Business...




GDPR AND INFORMATION SECURITY ASSESSMENT

HISTORY OF DATA PROTECTION

- 1950 Council of Rome, Privacy is a fundamental right
- 1984 UK Data Protection Act
- 1995 EU Directive 95/46/EC
- 1998 UK Data Protection Act (based on EU Directive)
- 2012 EU Commission review of data protection and privacy
- 2016 EU General Data Protection Regulation (GDPR) approved by EU Parliament
- 2018 EU GDPR enforcement date for all EU organisations

Since the Council of Rome established in 1950 that Privacy is a fundamental human right, the world has changed drastically decade upon decade in terms of the data we hold, how we hold it and the way that it is processed.

Privacy laws encompassing Electronic Communication and Data Storage legislation, both existing and planned, demand the attention of every organisation.

The new General Data Protection Regulation (GDPR) aims to increase both the accountability of organisations processing personal data and the information and control that individuals have over that processing.

WHAT IS GDPR?

GDPR replaces the Data Protection Directive 95/46/EC and becomes law on the 25th May 2018. By this date every organisation, within the UK, must become compliant or have detailed plans in place to do so soon after.

GDPR is designed to:

- Harmonise data privacy laws across Europe
- Protect and empower all EU citizens around their data's privacy
- Reshape the way organisations approach data privacy

BENEFITS OF GDPR COMPLIANCE

Adherence to privacy policies is vital for legal compliance, but the real driver for adopting GDPR compliance principles should be the benefits achieved by your organisation.

The systematic transformation of processes that it requires will ensure a more professional and profitable engagement with prospects and customers by providing:

- Greater customer confidence
- Enhanced Business Reputation
- Enhanced cybersecurity
- Improved data management and security
- Reduced data maintenance costs
- Increased alignment with evolving technology
- Better decision making

If you want to know more about what we can do to help you prepare for the new regulation, please contact us on 01773 513 513 or email us at info@tiedata.com

PENALTIES FOR NON-GDPR-COMPLIANCE

The Information Commissioners Office (ICO) is the UK Supervisory Authority for GDPR and Data Privacy. They have been granted similar powers and authority as HMRC. Under GDPR the ICO can impose fines on any organisation that fails to comply with the new legislation or suffers a data breach. These fines can be as high as €20 million or up to 4% of the combined global turnover of the organisation, its parent company and all subsidiaries.

YOUR GDPR OBLIGATIONS

- Understand the rights of an individual with regards to the data or information that you hold about them
- Transparency about personal data collected, stored and used
- Lawful basis for processing personal data
- Get informed consent to store and use personal data
- Protect the data
- Restrict access to data
- Ensure accuracy of information held
- Assess information retention and remove it when it is no longer relevant
- Transfer information from/to third parties when requested by data subject
- Suppliers – check personal data transferred/received complies
- Give access (free) to complete records for a data subject on request
- Have a point of contact (e.g. Data Protection Officer)
- Implement a plan to monitor for and notify the regulator and data subject of a breach
- Document policy, process and procedures with respect to processing activities to demonstrate compliance

INFORMATION SECURITY

Every organisation processes data during its daily activities and has a responsibility to maintain its Confidentiality, Integrity and Availability.

The use of computers, the Internet and telecommunication or information devices has brought us much convenience in all kinds of our daily business and personal activities. However, at the same time, the convenience of this virtual space has created a great potential for abuse by criminals.

It is vital to recognise the vulnerabilities and threats to the data and information that you hold and process and safeguard against these.

Depending on the nature of your business and the (computer or manual) systems that you use, the threats to sensitive and private information can be varied and from a wide variety of sources such as :-

- Computer Virus
- Malware
- Phishing Attacks
- Identity Theft
- Ransomware
- Distributed Denial of Service Attacks
- Unauthorised changes made by an intruder
- Malicious attacks by internal staff or other authorised personnel

It is also important to recognise that there are other, non-malicious threats to the availability of your information and data to your business such as: -

- Hardware Failure
- Accidental Deletions and Modifications
- Natural disasters
- Loss of key equipment or information systems or facility
- Disruption of external telecommunications services
- Utility outage, such as failure of power supply
- Loss of life, disease, health & safety issues

A thorough understanding of the threats to your business systems and data, the areas of vulnerability and the potential for malicious attacks will enable a coordinated and effective approach to threat prevention, detection and recovery to be implemented.

If you want to know more about what we can do to help you prepare for the new regulation, please contact us on 01773 513 513 or email us at info@tiedata.com

OUR APPROACH TO GDPR & INFORMATION SECURITY

1. Assess the Information that you hold
2. Determine the best approach to view, classify and categorise the data within your organisation to facilitate data governance.
3. GDPR specific actions
    i. Ensure organisation wide awareness of GDPR and its impact on your business
    ii. Ensure that information is
        a. Held securely
        b. Recorded and maintained accurately
        c. Accessible only by those authorised to do so
        d. Subjected to a Retention Policy
    iii. Review and implement Privacy Notices
    iv. Implement a Request for Information (RFI) process
    v. Implement procedures to encompass all the rights of an individual concerning data you hold about them
    vi. Assess and ensure a lawful basis for personal processing data
    vii. Review how consent is sought, recorded and managed if applicable
    viii. Implement an Incident Response Plan (IRP) to notify relevant parties within timescales of breaches
    ix. Assign Data Protection Officers and Data Stewards as necessary
4. Assessment of the: -
    i. Risks posed to the Confidentiality, Integrity and Availability of the data and information that your organisation processes
    ii. Threat detection and prevention systems that your organisation has in place
    iii. Policies, Processes and Procedures that your organization has in place (e.g. Email & Internet, BYOD)
5. Implement a Defence in Depth strategy using multiple security measures to protect the integrity of the information assets within your business
6. Help you identify the current folder structure and who has permissions
7. Assess the backup and recovery systems
8. Implement or update the required written Policies, Processes and Procedures as necessary

If you want to know more about what we can do to help you prepare for the new regulation, please contact us on 01773 513 513 or email us at info@tiedata.com

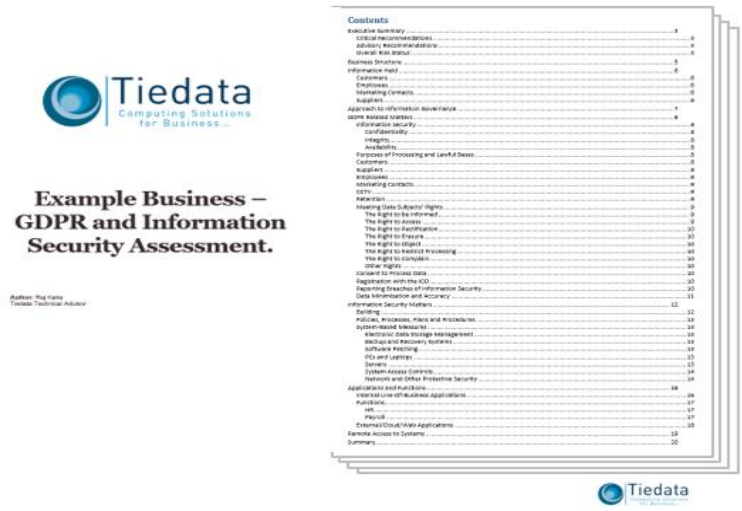
OUR SERVICES

GDPR and INFORMATION SECURITY ASSESSMENT

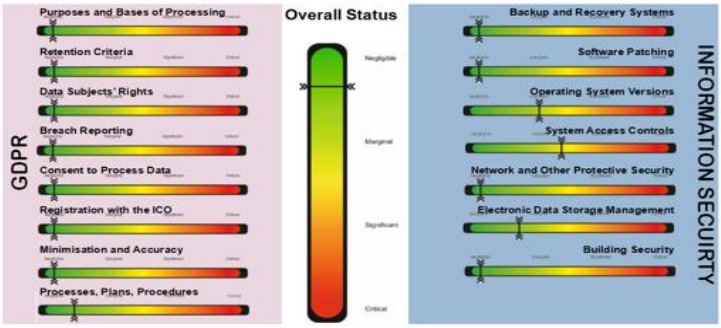
One of our consultants will arrange a site visit to your organisation for discussions with the relevant people and perform an assessment of how far your business has progressed in terms of implementing the requirements of GDPR.

He will further assess the vulnerabilities of your business and threats posed by cybercrime and other malicious and non-malicious threats.

The assessment will result in a report with our findings and recommendations for your business.



Example Business – GDPR and Information Security Summary Sheet



GDPR DATA INSPECTOR

Utilising specialist software we can assess all the electronic data stored across your business network on servers, desktop computers and laptops to 1) identify key personal information that is held and 2) identify who has access to it. Once we have a detailed understanding of your current environment and practices, our consultants will discuss with you the best approach for your organisation to achieve improved security, data management and GDPR compliance.

GDPR DATA MANAGEMENT

Implementation of best practice policies and procedures and an ongoing data management programme to ensure that your business continues to adhere to the requirements of GDPR and is protected against malicious and non-malicious threats.

If you want to know more about what we can do to help you prepare for the new regulation, please contact us on 01773 513 513 or email us at info@tiedata.com