ANNODATA'S GDPR READINESS ASSESSMENT

OUR PROCESS FOR HELPING ORGANISATIONS NAVIGATE A SAFE AND SUCCESSFUL PATH TO GENERAL DATA PROTECTION REGULATION (GDPR) COMPLIANCE

The GDPR is one of the most controversial and hotly anticipated pieces of European Union legislation of recent years. And it represents a fundamental change in the risks connected with data protection and data breach. With such wide ranging scope, the penalties for non-compliance can be massive; up to 4% of annual revenue or €20m, whichever is higher.

Annodata provide both Professional and Consultancy services to address the business, legal, financial and regulatory risks associated with Information Security including Cybercrime and Data Protection. Our services are designed to help clients understand their exposure to risks and the potential impact of those risks within the context of their organisations. We also provide guidance aimed at reducing risk, and work with our clients to ensure that their policies and controls adhere to appropriate regulation and drive compliance, education and awareness throughout their organisations.

For all of our Information Security services the initial engagement is to conduct a Discovery Workshop. This is designed to identify the current business security culture, the policies and controls that are in place and to assess the current risks for the company. The output from the workshop is a detailed report, which includes a gap analysis baselined with the appropriate regulation, standard or best practice.

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

www.annodata.co.uk

GDPR READINESS ASSESSMENT

In our experience, considerable numbers of organisations are either unaware or underestimating the significant impact that GDPR will have and the huge fines and reputational damage that can arise from non-compliance and data breach.

For GDPR our service assumes that a baseline Data Protection policy exists and that the organisation implements controls in line with UK Data Protection Act and existing European Data Protection Directive.

Our GDPR Readiness Assessment therefore focusses on the key differences that the GDPR brings to bear. The assignment is used to discuss how businesses need to adapt and develop new internal processes, leverage the use of IT technologies and educate employees, so that these resources have the capacity to identify, manage, control and monitor information and data within the GDPR regulatory framework. The scope of the GDPR Discovery Workshop covers the following 5 key areas of Data Protection law changes within the GDPR:

1. Data requirements review
    a. Privacy by Design
    b. Increased Territorial Scope
    c. Data Protection Officers
2. Consent
3. Managing Personal and Sensitive Data
4. Data Processing
5. Data Protection Officers

1. Data Requirements Review

GDPR imposes such a high bar for compliance, with significant sanctions to match, that often the most effective approach to minimise exposure is not to process personal data in the first place and to securely wipe legacy personal data or render it fully anonymous. This section is therefore designed to discuss with the organisation why they collect certain data types and re-affirm that personal data is required in its current format for business purposes. Collecting and using Pseudonymous data may be an appropriate strategy for GDPR compliance in certain cases. Organisations that control, collect or process PII data are also now required to carry out a Data Subject Risk/Impact assessment.

1a Privacy by Design

Also included in this section is the Privacy by Design concept, which is now part of a legal requirement within the GDPR. Privacy by Design calls for the inclusion of data protection from the onset of designing of systems and calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

1b Increased Territorial Scope

Arguably, the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the European Union, regardless of the organisation's location. Organisations therefore need to re-affirm their data transfer requirements and reflect GDPR regulation by understanding what types of data are being shared, with which organisations, in which jurisdiction. This section is used to highlight any remedial steps that need to be taken to align with the GDPR.

1c Data Protection Officers (DPOs)

Under GDPR it will no longer be necessary to submit notifications/ registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, and DPO appointment will be mandatory, only for those controllers and processors whose core activities consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. They collect certain data types and re-affirm that personal data is required in its current format for business purposes. Collecting and using Pseudonymous data may be an appropriate strategy for GDPR compliance in certain cases. Organisations that control, collect or process PII data are also now required to carry out a Data Subject Risk/ Impact assessment.

GDPR READINESS ASSESSMENT (CONT...)

2. Consent

In GDPR the conditions for consent and the rights to be informed have been strengthened and companies will no longer be able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

3 Managing Personal and Sensitive Data

GDPR has extended the definition of Personal Data to account for today's digital, online economy. Alongside the traditional categories of personal data, such as, name, telephone number, etc., online identifiers are expressly referred to in the GDPR as personal information with IP addresses, cookies and RFID tags all listed as examples. The context of Sensitive or Special Category Personal Data now also has a broader definition as well with genetic data and biometric data types included.

Organisations need to know where PII and sensitive data resides across their organisation. Departments may have duplicates of the same data and share this information without proper controls in place. Documents containing PII and sensitive data need to be classified, labelled, protected, monitored and accessed in a controlled way. This section of the GDPR Discovery workshop is used to identify how PII data is currently identified and managed and to quantify whether other information types within the organisation now also need to be identified and managed in the same way.

Data Processing

The GDPR has increased the Data Protection obligation for 'Data Processors' and in doing so changed their risk profile when supplying or processing personal data on behalf of their 'Data Controller' customers. Processors now face the threat of revenue-based fines and private claims by individuals for failing to comply with GDPR. Accumulating and monitoring consumer big data relating to purchasing and on line trending for profiling, is an example of where processors now need to understand the associated regulatory GDPR risk.

Data Subjects Rights Management

This section focuses on the expanded rights of data subjects mandated under the GDPR. Rights management ensures that each organisation is aware of the data protection rights of individuals and that they are adhering to those rights when collecting, storing, managing, using, sharing and deleting information. This section includes:

- The right of access
- The right to rectification
- The right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling
- Data breach notification

GDPR requires that all personal data collected is done so lawfully, for specific reasons and must be used for the purpose in which it was collected. It must also be accurate and up-to-date.

This obviously has implications for companies and the technology that they use. Whether it's responding to Subject Access Requests, managing consent or securing data, Annodata has the experience, accreditations and expertise to help organisations navigate a safe and secure path to compliance.