



GDPR
SERVICE PROCESS

2018



The General Data Protection Regulation (GDPR) comes into effect on **25th May 2018** and introduces some new requirements as well as enhancing those existing in the 1995 EU Data Protection Directive and related member state legislation (e.g. the *Bulgarian Law For Protection Of Personal Data 2002*).

SIGNIFICANT CHALLENGES

Data Security

The data controller and the data processor shall implement appropriate technical and organizational measures, to ensure a level of security appropriate to the risk.

Breach Notification

Data controllers must notify the supervisory authority (e.g. Information Commissioner's Office (ICO)) within 72 hours of awareness of a breach. If considered high risk, individuals affected may also have to be notified, depending on the circumstances.

Third Party Management

Data controllers must only use data processors that provide sufficient guarantees of their abilities to implement the technical and organizational security measures necessary to meet the requirements of GDPR

Subject Access Requests

The data subject shall have the right to be supplied with a copy of their personal data, usually within one month of it being requested and free of charge.

Privacy Impact Assessment

An impact assessment may be required before processing any potentially high risk data, which can identify the mitigating security controls required to reduce risk to acceptable levels.

Data Protection by Design

The principles of data protection by design and data protection by default are to be applied when developing, designing, selecting and using applications, services and products that process personal data.

Right to be Forgotten

The data subject should have the right to be forgotten where the retention of such data is not necessary.

Data Portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

OVERVIEW OF GDPR SERVICES

GOOMED can support organizations at every stage of the compliance journey, through:

- Assessments of current compliance readiness
- Gap analysis of planned or implemented controls
- GDPR focused services including:
 - Data Mapping
 - Incident Response
 - Privacy Impact Assessments Training & Awareness
 - Virtual Data Protection Officer.

GOOMED is data protection focused legal advisors and specialist information security professionals with knowledge and experience across many industry sectors and a successful track record of delivering information security and compliance programs to various organizations.

GDPR GAP ANALYSIS

- Provides clarity to customers unsure of their current GDPR readiness or scope
- High level assessment to determine areas requiring further focus
- Completion is dependent on organizational scale and complexity, volume or types of records and a partial or full analysis
- Typically, will include an assessment of:
 - Customer's understanding of their GDPR compliance scope and impact and examination of data flow maps and diagrams
 - Data classification policy and handling process
 - Third party processors' management e.g. security assessments (pre-contract and on a regular basis), contract appraisals
 - Information security policies and procedures

- Inventory of assets and technologies in scope
- Locations where personal data is processed including third parties
- Breach / incident handling
- Risk management framework
- Implemented security controls and processes
- Output will be a gap analysis report of existing processes and controls, and identification of additional activities recommended

GDPR PROGRAMME REVIEW

- For customers that have instigated a GDPR program or have begun mitigation
- Determine adequacy of existing program and/or provide support
- Production of data flow maps showing the collection, storage, usage, sharing/transfer, archiving, and deletion of personal data
- Output will be a report of planned and implemented GDPR mitigations, prioritized roadmap of remediation activities, and identification of additional activities recommended

GDPR AUDIT

- For customers that have completed a GDPR mitigation program or are at the later stages of it
- In-depth assessment to determine the adequacy of the GDPR program
- Timescales dependent on scope
- Will include the same scope as the program review but with audited evidence of implemented controls
- Output will be an audit report describing evidenced controls and Goomed's opinion of the client's likely compliance to GDPR
- May also include identification of any additional activities recommended

TRAINING AND AWARENESS

- GOOMED can create and present awareness material on GDPR Principles, compliance requirements and potential risks
- The material and delivery can be tailored to specific audiences from board members, to general employees and third parties

- Business units (IT, finance etc.) can be targeted individually with specifically relevant training if preferred

INCIDENT MANAGEMENT PROCESS REVIEW

Early identification and evaluation of breaches is essential as well as a timely response.

This service provides the customer with the confidence that incidents are managed appropriately to enable identification and confirmation of a breach and meet the need to notify the supervisory authority within the required 72 hours specified in GDPR.

The assessment can include:

- Review of existing event logging and alert notification in place where personal information is processed
- Review of incident management policies, standards and processes (including third parties processing data on behalf of the customer)
- Create and facilitate an incident response drill, to assess through safe execution of real-world scenarios - the adequacy of existing architectures, procedures, and training
- Areas for improvement and potential solutions identified and documented

THIRD PARTY ASSESSMENTS

GOOMED can create and implement vendor assessment questionnaires and review processes for evaluating security controls of third parties that will be processing personal information on your behalf.

The assessments should be performed at initial engagement with third parties as part of contractual requirements and on a regular basis (such as annually) to ensure the continued adequacy of security controls.

The service may also include on-site auditing of vendor controls, and penetration testing and/or vulnerability assessment services if requested.

DATA PROTECTION OFFICER

Many organizations have not considered the role of a Data Protection Officer (DPO) at all; or that the existing role has no gravitas; or it sits within an area of the business where it has little or no effectiveness.

Why engage a GOOMED DPO?

- To provide a level of independence where there are no conflicts of interest
- Politically neutral and not easily influenced
- Provides a highly skilled and knowledgeable resource, where that skillset or knowledge is not available internally
- Where creating a full-time role internally is not a viable option

What can a yDPO do for me?

- Help you understand the impact of legislation and regulation on your organization
- Implement the data protection framework or improve its effectiveness
- Conduct periodic assessments, including assessments of your third parties
- Drive the adoption of a proactive data protection culture, including provision of training and awareness
- Handle subject access requests and deal with data breaches
- Interface with the supervisory authority
- Support key projects where “privacy by design” is a necessary consideration
- Support readiness for GDPR and ongoing compliance
- Conduct data breach crisis management exercises
- Review adequacy of contracts
- Monitoring and reporting of data protection activities and control effectiveness
- Support development of proper documentation related to the data protection requirement at the level of client/customers with underlying citation and controls needed for compliance checks and continuous monitoring.
- Third Party Management
- Support Data Processing Activities mapping

SUPPORTING ACTIVITIES

- Preparation for introduction of ISO/IEC 27001:2013
- Building of complex data security information solutions
- Deploying Enterprise Threat Intelligence Solution

AN UNIQUE MODELL

Our services provide outputs, which could serve the whole structure of the company activities and providing actual solutions for mitigating respective risks such as:

- Legal Security
- Compliance Procurement
- HR Marketing and Customer Relations
- IT & Information Services
- PR & Communications
- Insurance

	Legal Security	Compliance	HR	IT & Information Services	Insurance	Security	Procurement	Marketing and Customer Relations	PR & Comm
Governance	■	■	■	■	■	■	■	■	
Accountability	■	■							
Fair Processing and Consent	■	■						■	
Notices / Vetting - HR	■	■	■	■					
Notices - Customers	■	■		■				■	
Children	■	■		■				■	
Data Subject Rights and Procedures	■	■	■					■	
Record of Processing	■	■	■	■		■	■	■	
Privacy by Design and Default	■			■		■	■		
Compliant Contracting And Procurement	■	■					■	■	
Data Breach Procedures	■			■		■			■
Data Export	■	■							

TIMELINE SERVICE CONGRUENCE

How we could absorb and cool down the pressure for compliance, reduce time and resources needed, consolidate best practices and provide sustainable platform for privacy data management

