

Are you ready to meet  
the challenges of  
GDPR?

## CAPABILITY STATEMENT: GENERAL DATA PROTECTION REGULATION (GDPR)

Digital advancements have resulted in consumer data being created, collected and stored within seconds. It is increasingly important to have clear laws and safeguards in place given the growing digital economy and associated cyber security risk.

In May 2018, the new European Union GDPR came into force across Europe – the legislation applies in each of the 28 EU Member States.

This new legal framework is the most monumental change to data privacy legislation in over twenty years and will affect businesses across the globe. Any company that holds or processes the data of an EU citizen is potentially affected with potential fines for non-compliance up to €20m or 4% of annual global turnover.

### HOW DOES THIS AFFECT ME AND MY BUSINESS?

Any company, anywhere in the world, that processes an EU based consumers' personal data will need to comply with the new requirements. Understanding the changes to the existing process under the new rules is paramount:

**Consent:** Do you have explicit consent from individuals for the data you hold on them?

**New responsibilities:** Are you a data processor or data controller responsible for processing personal data?





**Accountability:** Do you have a data protection program and are you able to provide evidence of how you will comply with the GDPR requirements?

**Mandatory breach notification:** Would you be able to notify a data protection supervisory authority of a data breach within 72 hours?

**New rights:** Do you know how you will comply with the new rights; the 'right to be forgotten' and the 'right to data portability', and the 'right to object to data profiling'?

**Data protection officers:** Do you conduct large scale systematic monitoring (including employee data) or process large amount of sensitive personal data?

### KEY CAPABILITIES

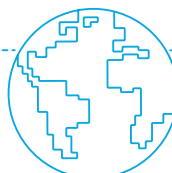
-  Internal audit
-  Regulatory and compliance
-  Governance and risk
-  Effectiveness and efficiency

### ABOUT RSM

The RSM global network is represented in 120 countries, enabling us to access best practice insights and local expertise in both the public and private sector to assist you, no matter where in the world you are operating. It is our strong, collaborative approach that differentiates us. This allows RSM Australia to work with our US and European firms to ensure our local clients can leverage off not only our local expertise, but that of our network in regards to GDPR projects that we have delivered. We strive to truly understand your business, your strategies and your aspirations and endeavour to be considered the adviser of choice.

Our one-firm national structure not only delivers exceptional results and value for money, it also enables us to provide a single, seamless client service. With 29 offices across Australia, our clients benefit from our geographic diversity by effectively utilising our shared expertise, ideas, technology and experience.

- 6th largest global audit, tax and consulting network
- Firms in 120 countries and in each of the top 40 major worldwide business centres
- Over 43,000 in 800 offices
- Clients from growth-focused entrepreneurial businesses through to leading multi-national, cross border organisations



## ROADMAP TO COMPLIANCE

While every project is unique with specific client needs, the following is a high-level sample approach.

### 1. Mobilisation

- Define scope confirming inclusions and exclusions
- Integrate with legal advice to ensure commensurate risk targeting
- Define expected outputs and outcomes
- Develop and delivery of an awareness campaign
- Agreement of the project plan across business units
- Commit resources with the correct expertise and business knowledge
- Establish governance processes

### 2. Discovery

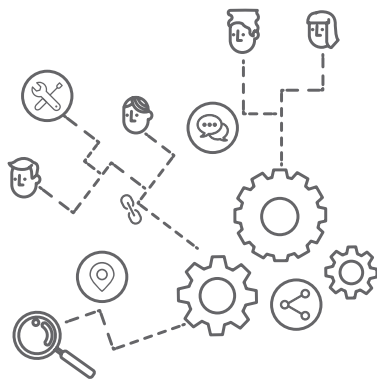
- Review policies, procedures
- Conduct interviews to capture key business processes associated with data capture and management
- Development of an information / data asset register
- Discuss functionality of systems to meet GDPR requirements

### 3. Analysis and evaluation

- Review processes and policies, identifying gaps that create GDPR exposures
- Determine and develop appropriate and proportionate policies and processes
- Assist with the implementation and testing of updated policies and procedures to ensure they meet project and risk objectives
- Review and assessment of the security over information processing

### 4. Reporting

- Concise reporting to Board and Executive Management
- Finalised post-client feedback
- Focus on key findings in gap analysis
- Recommendations reflected in budgeted roadmap to compliance



## CASE STUDIES AND BENEFITS

**GOVERNMENT** – We implemented an Information Security Management System privacy control framework using an associated software company. The system enabled the local government and its internal audit department to control and document data security and privacy policies and procedures within the organisation.

The end result is a privacy management system (PMS), based on the PDCA (plan-do-check-act) cycle. Using this, the organisation is able to demonstrate the operational effectiveness of their processes, and enhance the quality of privacy management whilst reducing costs.

**FINANCIAL SERVICES** – RSM undertook a Privacy Impact Assessment with regard to the current Loan Application process as operated by a Credit Union.

We conducted walk through testing of the existing data protection policies, procedures and processes and mapped data flows for the IT, Finance, HR, Compliance and Marketing functions. We also captured the nature of the data managed within the current process, including sharing of personal data with any third party organisations outside of our clients.

Senior staff at the company gained an increased awareness of their data protection obligations going forward, and their respective roles in ensuring compliance is achieved and maintained.

## HOW WE CAN HELP

RSM is committed to helping companies like yours improve at every turn. Whatever the challenge, we strive to understand your business and deliver objective advice and high quality customised services that help you make more confident business decisions.

Our specialists can help you to assess and prepare for compliance. Through robust analysis we will identify any risks and work with you to implement processes and systems to help you comply, including:

- GDPR gap analysis
- Data Asset and Privacy Impact Assessments
- GDPR education and awareness sessions
- Breach and GDPR management processes
- Security monitoring and reporting

For further information, please contact our Risk Advisory team.

[www.rsm.com.au/service/risk-advisory](http://www.rsm.com.au/service/risk-advisory)