GENERAL DATA PROTECTION REGULATION (GDPR)

RSM client case studies

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

GDPR CLIENT CASE STUDIES

- Financial services
- Aerospace
- Government
- Financial services
- International NGO
- IT and software
- Engineering
- Insurance
- Charity
- Healthcare
- Sport
- Engineering
- Pension provider
- Online gaming

CLIENT: **FINANCIAL SERVICES**

RSM firm: Ireland
RSM contact: Terry McAdam

Bringing RSM's ideas and insight – the work we carried out

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

The review assessed the incumbent process in light of both the prevailing Data Protection legislation and the pending General Data Protection Regulation.

Our team mapped the relevant data flows after conducting walk-through testing of the existing process. The nature of the data managed within the present process was also captured.

We prepared a concise report detailing the issues which presented, their implications and our considered recommendations to mitigate the risk associated with matters identified. Following feedback from management, we presented our report to a Board Committee.

Understanding our client – the benefits

The Board and Executive both gained an increased understanding of their data protection obligations (current and future) and their respective roles in ensuring compliance is achieved and maintained.

With respect to the in-scope process, the organisation was presented with clear recommendations which would address the shortcomings identified during our fieldwork. In conjunction with management, a time-bound action plan was agreed to address the risk of an individual's privacy being impacted during the operation of the Loan Application process.

CLIENT: **AEROSPACE**

RSM firm: Germany
RSM contact: Oliver Bungartz & Gregor Strobl

Bringing RSM's ideas and insight – the work we carried out

RSM Germany performed a GDPR-readiness check for a leading European aerospace company. The current established organisation and structure with regards to data privacy was reconciled to the future regulatory requirements.

The review assessed the current adjustment activities in light of both the prevailing Data Protection legislation and the pending General Data Protection Regulation.

Our team reviewed the most current procedural directory and conducted respective walk-throughs in order to understand the current processes and data processing activities. Our team also assessed the relevant data flows and respective risks and verified the appropriateness of the mapped technical and organisational actions.

The results were presented in a formalised report as well as in a presentation to the Board of Directors. Detailed observations, recommendations as well as the respective management report formed part of the report while the presentation highlighted our approach and the outcome. Further actions have been discussed with management during the soft close meeting after fieldwork on site.

Understanding our client – the benefits

The data protection officer, senior management as well as the Board of Directors gained an increased understanding of their data protection obligations (current and future) and their respective roles in ensuring compliance is achieved and maintained.

With respect to the in-scope process, the organisation was presented with clear recommendations and work packages which would address the shortcomings identified during our fieldwork. In conjunction with management, a time-bound action plan was agreed to address the risk of an individual's privacy being impacted during the day-to-day running of the company.

CLIENT: **GOVERNMENT**

RSM firm: Netherlands
RSM contact: Rien Hommes & Gerrit Goud

Bringing RSM's ideas and insight – the work we carried out

We implemented a privacy control framework using an Information Security Management System from Key 2 Control, a software company associated with RSM Netherlands. The system enables the local government and its internal audit department to control and document data security and privacy policies and procedures within the government organisation.

The approach is focused on the PDCA (plan-do-check-act) cycle with attention to risk management, in line with the GDPR. There is a strong focus on control of the privacy processes and the persons responsible for privacy management.

Understanding our client – the benefits

The end result is a privacy management system (PMS), based on the PDCA-cycle. The system is based on the GDPR as control framework. Using this PMS, the organisation can demonstrate the operational effectiveness of their processes, as these are documented in the system together with the related policies and procedures.

By using this system, the quality of privacy management is enhanced at reduced costs.

CLIENT: **FINANCIAL SERVICES**

RSM firm: UK
RSM contact: Sheila Pancholi

Bringing RSM's ideas and insight – the work we carried out

The review assessed their process with regards to the Data Protection legislation and the upcoming General Data Protection Regulation.

Our team 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 the Society.

We prepared a concise report detailing gaps identified between current practices and the requirements stipulated under GDPR, their implications and our considered actions to mitigate the risk associated with matters identified.

Understanding our client – the benefits

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.

With respect to the in-scope process, the Society was provided with a clear action plan to address the shortcomings identified during our fieldwork, in addition to the mapped data flows which they will maintain and update during business as usual processes.

CLIENT: **INTERNATIONAL NGO**

RSM firm: Ireland
RSM contact: Terry McAdam

Bringing RSM's ideas and insight – the work we carried out

We were retained by a high profile internal NGO to support the Board in considering their risk appetite with respect to the governance and management of data-related risks within the organisation.

The entity is involved in the provision of services to individuals across the globe and is frequently delivering its interventions in very challenging environments.

The Board subsequently agreed a relevant policy and we proceeded to undertake a review of current data management practices in light of the policy and using the EU Directive as a proxy for national data protection legislation which frequently was not enacted in the jurisdictions concerned.

We prepared a detailed report regarding the weaknesses and risks uncovered during our review which we shared with the Board. Our final report featured a multi-year budgeted roadmap detailing our recommendations for improvement across the integrated domains of governance, policy, process, technology and employee awareness/training.

Understanding our client – the benefits

The client received the consulting support required to develop an appropriate risk appetite statement and a related policy regarding data-centred risk.

The Board and Executive both gained an enhanced understanding of their data protection obligations (current and future) and their respective roles in ensuring compliance is achieved and maintained.

Thereafter, our final report detailed a very clear implementation plan to create a robust data governance and management environment within the entity at both field and headquarter level. This plan subsequently underpinned a successful project undertaken by the internal ICT function.

CLIENT: **IT AND SOFTWARE**

RSM firm: Netherlands
RSM contact: Rien Hommes

Bringing RSM's ideas and insight – the work we carried out

The software company received requests from some of their clients to become ISO27001 certified. The clients prescribed ISO27K certification as a new requirement for services of their suppliers to align to the new GDPR legislation, effective May 2018.

We hosted an ISO27K readiness-programme to ensure the company became ISO27K certified within six months.

Understanding our client – the benefits

The client set up the required control framework for information security under the NEN-ISO norm 27001. When the certificate was obtained, the company acquired a competitive advantage and has met the client's requirements.

The company will also have a system in place for data security and privacy which is based on an internationally-accepted security standard.

CLIENT: **ENGINEERING**

RSM firm: Ireland
RSM contact: Terry McAdam

Bringing RSM's ideas and insight – the work we carried out

An engineering consultancy retained RSM Ireland to undertake a review of their data management practices in respect of the outsourced services they provide to a public sector body under an existing contract. Such a third party review was required by their client.

Our consulting team undertook the review required in light of the current national data protection legislation and the upcoming General Data Protection Regulation.
Our team conducted walk through testing of the existing core processes and mapped the relevant data flows. We also captured the nature of the data managed within the in-scope processes.

We prepared a concise report detailing the issues which prevailed in the processes, their potential impact and our related recommendations to mitigate the risks associated with matters identified. Post the capture of the views of management we presented our report to a Director of the business who shared the document with the public body.

Understanding our client – the benefits

The client and its senior staff now understand their data protection obligations, both current and in the future, and how they are responsible for ensuring compliance is achieved and maintained.

Regarding the scope's outsourced service provision, RSM presented the organisation with clear recommendations and advice in order to address the shortcomings which became apparent during our review. Working with management, a clear action plan, including timelines, was develped to address the prevailing risks and develop an improved data governance environment.

CLIENT: **INSURANCE**

RSM firm: Netherlands
RSM contact: Maarten Mennen

Bringing RSM's ideas and insight – the work we carried out

An insurance broker requested our help in the design of gap analysis tooling that would enable them to advise their clients on non compliance with the GDPR.

Using the Control on Demand tooling, we developed a quick scan risk analysis and reporting tool. We also gave the necessary training to use the tool and to produce the reports.

Understanding our client – the benefits

The client obtained the tooling and training to perform quick scans on security and privacy requirements under the GDPR rules for their clients as an additional service.

CLIENT: **CHARITY**

RSM firm: UK
RSM contact: Steven Snaith

Bringing RSM's ideas and insight – the work we carried out

We delivered a GDPR controls gap analysis for this organisation with a remit that included the following:

- Data protection strategy and planning
- Data protection policies and procedures
- Raising of data protection issues for consideration by the senior management team
- Data protection staff awareness
- Information risk register framework
- Allocation and designation of data owners
- Co-ordination of data protection responsibilities;
- Data breach incident response planning
- Data breach investigations
- Data protection training (guidance and delivery)
- Data protection impact assessments
- Data protection audit requirements
- Information governance activity co-ordination
- Data retention processes
- Data consent capture mechanisms
- Data security controls
- Data protection board reporting
- Fair notice requirements

The output of this review was a detailed report setting out gaps in procedures that needed to be addressed to assist the organisation in meeting GDPR requirements.

Understanding our client – the benefits

The remediation plan and supporting advice provided by RSM has led to an improved control framework that more closely aligns with GDPR requirements.

Moreover, an initial focus on data mapping identified a number of repositories of personal identifiable data that were not sufficiently protected. The implementation of the corresponding recommendation led to the related risk of a data breach being reduced.

CLIENT: **HEALTHCARE**

RSM firm: Belgium
RSM contact: Steven Vermeulen

Bringing RSM's ideas and insight – the work we carried out

RSM Belgium performed a compliancy analysis with Belgian Privacy legislation.

Following the adoption of the General Data Protection Regulation, our mission was extended to fulfil the Data Protection Officer role within the client's company.

Our team conducted interviews and testing of the existing IT architecture, policies and processes. We helped our client with the identification of personal private data through their different data flows. As part of our mission we conducted detailed reviews on the subcontractors of the company that have access to the company's data.
As the company is publishing personal identifiable data on their website we performed a risk assessment on securing data and helped our client to take the necessary steps in being compliant to the rules and regulations both on a Belgian and an international level.

We prepared a management report detailing the flaws and issues found during our mission, including the implementation plan with mitigating actions the entity could undertake. As our role as Data Protection Officer, we followed up on the actions taken.

We were able to help our client convince Belgian Authority in granting them a legal basis on which they can operate, proving their investment in securing private data.

Understanding our client – the benefits

The Board and Executive both gained an increased understanding of their data protection obligations (current and future) and their respective roles in ensuring compliance is achieved and maintained.

Continuous assistance on a still evolving International and Belgian privacy legislation, assures the entity they will keep up to date with rules and regulations.

CLIENT: **SPORT**

RSM firm: Belgium
RSM contact: Steven Vermeulen

Bringing RSM's ideas and insight – the work we carried out

During break-out sessions to our clients we reached out to the management of a Premier League Football Club in Belgium.

We organised awareness sessions with the Board of Directors and the management of the football club, highlighting the specifics for their sector ranging from protection of minor football players to the rights and duties of professional football players. We enabled management to bridge the rules and regulations between Belgian level (issued by KBVB) and International level (FIFA) and the General Data Protection Regulation.

Our team performed a complete analysis and gap detection between the status as is and to be.

Assistance is provided to the entity to implement a secure architecture, procedures and policies to comply with the rules and regulations applicable.

Understanding our client – the benefits

The Board and Executive both gained an enhanced understanding of their data protection obligations (current and future) and their respective roles in ensuring compliance is achieved and maintained.

A full implementation plan is being set up in collaboration between the client and RSM Belgium. The client is lead implementator of the General Data Protection Regulation within the Premier League Football Clubs in Belgium and is setting the scene for other clubs to follow. A close collaboration between the club and the Belgian Football Association (KBVB) resulted from the awareness sessions we presented. Similar sessions are planned for the Belgian Football Association.

CLIENT: **ENGINEERING**

RSM firm: Ireland
RSM contact: Terry McAdam

Bringing RSM's ideas and insight – the work we carried out

An engineering consultancy retained RSM Ireland to undertake a review of their data management practices in respect of the outsourced services they provide to a public sector body under an existing contract. Such a third party review was required by their client.

Our consulting team undertook the review required in light of the current national data protection legislation and the upcoming General Data Protection Regulation.

Our team conducted walk through testing of the existing core processes and mapped the relevant data flows. We also captured the nature of the data managed within the in-scope processes.

We prepared a concise report detailing the issues which prevailed in the processes, their potential impact and our related recommendations to mitigate the risks associated with matters identified. Post the capture of the views of management we presented our report to a Director of the business who shared the document with the public body.

Understanding our client – the benefits

The Director and the Executive both gained an increased understanding of their respective data protection obligations (present and future) and their roles in ensuring compliance is achieved and maintained.

With respect to the outsourced service provision which defined our scope, the organisation was presented with clear recommendations which sought to address the shortcomings identified during our review. In conjunction with management, an action plan, with clear timelines, was agreed to address the prevailing risks and develop an improved data governance environment.

CLIENT: **ONLINE GAMING**

RSM firm: Malta
RSM contact: Gordon Micallef

Bringing RSM's ideas and insight – the work we carried out

The impact assessment looked into the existing processes, policies, procedures, structures and identified the gaps to the new regulation requirements. As well as providing the recommendations to address the gaps, we prepared the necessary tool sets to address a number of areas as part of our deliverables:

- Inventory of data sets, processes, and ownership
- Third-party privacy questionnaire
- Checklist to evaluate third-party contracts against privacy obligations
- Information system security questionnaire relevant to privacy obligations
- Consent inventory
- Data protection policy
- Incident response procedure
- Data archiving and retention policy

Understanding our client – the benefits

The primary benefit is that the organisation will have a clear picture where it stands in terms of compliance to the new regulation, and what action is necessary to address the gap through a detailed action plan. The objective of delivering a number of tools as part of our engagement is to continue providing management services for GDPR compliance on an ongoing basis once the regulation comes into force in May 2018.

RSM Global Executive Office
50 Cannon Street
London
EC4N 6JJ
United Kingdom

T: +44 (0) 20 7601 1080
E: riskadvisory@rsm.global

rsm.global