GDPR Gap Analysis Report

Power Diary

Release date: 21st June 2023

Author: Martin Fletcher & Janine Nowak

Table of contents

Copyright © GRC International Group 2023

1.0 Introduction

DQM GRC was commissioned to carry out a General Data Protection Regulation (GDPR) gap analysis using its GDPR RADAR™ process to examine Power Diary's adherence to the requirements of the EU GDPR, the UK GDPR and the Data Protection Act (DPA) 2018, and the maturity of its compliance activities.

This report summarises the GDPR gap analysis process and scoring for Power Diary.

1.1 Power Diary's Data Protection Context

Established in Australia in 2010, Power Diary specializes in delivering a streamlined practice management solution for healthcare professionals. The platform encompasses an array of features such as patient record-keeping, clinical note templates, appointment coordination, and financial management, including billing and claims processing.

Since its launch, the company has grown consistently and now operates globally, including in Europe and the UK. To strengthen its commitment to compliance, a specialised team focusing on privacy and security was established. To further ensure adherence to GDPR regulations, the company engaged DQM GRC to conduct an external review and assessment. This assessment aims to verify compliance with GDPR Regulations as well as to identify any opportunities for improvement.

The following areas were highlighted as affecting the data protection context for Power Diary:

Copyright © GRC International Group 2023

Issue	Impact
Processing of special category data	Power Diary's product involves the collection and processing of health data such as patient records and clinical notes. Because of this, an extra degree of protection is expected compared to companies processing lower-risk data.
Use of third-party processors	Power Diary conducts its business over Cloud platforms and is reliant on third-party storage for the personal data it processes. The business itself also acts as a processor on behalf of its customers. It is therefore important to ensure that controller/processor relationships are clearly defined, and appropriate contracts are in place.

1.2 About DQM GRC

At DQM GRC, we understand the critical importance of effectively managing risks and ensuring regulatory compliance in today's dynamic business landscape. We are a trusted industry leader, offering solutions and services that empower organizations to navigate the complexities of governance, risk, and compliance with confidence. With our expertise, we are your dedicated partner in safeguarding your business, enhancing operational resilience, and maintaining a competitive edge.

Our comprehensive suite of GRC solutions is designed to streamline and optimize risk and compliance processes. From policy management and risk assessments to control testing and reporting. By combining the expert knowledge of our consultants and industry best practices, we enable you to proactively identify, assess, and mitigate risks while ensuring adherence to regulatory requirements. With DQM GRC as your trusted ally, you can strengthen your governance practices, protect your reputation, and drive sustainable growth in an ever-changing business environment.

Copyright © GRC International Group 2023

2.0 GDPR Radar™ Assessment Methodology

DQM GRC assessed Power Diary using their specialized GDPR RADAR™ assessment process. This assessment focused on evaluating Power Diary's compliance with data protection regulations, specifically the EU GDPR, UK GDPR, and UK's DPA 2018. The assessment consisted of two parts: reviewing Power Diary's data protection context and reviewing their GDPR assurance.

During the review of Power Diary's context, the consultant examined various factors to determine which areas required higher priority. For example, if Power Diary receives a large number of Data Subject Access Requests (DSARs), it is crucial for them to have a scalable and efficient process in place, along with regular reports to management. This differs from an organization that only receives occasional DSARs.

Based on the review, the consultant determined the level of assurance needed to address the risks identified. For instance, an organization that frequently receives DSARs would require a more structured governance approach for managing those requests compared to an organization that receives them infrequently. The consultant compared the identified assurance levels with the actual levels observed during the review, highlighting any areas where the level of assurance did not match the risk based on Power Diary's specific context.

It's important to note that this assessment does not simply measure whether Power Diary is compliant or not, but rather focuses on evaluating whether Power Diary is effectively managing and controlling its risks. Appendix 2 of the report provides a list of individuals who were involved in the project, and any necessary documentation that was reviewed as part of the assessment to ensure Power Diary's GDPR compliance in light of the assessment findings.

Copyright © GRC International Group 2023

The GDPR gap analysis assessed Power Diary's compliance against a custom set of control measures in nine categories:

1. **Governance**

   The extent to which data protection accountability, responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and operating throughout the organisation.

2. **Risk management**

   The corporate arrangements for privacy risk management, the extent to which the corporate risk regime incorporates information-specific risks, and which risks to the rights and freedoms of natural subjects are addressed.

3. **DPO**

   Where a DPO is mandatory, the role is positioned appropriately, and the appointed DPO is capable of meeting the requirements of both the EU GDPR and the UK GDPR.

4. **Roles and responsibilities**

   The extent to which roles and responsibilities are defined and established throughout the organisation, including necessary training and awareness.

5. **Scope of compliance**

   It is essential that the scope of compliance is clearly defined, taking account of all the data processing in which the organisation has a role under both the EU GDPR and the UK GDPR, whether as a data controller or as a data processor, as

Copyright © GRC International Group 2023

well as any data-sharing activities and international transfers. To determine the scope of compliance, all databases that hold personal data, as well as all extraterritorial/cross-border processing, must be identified.

6. Privacy by design

The extent to which an appropriately staffed, funded and supported GDPR project is in place, and capable of achieving realistic objectives.

7. PIMS

A wide range of documentation is required to ensure that an organisation can demonstrate compliance with the requirements of the EU GDPR, the UK GDPR and the DPA 2018. The scale of the documentation should be appropriate to the size and complexity of the organisation. The PIMS should also address staff training and awareness.

8. ISMS

The technical and organisational measures in place to ensure there is adequate security of personal data held in hard copy or electronic form, or processed through the organisation's systems. This includes a review of methodologies for testing security, and established cyber security certifications, standards and codes of practice.

9. Rights of data subjects

The organisation needs processes that will enable it to both facilitate data subject rights and respond to data subjects exercising any or all of these.

Copyright © GRC International Group 2023

3.0 Power Diary GDPR Assessment Score

Overall assessment score
9.2

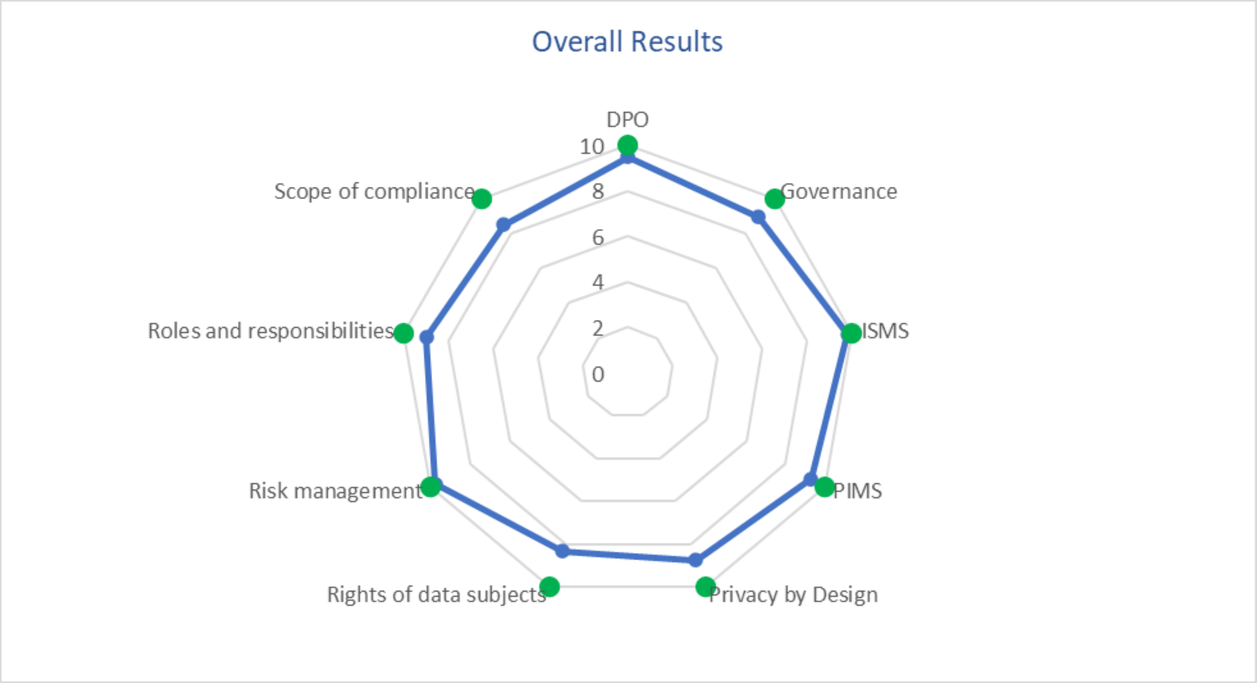
The assessment took place remotely in June 2023 using the Zoom and Google Meet teleconferencing platforms, along with a review of supporting documents to which the assessor was given access.

The assessor determined that Power Diary had achieved an overall compliance score of 9.2 out of 10 on our maturity scale.

This score demonstrates that Power Diary had processes and procedures that provided a very high level of assurance that it was conducting its activities in line with the regulations. There was an excellent understanding across the business of internal policies and the wider regulatory context. There was also evidence of teams within Power Diary accessing expertise when developing new projects or changing existing processing activities. Responsibilities and governance structures were clearly outlined and decisions regarding information risk were made at the appropriate level based on an informed understanding of the processing activity taking place.

Copyright © GRC International Group 2023

This overall score reflects a range of levels of maturity across nine critical areas of data protection compliance, as shown in the RADAR chart below.



The blue dots on the blue line show Power Diary's scores in each area. **The results show that Power Diary had a more than adequate level of assurance across all governance areas.**

The full report provided recommendations for further improvements. However, given the current level of assurance across the business, these will be largely advisory measures. They are presented as options for the business to review and decide if using resources to enhance assurance even further would be worthwhile.

Copyright © GRC International Group 2023

2.0 Headline findings – Areas of Good Practice

Power Diary demonstrated numerous examples of best practice across all governance areas reviewed in the GDPR gap analysis.

The assessor was particularly impressed with the following:

Senior level buy-in

Data protection and information security are taken very seriously by all senior managers in the business. The Management Team regularly engages with staff at all levels to discuss data protection and information security. There is an ongoing communications campaign that is spearheaded by senior management, and evidence that this support is driving compliance across the business. Indeed, many of the staff interviewed reported they were surprised at how seriously these issues were taken upon joining the business.

Risk assessment and escalation

There is a highly robust mechanism for ensuring that all new activities using personal data undergo a thorough risk assessment before going live. The company also demonstrated that risks are escalated and handled at the appropriate level.

Furthermore, the business actively engages with staff to seek out and address new risks that may have been previously overlooked.

Training programme

The company has an extensive programme of training in information security and data protection. All staff are expected to complete training and knowledge check tests, and completion rates are closely monitored.

Staff also have access to any expert knowledge and support that they require. All of this is supported by an extensive awareness raising programme of communications, the effectiveness and reach of which is regularly monitored.

Copyright © GRC International Group 2023

3.0 Headline findings – Areas for Development

The interviews did identify some minor gaps where the policies had not been fully applied, however these related to systems that only handle trace amounts of personal data and will be easy to remedy.

Most of the recommendations made in this report will be advisory, and it is up to Power Diary to decide if it wants to devote resources to enhancing its level of assurance even further:

Data retention

In some of the interviews, the assessor identified a handful of systems that had either not had retention schedules fully implemented or, due to being a new system, had not undertaken any deletion exercises in live situations. The company will need to address these minor retention gaps and keep newer systems under review to ensure deletion is carried out when the time comes for doing so.

Exploiting data opportunities

While Power Diary has been building its PIMS, it has taken a risk-averse approach to any new activities that would collect and use additional personal data. While this has allowed the company to assure itself that it is acting within the boundaries of the regulation, it may mean that it misses out on some opportunities to increase its customer base and revenue.

Power Diary is now in a good position to identify these opportunities, thoroughly risk assess them and make an informed decision on whether it wishes to expand its personal data processing activities in these areas in the future.

Copyright © GRC International Group 2023

Additional auditing and certification

If the company wishes to do so, it could gain additional assurance by having a complete external review of its PIMS. This would involve an external consultant reviewing all individual processing activities, data protection impact assessments (DPIAs) and third-party relationships in depth. The reviewer would then provide feedback on whether they think the work undertaken and the decisions made within the business are correct. However, given Power Diary has a qualified and dedicated internal Data Protection Officer, the additional assurance obtained by this process would likely be excessive. Finally, the business could consider certification in other standards alongside the ISO 27001 certification it currently holds, for example, ISO 22301 in business continuity management or ISO 27701 in PIMS.

Copyright © GRC International Group 2023

Disclaimer

The matters arising in this gap analysis report are only those that were brought to the attention of the consultant during the assessment and are not necessarily a comprehensive statement of all areas requiring improvement.

DQM GRC is not a licensed legal practitioner and, although its consultants draw on deep practical knowledge of data protection and privacy law and practice, none of the recommendations in this report should be construed as formal legal advice.

DQM GRC takes all reasonable care to ensure that its reports are fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred arising out of, or in connection with, the use of its reports, however such loss or damage is caused.

Copyright © GRC International Group 2023

Appendix 1: Resources examined

Individuals interviewed as part of the assessment:

Name	Role
Damien Adler	Founder/Accountable Director for Data Protection
Paul Adler	Founder/Accountable Director for Information Security
Tercyus Ribeiro	Data Protection Officer
Filipe Villar	Head of Information Security
Naomi Crosbie	People and Culture Manager
Diego Jancic	Engineering Manager
Danielle Hopkinson	Marketing Manager
Diana Golden	Customer Success Team Manager

DQM GRC processes the limited personal data provided by client staff and representatives for the purposes of conducting interviews and reviewing supporting documentation for this report. This data is not stored anywhere in our systems other than in this report and associated meeting records. It is retained until deletion is legally and contractually possible.

Copyright © GRC International Group 2023

Documents reviewed:

Title	Document date
Data Protection Policy	July 2022
Clear Desk and Screen Policy	November 2022
Acceptable Use Policy	December 2022
Access Control	December 2022
Internal Privacy Policy	December 2022
GDPR and UK GDPR Procedure for International Transfers of Personal Data	June 2022
Data Subject Rights Procedure	February 2022
Data Subject Request Procedure	October 2022
GDPR and UK GDPR Breach Notification	December 2022
Risk Assessment Policy	December 2022
Risk Assessment and Risk Treatment Methodology	December 2022
Information Security Policy	March 2023
Working from Home and BYOD Policy	December 2022
Network Security Policy	December 2022
Change Management Policy	December 2022
Data Retention and Disposal Policy	January 2023
Vendor Management Policy	December 2022
Software Development Policy	December 2022
Controller Contract Log	Updated on an ongoing basis
EU Standard Contractual Clause (UK Addendum)	May 2022
Online Privacy Notice	June 2023
Cookie Policy	May 2023
Staff Privacy Notice	December 2022
List of Security Incidents	June 2023
Breach Risk Assessment Example	February 2023
Breach Reporting Example	June 2023

Copyright © GRC International Group 2023

Data Subject Request Procedure	2023
Information Security Incident Communication Procedure	2023
Privacy Training Materials	April 2022
Privacy Awareness Training Report	September 2022
Interviewing Skills for Hiring Managers	2022
Information Security Awareness Training	2023
Privacy by Design Training	2023
Awareness raising communications	Various 2023
Staff suggestion box	2023
Staff survey	February 2023
Marketing communications examples	Various 2023
Records of Processing Activities	Updated on an ongoing basis
DPIA examples	Various 2023
List of employees and contractors	April 2023
List of third party vendors/contractors/controllers/processors	December 2022
ISMS Management Review Tracker	December 2022
Penetration Test Report	January 2023
Backup Test Report	February 2023

Copyright © GRC International Group 2023