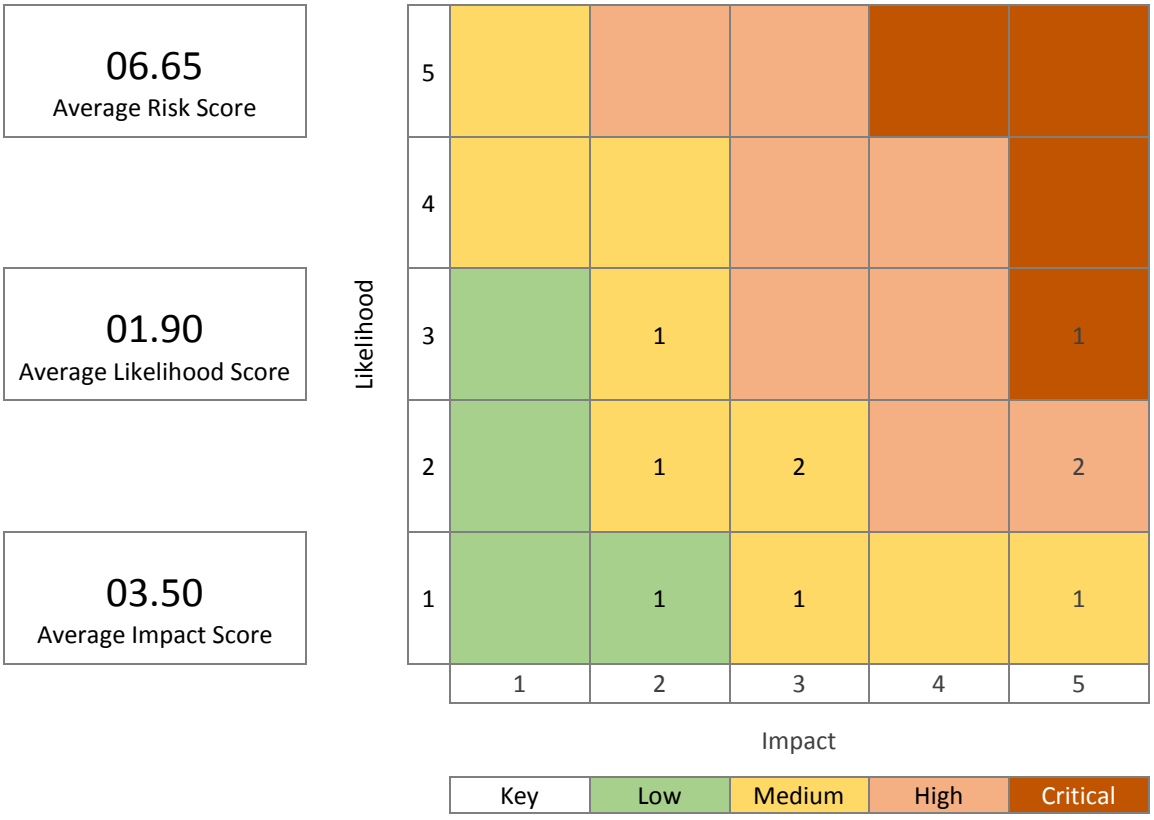
RMB Automotive

GDPR Risk Register

Last updated 30/04/2018

RMB Automotive GDPR Risk Register

RMB Automotive has established a risk register in relation to processing personal information via contracts with data controllers and processors, motor insurance companies and repair network management companies, via direct consent from individual customers and employees, and where there is a legitimate business reason. We have listed the risks identified and quantified using a risk matrix and scores. We have also stated our means of mitigation and how we intend to treat the risks.



Average	1.90	3.50	6.65	
Risk	Likelihood	Impact	Risk Score	Treatment
Loss of Business	3	5	15	Communicate Compliance
Loss of Reputation	2	5	10	Internal Systems in Place
Hacking & Cyber Crime	2	5	10	IT Security & Checklist
Complaints	3	2	6	Privacy Notice
Staff Misuse of Data	2	3	6	Training & Awareness
Third Party Misuse of Data	2	3	6	Contracts & Agreements
Fines of up to 4% of Turnover	1	5	5	GDPR Compliance
Slow Incident Response	2	2	4	Incident Response Procedure
Court Cases	1	3	3	Employee Awareness
Demotivated / Loss of Staff	1	2	2	Good HR Policies

Examples of Risks to Individuals

1. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.

2. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.

3. New surveillance methods may be an unjustified intrusion on their privacy.

4. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.

5. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.

6. Identifiers might be collected and linked which prevent people from using a service anonymously.

7. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.

8. Collecting information and linking identifiers might mean that an organisation is no longer using information that is safely anonymised.

9. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.

10. If a retention period is not established, information might be used for longer than necessary.

Examples of Corporate Risk

1. Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.

2. Problems that are only identified after the project has launched are more likely to require expensive fixes.

3. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.

4. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.

5. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.

6. Data losses that damage individuals could lead to claims for compensation.

Examples of Compliance Risks

1. Non-compliance with the DPA.

2. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).

3. Non-compliance with sector specific legislation or standards.

4. Non-compliance with human rights legislation.

Version History

01 – Risk Register 30/04/2018 – initial document approved by Chris Jennings