RMB Automotive

GDPR Data Breach Incident Management Policy

Last updated 30/04/2018

RMB Automotive GDPR Data Breach Incident Management Policy

Summary

Data breach reporting was only mandatory under the DPA98 if the breach was also covered by the Privacy and Electronic Communications Regulations 2011 (PECR covering any data security breach at telecoms providers or ISP). Otherwise, breach reporting was only considered advisory. Under GDPR, breach reporting is now mandatory and in many cases there is also an obligation to inform Data Subjects in specific circumstances as well.

Initial notification to the Supervising Authority (SA), normally the ICO, Information Commissioners Office, must come from RMB **within 72 hours** of the discovery. Processors must notify any data breach to a member of the Data Management Team, and without delay.

Data Breach, means a breach of security leading to the:

- Accidental or unlawful destruction
- Loss
- Alteration
- Unauthorised disclosure
- Access to personal data that has been transmitted, stored, or otherwise processed

Data Breach Transparency

Staff members of RMB are obliged to notify both the Data Management Team and the Data Subjects about data breaches in certain circumstances.

1) If a data breach is likely to result in harm to the Data Subjects or it is likely to result in a risk to the rights or freedoms of the individuals, then RMB must report this to the Supervisory Authority in less the 72 hours of the breach being discovered.

2) Where there is a high risk, Data Subjects need to be informed immediately.
    a. If possible directly
    b. Otherwise, the controller should consult the Supervisory Authority to determine the best way forward

Ways to Minimise Breach Impact

The Data Management Team and Processors are required to put in place appropriate technical and organisational measures to ensure a level of security proportional to the risk. This can be done in the following ways:

- Including the ability to restore availability and access personal data in a timely fashion in the event of an incident
- The regular testing and evaluation of technical and organisational measures is intended to ensure security of data processing
- Pseudonymisation and encryption
- Guaranteeing confidentiality, integrity, availability, and resilience of processing systems and service

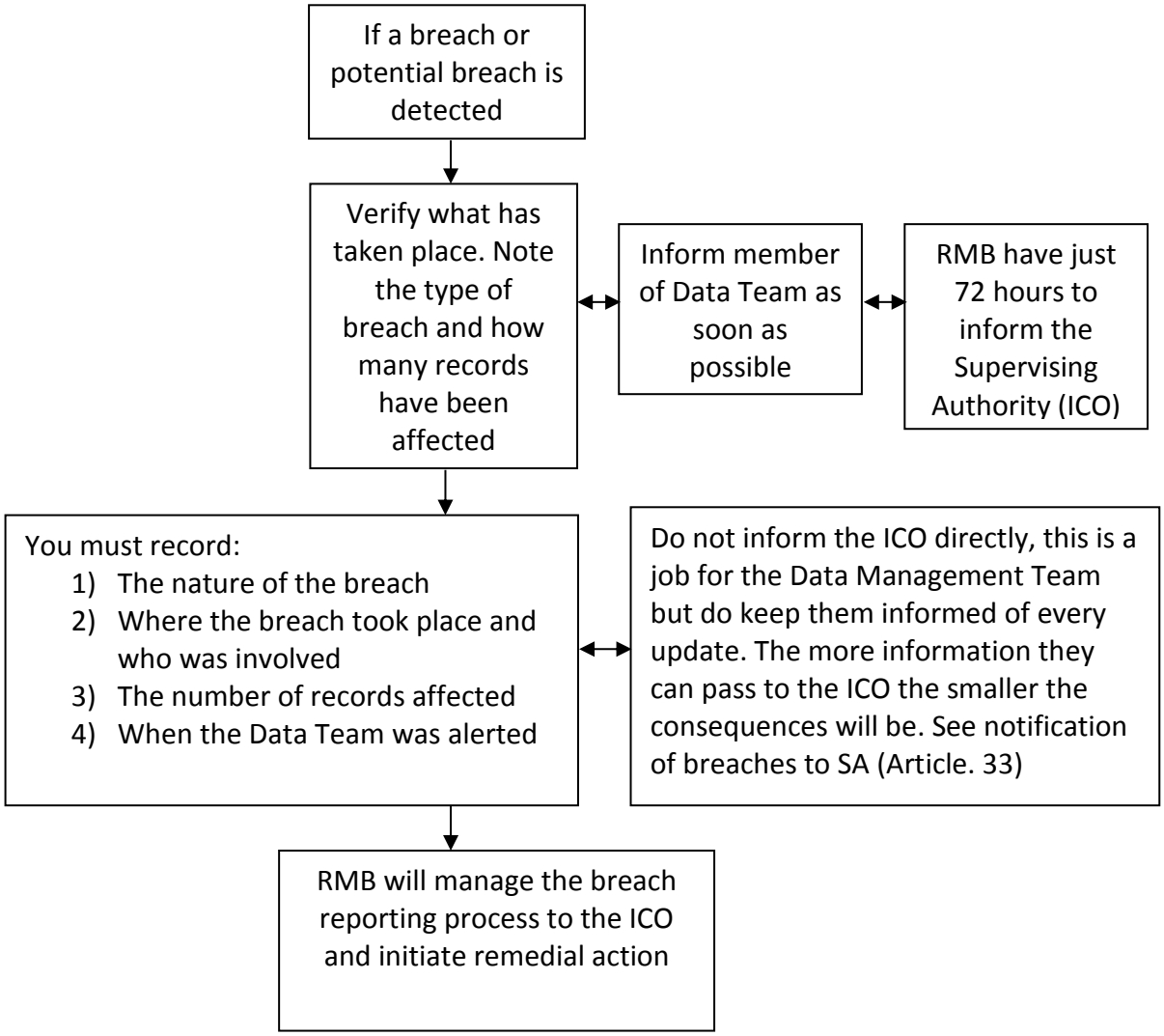
Impact of Data Breaches

- If the data subject's rights are breached they can sue you in your country, or theirs, for material and non-material damage – there is no upper limit set by GDPR. They can also sue individually and or collectively (class actions)
- Administrative fines will be levied by the supervisory authority for data breaches

It is a legal requirement that the Data Management Team only performs processing as defined by RMB's

policies

This is a flow diagram of the data security breaches reporting process adopted by RMB Automotive.



Make sure the Data Management Team at RMB is kept informed at all stages and is kept up to date throughout the whole process; the DPO will be able to advise and assist if required.

The Data management team can always be contacted at GDPR@rmbauto.co.uk

Version History

01 – Data Breach Incident Management Policy 30/04/2018 – initial document approved by Chris Jennings