DATA PROTECTION FOR INSURANCE INTERMEDIARIES

INTRODUCTION

Data protection can be a daunting subject for the uninitiated. There are onerous obligations in terms of compliance, storage, access, and reporting when data breaches occur. Non-compliance with relevant legislation or regulation can result in substantial fines, as well as litigation from disgruntled third parties.

Emma Erskine-Fox of TLT LLP presented a Technical Forum to the Membership, concerning data protection issues that are relevant to insurance intermediaries. This bulletin summarises those issues. The presentation slides and a recording of the Technical Forum are available on the Members' Portal of the Griffin website.

LEGISLATION

The purpose of the General Data Protection Regulation ("**GDPR**") and the Data Protection Act 2018 ("**DPA**") is to protect personal data belonging to individuals, sole traders, members of partnerships, directors, shareholders and employees. They encourage using data only when absolutely necessary. Data must be used accurately, fairly, transparently and lawfully, and those that use it are accountable if anything goes wrong.

Certain categories of personal data are defined as 'special', for example: health information, race, union membership and political affiliation. These categories require higher levels of protection, and a stronger justification for using them.

The relevant regulatory body in the UK is the Information Commissioner's Office ("**ICO**").

ROLES

The data protection roles that an organisation fulfils are, generally speaking:

- Controller – decides the purpose and means of data processing. Controllers are ultimately accountable for compliance with data protection laws.
- Processor – processes personal data on the controller's behalf, not making key decisions. Processors have some direct responsibilities under the law, for example to have security measures in place to protect data, but they have to follow the controller's instructions.
- Joint controller – jointly decides the purpose and means of data processing with another controller. Joint controllers are jointly responsible with the other controller(s) for the processing, and have to record in writing how each respective party meets relevant data protection obligations.

Insurance intermediaries tend to be controllers, for example if disclosing insureds' prior insolvencies to an underwriter. However, they could also be processors, for example if an insurer delegates underwriting authority to them. Intermediaries should carefully consider which roles they play, and ensure that contracts with third parties reflect this.

DATA REQUESTS

A data request is probably the most frequent way businesses see the impact of data protection principles. Businesses must comply with the various data requests (rights of subject access, rectification, erasure, etc) within a month, generally speaking.

Subject access requests are the most common kinds of requests. Such requests can be refused if they are manifestly unfounded or excessive. The target company must undertake a reasonable and proportionate search, not an exhaustive stone-turning exercise. If the requests are complex, the one-month response deadline can be extended.

Complaints to the ICO are common in this area, particularly in respect of deadlines being missed. No fines have yet been levied for missed deadlines, but this is possible and the more egregious the deadline breach, the greater the risk.

Intermediaries can prepare for such requests by training staff on how to recognise and respond to subject access requests.

DATA BREACHES

Data breaches must be notified to the ICO within 72 hours of anyone in the organisation becoming aware (time runs over weekends and public holidays). The ICO could levy two separate fines: one for the data breach itself and a second for missing deadlines. Intermediaries should maintain an internal record of any breaches.

Data breaches can take various forms. Companies are understandably worried about cyber attacks (phishing, ransomware, etc). However, breaches can often arise from, for example, disgruntled employees with an axe to grind, a lack of control over which employees can access certain material, or using the 'cc' field in emails rather than 'bcc'.

The most common data breach is where data is emailed to the wrong recipient because of human error, accounting for around 16% of reported breaches. No amount of training or procedures put in place will eradicate this risk completely, but robust staff training will help to justify your position if the ICO investigates.

The ICO says its focus is on 'areas of importance', which it judges to include data relating to children, AI risks, direct marketing and security. Its aim is apparently to focus on the harm caused, but there are low rates of investigation generally. Less than 1% of incidents are investigated, but 59% of investigations result in informal action being taken by the ICO, such as advice given that falls short of formal action like a reprimand, enforcement notice or a fine.

ENFORCEMENT EXAMPLES

In one example, where the 'cc' field was used in an email instead of 'bcc' and the recipients fell into a sensitive category (people living with HIV), the ICO issued a reprimand (a written warning with recommended steps to remedy the situation) and a GBP7,500 fine. This may seem relatively low but these decisions are in the public domain, so the bad publicity may be a worse punishment.

In another example, during a one-year period a company did not reply to around 40% of incoming subject access requests within the statutory timeframe. This resulted in a reprimand, but no fines. Although these results may seem lenient, intermediaries should nevertheless take their data protection obligations seriously.

LITIGATION

Article 82 of the GDPR establishes a right to compensation for material or non-material damage resulting from data protection breaches. This has contributed to a rise in speculative litigation with negligible prospects of success, for example claims for storage of online cookies.

Finally, recent case law shows that the courts are becoming less sympathetic to spurious claims by individuals in this area. One judge commented that no one of reasonable fortitude would have realistically suffered harm as a result of fairly anodyne information having been disclosed to a third-party. A complainant needs to demonstrate actual harm, not just that that they are annoyed or upset.

RISK MANAGEMENT MESSAGE

Members should ensure that they have appropriate privacy notices in place explaining to data subjects how their personal data is processed, as well as robust internal policies and procedures regarding processing of personal data. Also, employees should only have access to data that is necessary for the performance of their roles.

A review should take place where there are new, or changes to existing, processes or products which may have an impact on personal data. Furthermore, a data protection impact assessment should be undertaken for processing that is likely to result in a high risk to individuals, for example if medical information or protected characteristics are involved.

A suitable staff training programme should be in place to ensure that staff are aware and are continued to be made aware of their individual responsibility when handling personal data.

Griffin can provide a policy guidance template which outlines what information would be expected to be included in a data protection policy, from a regulatory compliance perspective.

Managers: Griffin Managers
Regis House
45 King William Street
London EC4R 9AN
Telephone 020 7407 3588
Email griffin@tindallriley.com
www.griffin-insurance.co.uk

First Issued: January 2025