Data Protection Breaches & Compensation/Litigation – Issues For Consideration

Date : September 26, 2018

Introduction

Class-action litigation (technically called group action/group litigation in the UK) in connection with data protection issues is on the rise in the UK. Under class-action litigation individuals with similar grievances can come together against an alleged wrongdoer and in effect act through strength in numbers (sharing advice and documentation etc.) and reduce costs.

In the UK there have already been a few key data protection class-action cases, most notably the 2017 Morrisons case, which we have written and made a film about here http://www.corderycompliance.com/client-alert-morrisons-data-breach-litigation-succeeds/, and the 2015 Vidal-Hall case, which we have written about here http://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/.

Recent press reports about a purported data security breach concerning British Airways suggest it is by all accounts a very large breach as it is said to involve many individuals and transactions. It has also been reported that (given the scale of the breach) litigation lawyers very quickly sprung into class-action mode and sent a formal notification of intended legal proceedings to British Airways. This article sets out in very rudimentary terms some of the issues to consider when compensation is sought for data protection infringements.

Some technical terms are used in this note which are explained in our glossary here www.bit.ly/gdprwords.

What are the issues?

Issues for consideration include the following (which are by no means exhaustive):

1. The basis for compensation – GDPR (Article 82) provides for a right to compensation from a data controller or a data processor for damage suffered which can be claimed by anyone who has suffered material or non-material damage as a result of an infringement of GDPR;
2. The scope of damage – under GDPR the concept of damage is to be interpreted broadly and affected individuals should receive full and effective compensation for the damage that they've suffered; the types of damage that could be covered (in the UK) include financial loss, inconvenience and distress;
3. Exemption – under GDPR a data controller or data processor is exempt from liability if they can prove that they are not in any way responsible for the event giving rise to the damage in question – the burden of proof falls on the data controller or data processor to demonstrate that they are not responsible for the damage. A data processor is liable either where it has not complied with GDPR data processor obligations or where it has acted outside or against a controller's processing instructions;
4. Shared liability – under GDPR where more than one data controller or data processor, or both a data controller and a data processor, are involved in the same processing and where they are (as per GDPR) responsible for any damage caused by the processing, each data controller or data processor can be held liable for the entire damage in question. Where a data controller or data processor has accordingly paid full compensation for the damage suffered, that data controller or data processor can claim back from the other data controllers or data processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage;
5. Representation – under GDPR, in accordance with national law, a representative body (as per UK law) can bring court proceedings for compensation on behalf of an individual;
6. Location for proceedings – under GDPR court proceedings for compensation are to be brought before the competent courts under national law. Proceedings against a data controller or a data processor are to be brought before the courts of the EU Member State where the data controller or data processor is established. However, in the alternative, proceedings may be brought before the courts of the Member State of the habitual residence of the individual concerned; GDPR also allows for the suspension of court

proceedings where there are parallel proceedings in another Member State;
7. Limitations – compensation claims may be time-barred, in accordance with rules under national law; and,
8. Insurance – cyber insurance may cover compensation claims brought.

What is the takeaway?

The takeaway is to consider the preparations that you might make in case you are faced with a claim for compensation for a data protection infringement:

1. Make staff aware (including through training) of the risk that compensation claims can be brought not only where there has been malicious external activity such as a hack but also where internally staff have been careless e.g. by losing computer hardware. Also ensure that the board is aware of compensation claim risks;
2. Set up and undertake regular compliance audits or reviews in order to identify, rectify and prevent issues that could involve a compensation claim;
3. Check the liability provisions in vendor agreements and revise them where appropriate, and, check in a given situation if you might be a joint controller and if so clearly set out your responsibilities;
4. Check your insurance – policies should be reviewed to check that they provide the necessary cover for the full range of potential civil claims under GDPR;
5. Consider setting up an ex gratia compensation scheme, which can be deployed quickly; and,
6. In an internal investigation of a data security breach, where appropriate, ensure that legal professional privilege applies.

Cordery's Data Breach Academy can be an effective way of helping manage a data protection breach. There are details here: http://www.corderycompliance.com/cordery-data-breach-academy-2-2/. To find out more about the work we do in connection with data breaches and our four point plan, visit our website here: http://www.corderycompliance.com/dealing-with-a-breach/.

We report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/. For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.
- For more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com