Cyber and Information Law Newsletter: Issue 1 - Cyber and Data Breaches

Published 30 April 2019

The demise of success fees: taking back control of privacy claims

In a welcome move for defendants, the CFA regime for privacy claims finally caught up with the rest of the litigation world on 6 April. From this date, a solicitor's success fee under a new conditional fee agreement (CFA) will no longer be recoverable from the losing party in publication and privacy proceedings. The change is expected to lead to a reduction of purely speculative claims for data breaches made by "no win no fee" claimant solicitors.

The ancient regime

Since April 2013, a CFA's success fee has not been recoverable from the unsuccessful party for the majority of litigated claims pursuant to s.44 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 ("LASPO"). However, pursuant to S.I. 2013/689, there has been an exemption for CFAs in certain categories of claims, including "publication and privacy proceedings", which is defined as proceedings for "*(a) defamation; (b) malicious falsehood; (c) breach of confidence involving publication to the general public; (d) misuse of private information; or (e) harassment, where the defendant is a news publisher*".

Before removing the exemption for these cases, the government wanted to first decide whether to implement qualified one way costs shifting (QOCS), as recommended by the Leveson Inquiry in 2012. In the meantime claimant solicitors have been increasingly using the publication and privacy exemption that was primarily intended for media cases, by joining claims that were ostensibly for breaches of the Data Protection Act (1998 or 2018) with claims for breach of confidence and misuse of private information. The financial risk of having to pay a the claimant's success fee can often outweigh the merits and quantum of a modest claim and force settlement.

The new order

In November, the government finally passed legislation (S.I. 2018/1287) reforming the costs protection regime for publication and privacy claims. It concluded that a more pragmatic approach should be taken than QOCS. Instead, for new CFAs entered into from 6 April, the success fee will no longer be recoverable from the losing party. Concerns over the impact on access to justice may be slightly mitigated by the fact that claimants can still seek to recover after the event insurance (ATE) premiums.

For defendant parties, this reform is long overdue. From a data breach perspective, it is hoped that it will lead to a reduction in opportunistic small claims for technical breaches that tend to be disproportionately costly to contest. It remains to be seen whether the changes will increase the number of third party litigation funders who are already active in the data breach litigation space (see *Lloyd v Google [2018]*). We also look forward to seeing whether claimant solicitors will now start to solely bring claims under specific data protection legislation, as there is less incentive to join common law claims for breach of confidence and misuse of private information, which are derived from media and defamation cases where the legal principles do not always fit with data breach claims.

Spanish regulator releases guidance on GDPR notification thresholds

Earlier this month, Agencia Española de Protección de Datos (AEPD), the Spanish Data Protection Agency released an English translation of its 'Guide on personal data breach management and notification'. The document is designed to provide data controllers and processors with an action plan for dealing with personal data breaches and the tasks involved in mitigating or minimising negative consequences.

Most notably, the Guide contains the Spanish regulator's recommended method of assessment of data breach severity, for the purpose of compliance with Articles 33 and 34 of the General Data Protection Regulation (GDPR) – breach notification to the Data Protection Authority (DPA) and data subjects, respectively.

Calculating the Risk

The method of assessment is located in Annex III of the document. It operates by converting relevant factors and circumstances of the breach and personal data involved into a mathematical equation:

Risk (in %) = Volume of data x Type of Data x Impact (Disclosure)

The specific values are set depending on circumstances of the breach. Factors to consider include:

- Based on the number of identification records affected, the Volume variable is given a value of 1 to 5, the larger number of records, the higher the value. A value of 4 or 5 is considered to belong to a separate category, called **"qualitative circumstances"**.
- The Type of Data variable is assigned a value of 1 or 2, corresponding to non-sensitive and sensitive data, respectively. A value of 2 falls into **qualitative circumstances**.
- The Impact variable is assigned an even-number value, ranging from 2 to 10. The values of 6, 8 and 10 are labelled as **qualitative circumstances**.

DPA Notification?

In order to trigger an obligation to notify the DPA within 72 hours of the breach (Article 33 GDPR), the document suggests that the following minimum criteria should be fulfilled:

- Risk percentage has a value of 20 or more; and
- Two or more **qualitative circumstances** are triggered.

Data Subject Notification?

The Guide recommends the controller or processor to consider a notification to the data subjects in situations where:

- Risk percentage has a value of 40 or more; and
- Two or more **qualitative circumstances** are triggered.

It should be noted that unlike older breach assessment guidelines, this approach only classifies the data as sensitive/not sensitive, without further assessment of additional circumstances or characteristics of the data subjects or the data itself.

Comment

It is possible that the Spanish DPA's risk assessment method, especially where there is a low number of data records affected, without any further assessment, would produce results to which the UK Information Commissioner's Office (ICO) or the Irish Data Protection Commissioner (DPC) may not agree with. It is therefore important that if an organisation suspects that it has experienced a personal data breach, it carries out a data risk assessment that would satisfy itself and regulatory bodies that appropriate steps have been taken to contain the breach and notify affected individuals if relevant.

The full text of the AEPD's Guide can be accessed here.

Author

Aleksandar Dimitrov

Authors

Alexander Dimitrov
London - Walbrook
+44 (0) 20 7894 6443
adimitrov@dacbeachcroft.com