3PB's Cyber Law Series
Data protection claims: A guide for defendants

By Matthew Wyard
3PB Barristers

1. This is the second article in 3PB's Cyber Series. As the title suggests, this article provides an overview of the types of claims brought for breaches of statutory duty under the UK GDPR and the Data Protection Act 2018 ("the 2018 Act"), how to go about considering the merits of any claims that are issued, considers how to address issues of quantum and also offers some practical hints and tips for dealing with claims.

The types of challenges being faced

2. The challenges typically being brought are led by claims for breaches of statutory duty under the UK GDPR and/or the 2018 Act, most commonly relying on breaches of the following data processing principles found in Article 5 of the UK GDPR:
    a. A failure to process data lawfully, fairly and transparently;
    b. A failure to process data in accordance with the purpose limitation principle;
    c. A failure to process data in accordance with the data minimisation principle;
    d. A failure to process data in a manner that ensures appropriate security of data.

3. Additionally, claims may be brought for a failure to comply with the data subject's rights including: not facilitating their right of access, not erasing data when requested, continuing to process data when the data subject has objected to the same.

4. Alongside the aforementioned, to ensure that claimants are able to try and issue their claim in the High Court (Media and Communications List) and thereby increase their prospects of cost recovery, or otherwise to intimidate the defendant, concurrent claims in misuse of private information and/or breach of confidence tend to also be pleaded.

5. Some more astute claimants also plead breaches of Article 8 of the ECHR.

6. Unfortunately, many claimants (in my view wrongly) plead claims in negligence, despite there (presently) being no duty of care owed in tort for the processing of personal data under the data protection legislation (see *Smeaton v Equifax* [2013] EWCA Civ 108 and its application in the recent decision of *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB) for more information).

7. As well as civil claims, claimants also typically send copies of their pre action correspondence to the Information Commissioner's Office to see if it can attract regulatory action; helpful findings from the ICO would then be relied upon in the civil claim.

8. It is worth noting at this point that claims are not confined only to the types of large scale breaches that attract media attention such as the well published claim against British Airways. The types of situations in small scale claims that I have recently had to address in practise range from a non departmental public body sending an email to an incorrect email address and a former employee aggrieved at her disciplinary process being recorded without her express authority, up to claims involving detailed legal submissions on the scope of the right to rectify allegedly incorrect personal data.

9. The point to take away is that data protection claims can be brought against any type of company of any size and, when brought, are aggressively fought by claimants with a vast range of causes of action being relied upon. But, with the volume of unmeritorious data protection claims currently floating around, how does one identify a claim that needs to be taken very seriously, as opposed to a claimant simply 'having a go'. We now turn to consider how to evaluate the merits of claim.

The merits

10. There are two preliminary points worth noting when considering a claim.

    a. Firstly, funding. Most claimants proceed on the basis of a Conditional Fee Arrangement with their representatives, including counsel. This means that the legal representatives are at a risk of not being paid for their work unless they are successful. Where the particulars of claim are not signed off by counsel, this is a helpful tell that the claimant may not have been able to obtain counsel to act on a 'no win no fee' basis, generally because the merits of the claim were poor and counsel did not want to take the financial risk.

b. Secondly, insurance. The majority of claimants (particularly those proceeding on a no win no fee basis) will be required to purchase After the Event Insurance. Privacy claims (including those for misuse of private information) are one of the very few causes of action whereby you may be able to recover your ATE premium from the defendant if successful at trial. Helpfully, claimants are required to notify the court and the defendant if they have ATE insurance and intend to seek to recover their ATE premium. Where you are not notified that the claimant does not have ATE coverage, the claimant is at risk of having to cover the legal fees of a defendant if they are unsuccessful at trial. Therefore this can be a useful bargaining tool for defendants. Interestingly, the recent decision in ***Warren*** (See §6 above) may stand as precedent in future cases where there has been no positive conduct on the part of the defendant, that claims for misuse of private information and breach of confidence cannot be brought and, consequently, ATE premiums may not be recoverable where there is no legitimate privacy claim.

11. Once you have considered the above, or, if irrelevant because you are considering a letter before claim, you then need to scrutinise the alleged wrong doings.

12. In respect of claims for breaches of statutory duty under the UK GDPR / 2018 Act:

a. Generally, the facts of a data breach claim will be fairly straightforward unless there are technical issues regarding the security systems operated by the defendant. Defendants will need to take advice from IT forensics experts to identify the systems in place and how they were breached, as well as considering the reasonableness of their systems in the circumstances of their industry. Whilst it is for the claimant to prove that a defendant's information security systems were not up to scratch, defendants should involve their IT experts early in order to properly prepare its defence and, frankly, to get on top of a lot of technical detail.

b. Consider whether any statutory exemptions under schedules 2 – 4 of the 2018 Act apply to the circumstance of the data processing under scrutiny.

c. Causation raises significant arguments as there is very little authority on the point. There may be a defence to a claim where it can be demonstrated that despite having appropriate technical systems in place, it was not the fault of the defendant that the breach occurred. Similarly, the reason for the loss suffered may not have been caused solely by the breach itself, for instance, what action did the claimant take when they became aware of the data breach? Could prudent action on their part have alleviated any adverse impact of a system failure?

13. In respect of claims under Article 8 ECHR:

a. The first consideration is limitation. Unlike the majority of the other causes of action that are likely to be pleaded, the limitation period for a claim under the Human Rights Act 1998 is one year from the act complained of. If the claim is brought over a year after the incident allegedly giving rise to the data breach, then the claim may be time barred.

b. The second consideration, as claims may only be brought against public authorities (or other authorities serving a public function) is whether your organisation is a public authority, or was carrying out a public function giving rise to the incident. If not, then the claimant is unlikely to be able to bring such a claim.

c. The third consideration is whether Article 8 ECHR was even engaged in the processing of the complainant's personal data. Regard should be had to the extremely helpful 'Guide on Article 8 of the European Convention on Human Rights' published by the European Court of Human Rights as well as the jurisprudence from the same.

d. The fourth consideration is whether you have a statutory defence. The right to a private and family life is a qualified right, meaning that even if you have interfered with that right, you may have been entitled to do so. Consider whether the purpose of your interference was in the interests of (i) national security, (ii) public safety, (iii) the economic wellbeing of the country, (iv) prevention of disorder or crime, (v) the protection of health or morals, (vi) or for the protection of the rights and freedoms of others.

14. Regarding claims for misuse of private information:

a. Claims for misuse of private information are regularly poorly pleaded and fail to address all the fundamental elements. The first step therefore in defending such a claim is to ensure the claimant has pleaded all the elements as set out in the decision of *Campbell v Mirror Group Newspapers Limited* [2004] UKHL 22. In summary, to succeed in such a claim a claimant must demonstrate: (i) that there was particular information about an individual, (ii) that the individual had a reasonable expectation of privacy over the information (iii) that the disclosure of the information would give substantial offence to the person of ordinary sensibilities placed in similar circumstances.

b. If a claim is properly pleaded then your first step in defending such a claim is considering whether the information relied upon by the claimant was in fact information over which the claimant exerted meaningful control in the first place?

c. Whether or not the claimant had a reasonable expectation of privacy over the information must be scrutinised. For instance, is the information inherently private by being personal? Is the information in the public domain? Was the claimant in the habit of regularly disclosing the information themselves? If so, then the first element of the tort may be defendable.

d. The misuse relied upon is typically the disclosure of data or interference with the same. Whether or not the third element of the tort is met will come down to (i) whether the defendant has positively done something to misuse the information and (ii) the likely objective reaction to the act that has occurred. It must be analysed as such. If, for instance, the claimant is being particularly sensitive, then the claim is likely defendable.

e. Depending on the type of organisation or rationale behind disclosure, the defendant may (although it is rare in pure data breach claims) to be able to rely on the public interest defence.

15. In respect of claims for breach of confidence:

a. Similarly to claims for misuse of private information, claims are regularly poorly pleaded and fail to address all the fundamental elements. Accordingly, the first step in defending such a claim is ensuring the claimant has pleaded all elements set out in the decision of *Coco v A N Clark(Engineers) Limited* [1969] RPC 41:

   i. That there is relevant information;

   ii. That the information was confidential in nature;

   iii. The information was imparted to the discloser in circumstances importing an obligation of confidence; and

   iv. Disclosed in a way that was detrimental to the person who imparted it.

b. It must be considered again whether the claimant exerted meaningful control over the information relied upon in the first place?

c. There must be an allegation that the defendant has positively disclosed by the information. If there was no positive disclosure then the claim will potentially fall at the first hurdle;

d. The way in which, and reason for the disclosure of the information from the claimant to the defendant will need to be carefully considered to determine whether it was imparted in conditions that imposed confidentiality, for instance, was it through an employment relationship? Was it disclosed one on one?

e. The claim may be defendable if the information was disclosed in the public interest.

f. Has the claimant actually suffered provable detriment through the disclosure? If not, then the claim fails.

16. In respect of claims for negligence, as above, these can largely be taken as lacking merit in light of the caselaw mentioned at §6 above.

Loss and Quantum

17. Alongside determining the merits of a claim, a defendant also needs to know whether the claimant has properly valued their claim. As observed by a frustrated judge in a recent hearing I was involved in "claimants need to be able to identify a reasoned basis for the value of their claim" they cannot simply pluck a figure from the air. Unfortunately, calculating the quantum of a claim brought for breach of the UK GDPR / 2018 Act is one of the trickier aspects of such a claim as there have been very few authorities addressing the point.

18. As a general rule, the more causes of action successfully proven at trial, the higher the level of damages that will be awarded. For the purpose of this article, loss and quantum will be considered in relation to the breaches of statutory duty only.

19. Both material and non material loss can be claimed for breaches of statutory duty under the UK GDPR and 2018 Act, although the specific heads of loss and quantum will vary depending on whether the loss of data is personal data or commercial data.

20. Insofar as direct loss is concerned typical heads of loss can include:

a. Profit loss;

b. Distress and inconvenience;

c. Loss of control over the data;

d. Wrotham Park damages.

21. Insofar as indirect loss is concerned typical heads of loss can include:

a. Loss of the option to negotiate over the use of data;

b. Diminishment in the value of the data;

c. Loss of use option.

22. The heads of loss relied upon should be carefully analysed against the factual scenario being pleaded and, where appropriate, technical advice taken.

23. In terms of the actual value, as when calculating personal injury damages, one must rely on the level of damages previously awarded in factually similar cases in a bid to pinpoint a likely award. This can typically be argued down:

    a. In commercial disputes, where a claimant has failed to provide any proper rationale for valuing its data, a defendant can obtain the services of a data valuer. Experts in data valuation can use a range of techniques, surveys, simulations and modelling to determine the value of the data and, this can be considered alongside the claimant's value;

    b. Where your legal team has the technical know-how they may be able to identify the market value of the data on both the web and dark web;

    c. Damages for distress and inconvenience have to be calculated having regard to the pre-existing case law. Generally damages for distress and inconvenience are low, often below £1000;

    d. Loss of control can be calculated with regard to pre existing case law, or, with regard to the purpose that the claimant intended to use the data for and the reduction in value to that use i.e. if the claimant had been intending to sell data but it has now lost commercial value then it may be claimable as a loss of control rather than loss of profits.

Tips and tricks

24. Here are my top 10 tips and tricks for dealing with data protection claims:

    a. As soon as an organisation believes there may have been a data breach, speak to legal as well as your Data Protection Officer to ensure that a legal as well as factual analysis is undertaken. Many a claimant is spurred on to issue a claim due to unnecessary admissions of liability made before anyone with legal training considers the scenario.

    b. Connected with the above, do not make an admission of liability simply on the basis that there has been a *de facto* data breach. Proper scrutiny needs to be had to the nature of the information allegedly disclosed and whether there is any potential loss.

c. Do not allow claims to be issued and then left in the High Court. Where a claim is low value or could more conveniently be dealt with outside of the High Court, then apply when you file your Defence, to transfer the claim to the County Court.

d. Where claims are issued in the County Court, do not fall on your sword at the point of track allocation. Plenty of data protection claims, can and should properly be dealt with on the Small Claims Track.

e. Do not be persuaded into accepting the argument often run by claimants that *Lloyd v Google LLC* means that they are automatically entitled to damages by the fact of a data breach. Ensure you have regard to paragraph 43 of the decision and the impact of *de minimis* claims.

f. Where, as is becoming more commonplace, claimants are failing to properly plead causes of action for misuse of private information and breach of confidence, consider whether a strike out/summary judgment application in relation to those causes of action should be made

g. Similarly, when a misconceived claim in negligence is pleaded, strike out/summary judgment may be appropriate.

h. Where it becomes obvious that a claimant does not have ATE then consider a security for costs application.

i. Push the claimant in relation to the quantum of their case. Where they appear to have pulled a figure out of thin air, seek further information on their legal analysis or, alternatively, make good use of the part 18 procedure.

j. Where the claim is likely to turn on expert evidence, there is no reason your own internal IT teams cannot undertake a similar exercise to that which will be conducted by any jointly appointed expert, with a view to reaching their own conclusions and giving you the 'heads up' on any potential problems that may arise further on in the claim's life.

25. Some of the issues in this article are currently being considered by the Supreme Court in the case of *Lloyd v Google LLC*. Depending on when the judgment is handed down, it is hoped that either parts 3 or 4 of the Cyber Series will be able to consider its implications. If the decision has not been handed down by that time, part 3 will consider the future of regulation for artificial intelligence.

This document is not intended to constitute and should not be used as a substitute for legal advice on any specific matter. No liability for the accuracy of the content of this document, or the consequences of relying on it, is assumed by the author. If you seek further information, please contact the 3PB clerking team.

22 September 2021

Matthew Wyard

Barrister
3PB

0117 928 1520
matthew.wyard@3pb.co.uk

3pb.co.uk