DATA CLASS ACTIONS: THE THREAT TO BUSINESS

23 July 2020 | London
Legal Briefings

Our Data Class Actions team has today published an article about the future of class actions in the August 2020 issue of PLC Magazine.

The article first appeared in the August 2020 issue of PLC Magazine.

The article follows the Supreme Court's decision in Various Claimants v WM Morrison Supermarkets Plc (Morrisons) - the first class action following a cyber and data security incident to be heard in the English courts.

Cyber and data security remains a priority for business with some 80% of UK CEOs stating that they are concerned about the risk of cyber threats to their business.[1]

Cyber and data security incidents continue to occur with concerning regularity.

There is greater public awareness regarding such incidents, as the new regime of mandatory notification of personal data breaches introduced by the GDPR surfaces data processing problems that remained hidden previously.

Accordingly, the threat of class actions following cyber and data security incidents is very real.

This is particularly the case where the regulators have taken enforcement action, which is why it is prudent for organisations to put considerable effort into containment and reducing potential harm to individuals following an incident.

The last 12-18 months have seen several high profile data class actions being brought in the UK by groups of customers against businesses on the back of the UK Information Commissioner's notices of intention to issue multi-million pound fines, demonstrating the clear risk that exists and setting a precedent for similar claims in the future.

Our article explains that the decision in Morrisons is helpful in that it gives clarity to the circumstances in which vicarious liability will apply in data class actions. It also notes that one effect of the judgment is that data class action claims are likely to continue to be pleaded in a number of different causes of action, including data protection, misuse of private information and breach of confidence.

However it is important to remember that Morrisons was an atypical class action case in that the court found the business not to be primarily liable.

Most cases will turn on primary liability – and, in particular, on whether an organisation had appropriate technical and organisational measures to ensure a level of security appropriate to risk. Increasingly, organisations are seeking guidance on which failures in technical measures are likely to attract severe criticism from regulators. Accordingly, the article covers primary liability and causation – and summarises what the court has said about expectations in key areas such as deletion of data or employee monitoring.

The article considers quantum in data privacy cases, drawing upon the case law in other causes of action based upon the Article 8 right to private and family life and with a particular focus on "loss of control damages". Lastly, it considers whether class action claims will be brought using the group litigation order procedure or the representative action procedure, as was the case in Lloyd v Google.

HSF supports clients with cyber and data security incident response, as well as with measures to prevent cyber and data security incidents and in the many disputes which can follow such incidents, including class actions.

HSF will be writing a further article on the future of data class actions following the Supreme Court decision in Lloyd v Google, which is expected late this year/early next year and is likely to influence heavily the future development of data class actions.

The team can be reached at: dataclassactions@hsf.com

Contact us on cyberanddatadisputes@hsf.com for support on disputes following cyber and data security incidents, which are not class actions.

Our IP Conference session on disputes following cyber and data security incidents, including class actions can be heard here:
https://event.on24.com/wcc/r/2331505/79F4EBFE9178F894756298A83D702BF6

Our global contacts in case of cyber incident are:

Cyber.UK@hsf.com

Cyber.US@hsf.com

Cyber.EMEA@hsf.com

Cyber.APAC@hsf.com

---

[1]PwC's 23rd CEO Survey, published on 20th January 2020

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

KATE MACMILLAN
CONSULTANT, LONDON
+44 20 7466 3737
kate.macmillan@hsf.com

MIRIAM EVERETT
PARTNER, LONDON
+44 20 7466 2378
Miriam.Everett@hsf.com

JULIAN COPEMAN
PARTNER, LONDON, NON-RESIDENT PARTNER, HONG KONG, LONDON
+44 20 7466 2168
Julian.Copeman@hsf.com

CHRISTINE YOUNG
PARTNER, LONDON
+44 20 7466 2845
Christine.Young@hsf.com

TIM LEAVER
PARTNER, LONDON
+44 20 7466 2305
tim.leaver@hsf.com

GREIG ANDERSON
PARTNER, LONDON
+44 20 7466 2229
Greig.Anderson@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.