

A person wearing a blue suit jacket and a black watch is holding a brown leather briefcase. The briefcase has a gold-colored clasp and handle. The background is a light, textured surface.

# RADIUS LAW

Bulletin no. 62 | November 2020

[www.radiuslaw.co.uk](http://www.radiuslaw.co.uk)

## COVID

### COVID measures extended

The Government has [announced](#) extensions of measures to help businesses through the pandemic, including:

- the allowance for companies to hold AGMs virtually until 30 December;
- restrictions on statutory demands and winding-up petitions until 31 December;
- modifications to the new moratorium procedure, which relax the entry requirements to it, until 30 March 2021.

It's important to note, however, that the temporary suspension of personal liability of directors for wrongful trading has not been extended.

### Coronavirus Job Retention Scheme

The Coronavirus Job Retention Scheme (CJRS) has also been extended until March 2021. The level of support available under the extended scheme mirrors that available under the CJRS in August, with the Government paying 80% of wages up to a cap of £2,500 (although the % payable will be reviewed in January). Flexible furloughing is allowed under the extended CJRS, as well as full-time furloughing. The Job Support Scheme, which was scheduled to come into effect on 1 November, has been postponed until the CJRS ends.

### Business Interruption insurance

In September the High Court [ruled](#) on the Financial Conduct Authority (FCA)<sup>1</sup> case that sought clarification on behalf of business interruption insurance policyholders— following the insurers' refusal to pay out claims that arose from the pandemic. The Court only reviewed a sample of policy wordings and *agreed with the FCA on most issues*. Whilst each case will need to be decided on its own facts and circumstances this decision will be welcome news for most policy holders. This is not however the end of the story as an appeal to the Supreme Court is scheduled for four days commencing on the 16th November.

## Corporate & Commercial

### Supply chain due diligence

The need for improved supply chain due diligence was highlighted in Alison Levitt QC's recent independent report into the fashion giant, Boohoo. The report confirmed an earlier Sunday Times' investigation that revealed poor working conditions and low rates of pay at some of Boohoo's UK suppliers and inadequate corporate governance by Boohoo's management. The report identified that Boohoo's senior management had been aware of serious issues about the treatment of factory workers since, at least, December 2019.

This news will inevitably support the Government new plans to [strengthen the existing modern slavery reporting requirements](#). These include new compulsory contents of modern slavery statements and an obligation to publish the statements on a government-run reporting service.

In addition, the Government has [announced](#) that it is developing legislation that would require large businesses to audit their supply chains to ensure they are not using ‘forest-risk commodities’ that have been produced unlawfully.

## Data Security

### Controller, Joint Controllers and Processors

Data Protection law places different obligations on parties depending on whether a party controls or jointly controls how personal data is used or is simply processing personal data on behalf of a controller. Deciphering which obligations are applicable is sometimes difficult. The European Data Protection Board (‘EDPB’) has published [new guidelines](#) (available on the EDPB website) on these concepts to hopefully provide more clarity.

### Age Appropriate Design Code

The [Age Appropriate Design Code](#) came into force in September, although it does allow a one year transition period. It applies to organisations providing online services and products likely to be accessed by children up to age 18 and sets out 15 standards how they should comply with data protection law.

The Code expects organisations to:

- create an open, [transparent](#) and protected place for children when they are online;
- follow a series of [standards](#) when designing, developing or providing your online services where they are likely to be accessed by children;
- consider the [best interests of the child](#) when processing their personal data. The code applies to apps, connected toys and devices, search engines, social media sites and online games; and
- implement and use language that is clear and easy for children at different development stages to understand.

### Subject Access Requests

Individuals, with a few exceptions, have a right to access personal data that organisations hold about them. This right known as a Data Subject Access Request (DSAR) is a common headache for organisations, particularly when the requests are frequent and unclear. The UK data regulator, the Information Commissioner’s Office (ICO) has now published further [guidance](#) for organisations on how to deal with DSARs. The guidance runs to 81 pages, but we think there are three key points, as follows:

- Organisations must provide copies of the individual’s personal data within one month of receipt of the request. The guidance however clarifies that the clock can be stopped to seek clarification of the DSAR. Extensions of up to two further months are also allowed where necessary.
- Employers can only charge a ‘reasonable fee’ for the administrative costs of complying with a DSAR if:

- it is manifestly unfounded or excessive; or
- an individual requests further copies of their data following a request.
- While an employer must make genuine and extensive efforts to respond to a DSAR, it does not have to go so far as to leave no stone unturned. The DSAR requirements are subject to the principles of proportionality.

### **Cyber-attacks, big data fines and insurance**

Big fines have been issued against British Airways (£20m) and Marriot Hotels (£18.4m) following findings that insufficient security had allowed cyber-attackers to access personal data. Whilst the fines are big, they were slashed from the original fine notices of £183m and £99m respectively – due to new ICO methodology of calculating the fines, mitigating representations and the impact of the COVID-19 pandemic. Both businesses also face class actions from individuals whose personal data was compromised.

The BA [penalty notice](#) (available on the ICO website) is worth reading as it provides some helpful guidance on how organisations can ensure that they have appropriate security measures in place. It's also worth noting that the ICO has issued a [consultation](#) about the calculation of fines. This consultation closes on the 12th November.

These cases highlight that Cyber-attacks are common threats to all businesses, but cyber insurance is often overlooked by businesses mistakenly thinking that it will be covered by other policies. The National Cyber Security Centre (NCSC) has published guidance for organisations of all sizes who are considering purchasing cyber insurance.

## Employment

### **Equality Act - Gender fluid/non-binary**

A recent tribunal decision<sup>3</sup> has found that person who identified as gender fluid/non-binary is protected by the Equality Act 2010 and was awarded £180,000 compensation for discrimination that she had suffered.

### **Monitoring employees**

H&M has been fined €35m by the Hamburg Data Protection Authority for privacy violations that included extensive staff surveys that collected details of holidays, medical symptoms and diagnoses for illnesses. The information was used build a profile of the employees which was then used in making employment decisions. H&M has provided an [unreserved apology and explained that the staff will receive compensation](#).

Uber is also under the spotlight for employee monitoring. A claim brought in the Netherlands on behalf of Uber drivers is challenging whether Uber broke data protection laws which, broadly, prohibit decisions that have significant effects on individuals being made solely via automated processing. Uber is defending the claim by stating that its algorithm merely identified the suspicious

activity, with human managers then reviewing the evidence and making final decisions. Uber's case is however not helped by its own privacy policy, which states that it uses automated decisions to deactivate drivers suspected of fraud.

### **Liability for employees' actions**

In *Chell v. Tarmac Cement and Lime Ltd*<sup>3</sup>, the High Court held that an employer was not liable for a contractor's personal injury suffered in its workplace because of an employee's practical joke. This follows the Supreme Court's decision in *Morrison Supermarkets plc v. Various Claimants*<sup>4</sup> earlier this year that stated an employer is not liable for the acts of an employee if those actions are unconnected with any instruction given to the employee in connection with his or her work and did not in any way advance the purpose of his employer.

## **Upcoming events**

---

### **Brexit – Survive or Thrive? Learn how other legal teams are preparing**

Wednesday 11<sup>th</sup> November 10:15 to 11:00

*We will observe 1 minute silence at 11.00*

[Register Now](#)

### **The fight against Modern Slavery**

Tuesday 8<sup>th</sup> December, 10:15 – 11:00

[Register Now](#)



### Are you an in-house lawyer?

Do you want to share ideas, make connections or get inspiration from other in-house lawyers?

If so – join our in-house lawyer Slack group. [Register here](#), its free!

### Cases, laws, decisions referred to in this Bulletin

1	The Financial Conduct Authority v - Arch Insurance (UK) Limited and others. Case No: FL-2020-000018
2	Taylor v Jaguar Land Rover ET1304471/2018
3	Chell v Tarmac Cement and Lime Ltd [2020] EWHC 2613 (QB)

---

#### Disclaimer

Nothing in this Bulletin, or on the associated website, is legal advice. We have taken all reasonable care in the preparation of this Bulletin, but neither we nor the individual authors accept liability for any loss or damage (other than for liability that cannot be excluded at law).