COVID-19: PEOPLE: DATA PRIVACY ISSUES (GLOBAL)

31 March 2020 | London
Legal Briefings

In these unprecedented times, COVID-19 has forced organisations to quickly put in to place measures with the aim of ensuring both business continuity and the protection of employees. In many instances, this has involved increased processing of health data, in ways that were not envisaged a short time ago. Organisations across the globe are also asking employees to work from home. Given the timeframes involved and speed at which government advice and directions have evolved, data protection regulators are recognising the challenges involved (please see the related article here), yet a global pandemic is not a general waiver for privacy compliance.

Here we explore some of the data privacy issues that organisations should be considering as they adapt to the COVID-19 crisis. For more information about general people issues, please see COVID-19: People – key issues for UK employers.

COVID-19 RELATED DATA PROCESSING: KEY COMPLIANCE ISSUES

- *Lawful basis for processing for COVID-19 related activities*

For all COVID-19 related activities involving the processing of health data of, whether it be as a result of: (a) employees voluntarily informing employers that they have tested positive for, or are suspected to have, COVID-19; (b) employers proactively asking employees about their health; or (c) other preventative measures introduced by employers (e.g. body temperature scanning for access on to premises), a lawful basis for processing is required under both Article 6 and Article 9 of the GDPR.

Article 6: The Article 6 ground which many organisations are likely to seek to rely on will be the "legitimate interests" of the organisation or third parties (e.g. other employees), provided that a risk assessment is carried out to check that any risks to individuals' interests are proportionate. This should be documented in a legitimate interests assessment. It is, however, recognised that organisations are being required to respond rapidly to evolving guidance and it may not always be feasible to carry out such an assessment. Alternatively, an organisation may seek to rely on other lawful bases, such as:

- the processing is "necessary to perform the employment contract", if ensuring health and safety is a term of that agreement; or
- the processing is "necessary to comply with legal obligations", in relation to health and safety.

Article 9: As health data is considered 'special category data' under the GDPR, a lawful basis will also be required under Article 9 of the GDPR. It is likely that much of the processing will be necessary to carry out obligations in relation to employment law, insofar as it is authorised by Union or Member State law (Article 9(2)(b)). Other relevant grounds may also be "public health" and "preventative and occupational medicine", again in each case insofar as authorised by Union or Member State law (Articles 9(2)(h) and (i)). As you will note, this aspect of the GDPR is devolved to Member States, meaning that local privacy and employment laws will need to be reviewed to assess what specific measures may be permitted locally when processing health data.

In respect of the UK, the UK Data Protection Act 2018 provides for these conditions at Schedule 1, Part 1, but imposes additional safeguards. For example, if relying on the basis that processing is necessary to carry out obligations in relation to employment law, the organisation must have an "appropriate policy document" in place, which should:

- explain the organisation's procedures for securing compliance with the principles set out in Article 5 of the GDPR; and
- explain the organisation's policies as regards retention and erasure of personal data, giving an indication of how long such personal data is likely to be retained.

◦ *Disclosing COVID-19 employee-related information*

Where an employee has tested positive for COVID-19, an employer may wish to carry out 'contact tracing' amongst other employees, or alert other employees. However, unless it has the explicit and freely given consent of the employee who has tested positive, it should not be divulging the name of that employee to anyone else, although employers can still communicate that employees may have been exposed. The Information Commissioner's Office (ICO) has indicated that employers that inadvertently share too much information in a bid to protect employees' health will not be penalised, although the more cautious approach would not be to test this and to avoid disclosing the names of affected employees.

◦ *Proportionality and other considerations*

The personal data that is processed should be limited to only what is necessary for the purpose of the response measure the organisation is implementing and making decisions as to action required. All other relevant GDPR principles and obligations will also need to be kept in mind and complied with - for example, data minimisation, the updating of Article 30 records, and appropriate retention periods.

COVID-19: REMOTE WORKING ISSUES

It is not just the increased processing of health data that has raised data privacy issues. Many organisations are now asking their employees to work from home, some for the first time.

◦ *Security risks*

Organisations are still under an obligation pursuant to Article 32 of the GDPR to ensure that the personal data processed are subject to appropriate technical and security measures. This applies in a work from home scenario as much as in the office environment.

- **Use of personal devices:** Where employees have been asked to use their personal devices as part of remote working, this typically raises more issues as these will often lack the tools built in to business devices - such as strong antivirus software, customised firewalls, and automatic online backup tools. This increases the risk of malware finding its way onto devices and both personal and work-related information being compromised. Even for company-issued devices, organisations will want to consider how to manage updates where machines are not connecting to the company LAN.

- **Use of third party technologies:** As organisations are embracing the use of third party technologies to adapt to this new 'normal', we have seen the advent of apps to replace processes and functionality that are no longer readily accessible or available

to employees in a home environment – for example, videoconferencing apps, team communication apps, scanning apps etc. Questions are already being raised over the security of these apps, and the due diligence that organisations should take before permitting, or encouraging employee use, of these technologies. It may be that organisations only permit use of these technologies in limited circumstances. However, once again, given the speed of developments at the macro/governmental level, organisations are having to respond extremely quickly to a new set of security challenges.

- **BAU risks are magnified:** During this time, all the more 'traditional' risks are likely to be magnified. Employees are working at home, possibly having shifted larger than normal amounts of confidential documents from the office to home, may also be surrounded by others – whether it be flatmates, family or partners – and so this can pose a security threat. Devices should be locked when unattended, privacy screens used where possible, and phone calls or online meetings carried out somewhere they cannot be overhead, particularly if what is being discussed is business critical or sensitive information. It may also be tempting for employees to forward emails and documents containing personal data to a personal email address if working from home and having issues with company-provided devices or the remote network. However, strictly speaking, this could often amount to a personal data breach under the GDPR as an unauthorised disclosure of personal data (albeit likely not a notifiable one, depending upon the consequences of the employee doing so). As a result, communications with employees regarding use of technologies and devices etc is more vital than ever to ensure that individuals are not inadvertently opening up the organisation to additional risk.

◦ *Introduction of new technologies*

As we look set to be working at home for the foreseeable future, organisations may seek to introduce new technology for a host of reasons, e.g. to facilitate home-working, to monitor employees etc, which would likely involve the processing of personal data. However, as is always the case when introducing new technology that involves the processing of personal data, organisations should consider whether a data protection impact assessment is required. In the context of employee monitoring in particular, this could present issues around impact on the individual where it involves monitoring an employee at home, on a personal device, or possibly even a shared device.

COVID-19: DIRECT MARKETING

Nothing has changed with respect to direct marketing rules and what organisations may or may not do, but just a reminder that businesses should be careful not to include marketing information in COVID-19-related communications that it is entitled to send to individuals, e.g. service communications. This could amount to a breach of the ePrivacy rules to the extent any of those individuals have opted-out of receiving direct marketing. Although the ICO has made it clear that public health messages sent by the government, NHS and healthcare professionals will not be considered to be 'direct marketing' for ePrivacy purposes, this should not be interpreted as meaning that all messages relating to the COVID-19 pandemic will fall outside of the ePrivacy rules.

KEY POINTS FOR ORGANISATIONS

We recommend you take the following key steps when considering data privacy risks associated with COVID-19 processing activities and remote working:

- Ensure that measures implemented are consistent with current public health advice, to help inform what is proportionate.
- Carry out legitimate interests assessment or data protection impact assessments if required.
- Review employee use of unauthorised third party applications.
- Ensure that adequate IT security is in place to take into account remote working on a large scale and for a prolonged period.
- Update company policies on remote working if needed.
- Remind employees to be alert to security issues and of best practices and expectations to ensure secure working from home.
- Consider ad-hoc training for those roles that typically do not work from home.

KEY CONTACTS

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

MIRIAM EVERETT
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

CHLOE KITE
ASSOCIATE, LONDON

+44 20 7466 2540
chloe.kite@hsf.com

LEGAL NOTICE