& REBOUND REMODEL

C/M/S/ Law . Tax

The new normal for data subject rights of access – Prepare for increased data compliance risk

Much has been said and written about the 'new normal' for staff that have been largely working from home during 2020. But these changes in working practices also bring significant shifts in the way that businesses and their workforces collect and use personal data. Health data is now routinely collected by many employers. A huge range of instant messaging tools such as Microsoft Teams and Slack have in large part replaced face-to-face office discussions. These changes have important consequences for businesses' compliance with their data protection obligations, in particular data subject access requests (DSARs). The new working reality has without doubt increased data compliance risk and businesses should ensure that they remain ahead of the moving goal posts.

Why are DSARs important?

Data protection law entitles data subjects to request access to any personal data that an organisation processes about them. Organisations therefore need to be prepared to recognise and respond to any DSARs they receive from data subjects, including their own staff, in order to meet their statutory obligations. The Information Commissioner's Office (ICO) is increasingly flexing its muscles and businesses are well advised to avoid the regulator's crosshairs. Poor compliance with the rights of access regime can also have a detrimental impact on trust and confidence within the organisation as well as management of litigation risk.

DSARs are commonly raised by staff in connection with an employment dispute, often to obtain additional information about the way that they have been treated and to find out what information the employer is holding about them. They are a potent tool available to employees as data subjects, given the breadth of the right of access (with only limited exceptions entitling an organisation to withhold disclosure of personal data). Responding to a DSAR can be costly and time consuming to handle, even assuming they are undertaken correctly. If a data subject considers that has DSAR has not been adequately complied with, the individual can also complain to the ICO and/or bring a civil claim for damages.

The global economic outlook, coupled with widespread redundancies and increases in whistleblowing relating to health and safety and furlough arrangements, are all likely to result in an increase in DSARs. Those responsible for HR data protection compliance should therefore ensure they are ready to handle these in accordance with the ICO's expectations, which are set out in long-awaited detailed guidance published in October 2020.

Key considerations

- Prepare for a likely increase in DSARs, either in the context of redundancies or whistleblowing relating to health and safety and furlough arrangements.
- Undertake a data privacy impact assessment before looking to process any special category data, including health data.
- Update internal policies and practices on data security, retention and file structure to reflect changes in communication methods.
- Review DSAR procedures to ensure they are fit for purpose.
- Ensure the availability of appropriate technology to locate and identify, and securely transmit, personal data in response to a DSAR.

New types of data being collected

Issues that many businesses did not expect to be grappling with “pre-COVID” include: whether to take employees’ temperatures when they come into work; should staff be required to take COVID tests; what is the most appropriate way to share staff health data with the workforce; should staff be required to have antibody tests; should staff be required to disclose medical results; can management track staff while they are working at home; and, last but by no means least, can or should employers require staff to be vaccinated?

Where businesses are processing health data in any of the above new and unexpected ways, there are serious data privacy considerations. Special category data, which includes health data, has additional protections under data protection law and businesses must process this data with caution and prior planning. Businesses should therefore undertake a data protection impact assessment (DPIA) before looking to process any special category data, which would include an assessment of whether it has a lawful basis to process the data, a determination of how long the data should be retained and used, as well as consideration of the risks to staff in processing the data and whether those risks can be mitigated. If the business is satisfied that the processing can be undertaken, it is also important that it is transparent with staff about the processing activity by making sure staff are given a privacy policy or notice that describes how their data will be used prior to undertaking the processing activity.

New ways of processing data

The benefits of a telephone call rather than email or IM are never more prescient than when it comes to DSAR response planning. The volume of personal data now being collected and processed via MS Teams, Slack, WhatsApp and many other applications is mind-boggling. Whilst most communications are no doubt anodyne, these methods tend to encourage informality, which can in turn breed rudeness, or worse. Staff may also feel emboldened to make certain types of comments while they are sitting at home on their computer, rather than amongst colleagues in an office.

Given the fast pace of change in business operations and risk management in the course of 2020, many businesses may not have updated their internal policies and practices on data security, retention and file structure to reflect these changes in communication methods. All of this will make responding to a DSAR in the pandemic world significantly more complex and arduous. Organisations should therefore consider putting in place clear policies and guidance regarding the use of these communication tools, as well as implementing appropriate retention policies which will limit the volumes of data which may need to be searched for DSARs.

Ensure your best practices are up to date

Given the potential for an increase in DSARs (including more complex DSARs), businesses should review their DSAR procedures to ensure they are fit for purpose. The ICO updated guidance contains some useful recommendations for preparing for DSARs which includes the following:

- Make sure staff understand how to recognise and respond to a DSAR. You should also look to provide detailed training for the staff who will be handling DSARs;
- Revise or put in place clear guidance on responding to DSARs (such as a DSAR procedure). You should also ensure that you make the guidance available to staff who will need to respond to DSARs;
- Put in place a team that is able to handle DSARs. This should consist of more than one person in order to ensure you have resiliency (e.g. if one of the staff members is unwell or on leave);
- Review and update your asset registers to ensure you know where all personal data is stored, so that you can quickly identify where to locate data when you receive a DSAR;
- Make sure you maintain a log of all DSARs so that you can monitor how you are handling DSARs. The log may include details of what data was supplied, whether any data was withheld and what reasons there were for withholding data.
- Review and document your retention and deletion policies for personal data. As noted above, this can help reduce the volumes of information you need to search if you have implemented appropriate retention periods of the personal data processed in the business.
- Make sure that you have appropriate security in place to send the DSAR response to the data subject. In most cases, organisations will wish to respond to DSARs electronically, so you should ensure you have a secure method for transmitting the response (e.g. encrypted pdf or secure portal).

Another key consideration when responding to DSARs is ensuring that you have the appropriate technology in place to locate and identify personal data relating to that data subject. Whilst some of the data will be relatively easy to locate (e.g. the staff member's HR file), other data could be more challenging to find. This will include data held in email accounts and in communications tools such as MS Teams or Slack or on personal devices being used under a BYOD policy. Organisations should therefore ensure they have the necessary tools available to search and extract this information, as it can be extremely challenging to locate this information without the appropriate technology in place to assist with the task.

As with many aspects of data protection compliance, good preparation is key. The new working reality has without doubt increased data compliance risk and businesses should ensure that they remain in front of the moving goal posts. Taking steps to improve your processes and procedures for responding to DSARs will put you in the best position to meet your statutory obligations and manage the risks to your business.

Key contacts

Hannah Netherton
Partner, Employment
T +44 20 7067 3634
E hannah.netherton@cms-cmno.com

Duncan Turner
Partner, Technology
T +44 131 200 7669
E duncan.turner@cms-cmno.com

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

Further information, including a list of our offices, can be found at **cms.law**