PAUL HASTINGS

STAY CURRENT

April 2020

Follow @Paul_Hastings

COVID-19: Business as Usual for Data Privacy Compliance in the UK and the EU?

By Sarah Pearce & Ashley Webber

COVID-19 has undoubtedly already had a massive effect on businesses: it has affected how they operate, where they operate and, in some unfortunate instances, whether they operate at all. But has it affected how they comply with the law? Over recent weeks data protection regulators across the EU and the UK have communicated a fairly clear message: **it is business as usual as far as possible**. This message has been confirmed by the European Data Protection Board (the "EDPB") in its COVID-19 Statement:

"The EDPB would like to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects".

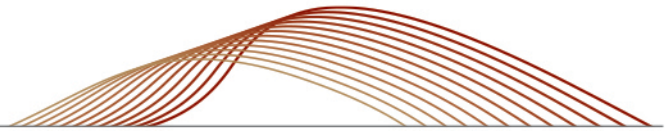
What reactions have we seen from regulators across the EU?

Across the EU, data protection regulators have been issuing statements, answering questions, posting articles, and otherwise acknowledging the effects COVID-19 is having, and will continue to have, on data privacy compliance within businesses. There are common threads of discussion amongst regulators, including the treatment of employee health data and the fact that the extenuating circumstances we all currently find ourselves in do not trump the principles of data privacy and, moreover, do not negate compliance with the law.

Employee health data

It is important to note that employment law matters are governed by each member state and are not regulated by European-wide data privacy legislation. That being said, employee data is also subject to data privacy legislation. Therefore, any acts by an employer that are deemed permissible under member state national employment law (for example whether an employer can dictate if an employee comes into work or not) must also be considered from a data privacy perspective if it means personal data of the employee is being processed when carrying out the particular act (for example if the determination is dependent on requesting the relevant employee provide his/her employer with health data).

The general consensus taken by regulators across the EU in relation to employee data is that whilst it may be reasonable to request employees notify their employers if they are experiencing symptoms and for the employer to take certain actions, such as requesting the employee not return to the office, the employers are still not permitted by law to collect and process disproportionate volumes of data about their employees and use it for purposes which are excessive and unnecessary in the context—this would wholly undermine the principles of the law.



Data principles remain in effect and require compliance

Věra Jourová (Vice President for Values and Transparency at the European Commission) reiterated the fact earlier this week during a discussion around surveillance and COVID-19. She was quoted saying: "*We definitely will not go the Chinese or Israeli way, where the use of these technologies to trace the people goes beyond what we want to see in Europe…Even in emergency situations the data privacy rules should be respected*". Jourová's stance is firm and clear—the laws continue to apply and should be complied with in the same way as they were before the outbreak of COVID-19. No doubt there then, it is business as usual when it comes to compliance with data privacy legislation.

Looking more closely at the data privacy regulators across the EU and the UK, we have highlighted below a few of the proactive statements and steps taken by regulators.

The United Kingdom

The ICO has been active in its response to COVID-19 and in doing so has developed a COVID-19 Information Hub. The Hub contains useful, high level information for both businesses (for example, with respect to requesting information from employees) and individuals (for example, a blog explaining the increase in online scammers relying on COVID-19 to access personal information), and encourages questions from those in need of clarification or assistance.

Of the ICO's guidance released so far, we highlight three key points of interest:

1. For those organisations that are able to initiate working from home procedures, data protection laws are not intended to bar that shift. However, businesses should ensure they have in place the same kinds of security measures as they would under normal circumstances. We discuss this point further below under "What should businesses be doing right now with respect to data privacy compliance?" in more detail.

2. There is express acknowledgement that if an individual has submitted a subject access request to a public authority, the response may be delayed due to such organisations diverting their resources to handle other challenges.

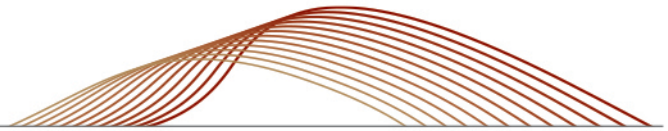
3. The ICO clarified that Government, the National Health Service and other such organisations do not require the consent of the individual to provide them with "vital public health messages". The ICO issued this guidance at about the same time that the Government started the process of sending a text message to each UK individual providing alerts about COVID-19.

France

The advice from the CNIL has been limited, to date, to the handling of employee data in the context of the existing data protection principles. The article from the CNIL largely follows the consensus explained above regarding employers' rights and obligations with respect to data privacy whilst also reinforcing the fact that employers should still act in accordance with the principles of data privacy laws.

Germany

Similar to the ICO, the Federal Commissioner for Data Protection and Freedom of Information in Germany has sought to prepare a central source of information on the effects COVID-19 is having on data privacy, whilst also directing readers towards their colleagues in the appropriate federal German states which handle data privacy (for example with respect to police powers).



The Commissioner has also expressed the view that data privacy compliance should not be completely outweighed in favour of the efforts to fight the pandemic, stressing that compliance with data privacy principles should still be a priority.

Sweden

The Swedish Data Protection Authority has created a similar repository for information relating to data privacy and COVID-19. The information in part operates on a "question and answer" format based on the most frequently asked questions, largely focusing on the employer and employee discussion. The information provided by the Swedish Data Protection Authority demonstrates the point raised above that the national employment and labour laws are key to shaping the employment relationship under the COVID-19 circumstances but that privacy laws are also important whenever personal data is being processed. For example, the Swedish Data Protection Authority acknowledges that, generally speaking, taking an individual's body temperature at work could be seen as a significant infringement of privacy. However, it also acknowledges that this potential infringement can still be deemed necessary and lawful as it may be necessary to allow employers to make the appropriate checks on their employees.

Italy

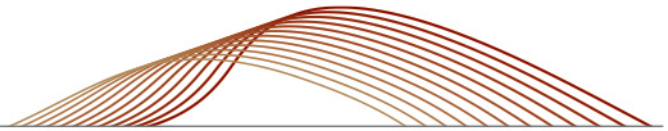
The Italian Data Protection Authority has published various statements, articles, and opinions over the past month on its website relating to COVID-19 which range from its views towards collecting employee data (discussed below) to its opinion on the first version of the draft decree relating to the delivery of electronic prescriptions. The Italian Data Protection Authority therefore appears to be taking a very practical approach by focusing on areas which are of great concern to both businesses and individuals and that have a key data privacy element.

Interestingly, on March 2, 2020, the Italian Data Protection Authority released a communication relating to the collection of personal data under the emergency legislation that had been adopted. The position of the Italian Data Protection Authority was clear—employers should refrain from collecting health data of employees relating to COVID-19 symptoms in "*a priori and in a systematic and generalized way*" or through specific requests to employees or unauthorized investigations carried out on employees. However, on March 14, 2020, the Italian Government and several trade unions signed a protocol which establishes specific procedures for fighting COVID-19 in the workplace. The protocol allows employers to subject their employees to proactive body temperature controls before entering their workplace (subject to certain requirements and restrictions). This of course cuts across the position taken by the Italian Data Protection Authority and in fact partially waives the restrictions imposed by it. The adoption of the protocol establishes a specific legal basis that supersedes otherwise applicable data protection principles.

So what do the reactions show us?

The reactions demonstrate to us that data privacy is not to be overlooked or ignored. Whilst it may not be "at the top of the list" of concerns during this surreal time, compliance with data privacy laws, and the internal policies and procedures of a business relating to the same, should still be a high priority.

The reactions also show us that the regulators do not wish to hinder any necessary acts required to combat COVID-19, so long as they do not undermine the principles of data privacy. The approach taken by certain data protection regulators is commendable as they have sought to adapt their rules and principles to a wholly unprecedented set of circumstances and are continuing to do so as COVID-19 develops.



What should businesses be doing right now with respect to data privacy compliance?

The simple answer to this question is BAU: businesses should be continuing to operate their business as usual with respect to data privacy rules, including complying with their established procedures and principles.

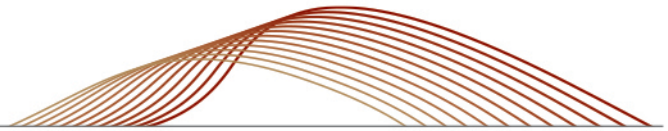
We have identified the following specific areas of data privacy compliance which we believe businesses should be conscious of as areas which are likely to expose businesses to greater risk during this time:

- **Security:** data privacy legislation requires businesses implement organisational and technical measures appropriate for their business to protect personal data against accidental or unlawful destruction, loss, alteration, and unauthorised disclosure or access. This obligation is in no way restricted to on-premises security—for example, in an office—and instead applies to the operations of a business wherever they may take place. Therefore, as many people in the world will today be logging into their work systems remotely, there is a responsibility on all businesses to ensure the personal data being processed is still secure. Remote working presents security risks in addition to those which usually exist—for example, if employees are using their own laptop, if they are working from a location which has other people present and, more generally, if the employees themselves carry out their role in a way which is different from how they would in the office.

  The law does not provide any allowances in respect of remote working and, as stated by the ICO, businesses "*need to consider the same kinds of security measures for homeworking that [they would] use in normal circumstances*". There are various ways a business can mitigate the security risks here, such as providing employees with clear guidance and procedures on remote working and monitoring the compliance with such guidance and procedures. Businesses should also ensure their systems are able to withstand a significant and likely unusual portion of the business accessing them remotely.

- **Timeframes:** certain obligations under data privacy laws contain specified timeframes for compliance—for example, in respect of reporting a personal data breach or complying with a request from a data subject to exercise a right. Whilst we may find in coming months that regulators choose to look leniently upon businesses which do not comply strictly with the timeframes because of COVID-19, we encourage those businesses which are still able to comply with the timeframes to do so. For certain businesses, resources will be significantly strained at this current time and therefore it is inevitable that timeframes in all areas of the business will be extended and deadlines will be missed. However, if a regulator were to investigate a breach or complaint that in part related to a missed deadline even once the pandemic has subsided, it will not look kindly upon a business which actively chose to take a slower approach than was necessary. In addition to encouraging compliance, we also recommend keeping an open dialogue, where possible, with any data subjects that have submitted rights requests.

- **Customer communications:** the recent month has seen a surge in customer communications related to COVID-19. Whilst many contain a well-wished message from the CEO, for example, businesses should still be aware of their regulatory obligations with respect to electronic communications and, before carrying out any mass communications, review their proposed approach in light of the legal requirements.



New forms of processing: for those businesses which have been able to continue to operate, there is a high chance that during the coming months, a new product or simply an internal procedure or process will be implemented which requires a new data processing activity to be undertaken by the business e.g. the implementation of a new data storage method. It is important that this new activity is treated in the same way it would have been before COVID-19 because the risks to personal data will still exist, and may even be more prevalent given remote working and the pandemic. It may, for example, be appropriate for a business to complete a data privacy impact assessment and/or a legitimate interest assessment. Businesses should also not postpone such tasks as the result will be backlog to complete once normality starts to resume.

- **Continual obligations:** there are certain provisions under data privacy laws which require constant attention and action, such as keeping records of processing up to date. It may be that compliance with such obligations do not create the most headlines or breach statistics, but they are key to maintaining the compliance of a business with data privacy laws and therefore should not be overlooked.

- **Enforcement:** whilst it is acknowledged that regulatory authority resources may be stretched during this time, it is crucial that businesses do not rest on their laurels based on the perception that enforcement will stop while the crisis is ongoing—this will simply not be the case. Regulators are duty bound to investigate breaches and complaints and will therefore continue to comply with their obligations to the best of their abilities. It is worth noting that the Swedish Data Protection Authority have published their notice of intent only very recently in March to fine Google approximately €7million.

What will businesses be able to take away from this experience?

We are still very much in the midst of the mayhem and it is difficult to predict possible outcomes for businesses or prepare an exhaustive list of lessons to be learned. That being said, we are already starting to identify key aspects businesses should consider when normality shows even the slightest sign that it might begin to resume. These include:

- Were your security measures sufficient to handle the majority of your staff working remotely?

- Were your procedures with respect to complying with data privacy obligations efficient?

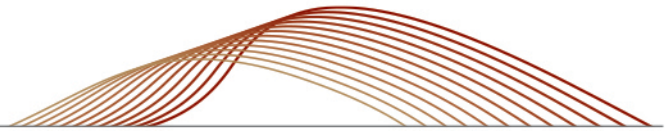
- Were your privacy policies reflective of additional processing that had to be undertaken due to COVID-19?

- Did your staff know their rights and your rights in respect of their personal data?

These are, of course, only a selection of areas that will be relevant to consider when the time comes.

While we wait for that time, and likely unearth other areas of data privacy which may be affected by COVID-19, the message to businesses in the UK and the EU is clear: compliance with data privacy principles and laws still needs to be a key consideration for businesses, to the extent possible—meaning it is, in fact, business as usual for data privacy compliance.

✧ ✧ ✧



If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings London lawyers:

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Ashley Webber
44.020.3023.5197
ashleywebber@paulhastings.com