Client Alert: Coronavirus (COVID-19) & Data Protection FAQs

Date : May 7, 2020

We first sent out this alert on 9 March and we're updating it with some announcements from regulators in other countries and with some of the questions we've been asked by our clients.

There are some data protection specific terms in this note which are explained at www.bit.ly/gdprwords

What is the issue with employees?

It seems that a number of organisations are asking third parties to help manage employee health. This might involve using third parties to do health screening, analyze travel records or installing apps asking employees to input their data for analysis. In some cases organisations are not doing their usual supplier due diligence to enable them to respond quickly.

As a reminder health data is special category data under GDPR Article 9 (it was called sensitive personal data prior to GDPR). So handling health data requires special care under GDPR. There are a number of ways to legitimize the handling of health data but most of these possible bases are subject to a necessity test. Necessity means what it says – some apps or third party providers offer ways of processing which are convenient but there may be less data protection intrusive alternatives.

Can't we just rely on consent?

Some employers seem to be seeking to rely on a data subject's consent but in an employee/employer context consent could be problematical (essentially because of the inequality of bargaining power) and it can be withdrawn. As a result consent will not always be the best solution.

What are regulators saying?

It is important to remember that for EU countries whilst GDPR sets out a basic framework local law can differ even within the EU. It is also important to stress that guidance from regulators is just that – we can expect to see litigation and the courts may not follow that guidance. For example an employee disadvantaged as a result of data processed relating to their health may well contemplate litigation alleging that data processing was unlawful. There is a special risk of exercise of GDPR rights from employees who have been furloughed or let go.

Some regulators expressed concern about the action of employers quite early in the spread of the virus. For example on 2 March 2020 the Italian DPA published guidance in both English and Italian. Their guidance made it clear that the primary responsibility for collecting health data relating to the virus is with the public health authorities and not with employers. It said:

"*employers must refrain from collecting, in advance and in a systematic and generalised manner, including through specific requests to the individual worker or unauthorized investigations, information on the presence of any signs of influenza in the worker and his or her closest contacts, or anyhow regarding areas outside the work environment*."

Since then regulators in other countries have also issued statements. In Austria the DPA has issued a reminder that even a step like taking mobile/cell phone numbers from employees could have data protection implications. There are links to some announcements and guidance from DPAs in alphabetical order at the end of this note.

The Chair of the EDPB has also issued guidance at an EU level which you can read here https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en. The EDPB itself followed that up on 19 March with its own guidance - https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

In most cases where GDPR applies a Data Protection Impact Assessment (DPIA) will be required. Impact assessments are not just confined to the EU however – on 27 March 2020 the Australian data protection authorities said they would also like to see an assessment, and even where it isn't legally required an assessment is generally good practice.

What about working from home?

Many organisations are now asking employees to work from home – some for the first time. It is important to remember that there are compliance implications here too. Businesses have to take appropriate technical and organizational measures (TOMs) under GDPR to secure personal data. That will include securing the personal data of customers and other employees as well. If you are asking or permitting employees to work from home you will have to make sure that you have the right protections in place for personal data both at the employee's home and in transit. A recent Danish case for example (here https://bit.ly/2QJjiel) shows that regulators expect organisations to make sure data is secure even when it's being worked on outside the company's offices.

If employees are being asked to work on their own personal devices rather than the company's this can have security and data protection implications too. For example we have had cases in the past where DPAs have intervened after home security software backed up sensitive data into the cloud. There's an example here https://bit.ly/2vH8dmM. Some software vendors are offering software without charge which might help – see for example TrendMicro here https://resources.trendmicro.com/Work-From-Home-Assistance-Program-UK.html and Cisco here https://www.cisco.com/c/en_uk/solutions/collaboration/working-from-home.html.

Again a DPIA can be useful. We have also had experience of doing specific training for working from home and we have produced fact sheets reminding employees of some of the most common security risks – something like a 10 top tips sheet or a short film can get the message across quickly and effectively.

You might also want to check your insurance provisions - some cyber insurance policies have different requirements when data is processed on an employee's home device. There may also be obligations to notify insurers if working from home presents additional risk.

Be aware of the fact that different employees may require different security measures – for example someone with network administrator rights may require extra security around their access.

What about hard copy data?

Remember its not just about IT security – if employees are working on hard copy documents you might also need to think about things like shredders and lockable cupboards to keep documents safe. We've worked on a significant breach for example which was caused by an opportunistic criminal entering through an open window. You might also want to look at providing guidance on where employees will work – ideally so that documents can't be overlooked by flatmates for example. The Polish DPA issued specific guidance on 4 May 2020 on the use of hard copy documents when working from home. That guidance said (in our unofficial translation):

"Employees during remote work may process personal data only for purposes related to the performance of their official duties and must ensure the security of personal data by observing internal policies and other procedures adopted in this regard by the employer. Employees may not arbitrarily take out paper documentation outside the data processing area specified by the employer. The employer must implement appropriate procedures and technical and organizational measures so that employees have sufficient awareness and tools to comply with the provisions on the protection of personal data."

The Polish guidance goes on to describe the steps a data controller will need to take where hard copies of personal data are necessary. In addition to the points which we've mentioned that guidance includes:

1. ensuring that the removal of hard copy data from the office is recorded
2. making sure that the documents aren't kept outside the office for longer than is necessary

Again a DPIA can be useful even if it is not mandatory.

Is phishing a worry?

Phishing attacks are on the rise and employees at home might be especially vulnerable. We've expressed concerns before that a lot of 'off-the-shelf' phishing training is not fit for purpose. It's important to make sure employees are trained and that they have regular reminders. Organisations using Office 365 may be especially vulnerable at this time. We've looked at the additional risks with ransomware here https://bit.ly/cvransom.

Can I monitor people working at home to make sure they're working?

This is an area that requires careful handling. Even things like home IP addresses can be personal data – it's very hard to monitor employees on a truly anonymised basis (for definitions of anonymisation and pseudonymisation see www.bit.ly/gdprwords). Occasionally location data could also expose special category data – for example where it identifies the individual as being part of a particular religious community. If you don't intend to monitor staff make sure your software is configured correctly – for example applications like Office 365 and Zoom can provide productivity data unless you turn this feature off. Again it's very likely that you'll need to do a DPIA and to take proper advice. You may even need to inform or consult with works councils if monitoring is taking place.

What about communications with customers?

The normal rules apply for communications with customers. Be careful about advertising or marketing messages being included in virus-related communications. This might make the message unlawful and some customers won't like it. We understand that complaints have already been made to DPAs about this.

If you need a customer's details (for example to process a cancellation refund or to check visitors when they come on site) be careful what you ask for and follow the 6 GDPR principles when processing that data. Be especially careful when taking decisions about customers based on data you are processing on them. For example we are hearing that some financial services organisations are being encouraged to collect large amounts of data from customers to decide who is an 'at risk' customer. Again work like this is likely to require a DPIA and consent will usually not work to justify processing.

Be wary of monitoring customers too. For example some applications check the accessing IP address to make sure there are no intellectual property infringements. You'll need to be careful how you do this if you're used to collecting business IP addresses and you're now collecting home IP addresses instead.

What if I am a data processor?

Data processors must also comply with data protection law. They will need to be careful about making their own decisions on data processing (for example by changing the processing location to the homes of remote workers) as that might breach the contract they have with the data controller and could also make them a data controller in addition if they then determine the purposes and means of processing. Similar considerations can apply outside of the EU – for example the Serbian DPA's guidance makes this point too.

What can we do to minimise risk?

To minimise risk it is important to consider a number of things including:

1. **Look at simple communications to employees etc. –** for example a 10 Top Tips document might help.
2. **Do detailed due diligence into any possible provider -** who are they? Where will they hold data? Are they prepared to enter into an appropriate written agreement to help you meet your GDPR obligations?
3. **Minimize the sharing of data –** consider who health data needs to be shared with and the measures put in place to keep health data confidential and secure. Recent cases (see e.g. the Doorstep Dispensaree case here http://bit.ly/gdprdoor) have told us that even healthcare professionals often do not take as much care with data as they should.

4. **Only process the data you need** – there's a distinction between data which is 'nice to have' and data which is necessary. Make sure you can justify all of the data you hold. There's likely to be a particular problem with location-based data especially if this is being collected without proper notice to an employee (for example by geo-location from a mobile/cell phone or laptop).
5. **Do a Data Protection Impact Assessment (DPIA) -** it is likely that in many circumstances a DPIA will be mandatory to comply with your GDPR obligations and even if it isn't its likely to be a good idea. DPIAs have been in the news in the last few months given the Irish DPA's raid on Facebook for a DPIA (see http://bit.ly/faceraid). There's a 3 minute film with some tips on the DPIA process here http://bit.ly/dpiafilm. Any responsible provider should be able to help you with the DPIA.
6. **Look at your transparency obligations –** if you are collecting health data on employees or visitors to your premises how will you tell them that? How will you tell them how the data will be processed? How long will you keep the data for? If you're using new ways of connecting like Zoom or Microsoft Teams are they covered in your privacy policies?
7. **Keep up to date –** DPAs are changing their advice or clarifying it on an almost daily basis. Make sure you are following the latest guidance. Under GDPR a Data Protection Officer (DPO) must be provided with sufficient resources to fulfil their obligations and DPOs are expected to have expert knowledge of data protection law. These are tough times for a DPO but the law requires them to have the resources to do their job.
8. **Consider your wider compliance obligations -** for example some countries like China also have specific laws which may place obligations on you. Do you have a process in place to make sure you can fulfil your legal obligations? How would you handle a request from government for data relating to your employees or visitors to your promises?

More information

There is more information about DPIAs and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav

You can read guidance from DPAs here (note that some countries have issued multiple guidance notes):

- Australia - https://bit.ly/2Jg4mQP & joint statement re impact assessments here https://bit.ly/2xE3IK3
- Austria - https://www.dsb.gv.at/informationen-zum-coronavirus-covid-19-
- Belgium - https://bit.ly/2QIPMoO
- Bulgaria - https://bit.ly/3bFW8gP
- Croatia - https://azop.hr/aktualno/detaljnije/obrada-osobnih-podataka-o-zdravlju-u-kontekstu-izvanredne-situacije-izazvan
- Czech Republic - https://bit.ly/39ETZRn
- Cyprus - https://bit.ly/2UPBvYY
- Denmark - https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/gode-raad-om-hjemmearbejde/
- Estonia - https://bit.ly/3azN650
- Finland - https://bit.ly/3a6lLHt
- France - https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles
- Germany - https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/07_Empfehlungen_Datenschutz_Corona.html (note this is from the Federal DPA. Some individual DPAs have also issued guidance which should also be checked depending on your operations).
- Gibraltar - https://www.gra.gi/data-protection/data-protection-and-coronavirus-what-you-need-to-know
- Greece - http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=245,159,191,237,221,64,110,214
- Guernsey - https://bit.ly/2wUV9dT
- Hong Kong - https://www.pcpd.org.hk/english/media/media_statements/press_20200211.html
- Hungary - https://bit.ly/2WG9Z2k

- Iceland - https://bit.ly/2UAfwGp
- Ireland - https://dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19
- Italy - http://bit.ly/virusitalia
- Japan - https://bit.ly/2X8nfgu
- Jersey - https://bit.ly/2UKXxf6
- Latvia - https://bit.ly/2wvAuwV
- Lithuania - https://www.ada.lt/go.php/lit/Eng
- Luxembourg - https://cnpd.public.lu/en/actualites/national/2020/03/coronavirus.html
- Malta - https://bit.ly/2Jr73im
- Mexico - https://bit.ly/3dYMpUW
- Netherlands - https://bit.ly/3ah0pqT
- New Zealand (specific to hospitality but with some good general points) - https://bit.ly/2QAaBCU
- Norway - https://bit.ly/2UlbOPH
- Philippines - various guidance notes are available – there is a mini-portal here https://bit.ly/3bTA2HL
- Poland - https://uodo.gov.pl/en/553/1103
- Romania - https://bit.ly/2JAln89
- Serbia - https://bit.ly/2wWUSai
- Singapore - https://bit.ly/35aYli9
- Slovakia - https://bit.ly/3aLMBVq
- Slovenia (includes opinions as well as guidance) – the mini-portal with various resources is here - https://bit.ly/2QI6Ziq
- Spain – there are now different guidance notes in Spain dealing with different considerations – you can see some of the guidance here https://bit.ly/3dvNumK
- Sweden - https://bit.ly/2U6oMSo
- Switzerland - https://bit.ly/2QGqyHM
- UK - https://bit.ly/3brHN7z. The UK has also revised its enforcement strategy which we have summarised here https://bit.ly/icocovid

Cordery has helped organisations large and small with DPIA tools, templates and training. There's a short film on doing DPIAs here http://bit.ly/facedpia.

There is up-to-date information on health measures being taken around the world on the Elsevier portal - https://www.elsevier.com/connect/coronavirus-information-center. In addition John Hopkins University has figures on the current number of infections around the world - https://bit.ly/39kctX3

Please note that we're trying our best to keep this note up-to-date but to state what should be obvious: Events are moving quickly and you should not act or refrain from acting on the basis of anything in this note. Proper legal advice should be taken. We're also providing links to third party software in an effort to help organisations cope with the crisis. We have not completed a technical analysis of these products and the inclusion in this note should not be taken as an endorsement or some sort of guarantee that these products will meet your needs.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1784
jonathan.armstrong@corderycompliance.com

Andre Bywater
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1785
andre.bywater@corderycompliance.com