COVID-19: Data Protection Checklist

March 13, 2020

The coronavirus outbreak has now been labelled a pandemic by the World Health Organisation. Many organisations have been taking active measures to contain the virus by asking staff to be vigilant for symptoms and sending staff home in the event of positive tests. Inevitably, this involves the capture and use of a new tranche of special category data under GDPR.

At the same time, COVID-19 will result in increased levels of home working. In addition, diverting resources to deal with COVID-19 may have an impact on data protection practices (for instance, on the timeframes for responding to data subject requests or complaints).

Here is our checklist of issues to consider:

- What is the status of COVID-19 data?
- Be proportionate
- Shred it when you are done
- Do not compromise security
- Do the thinking on conditions for processing
- Update records of processing
- Check the local rules across your footprint
- Other issues
- ICO Guidance

What is the status of COVID-19 data?

This is likely to include information about individuals who have travelled to/from certain places, have symptoms or who have tested positive (or negative). It may also include information as to which employees have been sent home to self-isolate and/or which visitors have been denied access to your premises. This will all be personal data under GDPR. Much of it will also be "data concerning health" as this refers to the physical health of a natural person including data which reveals information about health status. In other words, this is also likely to be special category data under Article 9, GDPR. This means COVID-19 data is high risk and needs special protection. **Check your privacy notices.**

You need to make sure that employees, staff, their dependants and office visitors are informed as to the purposes of

processing, legal basis and other requirements of Article 13, GDPR. This may already be covered in the HR privacy notice, but check this. If you collect information about non staff (e.g. visitors), the information could be provided on forms used to collect the data or perhaps with a link to the website privacy notice.

Be proportionate

The information should only be used for necessary purposes such as managing the immediate health risk and making decisions as to action required. Depending on insurance cover, it may be necessary to retain some of this information for insurance purposes and this should be considered in advance. It would also be useful to have a protocol/guidance for recommended actions given particular risk scenarios – including who gets notified in the event that someone tests positive. This will require a balancing of the interests of the individuals and the organisation. The situation may change quickly as the situation unfolds. Therefore, this needs to be kept under review. In addition, only the minimum amount of information should be collected to comply with the principle of Minimisation.

Subsequent processing for related purposes, such as lessons learnt about planning, management and business continuity matters, should be carried out with genuinely anonymised data to the extent possible. If the processing of personal data is required, then you should satisfy yourself that the purposes are compatible with the original purpose.

In carrying out necessity and proportionality assessments, balancing the processing against the interests of the individuals and deciding whether to process and/or share data (see below), organisations should apply legal and business common sense. Employee privacy is, of course, a matter of great importance, but it is not an unlimited right and needs to be balanced against other duties, rights and interests, such as the employer's health and safety obligations, duty of care and responsibility to ensure business resilience and continuity. These considerations are underpinned by public health considerations. Clearly, these matters should be factored in when making data collection and processing decisions. Good intentions, careful thinking (and documentation of the decision-making process) and coordinated implementation are recommended. We expect that EU data protection regulators, or at least some of them, will support this approach – see, for instance, the UK ICO's guidance of 12 March 2020 here.

Shred it when you are done

Test/health status data should only be used for these purposes and retained for the period necessary to identify risk scenarios and to take immediate action. You can retain the data to follow up with those who have tested positive to ensure they have appropriate support and know when they should self-isolate and when it is safe to return to the office – and also if retention is necessary to comply with legal obligations. If some of this information is generated in hard copy (visitors' confirmation that they have not been exposed to the virus), this may make shredding more important. However, once the purposes are fulfilled, you should shred or delete it.

Do not compromise security

This information (as with all personal data) should be processed and retained securely in line with good practice. This also means that guidance and protocols on what should be collected and who gets to see it will be very important.

In addition, the increased levels of home working mean that now is a good time to review your home working policy and remind members of staff of what they are expected to do to continue working securely away from the office. Ad hoc training may be required for roles that are not normally performed from home.

Do the thinking on conditions for processing

GDPR requires you to identify certain conditions for processing. As this largely concerns HR data, consent will not usually work. This is because there may be no genuine choice for an employee as to whether to provide data about tests data/symptoms.

Under Article 6, GDPR, you can likely rely on legitimate interests, provided the collection and use of this data is legitimate, necessary and strikes a fair balance between the interests of the individual and the organisation. This should be recorded in a Legitimate Interests Assessment and fed into any protocols and guidance for how the organisation responds. Alternatively, there may be opportunities to rely on the fact that the processing is necessary to perform the employment contract (on the assumption that ensuring health and safety is either an express or implied term of that agreement), that the processing is necessary to comply with legal obligations (again relating to health and safety) or, in extreme cases, that the processing (e.g. sharing information with a healthcare professional) is necessary for the individual's vital interests. Vital interests are, however, only relevant in cases of an emergency.

As the data is also likely to be special category data, you also need to find a condition for processing in Article 9, GDPR. Again, explicit consent will not necessarily work given the context. However, it is likely that much of the processing will be necessary to carry out obligations in relation to employment law (Article 9, paragraph 2(b)). There is a mirror condition available under Schedule 1, Part 1, paragraph 1(1)(a) of the Data Protection Act 2018. This is a UK law that fleshes out certain requirements of GDPR as authorised by GDPR. As we are in the Brexit Transition Period, these GDPR/UK rules continue to apply as they did before. However, the UK rules impose certain additional requirements as follows:

- the controller must have an "appropriate policy document" in place. This should explain procedures for securing compliance with the principles set out in Article 5, GDPR, the policies as regards retention and erasure of personal data, giving an indication of how long such personal data is likely to be retained;
- the controller must also retain and review/update this policy document during the period of processing and for six months from the point when it ends.

Please note there are other conditions for processing by healthcare professionals which are not addressed in this note.

Update records of processing

Under Article 30, GDPR, controllers (and processors) are required to have records of processing with prescribed details. These should be checked to ensure they cover COVID-19. Specifically, for the UK, the Article 30 records should specify the DPA 2018 condition relied upon, the Article 6 condition for processing and whether the personal data is retained in accordance with the relevant retention schedule (or the reasons if not).

Check the local rules across your footprint

Other additional rules may apply according to local law in other member states. You should check the position on local rules and approach them with a proportionate and pragmatic mindset, especially if you are trying to achieve consistency of approach and efficiency across jurisdictions.

Consider doing a Data Protection Impact Assessment (DPIA)

One way to ensure that all GDPR and data protection rules have been considered is to conduct a Data Protection Impact Assessment (DPIA). This is because the data involves employees (a vulnerable group) and special categories of data (higher risk data). For large organisations with large numbers of employees, a DPIA is likely a mandatory requirement.

Other issues

Any sharing of COVID-19 data with vendors or suppliers should be subject to Article 28 processor clauses in the normal way. In addition, if the information is to be shared with entities outside the EEA (for these purposes, "in the EEA" includes the UK as we are in the Transition Period) then an appropriate export solution would be required. This would typically be Standard Contractual Clauses and would also apply intra-group.

If data sharing is necessary on a controller-to-controller basis (for example, with medical services, healthcare providers or public authorities (such as public health organisations)), carry out proportionate due diligence.

If, as a result of COVID-19, there is an impact on your data protection practices, do take all steps you can to manage or mitigate the adverse impact. For instance, if a delay in responding to a Data Subject Access Request is genuinely unavoidable because of COVID-19, write to the requestor and explain this to them.

ICO Guidance

The ICO has just published helpful guidance on these issues and makes the following points:

- it recognises the unprecedented challenges we are all facing and that data protection will not stop you sharing information quickly or adapting the way you work. It is about being proportionate. If something feels excessive from the public's point of view, then it probably is;
- it appreciates that the usual practices and standards (e.g. responding to rights requests) may take longer during the pandemic;
- there is no barrier to increased and different types of home working. You just need to think about the appropriate kinds of security measures required in the usual way;
- it is acceptable to tell staff that a colleague may have tested positive. You should keep staff informed about cases in your organisation. However, you do not need to name the individuals and you should not provide more information than necessary. In addition, you have an obligation to ensure the health and safety of your employees;
- it is reasonable to ask people to tell you if they have visited a particular high-risk country or are experiencing virus symptoms, but do not collect more information than you need.

Your Key Contacts

Nick Graham
Partner, London
D +44 20 7320 6907
M +44 7795 618 315
nick.graham@dentons.com

Simon Elliott
Partner, London
D +44 20 7246 7423
simon.elliott@dentons.com

Antonis Patrikios
Partner, London
D +44 20 7246 7798
M +44 7919 491029
antonis.patrikios@dentons.com