OMBUDSMAN
CAYMAN ISLANDS

DATA PROTECTION AND COVID-19

What is the Ombudsman's approach to regulatory action during the coronavirus (COVID-19) pandemic?

The Ombudsman recognises the extraordinary challenges humanity is facing due to the pandemic. We fully appreciate that the health and wellbeing of you and your family are paramount and encourage you to take steps to remain safe during these uncertain times.

We understand that resources such as finances, supplies and staff may be strained due to the outbreak of COVID-19, which may consequently impact data controllers' compliance functions under the Data Protection Act (2021 Revision) (DPA). We will take those factors into account when determining appropriate enforcement action.

To further assist everyone in understanding their data protection obligations during this time, we have compiled this brief guidance note to include critical points that are relevant to the DPA as it relates to the impacts of COVID-19.

What happens if we fail to meet the statutory deadlines set out in the DPA?

While we cannot extend statutory timelines (e.g. the data breach notification period of five days or the time for compliance with data subject requests), we will take into account the fact that the pandemic may result in delays and adjust our enforcement action, including penalties, accordingly.

Office of the Ombudsman
Anderson Square
64 Shedden Road, PO Box 2252
Grand Cayman KY1-1107
Cayman Islands
T +1 345 946 6283
F +1 345 946 6222
info@ombudsman.ky
ombudsman.ky

Does the DPA prevent us from sharing medical data during the pandemic?

The Public Health Law (2002 Revision) (PHL) was recently amended to include COVID-19 as a notifiable disease under the schedule of the PHL. Consequently, under the Public Health (Communicable Diseases) Regulations (1997 Revision) occupiers, controllers of premises, and medical practitioners are obliged to share data which is relevant to identifying a notifiable disease with appropriate parties.

Examples of legal processing of sensitive personal data are:

(a) Where the processing is done with the consent of the individual ("consent").

(b) Where the processing is necessary because there is a medical emergency and it is necessary for the protection of life ("vital interests").

(c) Where the processing is necessary for medical professionals to perform their duties, including public health messaging ("medical purposes").

Other legal bases may also apply, and we advise organisations to review our guidance on Schedules 2 and 3 to identify those most relevant to their work.

Does this apply to employers, landlords and heads of household?

Employers, landlords and heads of a household have a legal obligation to notify the appropriate parties concerning potentially infected individuals under public health law. This would constitute a legal basis for processing under the DPA.

Employers can share staff health data with authorities for public health purposes.

Can we send information out to individuals about how to respond to COVID-19?

The DPA does not prohibit a public health authority, the Government or health professionals from sending public health messages to individuals, provided the correspondence serves the purpose of protecting against severe threats to public health.

What information can we collect about individuals during the COVID-19 pandemic?

The third data protection principle requires personal data to be adequate, relevant and not excessive in relation to the purpose or purposes for which the data are collected or processed. Therefore, data controllers should consider whether collecting and processing personal data is necessary for combating the risks associated with COVID-19.

You have an obligation to protect your employees' health, but that doesn't necessarily mean you need to gather lots of information about them.

It's reasonable to ask people to tell you if they have visited a particular country or are experiencing COVID-19 symptoms. You could ask visitors to consider government advice before they decide to come to your office. And you could advise staff to call the 24-hour Flu Hotline on 1-800-534-8600 or 925-6327 (Flow) or 947-3077 (Digicel), or email flu@hsa.ky if they are experiencing symptoms or have visited particular countries. This approach should help you to minimise the information you need to collect.

If that's not enough and you still need to collect specific health data, don't collect more than you need and ensure that any information collected is treated with the appropriate safeguards.

What data protection issues do we need to consider when using videoconferencing and collaboration apps to work from home?

In response to the pandemic, many people have transitioned to work and study from home. As a result, more use is being made of apps and other online services that allow for videoconferencing and collaborative working. This could be for communication between colleagues, or with customers, suppliers, students, patients and clients.

Due to the many reservations expressed by other data protection regulators (and other security and privacy experts) we strongly urge data controllers and users to verify the suitability of even popular apps like Zoom.

This section is a reminder to data controllers of points they should consider when using these apps. Following this guidance will help organisations to comply with the data protection principles when collaborating online. Follow the links in each subheading for more detailed guidance on each of the principles.

First DPA Principle – Fair Processing

It is likely that you may not be doing anything different with personal data and are just using different tools to process it. However, you may wish to provide an updated privacy notice to any customers, clients or patients if you are using an online chat or video conferencing tool, so that they understand how their data will be collected and used.

Second DPA Principle – Purpose Limitation

Again, while you might not be using personal data for any additional purposes, you should make sure that the online tool you choose does not further process the personal data you provide to it for any incompatible purposes. Examples of incompatible purposes include

harvesting contact details and online activities to disclose to third parties for targeted online advertising or sending direct marketing communications using the email addresses people sign up with.

Third DPA Principle – Data Minimisation

You must ensure that you aren't capturing any more personal data from people than you would be doing in a face-to-face meeting. Ensure that you choose an app that minimises the data collected for these online services.

Fourth DPA Principle – Accuracy

If personal data is being collected online, ensure that you take appropriate steps to verify its accuracy, just as you would face-to-face.

Fifth DPA Principle – Data Storage

You should check what the retention periods for personal data are on the online service or app you are utilising. Obtain confirmation from the service whether you can define or amend these periods if they are incompatible with your organisation’s retention policies. If you can set the retention periods to be automatically implemented, that will assist you in your compliance efforts.

Sixth DPA Principle – Data Subject Rights

Data subjects' rights apply in the same way they would offline. For example, you must provide them with access to their personal data if they make a subject access request.

Seventh DPA Principle – Security

Ensure that the online services you choose provide an adequate level of security for personal data. Some issues you may wish to consider include proper access control and encryption of the data both in transit and at rest. If you have engaged a third-party software provider as a data processor, you will need to have in place a data processing agreement, in line with the requirements of the DPA.

Eighth DPA Principle – International Data Transfers

Many of these online services are based in countries that may not provide an adequate level of protection for individuals' personal data. If the country does not appear on the EU's adequacy list and none of the exceptions in Schedule 4 of the DPA apply, you will have to make your own assessment of the adequacy of the transfer, following the criteria in our guidance linked above.

Queries and further information

Our offices are currently closed and not available for walk-in queries. Postal services may not be available and mail may be received with significant delays. Please send any questions, complaints or data breach notifications to info@ombudsman.ky or call our main telephone line on +1 345 946 6283.