OMBUDSMAN
CAYMAN ISLANDS

Data Protection Act (2021 Revision)

Guide for Data Subjects

Data Protection Act (2021 Revision) - Guide for Data Subjects
Last update: 25 August 2023

Table of Contents

Introduction

The Data Protection Act (2021 Revision) (DPA) is a powerful piece of legislation that introduces globally recognized principles surrounding the use of personal information in the Cayman Islands. Most importantly for individuals, it introduces several rights you can exercise and enjoy for your benefit – both towards public and private organizations.

This guide explains your new rights so you feel comfortable using them.

Before we get to your rights, though, you will need to learn a bit about data protection. Having a basic understanding of the law will help empower you in today's world and make you a savvier consumer of both private and public services.

If you think about it, almost everything we do today, whether online or offline, leads to information about us being gathered, stored and otherwise used.

Your email provider can read your emails, your doctor knows what illness ails you, your favourite social network knows who your friends are and what political opinions you hold, and your supermarket might very well know what special offers to send to you at home, so you can visit the store and get our favourite cheese on sale.

We trust that this information will be used responsibly, that our privacy will be respected, and that it is kept safe and secure – and that is precisely what data protection is about.

What is data protection?

A set of rules. Data protection is a set of rules that defines what organizations may and may not do with the information they hold about an individual. Importantly, it applies equally whether you are dealing with government administration or a private business.

Personal data. The technical term for the information regulated by data protection rules is 'personal data', and it covers any type of information that can be used to identify you. This may be your employee file, the history of your posts to your favourite social network, or a record of your bank transactions.

Data controller. This is the technical term for the business, public authority or organization that uses your personal data and is responsible for what happens with it. For your bank transactions, this will be your bank. For your employee file, it will be your employer.

Processing of personal data. The Data Protection Act covers every imaginable use of personal data, starting from its collection to its storage to its use in daily business and even its destruction. The technical term used for all these different uses is the "processing" of personal data.

Privacy. The Data Protection Act aims to protect the privacy of the individuals concerned while striking a fair balance with the legitimate interests of those entities that need to use the personal data. You're happy for your doctor to use your health information to treat you, but you probably wouldn't be too happy to find an article penned by your doctor telling everyone about your medical condition in the local newspaper.

The Data Protection Act is closely related to the fundamental right to privacy, which is enshrined in the right to private and family life of the Cayman Islands' Bill of Rights, Freedoms and Responsibilities (BoRFR)

and in Article 12 of the Universal Declaration of Human Rights. The right to privacy includes the right of individuals to determine who holds information about them and how that information is used, which leads us back to the goals of data protection.

Why do we need data protection?

Data protection protects the privacy of everyone in Cayman, and it encourages organizations to treat our personal information responsibly.

What are the principles of data protection?

The Data Protection Act (2021 Revision) is centred around eight data protection principles that set out a framework within which personal data is processed. These eight principles are a good starting point to assess the processing that is being undertaken.

First data protection principle: Personal data must be processed in a fair and lawful manner (fair and lawful use)

Fair processing means that you should be informed by the organization using your personal information (the data controller) who they are and for what purpose they will be using it. This information is usually provided to you via a privacy notice hosted on the data controller's website but may also be done via other means. The privacy notice should generally be provided to you at the moment your personal data is being collected from you, such as when you sign up for a service the data controller is providing.

Lawful processing means that there must be a legal ground that permits the organization to use your personal information. E.g., obtaining your consent or because there is a contract in place with you and using the personal data is necessary to perform the terms of that contract with you.

Second data protection principle: Personal data may only be processed for the purpose it was collected for (purpose limitation)

Purpose limitation means that an entity may not collect your information for one purpose and then use it for another incompatible purpose.

> **Example**
>
> If you go to a doctor, you trust that your information will only be used to treat you and to bill you or your insurance company. The doctor may not sell your diagnosis and contact information to a pharmaceutical company so they can market a new medicine to you. That would be an incompatible use of your data.

Third data protection principle: Personal data should only be collected if it is necessary for the purpose (data minimization)

Data minimization means that an entity should only collect information that is necessary for the stated purpose and not more.

In practice

When providing your information, ask yourself whether the information is needed. If you don't think so, ask what the intended purpose is. If you still think you shouldn't be required to provide the information, but the organization demands it, consider making a complaint to the Ombudsman.

Example

If you shop at a supermarket, they should not require you to provide your phone number. An email provider you sign up with does not need to know your date of birth. Similarly, a credit card application should not require you to give the contact details of your closest living relative.

Fourth data protection principle: Personal data must always be accurate (data accuracy)

Data accuracy means that the information about you should be correct. This is especially important because personal information is often used to make decisions about you.

Example

An insurance company might base its rates on the years of your driving experience and your age. If the records say that you have 12 years of driving experience when, in fact, you have 22 years, you have a right to have the record corrected.

Fifth data protection principle: Personal data may not be kept for longer than necessary (storage limitation)

Storage limitation means that once personal data is no longer needed, it should be destroyed.

Example

If you no longer wish to use a digital service you signed up for, be it an email provider, a social network, or an online video-calling application, you can ask to have your account and all associated personal data deleted, in so far as there are no obligations on the service provider to keep some of the information, for example for accounting purposes.

Sixth data protection principle: Personal data shall only be processed in accordance with the rights of the individual in mind (respect for the individual's rights)

Individual rights mean that any processing done must take the rights of individuals into account. It is a reminder to businesses, public authorities and organizations that they have obligations towards the individuals whose personal data they process.

> **In practice**
>
> Take the time to learn about the data protection principles and get to know your rights. Be comfortable using them. Contact the Ombudsman if you think we can help you in any way.

Seventh data protection principle: Personal data must always be kept safe (security – integrity and confidentiality)

Security, integrity and confidentiality means that personal data must be kept secure using both technical and organizational means and that only individuals and entities who need to use it should have access to it. Keeping personal data secure means not just from malicious attacks but also from inadvertent harm.

Eighth data protection principle: Personal data may not be transferred outside the Cayman Islands unless it is adequately protected (international transfers)

International transfers mean that personal data may not leave the Cayman Islands unless the destination offers a level of protection that is on a broad level, the same as here, or adequate safeguards are in place to protect the information. This prevents data from being transferred abroad with the goal of skirting the robust protections the Cayman Islands Data Protection Act provides.

Your data protection rights

Your data protection rights flow from the principles we just outlined. They are powerful tools you can – and should – exercise. The below explains your rights on a high level. Certain exemptions apply in some cases. You may read more about the exemptions in our guidance for data controllers, available on our website.

Your right to be informed

You have the right to be informed about

- The identity of the organization processing your personal data and
- The purposes for processing the personal data.

You should find this information in the organization's privacy notice. The information should be provided to you as soon as reasonably practicable. This will generally be when the organization collects the personal data from you.

If you're interested in learning more about this topic, visit our guidance for organizations.

Your right to access your data

You also have a right to obtain a copy of your personal data within 30 days of your request.

All you need to do is submit a request in writing to the organization in question. You may need to identify yourself to the organization so they are sure it is actually you – note that the time limit is suspended until your identity has been determined.

In addition, you have a right to be provided with the following information:

a) where the personal data came from;
b) the recipients or classes of recipients of the personal data;
c) any countries or territories outside the Islands to which the personal data is transferred;
d) how the security, integrity and confidentiality of your personal data is maintained; and
e) the right to make a complaint to the Ombudsman.

You can use our model form to submit your request to access your personal data.

If you're interested in learning more about this topic, visit our guidance for organizations.

Right to correct your data (Rectification)

You have the right to correct data – and where it is wrong, you have a right to have it corrected.

If you're interested in learning more about this topic, visit our guidance for organizations.

Rights regarding automated decisions without human involvement

Decisions that used to be made by humans are increasingly being handed over to computers – for a number of very good reasons, such as efficiency and speed. However, computers can make mistakes, and the algorithms underlying the decision-making may be subject to (unintended) bias in their decisions.

The DPA seeks to address these concerns by giving you the right not to be subject to such a decision where it significantly affects you. It also gives you the right to have the data controller reconsider the decision on a different basis (i.e. by a human).

However, this does not apply where the decision is necessary in relation to a contract with you and where either the outcome is a positive one in your favour or where the organization safeguards your interests and allows you to make representations.

If you're interested in learning more about this topic, visit our guidance for organizations.

Right to stop processing

You have the right to require that the processing of your personal data by a data controller stop, not begin, or cease processing for a specified purpose or in a specified way. However, this will not apply in certain circumstances, i.e., where the processing of your personal data is necessary because of a contract that is in place with you or because the organization is legally obliged to process your personal data, it is necessary to protect your vital interests. Otherwise, you have the right to have the processing stopped.

Depending on the use of your personal data, this may mean having it outright deleted or that only a specific processing activity should be stopped.

Example

If you no longer wish to use a digital service you signed up for, be it an email provider, a social network, or an online video-calling application, you can ask to have your account and all associated personal data deleted, in so far as there are no obligations on the service provider to keep some of the information, for example for accounting purposes.

If you're interested in learning more about this topic, visit our guidance for organizations.

Right to stop direct marketing

You have the absolute right to stop direct marketing, whatever the medium. Be it SMS, postal mail, or emails. If you no longer want to receive such advertising, you can have the sender stop by providing your request to the data controller in writing.

If you're interested in learning more about this topic, visit our guidance for organizations.

Right to compensation for damage

You have a right to be compensated for any damage suffered due to a breach of the DPA by a data controller. However, this must be pursued through the courts.

If you're interested in learning more about this topic, visit our guidance for organizations.

Right to make a complaint to the Ombudsman

Rights are only as good as their enforcement – and where you feel that your rights are not being respected, you should submit a complaint to the Office of the Ombudsman.

The Ombudsman will assess your complaint and decide whether to investigate based on its substance. A complaint that is upheld following an investigation may lead to enforcement action against the organization. This could be an order to provide information, to do or not to do something specified by the Ombudsman, or even a monetary penalty of up to CI$250,000.

If you're interested in learning more about this topic, visit our guidance for organizations.