Data Protection Guidance for Small Businesses and Organizations

The Data Protection Act applies to a wide range of entities, including small businesses, volunteer organizations, strata plans, churches, clubs and associations, charities, public authorities, etc. They may come in all different sizes, and may process different types of personal information which carry different levels of risks for the privacy of the individuals whose information they hold.

This guidance is intended for entities that do **not** deal with sensitive types of personal information which would permit more than a superficial insight into the individuals' characteristics, such as:

- behaviour (e.g. through profiling),
- finances,
- race or ethnicity,
- political opinions,
- religious or similar beliefs,
- trade union membership,
- genetic data,
- physical or mental health and conditions,
- medical data,
- sex life,
- proceedings for any offence, or commission or alleged commission thereof.

If your business or organization **does not** hold personal information that gives more than a superficial insight into the above matters, this guidance applies to you.

If your business or organization **does** hold personal information that gives meaningful insight into the above matters, you should consult our in-depth Guide for Data Controllers.

Last update: 19 April 2021

OMBUDSMAN
CAYMAN ISLANDS

Data Protection in a Nutshell – A Quick Reference Guide

This document is intended as a **quick reference tool**. It provides a walkthrough of data protection act and can serve as a refresher to the in-depth guidance available on our website. There is also an easy to use checklist with which you can assess your organization against the requirements put forward by the Data Protection Act (the DPA).

We understand what information the DPA applies to

- The DPA applies to '**personal data**'. Understanding whether you process personal data is critical to understanding whether the DPA applies to your activities.
- Personal data is **information that relates to a living, identified or identifiable individual**.
    - Examples: a name or number, online identifiers such as an IP address or cookie identifier, or other factors such as a bank account statement or an invoice.
    - An individual may be **directly identifiable**, for example through a name.
    - An individual may be **indirectly identifiable**, for example through an account number that can be linked to an individual. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.
- The DPA applies to personal data that you are '**processing'**. Processing is a catch-all term and covers anything you do with the personal data, e.g. collection, storage, deletion, analysis, disclosure, etc.

We understand whether the DPA applies to us

- The DPA applies to personal data processed by '**data controllers'** and '**data processors**'.
- A '**data controller**' determines why and how personal data is processed and is the entity ultimately responsible for the personal data.
- A '**data processor**' processes personal data on behalf of a data controller and does not itself determine why personal data should be processed. A data processor may, to a certain extent, decide on how the personal data should be processed.
- Employees of the data controller are not data processors, they are considered part of the data controller.

- A data controller who engages the services of a data processor must ensure that the engagement is based on a written contract, called a **data processing agreement.** The data processing agreement contains certain prescribed conditions for the processing of personal data by the data processor.
- The DPA does not apply to processing carried out by individuals purely for personal/ household activities.

We process personal data fairly

- You must handle personal data in a way that is **fair**. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

We process personal data in a lawful manner

- You must identify one of the permissible grounds under the DPA (known as a '**legal basis**') for handling personal data. You may not handle personal data without a valid legal basis.
- You must ensure that you do not do anything with the data in breach of any other laws.

We inform the individuals about the purposes we use their personal data for and we use it only for these purposes

- You must be transparent, i.e. clear, open and honest with people from the start about why and how you handle their personal data. This information is typically communicated in a **privacy notice**.

We collect only the necessary amount personal data

- You must ensure the personal data you are processing is **limited to what is necessary** for the purpose it was collected for – you should not hold more than you need for that purpose.

We keep the personal data correct and current

- You should take all reasonable steps to ensure the personal data you handle is **correct**.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.

- You must consider any challenges individuals make regarding the accuracy of their personal data.

We keep the personal data only as long as necessary

- You must keep personal data **only as long as you need it**.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- As best practice, you should have a policy that specifies how long you keep each type of personal data you process.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

We respect the individual's data protection rights

- The DPA grants certain **rights to individuals** in relation to their personal data and how it is processed, for example the right to receive a copy of one's own personal data.
- You must process all personal data in accordance with the rights of individuals.
- You should plan ahead in order to prepare for responding to each of the likely requests and notices you may receive and meet the statutory timelines.

We keep the personal data secure and confidential

- You must **keep personal data secure and confidential** by means of 'appropriate technical and organizational measures'.
- Depending on the risks assessed, **appropriate measures** can be such simple measures as using password-protected accounts on your computers or using physical locks on your filing cabinets.
- The security requirements also apply to any data processors you may use.

We know whether personal data leaves the Cayman Islands

- The DPA imposes specific safeguards for the transfer of personal data to countries that are located outside the European Union (EU) and to countries where the standard of data protection is deemed to be too low from a Cayman perspective.
- These safeguards are in place to ensure that the level of protection of individuals afforded by the DPA is not undermined.

OMBUDSMAN
CAYMAN ISLANDS

Data Protection - Checklist Overview

Always required

☐ We understand what 'personal data' and 'processing' of personal data are.

☐ We understand the concepts of 'data controller' and 'data processor'.

☐ We know what personal data we process.

☐ We only handle people's data in ways they would reasonably expect.

☐ We only collect the personal data we actually need for our specified purposes.

☐ We have identified an appropriate lawful basis (or bases) for our processing.

☐ We are transparent about what we do and we include details of our purposes in our privacy information for individuals.

☐ We keep our personal data accurate.

☐ We delete personal data that is no longer required.

☐ We respond to an individual's data protection request, such as requesting a copy of the personal data or stopping direct marketing.

☐ We keep our personal data secure and confidential.

Required depending on your organization

☐ We have data processing agreements in place for all the data processors we use.

☐ We notify individuals when we take decisions that affect them based solely on automatic means, and we are ready to reconsider such decisions on a different basis.

☐ If we plan to use personal data for a new purpose, we check that it is compatible with our original purpose or we get specific consent for the new purpose.

☐ As best practice, we have a policy that specifies how long we keep each type of personal data we process.

☐ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

☐ We are aware whether we need safeguards in place if we or our data processors transfer personal data abroad.