# Data Protection Fact Sheet - Ten steps to take now

1. Become aware
2. Know the data you hold
3. Privacy notices
4. Individuals' rights
5. Subject access requests (SAR)
6. Legal basis of processing personal data
7. How to use consent
8. Data breaches
9. Privacy Impact Assessments (PIA)
10. Cross-border issues

As a responsible business you are conscientious about the use of personal data under your control. If so, you may already meet some or most of the common sense requirements of the new Data Protection Law.

The Cayman Islands decided in 2009 to develop Data Protection legislation employing the model of the European Union (EU). The resulting Data Protection Law (DPL) was enacted in 2017 and comes into effect in January 2019. It follows many of the same definitions and provisions as the 2016 General Data Protection Regulation of the EU (GDPR).

Besides this simple 10-point checklist the Office of the Ombudsman will be producing other tools and guidance, which will be available on our website www.ombudsman.ky . More advice is available on the websites of other Data Protection Supervisory Authorities, such as the UK's Information Commissioner's Office (ICO)[1], and the Irish Data Protection Commissioner.[2]

This guidance is focused on small businesses, organizations and persons who hold personal data.

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
[2] https://www.dataprotection.ie/docs/A-Guide-for-Data-Contollers/y/696.htm

## 1. Become aware

You should make sure that decision makers and key people in your organization are aware that the DPL is coming into effect. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the DPL. It is useful to start by looking at your organization's risk register, if you have one.

Implementing the DPL could have significant resource implications for larger and more complex organizations. But even for small businesses and organizations, preparation is a good idea. This is particularly true if you hold certain types of high-risk data, such as health, genetic or biometric data.

You may find compliance more challenging if you leave your preparations until the last minute!

## 2. Get to know the data you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to map your data across the organization or target particular business areas.

The DPL does not require that you maintain upfront records of your processing activities. However, having the right information at your fingertips makes life easier down the line. For example, under the fourth data protection principle, the personal data you hold must be kept up to date, and individuals have a right to get their data corrected. If you have inaccurate personal data and have shared it with another organization, you will have to tell the other organization about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you shared it with. It will also help you put effective policies and procedures in place.

More advice on data mapping[3] is available from the Information Commissioner of the Isle of Man.

## 3. Privacy notices

Under DPL, when you collect personal data you will have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice.

If you do not already use privacy notices, you should put a plan in place for making them available in time for DPL implementation. Privacy notices should be provided to the data subject upfront, in easy to understand and clear language.

The Office of the Ombudsman considers it best practice to give people some additional information as well. For example, you can use the privacy notice to explain the basis for processing the data,

[3] https://www.inforights.im/media/1271/gdpr_part-1_toolkit_mapping_may2016.pdf

how long you intend to retain the data, and explain that individuals have a right to complain to the Ombudsman if they think there is a problem with the way you are handling their data.

## 4. Individuals' rights

You should check your procedures to make sure you can cover all the rights individuals have, including how you would delete personal data, or provide data electronically in a commonly used format.

The DPL includes the following rights for individuals:

- the right to be informed (privacy notice)
- the right of access
- the right to rectification
- the right to stop processing
- the right to stop processing for direct marketing
- the right not to be subject to automated decision-making
- the right to complain to the Ombudsman
- the right to seek compensation in the courts

These rights flow from the fundamental right to private and family life in the Cayman Islands Bill of Rights.

If you gear up to give individuals their rights now, then the implementation of the DPL should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make sure the deletion takes place?

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a commonly used form and provide the information free of charge.

## 5. Subject access requests (SAR)

Individuals have a right to get a copy of their own personal data, and certain information about it, such as its source, who you share it with, whether it is transferred abroad, etc. You should update your procedures and plan how you will handle requests to take account of the new rules:

- You will have 30 days to comply with a SAR, although that time can be extended in exceptional circumstances
- In most cases you will not be able to charge for complying with a request, but you can refuse or charge for requests that are manifestly unfounded or excessive

- If you refuse a request, you must tell the individual why. They have the right to complain to the Office of the Ombudsman, and the Ombudsman is authorized to enforce the Law. You must do this without undue delay and at the latest within one month.

If your organization handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

## 6. Legal basis of processing personal data

It is best practice to review and document the legal bases of your processing activities in order to help you comply with the DPL.

Many organizations will not have thought about the legal basis for processing personal data. However, most processing activities you currently undertake will likely not have to be changed since you will be able to rely on one of the conditions for processing in schedule 2, including:

- consent
- contract
- legal obligation
- vital interests
- exercise of public functions
- legitimate interests

There are additional conditions for processing of sensitive personal data in schedule 3, including:

- employment
- non-profit associations
- information made public by the individual
- legal proceedings
- medical purposes

## 7. Consent

You should review how you seek, record and manage consent and whether you need to make any changes, in order to meet the DPL standard.

Under the DPL, consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Consent also has to be verifiable.

The UK ICO has published detailed guidance on consent under the GDPR[4], as well as a consent checklist to review your practices, which may be helpful.

In many cases, there are alternatives to using consent as a basis for processing personal data, such as the conditions for processing listed above.

## 8. Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

The DPL imposes a duty on all organizations to report data breaches to the Ombudsman, and to the individuals whose data has been breached. By law, any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of personal data must be reported no later than five days after the breach occurred.

Information that has to be reported includes:

- nature of the breach
- consequences
- measures taken to address the breach
- measures the individual can take

Organizations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine.

## 9. Privacy by Design and Privacy Impact Assessment (PIA)

Although not mandatory under the DPL, it is good practice to adopt a Privacy by Design approach and to carry out a Privacy Impact Assessment (PIA) as part of this.

Privacy by Design means that you build data protection safeguards into your products, services and business practices from the earliest stages of development.

A PIA is best practice in situations where data processing is likely to result in high risk to individuals, for example where:

- a new technology is being deployed
- a profiling operation is likely to significantly affect individuals, or
- there is processing on a large scale of the special categories of data

[4] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

A PIA can help you prepare to identify and address particularly risky processing activities. You should plan to set up policies and procedures to make sure Privacy by Design and PIAs become integrated into your normal business practice. Who will do it? Who else needs to be involved? How will the process be linked to your standard organizational processes such as risk management and project management?

The UK ICO has further guidance on Data Protection Impact Assessments[5] (note that not all of the requirements of the GDPR on DPIAs apply under the Cayman Islands DPL).

## 10. Cross-border issues

Under the eighth data protection principle personal data must not be transferred to a country or territory that does not ensure an adequate level of protection for the data protection rights and freedoms of the individual.

Whether adequate protection is in place will depend on the circumstances of the processing, including:

- nature of the personal data
- purposes for which the data is processed
- how long the data will be kept
- law in force in that country or territory
- security measures in place

The DPL allows a number of exceptions:

- consent
- contract
- public interest
- legal proceedings
- vital interests
- public register
- international cooperation between intelligence or regulatory agencies

Some countries have been recognized by the European Commission[6] as having adequate protection. If your organization operates in the EU, you should make sure to be compliant with the GDPR. If you operate in more than one EU member state, you should determine your lead data protection supervisory authority[7] and document this.

[5] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[6] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[7] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235