THE OFFICE OF THE
Data Protection Authority

Transition: a plain English guide for organisations.

Your guide to achieving full compliance with the transitional aspects of *The Data Protection (Bailiwick of Guernsey) Law, 2017.*

Index

About this Guide

The aim of this guide is to **help you understand what your organisation needs to do** in order to comply with all aspects of ***The Data Protection (Bailiwick of Guernsey) Law, 2017*** that were subject to 'transitional relief'.

Most aspects of our local Law came into force on 25 May 2018, on the same day as the EU's General Data Protection Regulation (GDPR).

Local organisations had an additional year long transition period before they had to comply with these more complex aspects of our local Law:

(1) **Duty to notify pre-collected data (sections 12 & 13)**

(2) **Duties of joint controllers (section 33)**

(3) **Duty to carry out impact assessment (sections 44 & 45)**

(4) **Processor-use duty (section 34)**

(5) **Processor duty to establish measures (sections 35 & 36)**

(6) **Duty of processor to obtain controller authorisation (section 36)**

(7) **Delay of right to data portability (section 14)**

(8) **Validity of consents obtained before 25 May 2018**

(9) **New registration requirements (sections 39 & 40)**

After the end of the transition period in May 2019, all organisations must comply with the aspects above, and the rest of their legal responsibilities defined in our local Law.

Not sure what your organisation's legal responsibilities are?

These are defined by The Seven Data Protection Principles (see page 3) or visit ***odpa.gg/all-about-transition***

GDPR vs. our local law

Our local Law was written to make it equivalent to the GDPR – which means it offers the same rights to local citizens and the same standard of **personal data** protection. GDPR governs EU citizens' rights within the EU and in other specific situations when their data is processed by organisations outside the EU.

The Bailiwick had to devise its own similar legislation to: protect Bailiwick citizens' rights; ensure local organisations offering goods or services to people within the EU do so in a GDPR compliant manner; and to ensure local organisations can transfer **personal data** easily between the EU (and other jurisdictions the European Commission deem 'adequate').

What is this column?

To help you understand these more complex areas of **the Law** we have created a hypothetical local estate agent. We've called them Moving & Shaking, and we will use them as an example throughout this guide to put our advice in a real-world context. Data protection can sometimes seem complex, and we hope that this approach makes it easier to understand.

So, let's meet **MOVING & SHAKING**:

Moving & Shaking is a Guernsey-based estate agency that employs 15 people. They handle advertising and sales/rentals of property on Guernsey's open and local markets. They manage some privately-owned rental properties. They are a well-regarded, professional organisation who take their legal duties and corporate governance seriously. They know that as a **controller** of the **personal data** they hold on their staff, clients, suppliers and other people that they are responsible for: how that data is used, how it is kept safe, and respecting the legal rights of the people the data relates to.

Let's rewind to May 2018 - Moving & Shaking were aware of the new data protection law that was about to come into force in the Bailiwick. They were focused on amending and updating their processes and procedures to ensure that any new processing of **personal data** was compliant with the new legal requirements.

Fast-forward to the run-up to May 2019, with the transition period of **the Law** ending, they are now turning their attention to the **personal data** they held before May 2018, to ensure they are processing it legally.

Key Definitions

These plain English definitions should help you with any legal terms you find in this publication – which are highlighted in green throughout. For full definitions please refer to section 111(1) of *The Data Protection (Bailiwick of Guernsey) Law, 2017*.

Controller

The **controller** is any entity (such as an organisation or person) who is responsible for the decisions made about how they use **personal data** about staff, customers, suppliers, or any other people.

Data subject

This is the legal term for the living person the **personal data** is about, or relates to.

DPIA

DPIA is an acronym for 'Data Protection Impact Assessment', which is an exercise that certain organisations must do if they are handling a large volume of **special category data**, or if they are doing any processing of **personal data** that could pose a high-risk to the individuals whose data it is.

Legitimate interests

This is one of a number of legal reasons that organisations can rely on when they want to process a person's data. It's complex, but put simply, if an organisation can: prove it has a very good reason for processing your data; and they have balanced this reason against your legal rights, then they can say they are relying on '**legitimate interests**' as the reason for processing your data.

Office of the Data Protection Authority (ODPA)

ODPA is the independent regulator of the data protection law for the Bailiwick of Guernsey.

Personal Data

This is any detail about (or relating to) an identifiable living person. Once a person dies, any details about them is no longer classed as **personal data** and data protection laws no longer apply.

Processing personal data

This is a catch-all term for anything you do with **personal data**. Examples include: collecting, recording, storing, organising, handling, or any other use of data about living people.

Processor

This is an organisation that is given the task of processing **personal data** by a **controller**. The difference between a **processor** and a **controller** is that a **processor** does not decide how the data is used, they just perform the task as instructed by the **controller**.

Significant interests

This is a very broad term for any aspect of a person's life that could be put at risk due to their **personal data** being breached. This could include their physical safety and their reputation. It also extends to placing them at risk of identity theft, fraud, financial loss, psychological distress, humiliation, or a host of other potential harms.

Special category data

This is a sub-category of the term '**personal data**' which refers to particularly sensitive details about a living person, such as their health, sexuality or sex life, political views, race, religion, membership of a union, genetic or biometric information, or any criminal activity they've been accused or convicted of.

The law

The Law means *The Data Protection (Bailiwick of Guernsey) Law, 2017*. This is **the Law** that governs how **personal data** is handled in the Bailiwick. It is equivalent to the EU's legislation, the General Data Protection Regulation (GDPR).

The Seven Data Protection Principles

At the heart of data protection are the rights of the individual whose personal data is being processed. Surrounding that person are these seven principles, outlined in *The Data Protection (Bailiwick of Guernsey) Law, 2017* which all local controllers and processors are legally obliged to adhere to:

1. LAWFULNESS, FAIRNESS & TRANSPARENCY

They must have a valid legal reason for processing your information, they must obtain it without deceiving you, and they must make it clear to you exactly how they are going to use it.

2. PURPOSE LIMITATION

They must only use your information for the reason (or reasons) they have told you they're using it for.

3. MINIMISATION

They can only ask for the minimum amount of information necessary from you.

4. ACCURACY

They must ensure that any information they hold about you is accurate and up-to-date.

5. STORAGE LIMITATION

They must not keep your information for longer than is needed.

6. INTEGRITY & CONFIDENTIALITY

They must keep your information safe so that it doesn't get accidentally deleted or changed, or seen by someone who is not allowed to see it.

7. ACCOUNTABILITY

This is the big one. They must show that they take responsibility for how they look after your information.

Duties | 4.1 | To notify pre-collected personal data

Plain English | You need to tell people what you do with their data.

Overview.

The Law requires controllers to tell people exactly who they are and what they are going to do with their personal data:

- When they collect their personal data from them, or
- When they start processing personal data received from a third party.

This is known as the controller's **'notification duty'** to provide people with **'fair processing information'**, which is normally known as a privacy notice or fair processing statement.

What is the transitional aspect of this?

If an organisation **already had** a person's data **before** the Law came into force on 25 May 2018 the organisation did **not** have to provide that person with new 'fair processing information', unless, the person specifically asked for it.

Why were organisations given extra time to get ready for this?

When the Law was being drafted, it was recognised that organisations would have to provide **much more information** to people about how their information was going to be used compared to the previous (2001) law. So, to ease the burden on organisations, the Law made any 'pre-collected' data exempt from this duty until 25 May 2019.

What do organisations have to do to comply with this new duty?

You must provide your privacy notice to anyone who asks for it. And by 25 May 2019 you must proactively make your privacy notice available to all people whose personal data you are processing regardless of when you collected that data.

How this might work in the real world...

Moving & Shaking have been providing its new privacy notice to all new clients since May 2018.

However, they know that they have ten properties on their books from early 2018. The property owners have not been given the new privacy notice, because of Moving & Shaking's focus on new clients.

To make sure they are now fully compliant they will be sending the new privacy notice to the long-standing clients, with a covering note explaining it replaces the one they gave them under the old (2001) law.

Duties | 4.2 | Duties of joint controllers in relation to continued processing

Plain English | You need to define exactly how you use people's data when you are sharing data with another organisation to achieve a common goal.

Overview

This duty applies whenever a **controller** of **personal data** works with one or more other organisations who share the decision-making around the **personal data** they hold. In this situation **the Law** puts new obligations on **controllers** to provide more detail to the people whose data they look after alongside other **controllers**.

What is the transitional aspect of this?

If an organisation **already had** a person's data **before** **the Law** came into force on 25 May 2018 the organisation did **not** have to comply with this duty.

Why were organisations given extra time to get ready for this?

When **the Law** was being drafted, it was recognised that organisations would have to provide **much more information** to people about how their information was going to be used compared to the previous (2001) law. So, to ease the burden on organisations, **the Law** made any 'pre-collected' data exempt from this duty until 25 May 2019.

What do organisations have to do to comply with this new duty?

If you are a **controller** you have to precisely define **how** you work with other **controllers** to protect the **personal data** you both look after, regardless of **when** you started working together. This means you must write into a contract with each other **what** your respective responsibilities are. You must also detail your responsibilities to provide **support to each other** as/when a **data subject** wishes to exercise their rights, or when a data protection authority requests information from either of you.

How this might work in the real world...

Moving & Shaking act as a property management company for several private landlords.

They enter into tenancy agreements on the landlord's behalf, deciding what **personal data** they need for this and sharing that data with the relevant landlord. They collect rent for the landlord and chase any arrears, and pass this money to the landlord after taking their commission. So, this is a joint **controller** situation – as Moving & Shaking and the landlord are both **controllers** of the **personal data** relating to the tenancy and the rental payment.

Moving & Shaking have made sure any new contracts between themselves and a landlord cover the joint **controller** requirements of **the Law**. However, with transition coming to an end, they now need to amend the contracts that were in place before May 2018.

The amended contracts outline which party is responsible for compliance with the relevant aspects of the new Law and what each party must do. Moving & Shaking specifies in the new contracts that they will be the primary point of contact for anyone wanting to exercise their **data subject** rights and they commit to telling the relevant tenants this. The contract also defines the assistance that the landlord and Moving & Shaking must give to each other if any tenant wishes to exercise their rights to their **personal data**, or if a data protection authority requests information.

Duties | 4.3 | Impact assessment in relation to continued processing

Plain English | You must identify and mitigate any risks that might arise from what you want to do with people's personal data.

Overview

This duty applies in three **separate** circumstances:

1. Firstly, it applies whenever a **controller** is about to start doing anything with **special category data** on a large scale.

2. Secondly, it applies whenever a **controller** is about to start systematic and extensive automated processing and decision-making (e.g. profiling).

3. Finally, it applies whenever a **controller** is about to start large-scale and systematic monitoring of a public place (e.g. installing CCTV cameras).

If you are not sure whether what you're planning is high-risk, you can go through some screening questions to find out – these can be found at: ***odpa.gg/all-about-transition***. You will also find a suggested template for a **data protection impact assessment (DPIA)** on that page.

What is the transitional aspect of this?

If an organisation was **already doing** any of the activities above they wouldn't have to do impact assessments **until** 25 May 2019.

Why were organisations given extra time to get ready for this?

The transitional relief on this duty is recognition of the additional requirement this duty puts on organisations to **prove** that they fully thought through the implications of their processing of **personal data**.

Doing an impact assessment requires a diligent and methodical approach to considering the privacy and data protection issues that may arise from your organisation's planned activities. It also requires you to **follow through** with any activity that may mitigate the risks the assessment identifies, and to keep the people whose data it affects informed (and even **involve** those people, or their representatives, in this **DPIA** process if appropriate).

All of this is new activity that many organisations would not necessarily be used to doing, so the extra year to prepare themselves for it recognises that.

What do organisations have to do to comply with this new duty?

In short, you have to assess the impact of any **high-risk processing** before you do it.

How this might work in the real world...

Back in 2016, Moving & Shaking bought a new IT system to manage their HR activity. They did a basic privacy impact assessment before the system was purchased to check it would comply with the old (2001) data protection law.

Fast-forward to June 2019, they are now in the middle of doing a more in-depth impact assessment to establish any risks that could arise from poor processing or compromise of staff sickness data contained in the IT system. They used the suggested template on the **ODPA's** website to document the impact assessment and are confident the suggested mitigation will reduce the risk to an acceptable level.

The mitigation activity is simply: restricting who can access the staff sickness information to only the small number of people who need to access it and making sure that they train those people well enough to understand that they are only allowed to access it in clearly defined, limited circumstances. In addition they will put in place suitable IT safeguards to prevent the data being accessed from outside the organisation.

Duties | 4.4 | Processor / Controller contracts

Plain English | You must have legally-binding contracts that define exactly how you work with other organisations to keep personal data safe.

Overview

This is the most complicated aspect of transition. Put simply, this duty is split into three separate parts:

1. Processor-use duty

This duty covers new conditions which must be met where a **controller** employs a **processor** to perform certain tasks with **personal data**. **Processors** must **prove** they comply with **the Law**, and must enter into a legally-binding contract that says exactly who is responsible for what.

2. Processor's duty to establish measures

This duty means that **processors** must help the **controller** meet their legal obligations to the people whose **personal data** they hold.

3. Processor's duty to obtain controller authorisations

This duty means **processors** must get the **controller's** permission before it outsources any of its work to another **processor** (known as a 'secondary **processor**' in **the Law**).

What is the transitional aspect of this?

If you were **already** working in a **controller**/**processor** arrangement before May 2018, you don't have to enter into any new contracts with each other **until** 25 May 2019.

However, if you start any **new** processing of **personal data** from 25 May 2018 you will need to fully comply with all aspects of this duty.

Why were organisations given extra time to get ready for this?

As with previous duties, this duty requires **controllers** and **processors** to put in time and effort to contractually define their working relationship, and to operate in a way that keeps the **personal data** they work with safe. The year's transitional relief on this duty recognises that organisations would benefit from having extra time to review their existing contractual arrangements and put these working practices in place.

What do organisations have to do to comply with these new duties?

These duties are special, because they put as much emphasis on the **processor** being compliant with **the Law** as it does the **controller**. So, regardless of whether your organisation is the **processor** or a **controller** of any given **personal data**, you need to make sure you are **proactively** setting up contracts with any other organisations you work with. These contracts should be written in a way that protects both the legal rights of the people whose **personal data** you hold, as well as defining what your own organisation is legally responsible for.

How this might work in the real world...

Since 2015, Moving & Shaking have employed a payroll firm called ***PayEm4U*** to deal with payment of their staff salaries.

PayEm4U is a **processor** in this situation as they are told how to perform this task by the **controller** of the **personal data** – Moving & Shaking.

With the end of transition approaching in May 2019, Moving & Shaking has drafted an amendment to the existing contract between itself and PayEm4U, because without this amendment their processing would not be compliant.

The contract amendment requires PayEm4U to provide guarantees to Moving & Shaking that the processing they are doing for them will be compliant with **the Law**, and will safeguard their staffs' rights. The amendment also outlines the processings:

- **Subject matter**
- **Duration**
- **Nature, scope, context and purpose**

As well as:

- **The category of personal data being processed (i.e. whether it's special category or not)**
- **The category of data subject (i.e. types of people: staff, suppliers etc.)**
- **The controller's duties and rights**

And finally, the contract outlines the **processor's** duties, in particular their duty to:

- **Help the controller with any request linked to data subject rights (e.g. providing relevant personal data to the controller to help them respond to a 'subject access request' – this is where someone requests a copy of the personal data an organisation processes about them)**
- **Ask the controller for permission, in general or specific terms, before they outsource any of their processor duties to a secondary processor.**

Duties | 4.5 | Delayed effect of section 14 (right to data portability)

Plain English | You must allow someone to transport their personal data from your organisation's IT systems to another.

Overview

This aspect of **the Law** relates to individuals gaining the right of 'data portability' on 25 May 2019. It means a person can tell an organisation to transfer (or copy) their **personal data** from an organisation's systems and give it to them in a format that is 'machine readable' so that it can be easily transported and entered into another organisation's IT system.

What is the transitional aspect of this?

People cannot make use of this right until 25 May 2019.

Why were organisations given extra time to get ready for this?

Because there is not one universal way that **personal data** is recorded and stored across all organisations it was recognised that organisations needed more time to prepare.

What do organisations have to do to comply with this new duty?

All local organisations should investigate **how** they could easily transfer or copy all data relating to a specific person from their system and provide it to that person in a structured, 'machine-readable' format that can be plugged into another organisation's system. This could be as simple as using specific types of software files (such as a .CSV or .XML).

How this might work in the real world...

Moving & Shaking have used the year since May 2018 to work out how to get the relevant **personal data** from their HR and customer relationship management systems in a structured, machine-readable format.

Their IT provider has considered using .CSV or .XML files amongst other options and is working to get its data extraction process in place for May 2019.

Duties | 4.6 | Validity of consents obtained before commencement

Plain English | You need to check whether the consent you had from people before 25 May 2018 was freely given.

Overview

All organisations must identify a reason (or 'lawful condition') they can rely on **before** they process **personal data**. One of these conditions is consent. There are several others that you could rely on instead.

If you are relying on a person's consent to process their **personal data**, **the Law** states that their consent is only valid if you can **prove it was given in very specific circumstances.** Consent is considered valid if a person has given it based on an organisation providing clear, unambiguous information about how their data will be used. Organisations must be able to demonstrate that a person's consent was 'freely given', and not based on misleading or deceptive information.

What is the transitional aspect of this?

If you are seeking consent from people to process their data after 25 May 2018 you have to meet **the Law's** stricter conditions immediately. You can find out how to meet these conditions on ***odpa.gg/all-about-transition.***

However, if you were already processing a person's data before 25 May 2018, and were relying on their consent then you must use the extra year to check whether you can prove that you got their consent in a way that meets the stricter conditions of **the Law**.

Why were organisations given extra time to get ready for this?

Because you will need to take time to sort through the **personal data** you hold, to find any people whose consent you got before 25 May 2018. You will then need to find evidence of the circumstances these people gave their consent in. And finally, you will need to work out whether that consent is considered 'valid' under **the Law** now. This could be a time-consuming exercise, hence why organisations were given an extra year to do it.

What do organisations have to do to comply with this new duty?

You need to review the stricter conditions for consent under **the Law** (see ***odpa.gg/all-about-transition*** for detailed guidance and checklists on how to get consent right).

You must ensure that people can give and withdraw consent to processing of their **personal data** easily, and that they have genuine ongoing choice and control over how their data is being used in your organisation.

How this might work in the real world...

Moving & Shaking send marketing material once a fortnight to an established list of email addresses. They have historically used implied consent to add people to this list – the paperwork for any new client required the person to tick a box on the form if they did not want marketing material. This is not good enough under the new Law.

In May 2018, Moving & Shaking amended the form so now they ask people to tick the box if they want to receive marketing material (i.e. a positive opt-in). This small change means that Moving & Shaking can prove any people added to the marketing list since May 2018 have positively consented. This is proper consent under the new Law.

Fast-forward to early May 2019, Moving & Shaking has sent an email to the people on the older marketing list (i.e. those who hadn't positively opt-ed in). The email asks them to reply if they still want email marketing to be sent – this demonstrates that Moving & Shaking are relying on people's consent to marketing.

They cannot switch to relying on another lawful condition such as '**legitimate interests**' to continue to send them marketing emails if they receive no response from the person. If someone does not reply, Moving & Shaking are obliged to remove that person's email address from their marketing list.

Duties | 4.6 | Validity of consents obtained before commencement **(continued)**

Plain English | You need to check whether the consent you had from people before 25 May 2018 was freely given.

What do organisations have to do to comply with this new duty? (Continued)

You can no longer rely on pre-ticked boxes on forms, or confusing wording such as *'do not click here if you do not want to be added to our mailing list'* – you must be clear, concise, and transparent. And you must name any other organisations that will be relying on the consent. A record must be kept of how and when people gave or withdrew their consent.

Also consider whether it is appropriate to be asking for consent. You should only seek it if you are genuinely offering people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the **personal data** without consent (by legally relying on another lawful condition, like 'legitimate interest'), asking for consent is misleading and inherently unfair.

Duties | 4.7 | New registration requirements

Plain English | You must register your organisation with the ODPA if you are doing anything with personal data whatsoever.

Overview

Under the old (2001) Law **controllers** were required to 'notify' the Data Protection Commissioner (i.e. formally let them know via their website form) that they were processing **personal data**, and to provide certain details around the reasons for their processing.

What is the transitional aspect of this?

Following the introduction of the new Law, organisations meeting the following conditions were exempt from this need to notify:

- **Controllers** that processed **personal data** only for accounts and record-keeping purposes, for staff administration and to market their own goods or services were exempt from needing to notify.
- **Processors** weren't required to notify at all, regardless of what they were doing.

Note:

The process of 'notification' was also re-badged under the new Law and it is now known as 'registration'.

Why were organisations given extra time to get ready for this?

To give **controllers** and **processors** a chance to adapt to this new requirement to register with the **ODPA**, a year's transitional relief was given.

What do organisations need to do to comply with this new duty?

The new Law will likely remove the exemptions above on 31 Dec 2019. Note this is different to all the other duties in that the transition extends beyond 25 May 2019.

This means that from 2020 onwards **all organisations processing personal data** are legally required to register with the ODPA and pay the annual fee, regardless of why they are processing personal data or whether they are a **controller** or **processor**. Charities, not-for-profit organisations and elected members of government must register, but they don't have to pay the fee.

Organisations can register with the **ODPA** online at ***odpa.gg/online-notification.***

Work is underway to put together a new fees regime, more details on what this looks like will be released in 2019.

How this might work in the real world...

Moving & Shaking have been aware of their need to be registered with the **ODPA** as a **controller** under the old 2001 data protection law. So they will continue to renew their registration each year, and will continue to pay the associated cost.

The landlords they work alongside may have been exempt from the need to register with the **ODPA** under the old law.

In the run-up to January 2020, Moving & Shaking will be contacting all the landlords they work with to encourage them to complete their own registration with the **ODPA** if they have not already done so. This is good business sense, as Moving & Shaking are in a joint-**controller** relationship with their landlords so it's essential that all parties are conducting themselves in a reputable way and are meeting their respective legal responsibilities.

Advice & guidance

The **ODPA** is here to help all local organisations achieve compliance with ***The Data Protection (Bailiwick of Guernsey) Law, 2017.***

- You will find more guidance, templates, checklists, Q&As at **odpa.gg/all-about-transition.**
- If you have a specific issue you would like to talk to us about please visit **odpa.gg/contact-us** and **request an appointment**, or come along to our fortnightly drop-in sessions every other Wednesday morning from 09:00 – 12:00.
- You can also call us on **+44 1481 742074** or email **enquiries@odpa.gg** for general advice.