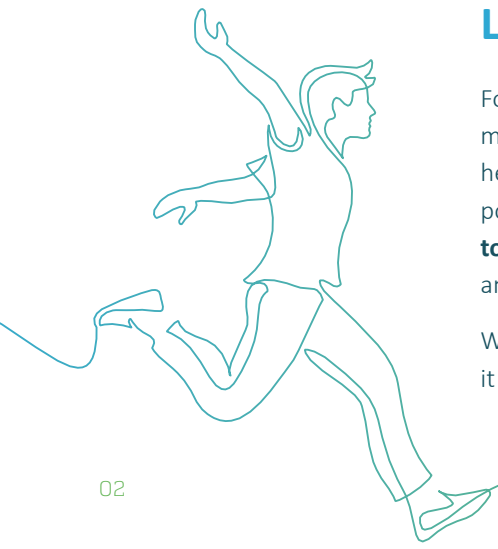
THE OFFICE OF THE
Data Protection Authority

The Feel-Good Guide to Data Protection

Visit **odpa.gg** for more detail on everything covered in this Guide.

THE OFFICE OF THE
Data Protection Authority

This guide is for those of you who may be new to data protection, or anyone who just wants an easy and enjoyable introduction that will help get your organisation/business up to speed, and inform/empower you as a citizen.



Let's be positive

Forget any negative preconceptions you may have. This guide has been written to help you engage with data protection in a positive way. We want you to see its **value to individuals**, its **benefits to business**, and its **place in human society**.

We want to leave you feeling so good about it that you are motivated to learn more.

In this guide you will discover that data protection boils down to treating people well. If you take away one thing from reading this guide, let it be that.

We know that data protection can feel complicated, particularly some of the terminology used, so please remember that we are here to make it as simple as possible.

In this guide you will discover that **data protection boils down to treating people well.** If you take away one thing from reading this guide, let it be that.

IF YOU NEED HELP WITH ANYTHING PLEASE GET IN TOUCH.
Or come along to one of our drop-in sessions, request a study visit, take a look at our events, or see if any of our online resources can help you.

In this guide we cover:

1. What 'personal data' is (and is not).

2. What 'processing' personal data means.

3. What the aim of data protection is.

4. Why you should care about protecting people's data.

5. What your organisation/business's duties are under local data protection law.

6. How to get started on bringing your activities in-line with the Law.

7. How your organisation/business benefits from protecting the personal data in its care.

8. Where to get advice, support and guidance.

THE OFFICE OF THE
Data Protection Authority

1: What 'personal data' is (and is not)

'Personal data' has a very broad legal definition, it is: 'any information relating to an identified or identifiable [living] individual'.

The scope of what is considered 'personal data' expands even further when you consider that it includes both **factual** information about people as well as **opinions** expressed about people. It also includes anonymised data that could identify people if it was combined with other information.

Examples of personal data include:

- ✔ Your name
- ✔ Your address
- ✔ Your email
- ✔ Your browsing history
- ✔ Your car's registration
- ✔ What your boss once wrote in an HR file about you
- ✔ Your social security number
- ✔ Any other information related to you

Personal data does not include:

- ✖ Any data about a **dead person**
- ✖ Any information, facts or opinions that **do not relate to, or identify people** (e.g. employment statistics, or anything else that has been irreversibly anonymised)

What about 'special category data'?

Within the overarching term 'personal data' there is a sub-category called 'special category data' – this is a specific list of types of data that need **extra protection** because of the harms that may result if this data is mis-used:

- Racial or ethnic origin
- Political opinion
- Religious beliefs or similar
- Trade union membership
- Physical or mental health or wellbeing
- Sexual life
- Criminal proceedings
- Convictions
- Genetics
- Biometrics

WHAT'S NEXT? Now that we know what personal data is, let's move on to what is meant by 'processing' it.

2: What 'processing' personal data means

If you thought the definition of 'personal data' was broad, the legal definition of 'processing' it is equally broad: 'Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.'

In plain English, 'processing' can be summed up as: **anything you do with personal data.**

Examples of processing include:

- ✔ Collection
- ✔ Consultation
- ✔ Recording
- ✔ Use
- ✔ Organisation
- ✔ Disclosure
- ✔ Structuring
- ✔ Dissemination
- ✔ Storage
- ✔ Restriction
- ✔ Alteration
- ✔ Erasure
- ✔ Retrieval
- ✔ Destruction

What is 'high-risk' processing?

This is if you are doing something with people's data that could pose a high-risk to what the Law refers to as their '**significant interests**'.

'Significant interests' are **any aspect of someone's life** that could be negatively impacted due to the way their personal data is used. This could include their physical safety, and their reputation, and could extend to placing them at risk of identity theft, fraud, financial loss, psychological distress or humiliation.

This means you must think carefully about how what you are doing with the data will, or may, **affect people**.

As with most risk, it is very **context dependent** and you will need to think carefully about how you make assessments. There are certain areas of processing which often bring higher risks and these could include things like:

- ✔ Using artificial intelligence/machine-learning or other automated systems to make decisions about people
- ✔ Refusal of service activity (e.g. credit checks, mortgage/insurance applications etc)
- ✔ Large-scale processing of special category data (e.g. for healthcare purposes)
- ✔ Large-scale and systematic monitoring of a public place (e.g. CCTV)

WHAT'S NEXT? Now that we know what personal data is and what's meant by processing it, let's move on to what the aim of data protection is.

THE OFFICE OF THE
Data Protection Authority

3: What the aim of data protection is

Myths, confusion and misunderstandings swirl around data protection. But at its heart, it's very simple indeed – data protection is about treating people well.

In some people's minds, data protection is: optional, an inconvenience, a burden, a barrier. Others see it as: a pre-condition to good business practices, a framework for the fair treatment of people, and an enabler of innovation. Regardless of your personal view, the undeniable reality is:

data protection = people protection

Its aim is to ensure people are treated fairly and lawfully, protecting them from harms that can arise from their personal data being mis-used. Data protection legislation (globally) provides the legal framework and protections for people and their data, recognising that it matters how people are treated.

The human at the heart

Our local data protection law gives individuals 10 specific rights around how information about them should be treated. And it places obligations on organisations/businesses to ensure that they use people's data properly.

The Law defines the 'rules of the road', and aims to ensure our rights as individuals are respected by those organisations/businesses who need to use our personal data to perform a task or function.

Data protection says 'no'

To be clear, data protection legislation does not aim to stop any particular activity.

✖ **Myth:** "I can't do that because of data protection."

Quite the opposite, it exists to facilitate the safe, legal, and proper use of people's data.

✔ **Reality:** "I can do that as long as I treat people properly."

Data protection as an enabler

Going further: looking after data well, within the legal confines that exist, assists you in performing your organisation/business's tasks and functions.

If you are using your customer/supplier/staff/service-user/member/citizen's personal data to do something for your organisation/business you need to be sure the data you are using is:

- ✔ Secure
- ✔ Accurate
- ✔ Accessible*
- ✔ Fit for purpose
- ✔ Has been obtained and used legally
- ✔ The people whose data it is knows you have it and what you're doing with it

**(only to those that need it)*

If you are adhering to your duties under the data protection law all the above is taken care of. This will give you confidence to know that you can rely on the data you have and the decisions you make off the back of its use.

WHAT'S NEXT? Now that we know what personal data is, what's meant by processing it, what the aim of data protection is, let's move on to why you should care about all this.

4: Why you should care about protecting people's data

The world is changing fast. One important change continues to be the role of data. We are, both in our personal and professional lives, immersed in data and it influences us in ways we are aware of and also ways we may be entirely ignorant about. It can inform and empower when used well and it can exploit and disempower when used badly.

We want the Bailiwick to recognise the importance of data governance for our economy and for the wellbeing of our citizens because, as you now know, data protection is people protection. So if you care about treating your fellow humans with the dignity and respect you'd like for yourself and your loved ones, then you will care about protecting people's data. Always keep in mind data protection is about preventing people from being harmed.

When data is not protected it can lead to **data harms**.

Data harms are what happens when people are negatively impacted because information about them has been mis-used or mishandled.

You are fortunate if you, or someone you know, has not suffered a data harm. Anyone who has will tell you that mishandling personal data can, in extreme cases, ruin people's: lives, careers, reputations, and relationships.

Also remember that data harms can also affect a business's (or jurisdiction's) reputation because trust and confidence is at the heart of much economic activity too.

If you care about treating people well and preserving your organisation's reputation, you will want to avoid being responsible for harming people.

If you only start caring about looking after people's data **after** something has gone terribly wrong – that harm can often not be undone.

Examples of data harms:

- Loss, or alteration, of medical records leading to serious health problems
- Disclosing someone's sensitive information to their colleagues
- Disclosing false information about someone which damages their reputation
- Accessing information about people for inappropriate/illegal use
- Failing to secure people's data against a cyber attack on your systems
- Deleting personal data deliberately to remove evidence of your wrongdoing
- Failing to store people's data securely putting them at risk of identity theft
- Illegally obtaining and selling people's data
- Basing decisions on out of date or incorrect data

WHAT'S NEXT? Now that we know what personal data is, what's meant by processing it, what the aim of data protection is, and why you should care about all this, let's move on to what your duties as an organisation/business are.

THE OFFICE OF THE
Data Protection Authority

5: What your organisation/business's duties are under local data protection law

As detailed already, the local data protection law gives individuals 10 rights and puts certain duties (or legal obligations) on organisations/businesses who use personal data.

These duties all flow from these seven principles:

1. LAWFULNESS, FAIRNESS & TRANSPARENCY

You must have a **valid legal reason** for processing personal data. You must obtain it without deceiving the person whose data it is, and you must make it clear exactly how you are going to use their data.

2. PURPOSE LIMITATION

You must **only** use personal data for the reason (or reasons) you have told the person you are using it for.

3. MINIMISATION

You must only ask for the **minimum amount** of personal data necessary from the person.

4. ACCURACY

You must ensure that any personal data you hold is **accurate** and where necessary, up-to-date.

5. STORAGE LIMITATION

You must not keep personal data for **longer than you need it for**. But bear in mind that this includes **keeping** data when necessary as well as **deleting** it when necessary.

6.INTEGRITY AND CONFIDENTIALITY

You must **keep personal data 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. You must be able to **demonstrate that you take responsibility** for how you look after personal data.

Because the law is principles-based, there isn't exactly a helpful set of precise rules for you to follow (e.g. 'you must delete data after x number of years'). But the good news is that in many cases (except where required by law/statute) you are free to make your own decisions about how you apply the principles above to your activities. The key thing is to **get to know your own data processing practices, the Law and its principles as well as you can, keep protection of individuals' rights at the heart of what you do, and document your decision-making.**

WHAT'S NEXT?
Now that we know what personal data is, what's meant by processing it, what the aim of data protection is, why you should care about all this, what your duties as an organisation/business are, let's move on to how to start putting all this into practice.

6: How to get started on bringing your activities in-line with the Law

First, a caveat: you are not expected to do all of this overnight. Data protection is never 'done'. It is not a once-a-year box ticking exercise, it is a continuous process, determined by human behaviour, choices and attitudes.

Here are some steps you can take to start on the journey:

Step #1

Read up on and **increase your own understanding of the Law**, this is the single most useful step you can take.

Step #2

Got a board of directors/ management team? Make sure understanding of and compliance with data protection law is firmly on their agenda and that they know **they are responsible** for it.

Step #3

Add data protection to your **risk register**.

Step #4

Get to know your data. Treat the data you process as you would any other item of value. Do an inventory - What do you have? Where is it? Who has access to it? What are the policies and procedures around it? A comprehensive data audit is fundamental.

Step #5

Determine, and document in your Data Processing Notice which **lawful processing conditions** you rely on for each area of processing (note: you are likely to be using different conditions for different purposes).

Step #6

Document your processing. This fulfils **your legal duty to keep records**.

Step #7

Look at each data collection point you have and ensure you are fulfilling **your legal obligation to provide detailed information about the processing to people** (aka: publish your Data Processing Notice). If you are relying on consent, check that the method you're using meets the higher standard required under the law.

Step #8

Ensure data protection is covered in your staff contracts and handbook, and hold **regular awareness-raising activities** with all your staff.

Step #9

Ensure all your staff understand their responsibilities and understand what **individuals' 10 rights** are.

Step #10

Ensure you have **appropriate security and safeguards** around all your data, both electronic and hard copy.

Step #11

Be aware of **your legal requirement to report data breaches**.

Step #12

Review all relationships you have with **third parties** where data is involved. Review and update the contracts you have with them.

Step #13

Maintain your annual registration with the ODPA.

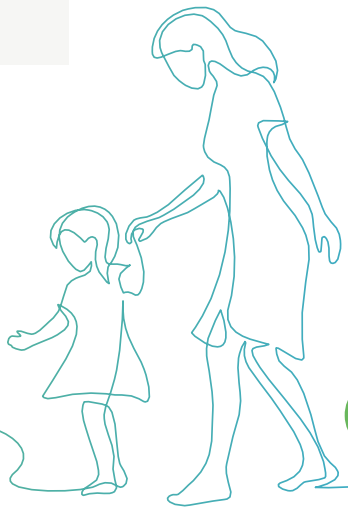
Step #14

Focus on the **accountability principle** – how will you demonstrate that you are taking responsibility for what you're doing with people's data both for internal governance purposes but also in case you have to respond to an enquiry from the ODPA?

WHAT'S NEXT?

Now that we know what personal data is, what's meant by processing it, what the aim of data protection is, why you should care about all this, what your duties as an organisation/ business are, and how to put it all into practice. Next let's find out how your organisation/ business will benefit from all this.

FOR MORE INFORMATION TO HELP YOU TAKE THESE STEPS VISIT:
odpa.gg/for-organisations/your-obligations



THE OFFICE OF THE
Data Protection Authority

7: How your organisation/business benefits from protecting the personal data in its care

If your organisation/business treats every person it encounters with dignity and respect, and takes account of the data protection principles you will reap the following rewards:

✔ Trust and confidence

If your customers/staff/service users/members/citizens can see that you are **treating them properly** and that you care about looking after their data well they will trust you more and have greater confidence that you are operating with their interests in mind. This in turn leads to:

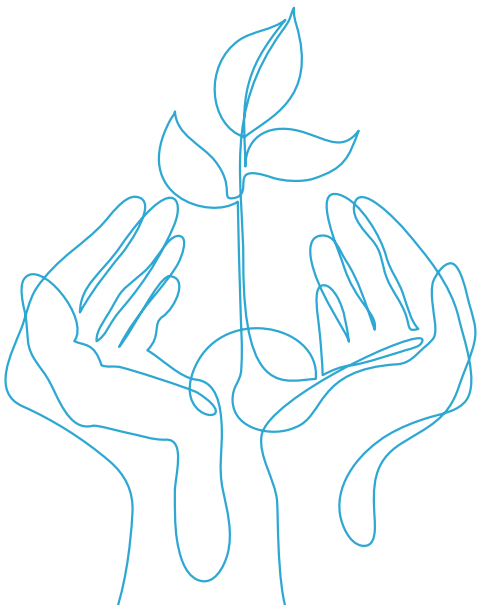
✔ Customer retention

A person who trusts you and has confidence in what you're doing is **more likely to be loyal to you** and continue the established relationship you have.

✔ Reputation

If you are keeping people happy by treating them well, and taking your legal obligations seriously you are likely to retain (or build) a good reputation.

Conversely, if you are not taking any of this seriously and you accidentally, or negligently, cause serious harm to someone your organisation/business will, rightly, take a major hit to its reputation as a result. Trust is built up over a long time but can be lost in a single moment.



✔ Harm prevention

Taking all reasonable steps to avoid causing serious harm to people (which is exactly what you are doing if you are adhering to data protection law) should be seen as a **bare minimum** for running your organisation/business well.

✔ Effectiveness

If you are making decisions about people, or making use of people's data in the course of your working day, the **data you have must be reliable and fit-for-purpose**. Data is a valuable asset for all organisations and should be treated as such. If the data is of poor quality or badly handled how well can you perform the tasks you are using it for?

WHAT'S NEXT? Now that we know what personal data is, what's meant by processing it, what the aim of data protection is, why you should care about all this, what your duties as an organisation/business are, how to put it all into practice, and how your organisation/business will benefit from all this. Let's finish up on where you can go for advice, support, and guidance.

8: Where to get advice, support and guidance

We know, even with the best of intentions, data protection can sometimes feel 'too difficult'. We hope that this guide has communicated the real benefits and value of protecting personal data, and that you feel motivated to discover more.

Visit odpa.gg for accessible, useful, and hopefully inspiring content: including our official guidance, blogs, podcasts etc. You will also find details of how we can help you in-person via our events, drop-ins, and study visits.

Who we are

We are the Bailiwick of Guernsey's independent authority which regulates data protection legislation through an ethics-based approach, empowers individuals and protects their rights, promotes excellence in data protection, and supports the data economy to embrace innovation.

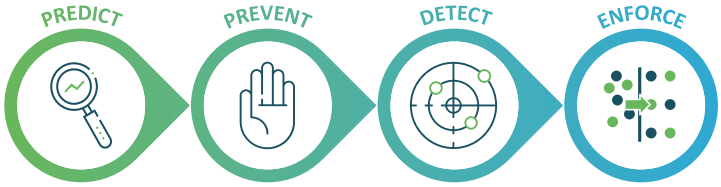
Our mission

We promote high standards of data protection in our community by:

- ✔ Promoting responsible handling of personal data through education and information
- ✔ Preventing poor data handling which would not meet legal or ethical requirements
- ✔ Taking action against significant non-compliance

This mission aims to benefit individuals, organisations, and our society, against the backdrop of major technological and social change.

Our strategy: We seek to predict and prevent harms to individuals from poor handling of their personal data and ensure that our detection and enforcement activities are proportionate and effective.



Our key strategic objectives are:

1. To develop our capabilities to deliver on our enhanced statutory duties.
2. To be a relevant, responsive and effective regulator.
3. To support organisations in delivering their obligations and empower individuals to exercise their rights.
4. To develop and maintain effective relationships.
5. To elevate discussions around the protection of personal data to engage the community and individuals in a relevant and positive way, recognising the personal, social and economic opportunities and threats that the data economy poses.

If you have any feedback on this guide please email **communications@odpa.gg**

+44 (0) 1481 **742074** | **enquiries**@odpa.gg | **odpa**.gg

THE OFFICE OF THE
Data Protection Authority