THE OFFICE OF THE
Data Protection
Authority

Why you should care about data protection

Hint: it's about protecting you

What is data protection & why should you care?

Data protection, in a nutshell, is in fact people protection. So, if you care about protecting yourself, and your loved ones, you should care about data protection. Data protection legislation requires organisations to look after your **personal information*** in a way that protects your privacy and respects your rights under that legislation.

Good data protection is when organisations treat your information with the care and respect it deserves, they maintain an accurate and up-to-date record of it, and they give you control over how it is used.

Bad data protection is when organisations do not look after your information. They could delete it accidentally, they may send it to someone else in error, they might deliberately sell it to someone else, or they could start using your information for purposes you were not aware of. Or they could damage your reputation by sharing incorrect information about you.

Three reasons why you should care about data protection:

- It helps **protect you** and your loved ones**
- It gives you the power over how organisations use your personal information
- It gives you legal means to pursue organisations who don't look after your personal information

***'Personal information' under data protection legislation can mean a huge range of things such as:**

Your name, your address, your medical records, CCTV footage of you, your social media activity, your internet browsing history, what your boss once said in an email about you, your political views, your sexuality – in short, ***it's any information that relates to an identifiable living person.***

****'It helps protect you and your loved ones' from risks to:**

Your physical safety, identity theft, fraud, financial loss, psychological distress, humiliation, or ***any other aspect of your life that could be put at risk by your personal information being misused.***

Message from the Data Protection Commissioner

Thank you for taking an interest in how you can protect yourself and your loved ones through understanding more about data protection.

My office regulates the local data protection legislation, and as such, we stand shoulder to shoulder with you, as a citizen of Herm, Sark, Alderney or Guernsey. Our role is to raise awareness of your rights under our local Law, and to make sure all local organisations respect them. If organisations ignore your rights, we can take action against them, and since our Law was strengthened in May 2018, this action can include issuing of fines up to £10 million to the worst offenders.

Remember - **you are the reason data protection legislation exists**. **You** are at the heart of our local Law. This Law gives **you** ten legal rights that local organisations must respect – details of these are overleaf. If you feel that a local organisation is not respecting **your** rights read the ***Five Steps to Exercising Your Rights*** included in the back pages of this leaflet.

I hope that after reading this leaflet you feel more informed about why data protection matters, why you should care about it, and how you can exercise your legal rights. But more than that, I hope that local organisations treat you with the care you deserve so that you never need to exercise your rights.

> **You are the reason data protection legislation exists. You are at the heart of our local Law.**

Emma Martins

Data Protection Commissioner (Bailiwick of Guernsey)

You have the following ten rights under

The Data Protection (Bailiwick of Guernsey) Law, 2017

1. Right to information about why personal data is collected from you

When you are asked to provide any information about yourself to any organisation, there is a legal requirement for them to make it clear who they are and what exactly is going to happen to your data – in legal terms this is known as giving you 'fair processing information'. Organisations usually provide this information in their Privacy Policy or a Data Collection Statement.

2. Right of access

This entitles you to ask what data an organisation holds about you and why by submitting a 'subject access request'. Organisations must respond to your request within one month, although this can be extended if the request is complex.

3. Right to object to processing for direct marketing purposes

If an organisation is using your personal data to market products or services to you, you have a right to tell them to stop. You should write directly to the organisation to request they stop, and they must stop sending you material when you ask.

7. Right to erasure

This right is sometimes called the 'right to be forgotten'. In certain circumstances, you have the right to tell an organisation to delete your information from their records entirely.

8. Right to restriction of processing

In certain circumstances you have the right to tell an organisation that they can only use your information for a specific purpose, or purposes.

4. Right to object to processing on grounds of public interest

This right is difficult to sum up as there are occasions where it doesn't apply. Broadly speaking, it means that if any organisation (including public authorities, such as the States of Guernsey) says it is processing your personal data because it is in their 'legitimate interests', or in the public interest, you have a right to ask them to stop. However, they can refuse your request if they can prove their reasons outweigh your reasons for wanting them to stop.

5. Right to object to processing for historical or scientific purposes

If an organisation is using your personal data for historical research or scientific purposes, you have a right to ask them to stop.

6. Right to rectification

If an organisation has information about you that is not factually correct or accurate you have the right to have the information put right.

9. Right to not be subject to decisions based on automated processing

This means that you have the right to ask for a human being only to make decisions about your information. This is to avoid the "computer says no" scenario whereby you may be refused a product or service solely based on an algorithm, or other automated decision-making processes.

10. Right of data portability

You can use this right from 25 May 2019 onwards. It means you can tell an organisation to remove your information from their systems and give it to you in a format that is 'machine-readable' so that it can be easily transported and entered into another organisation's IT system.

Five steps to exercising your rights

1. If you need any **advice** on your rights give us a call on **+44 1481 742074** or email **enquiries@odpa.gg**.

2. Contact the organisation you are concerned about, in writing, and explain to them **which of your ten rights** you want to exercise.

3. If the organisation doesn't respond **within one month,** send a chaser message, and if they still don't respond let us know and **we will intervene on your behalf** with the organisation.

4. If you are not happy with the response you get contact us and **we will investigate** whether the organisation has fulfilled their legal responsibilities to you.

5. Remember that whilst you can make a request to an organisation - the organisation **may be able to refuse your request** whilst still acting within the Law. In this circumstance we will assist you in understanding why, and whether there are other legal avenues you can pursue in order to get the matter resolved.

The Seven Data Protection Principles

Any organisations who handle (or 'process') your personal information must adhere to these principles:

1. Lawfulness, fairness and 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 and 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. Organisations must show that they take responsibility for how they look after your information.

THE OFFICE OF THE
Data Protection Authority

The Office of the Data Protection Authority:

- Empowers individuals and protects their rights
- Promotes excellence in data protection
- Supports the data economy to embrace innovation
- Regulates data protection legislation through an ethics-based approach

Excellence Through Ethics.

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