#ItsAllAboutYou

PRIVACY
TOOLKIT

WWW.JERSEYOIC.ORG

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

V1.1

CONTENTS

Please click on the titles to go to each sub section.

Privacy Toolkit

Organisations collect, store and use vast amounts of information about YOU.

Your personal information is important - take care of it.

The more organisations know about us, the more power they can have over us. Personal data is used to make very important decisions in our lives.

Personal data can be used in a way that affects our reputations; and it can be used to influence our decisions and shape our behaviour. And in the wrong hands, personal data can be used to cause us great harm.

Who we are & what we do

The Jersey Office of the Information Commissioner is part of the Jersey Data Protection Authority. We are the independent office responsible for overseeing the Data Protection (Jersey) Law 2018 and the Freedom of Information (Jersey) Law 2011.

The Data Protection (Jersey) Law 2018 gives individuals important rights including (but not limited to) the right to know what information is held about them, how that information is going to be handled, and the right to request correction of their information. This Law helps to protect the interests of individuals by obligating organisations to manage the personal information they hold in a fair, lawful and transparent way, as well as being accountable to their customers and to themselves for their actions.

The Data Protection (Jersey) Law 2018

Gives **YOU** important rights when it comes to your personal information.

Our **'Privacy Toolkit'** demystifies your rights and key data protection matters to help in your busy everyday lives.

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

2nd Floor, 5 Castle Street,
St. Helier, Jersey, JE2 3BT

Email: enquiries@jerseyoic.org
Telephone: +44 (0) 1534 716530
Web: www.jerseyoic.org

SURVEILLANCE
AT HOME

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

CCTV is, arguably, the most privacy intrusive form of data processing undertaken which presents the greatest risk to data subjects.

- CCTV should be used only to address real and serious threats to individual health and safety or the protection of property.
- CCTV should be used only as a last resort, when other less intrusive approaches have failed.

It is important to take every reasonable measure to limit the collection of personal data from innocent people and to destroy it when it is no longer required for the original purpose.

Disclosure of video images can cause mental distress, loss of dignity, and loss of rights and freedoms for innocent people.

The awareness of being filmed by a camera may cause individuals to alter their behaviour and can cause discomfort or stress. In any case, the mere existence of the camera has potential to undermine personal freedom.

Domestic CCTV systems - checklist for people using CCTV around the home

Before installing a CCTV system or continuing with an existing CCTV surveillance system the following checklist will help you to determine whether you are required to comply with the Data Protection (Jersey) Law 2018.

FYI

Recording images of family members in a home JUST for a family purpose is not subject to the Data Protection (Jersey) Law.

The Data Protection (Jersey) Law 2018 (DP(J)L) sets out the rights of individuals in respect of their personal information as well as the obligations and conditions organisations must follow to process it. The collection, use, disclosure and retention of personal data, including still or moving images, film footage and voice recordings, are all subject to the requirements of the DP(J)L.

Depending on the location and positioning of your CCTV camera, you may need to comply with the DP(J)L.

Does your CCTV capture images of people outside the boundaries of your private domestic property – for example, in neighbours' homes or gardens, shared spaces or on a public footpath or a street?

NO

It records just my property – and my family. You will not need to comply with the DP(J)L.

YES

You will need to meet certain requirements of the DP(J)L. See next page.

Purpose of your CCTV

Is there a pressing need to install a 'surveillance' type of system?

→ *What are you trying to observe taking place and why?*

Is there any less privacy-intrusive alternative other than using a surveillance system?

→ *Have you tried those alternatives and have they failed?*

What is the specific purpose for the use of the surveillance system?

→ *Security of my property?*

→ *Personal safety?*

→ *Do you have a different purpose?*

Clarity of purpose is essential under DP(J)L, as it ensures everyone understands what and why you are 'collecting' identifiable personal information. PLEASE NOTE that you are required to put up a sign, in the area of the camera(s). The sign must;

→ *Be clear, visible and readable.*

→ *Contain details of the **purpose** of the surveillance and who to contact about the recording.*

→ *Include contact details such as website address, telephone number or email address.*

PLEASE NOTE

If, for example, your notice says that you are recording the footage for monitoring the alleyway between houses for security reasons you cannot then decide to publish the footage on social media just because a 'funny' thing happened. This would be unlawful and in breach of the DP(J)L for which there are sanctions. It would be unlawful because you would be using the footage for a different purpose than set out on your sign and people wouldn't be expecting their information to be used in this way.

How do I use CCTV responsibly at home?

- If you install CCTV for other than a purely personal or domestic purpose, you will need to **register** with the Jersey Office of the Information Commissioner and pay a fee.
- Consult with your neighbours or those individuals likely to be affected with your CCTV use, to discuss your plans and what you will be doing with the footage. Address their worries and consider the impact on them.
- Consider if you really need CCTV and regularly review whether you still need it.
- Preferably disable any audio facility.
- Make sure date and time on the system are accurate.

Retention & Security

- Are you keeping the images recorded only as long as absolutely required for your purposes?
- Can you delete any unnecessary footage (for example footage of people innocently walking past your property) at the earliest opportunity? You must have access to the relevant technology to do this.
- What physical security measures are in place to prevent hacking or loss of footage?

- How are you restricting access to the footage within your family? Does your whole family need access to the footage or can access be restricted to one/two family members?
- If the States of Jersey Police or insurance companies request copies of your recording – ensure they provide you with an authority form and keep a copy of what you send until the conclusion of any investigation.
- If you share the footage with the States of Jersey Police or your insurance company you should only send as much footage as is needed to support your claim (if only 5 minutes of footage is relevant, you shouldn't need to send 24 hours worth).

Individual rights

[known as 'Subject Access' Rights in DP(J)L]

- Are you able to respond to subject access requests? [Information rights for individuals specified within the Law] You must be able to provide individuals [data subjects] with access to their own information without disclosing that of others.
- Do you have the ability to locate and provide an individual with a copy of their own information while deleting or blurring the images of others to prevent third party identification? If you cannot delete or blur the images electronically, can you provide the information in another way e.g. by providing stills/screenshots of the images captured and blanking out the faces of other individuals?

What happens if I break the law?

- You may be subject to investigation and possible enforcement action.
- You may also be subject to legal action by affected individuals.

FYI

The DP(J)L is very clear about disclosing 3rd party information in response to a subject access request.

If the supplying of information under Article 28 (4) requires the disclosing of information relating to another individual who can be identified from that information, the controller is not obliged to enable such information to be supplied unless –

(a) the other individual has consented to the disclosure of the information to the person making the request; or

(b) it is reasonable in all the circumstances to do so without the consent of the other individual

Background information

The DP(J)L defines 'data' as meaning any information that:

- Is being processed by means of equipment operating automatically in response to instructions given for that purpose
- Is recorded with the intention that it should be processed by means of such equipment
- Is recorded as part of a filing system or with the intention that it should form part of a filing system
- Is recorded information held by a scheduled public authority and does not fall into any of the above three categories

Personal data

The DP(J)L applies to 'personal data' meaning any information relating to an identifiable, natural, living person who can be directly or indirectly identified in particular by reference to an identifier (the "data subject").

CCTV AND ME

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

CCTV & ME

CCTV is the most privacy intrusive form of personal information processing undertaken presenting the greatest risk to individuals (data subjects).

With the consistent evolution of technology, it's no surprise that the use of CCTV surveillance has become part of our daily lives. CCTV has many legitimate uses particularly in relation to security, prevention and detection of crime, however, with the technology so readily available it can also raise concerns in relation to an individual's rights should excessive monitoring be taking place.

Organisations and businesses use CCTV and sometimes individuals do too. Some users of domestic CCTV need to comply with the **Data Protection (Jersey) Law 2018** (DPJL); it depends on what the camera can see. If a CCTV system captures images of people outside the boundary of their private domestic property – for example, from neighbours' homes or gardens, shared spaces, or from public areas, then they will need to comply with the DPJL. The DPJL doesn't apply, however, if the cameras only cover the user's private property and it doesn't capture images beyond their boundaries.

It's not a breach of the law for people to have CCTV, they just need to comply with the law when it applies to them and when it does, respect the data protection rights of those whose images they capture.

Is CCTV Personal Information?

Personal information is information that relates to an identified or identifiable living individual. Frequently the terms personal information and/or data are associated with details than can be written down such as names, address, social security number etc. However, a person's image or voice is a visible identifier therefore recordings via CCTV are a form of personal information.

Legal Basis - Is Consent Required?

All processing of personal data requires a legal basis and if an organisation or business (the data controller as defined in the DPJL) is recording CCTV they must clearly understand what the legal basis for doing so is. In the majority of cases, CCTV footage may be recorded based on an organisation's legitimate interest to protect their premises and property from crime or damage, or to ensure the health and safety of staff members and the public

If a data controller uses CCTV based upon their legitimate interests, they must be able to clearly demonstrate the reasons for doing so. If you are not satisfied that their use of CCTV is justified or proportionate in terms of its impact upon you, you have a right to make a complaint to the JOIC.

What are my rights?

RIGHT TO BE INFORMED

Under the DPJL you have the right to be informed about the collection and use of your personal information. This applies to the recording of your image and or voice by CCTV Surveillance.

If CCTV recording is taking place there should be clear signs informing you of this and the purpose for this information being collected. The signs should also provide the contact details of the relevant data controller or their agent, should you wish to get more information or access your personal data.

RIGHT TO ACCESS

To ask for a copy of the information that is held about you. This is known as making a **subject access request**. You can ask verbally or in writing for copies of any footage where your image is identifiable. The CCTV user must respond to this request within one month. Bear in mind that if they regularly delete footage they no longer need, they might not hold your images.

RIGHT TO ERASURE

To ask the CCTV user to **erase** any personal data they hold about you.

RIGHT TO OBJECT

To ask that the CCTV user **does not capture** any footage of you in future. However, the nature of CCTV systems may make this very difficult and it might not be possible for the user to do this.

You have a complaint

Where you consider that your rights have been infringed by the use of CCTV, in the first instance contact the organisation, business or person responsible for the camera. You can use a **template letter** from our website. If they do not respond to you in 4 weeks or you feel that the answer is unsatisfactory you have the right to **complain to us**.

There is further information on our complaint handling process available on our website.

Covert Filming

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on an exceptional, case-by-case basis, where the data are kept for the purposes of preventing, detecting, or investigating offences, or apprehending or prosecuting offenders.

Online Publication of Recordings

If you are aware that your image or recorded footage has been published on a social media platform online, you can request that the social media platform used remove it.

All social media platforms now have functions to report content that are in breach of their code of conduct. With millions of users accessing social media every day each platform will have a specified timeframe that they aim to review and action any reports that have been made.

1

CCTV & ME

What rights does an individual have in relation to CCTV recording?

2

What you should be informed of if you're subject to CCTV Recording;

- *The purposes for doing so i.e. Prevention of Crime, Health & Safety etc.*
- *Contact details of the data controller*

3

If you think you have been recorded without your knowledge;

- *Contact the data controller. Subject Access Request*
- *If unsatisfied contact JOIC to discuss further*

RIGHTS REGARDING **AUTOMATED DECISON-MAKING**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

Rights regarding Automated Decision-Making

Some service providers use computer programs and algorithms, rather than the personal judgement of employees, to adjudicate applications from individuals for services or financial benefits. This is called 'automated processing'.

Except where automated processing is expressly authorised under another law, you have a right under the Data Protection (Jersey) Law 2018 to:

- object to having your application decided by automated processing.
- In cases where you have provided your consent or entered into a contract with a service provider where automated processing is necessary, you retain the right to request human intervention so that you can express your point of view and contest the decision.

Human intervention

If you request such human intervention, the service provider must ensure:

- that it carefully analyses the decision and considers all the relevant information. Merely conducting a token review is not acceptable. Someone who has the authority and competence to change the decision should conduct the review.

FYI

If you wish to exercise this right, inform your service provider. If you are dissatisfied with the response of the service provider, you may make a formal complaint to the **Jersey Office of the Information Commissioner**. Further useful information can be found by clicking here.

You also have the right to request access to any of your personal data used by automated processing to make a decision about you. If you wish to exercise this right, make a subject access request to the service provider. If you are dissatisfied with the response of the service provider, you may make a formal complaint to the Jersey Office of the Information Commissioner.

Click here for more information about making a request.

KEY TERMS IN
DATA PROTECTION

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

Personal data

The term ‘personal data’ means any data (information) concerning or relating to a natural, living person who is either identified or identifiable (such a person is referred to as a ‘data subject’).

An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Processing

The term ‘processing’ refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

Supervisory authority

The Jersey Office of the Information Commissioner (JOIC) is part of the Jersey Data Protection Authority. JOIC is the independent supervisory authority responsible for overseeing the Data Protection (Jersey) Law 2018 (DP(J)L) and the Freedom of Information (Jersey) Law 2011 and promoting respect for privacy and information rights of individuals.

JOIC’s misson

→ *provide the people of Jersey with a high standard of data protection;*

→ *practically and ethically promote the information rights of individuals;*

→ *carry out our regulatory role so as to support the delivery of public services; and promote the social and economic interests of the island*

The DP(J)L gives individuals important rights including (but not limited to) the right to know what information is held about them, how that information is going to be handled, and the right to request correction of their information. It helps to protect the interests of individuals by obligating organisations to manage the personal information they hold in a fair, lawful and transparent way, as well as being accountable to their customers and to themselves for their actions.

Data Controller

A ‘data controller’ refers to a natural person, legal person (e.g. a company), charity or other body that whether alone or jointly with others decides the purposes and means of processing personal data.

Data Processor

A ‘data processor’ refers to a person, company, or other body which processes personal data on behalf of a data controller and in accordance with the data controller’s written instructions.

Consent

Some types of processing are carried out on the basis that you have given your consent. Under the DP(J)L, consent to processing must be freely given, specific, and informed. You cannot be forced to give your consent, you must be told what purpose(s) your data will be used for, and you should show your consent through a 'statement or as a clear affirmative action' (e.g. actively ticking a box as opposed to unticking it).

Consent is not the only lawful basis on which your personal data can be processed. Schedule 2 Part 1 of the DP(J)L sets out the standard list of lawful reasons for processing 'ordinary' (so non-special category) personal data as:

- *Consent.*
- *To carry out a contract.*
- *In order for an organisation to meet a legal obligation.*
- *Where processing the personal data is necessary to protect the vital interests of a person.*
- *Where processing the personal data is necessary for the performance of a task carried out in the public interest.*
- *In the legitimate interests of a company/organisation (except where those interests contradict or harm the interests or rights and freedoms of the individual).**
- **It is important to note that Schedule 2, part 1-5(b) provides that the 'legitimate interests' reason is not available to public authorities where the processing is being conducted in the exercise of their functions.*

'Ordinary' data may also be processed under one of the categories as set out in Schedule 2 Part 2.

Special category data

Special category data is personal data which the DP(J)L says is more sensitive, and so needs more protection. In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms if it is lost. For example, by putting them at risk of unlawful discrimination.

These are listed under Article 1 of the DP(J)L

- *data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;*
- *genetic or biometric data that is processed for the purpose of uniquely identifying a natural person;*
- *data concerning health;*
- *data concerning a natural person's sex life or sexual orientation; or*
- *data relating to a natural person's criminal record or alleged criminal activity*

In order to process special category data an organisation must be able to specifically satisfy one of the requirements as set out in Schedule 2 Part 2 Profiling

Profiling is any kind of automated processing of personal data that involves analysing or predicting your behaviour, habits or interests.

Privacy Policy

A privacy policy (also sometimes called a privacy 'notice' or 'statement') is a statement that explains the ways a data controller or data processor gathers, uses, discloses, and manages a customer, staff or client's data. It is used by controllers and processors as a way of fulfilling the legal requirement to inform data subjects as to how personal data is being collected and used.

It also informs the individual whether that information is shared with partners, sold to other firms or enterprises or transferred outside of Jersey. Information about retention and data subjects' rights (including the right to make a complaint) will also be set out in the policy.

TOP SOCIAL MEDIA
PRIVACY TIPS

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

How to take control of your personal information on social media platforms

The privacy and advertising settings on social media apps and websites should give you control over how your personal information is used. We always advise those who use social media to check their privacy and advertising settings before using a particular service and to review them regularly, particularly after any new settings are introduced.

Setting up an account

- *Make sure you're signing into the real social network website.*
- *Use a strong, unique password for each social network. If it is strong you shouldn't need to change it regularly but you should change it if you think your social media account has been accessed unlawfully. You may wish to use a password manager application to help generate unique passwords and keep a record of them for you.*
- *Set up your security answers. This option is available for most social media sites.*
- *Set up two-factor authentication*

Proceed with caution

Be wary of suspicious direct messages and connection requests.

Do not share, retweet or tag profiles you don't recognise.

Click links with caution. Social media accounts are regularly hacked. Look out for language or content that does not look like something a connection of yours would post.

Think twice about

- *responding to ad hoc surveys ' which rock star are you most like' / 'what is the name of the street you grew up on' / ' what is the name of your first pet' as all too often surveys like these are trawling for personal information and may coincide with the answers to security questions used on banking platforms.*
- *Sharing images of your children, home etc – can you control who sees the images once they have been shared?*
- *Posting to say that you are away on holiday.*

Settings

Become familiar with the privacy policies of the social media channels you use and customise your privacy settings to control who sees what.

Protect your computer by installing antivirus software to safeguard. Also ensure that your browser, operating system, and software are kept up to date.

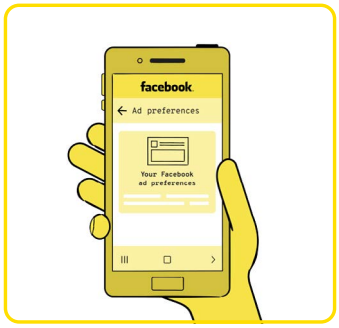
Audit social media access and permissions quarterly if using for business/club or other group type purposes.

How to view and change your advertising settings on Twitter

View your advertising information Under Personalisation and Data, you can control how advertisers target you with ads. You can turn off all personalised ads.

View your advertising information Under Personalisation and Data, you can control how advertisers target you with ads.
You can turn off all personalised ads.

How to view and change your advertising settings on Facebook



View your advertising information
Here you can make a number of choices about what information advertisers can use to target you, and which organisations can show you ads.

See what information third-party apps are currently collecting from you
Any app you use through Facebook that hasn't been created by a Facebook would be considered a third-party app.

This shows any apps linked to your Facebook account. You can see what personal data the app collects from Facebook. You can stop apps from continuing to collect data through. Facebook.

How to stop all third-party apps collecting data through Facebook
If you want to restrict all apps from collecting your personal data through Facebook, you can do so by disabling this function in the Facebook app.

This will turn off all third-party application access to the personal data you have on your Facebook account.

Following any of the above steps doesn't guarantee that the app provider has deleted or stopped using the data they have already collected. If you wish to be certain that this has happened, you can contact the organisation directly.

RIGHTS OF
DATA SUBJECTS

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

Rights of Data Subjects

Data protection is about the fair and proper use of information about people. It sits alongside the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

Every individual is entitled to have their personal information protected, used in a fair and legal way, and made available to them when they ask for a copy. If an individual feels that their personal information is wrong, they are entitled to ask for that information to be corrected.

Whilst data protection is key to innovation, good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.

Part 6 of the Data Protection (Jersey) Law 2018 gives rights to individuals in respect of personal data held about them by others.

The rights are:

- *Right to be informed*
- *Right to subject access*
- *Right to rectification*
- *Right to erasure*
- *Right to restriction of processing*
- *Right to data portability*
- *The right to object to processing for the purpose of public functions or legitimate interests for direct marketing purposes and for historical or scientific purposes*
- *Right regarding automated individual decision-making and profiling*

This is part of a series of guidance to help organisations fully understand their obligations, as well as to promote good practice.

THE RIGHT TO BE INFORMED
IF YOUR PERSONAL INFORMATION IS BEING USED

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

An organisation must inform you if it is using your personal data. Your personal information can only be used if it is being done so lawfully, fairly and transparently.

As per Article 28 of the Data Protection (Jersey) Law 2018

'An individual is entitled to be informed by a controller whether personal data of which that individual is the data subject are being processed by or on behalf of that controller'

Our 'no-nonsense' infographic explains your right to 'be informed' if your personal information is being used.

HAVE YOU BEEN INFORMED?

There are several things an organisation must inform you of at the time it collects your personal information:

- *How it's using your information*
- *What type of personal information they're using*
- *How long it will be kept*
- *Purpose (and legal basis) for using your information*
- *Reason they rely on 'legitimate interests' (if that's their legal basis)*
- *How you can withdraw consent for its use*
- *If they share your information, who with and why*
- *Whether they transfer your information outside the EEA and, if so where to*
- *Your information rights under the Data Protection (Jersey) Law 2018*
- *Automated decisions made about you using technology*
- *Your right to complain to JOIC*
- *Where your information was obtained from (if not from you)*
- *The organisation's name and contact details*

THE RIGHT TO ACCESS YOUR **PERSONAL INFORMATION**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

You have the right to find out if an organisation is using or storing your personal information. This is called the right of access. You exercise this right by asking for a copy of the information, which is commonly known as making a 'subject access request'.

Personal information means any information relating to a living, natural person who can be directly or indirectly identified. Examples of personal information could include but are not limited to; CCTV recordings, images, voice recordings, biometric, genetic information, names, addresses, numbers such as passport numbers etc. Remember that it is a right to information not documentation.

Article 27 of the Data Protection (Jersey) Law 2018 provides for the requests by individuals to access their personal information.

Our 'no-nonsense' infographic explains your right to 'access' your personal information.

THE RIGHT TO GET YOUR **INFORMATION CORRECTED**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

You can challenge the accuracy of personal information held about you by an organisation, and ask for it to be corrected or deleted. This is known as the 'right to rectification'. If your information is incomplete, you can ask for the organisation to complete it by adding more details.

Article 31 of the Data Protection (Jersey) Law 2018 affords individuals the right to rectify their personal information.

Our 'no-nonsense' infographic explains your right to 'rectify' your personal information.

THE RIGHT TO GET YOUR **PERSONAL INFORMATION ERASED**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

You can ask an organisation that holds information about you to delete that information and, in some circumstances, it must then do so. This is known as the right to erasure. You may sometimes hear it called the 'right to be forgotten'.

Article 32 of the Data Protection (Jersey) Law 2018 affords individuals the right to erase their personal information.

Our 'no-nonsense' infographic explains your right to request that your personal information be erased.

THE RIGHT TO LIMIT HOW **ORGANISATIONS USE YOUR PERSONAL INFORMATION**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

You can limit the way an organisation uses your personal information if you are concerned about the accuracy of the information or how it is being used. If necessary, you can also stop an organisation deleting your information. Together, these opportunities are known as your 'right to restriction'.

This right is closely linked to your rights to challenge the accuracy of your data and to object to its use.

Article 33 of the Data Protection (Jersey) Law 2018 affords individuals the right to restrict the use of their personal information.

Our 'no-nonsense' infographic explains your right to restrict the use of your personal information.

THE RIGHT TO PERSONAL **INFORMATION PORTABILITY**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

You have the right to get your personal data from an organisation in a way that is accessible and machine-readable, for example as a PDF file.

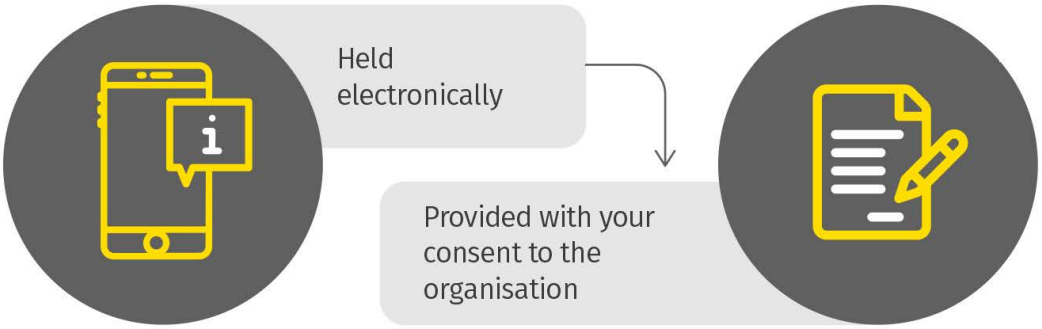
You also have the right to ask an organisation to transfer your data to another organisation. They must do this if the transfer is, as the law says, 'technically feasible'.

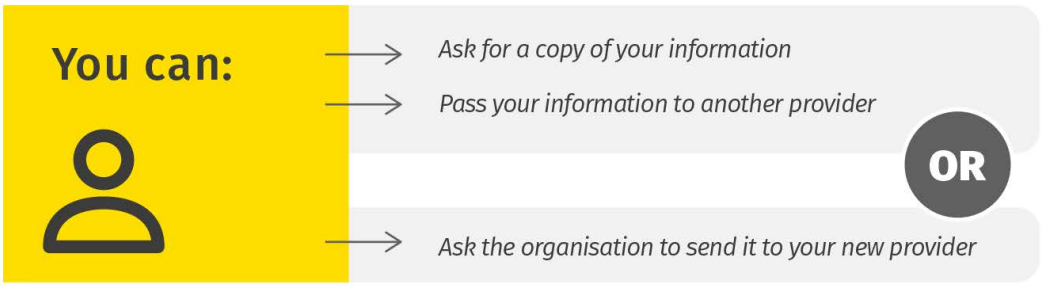
This is known as the right to data portability. It only applies to information you have provided to the organisation.

Article 34 of the Data Protection (Jersey) Law 2018 affords individuals the right to personal information portability.

Our 'no-nonsense' infographic explains your right to personal information portability.

Applies when the information being used is:





THE RIGHT TO OBJECT TO **THE USE OF YOUR PERSONAL INFORMATION**

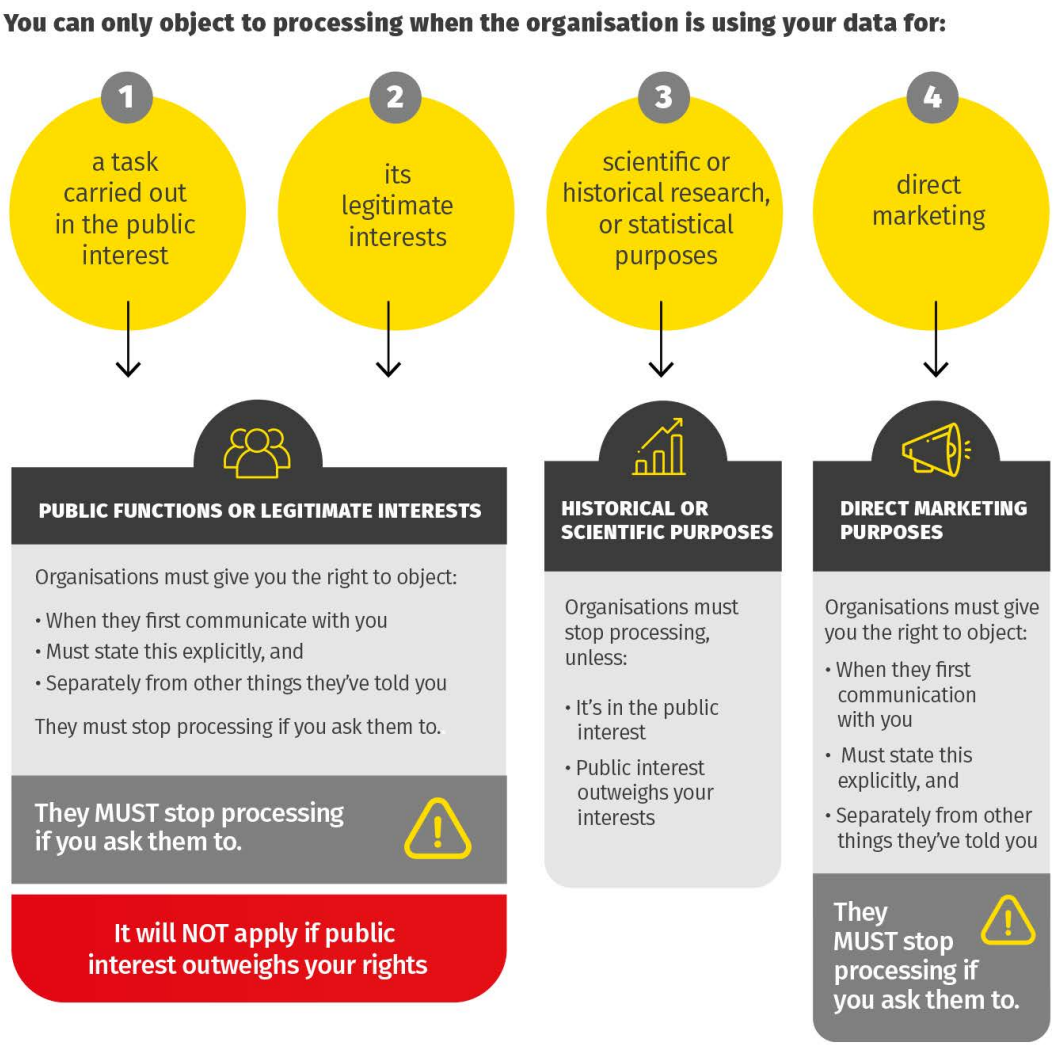
JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

You have the right to object to the processing (use) of your personal information in some circumstances. If an organisation agrees to your objection, it must stop using your information for that purpose unless it can give strong and legitimate reasons to continue using your information despite your objections.

You have an absolute right to object to an organisation using your information for direct marketing – in other words, trying to sell things to you. This means it must stop using the data if you object.

Articles 35 to 37 of the Data Protection (Jersey) Law 2018 afford individuals the right to object to processing personal information in certain circumstances.

Our 'no-nonsense' infographic explains your right to object to the use of your personal information.



THE RIGHTS RELATING TO **DECISIONS BEING MADE ABOUT YOU WITHOUT HUMAN INVOLVEMENT**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

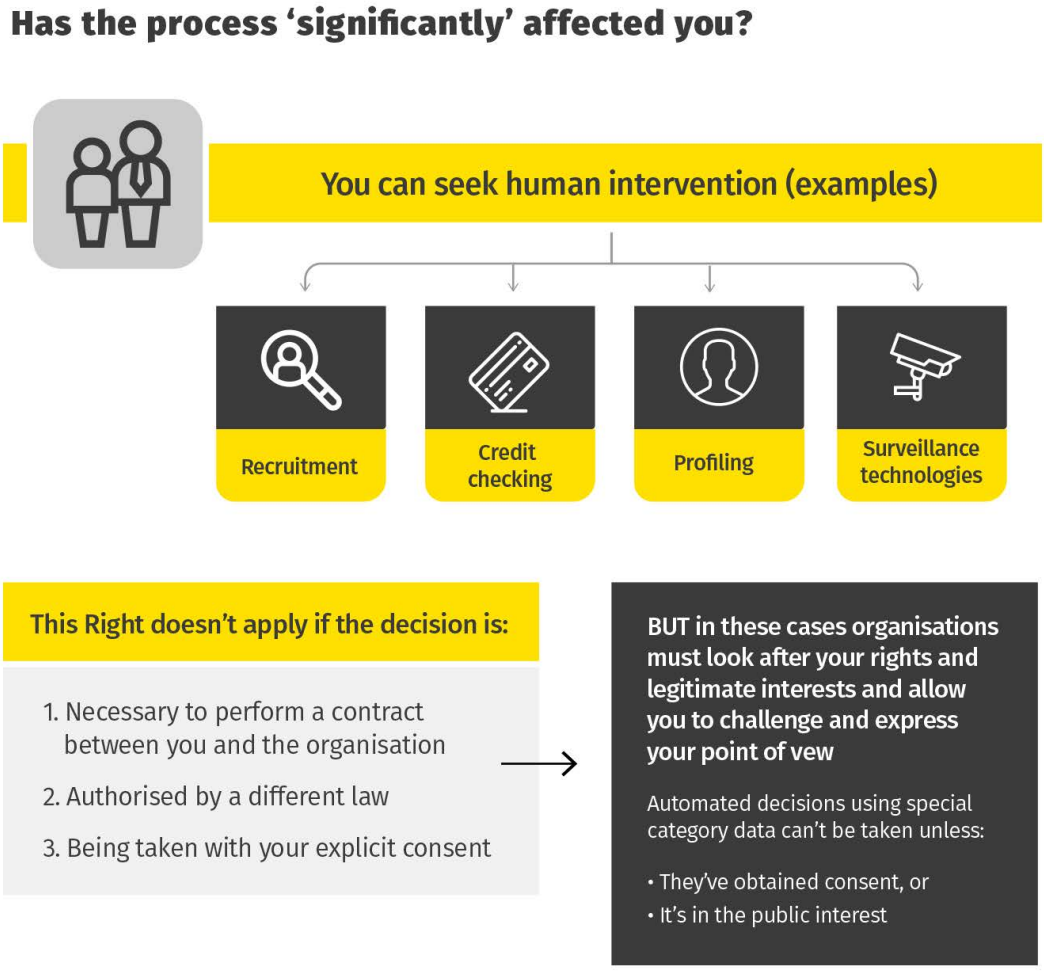
When decisions are made about you without people being involved, this is called 'automated individual decision-making and profiling' or 'automated processing,' for short.

In many circumstances, you have a right to question a decision that has been made solely on that automated processing.

This guidance describes your rights in respect of automated processing including profiling.

Article 38 of the Data Protection (Jersey) Law 2018 relates to the rights of individuals regarding automated individual decision-making.

Our 'no-nonsense' infographic explains your right relating to decisions being made about YOU without human involvement.



YOUR RIGHT TO RAISE A **CONCERN WITH AN ORGANISATION**

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

You have the right to be confident that organisations handle your personal information responsibly and in line with good practice.

If you have a concern about the way an organisation is handling your information; if it:

- *is not keeping your information secure;*
- *holds inaccurate information about you;*
- *has disclosed information about you;*
- *is keeping information about you for longer than is necessary;*
- *has collected information for one reason and is using it for something else,*

We believe that the organisation responsible should deal with it. We expect them to take your concern seriously and work with you to try to resolve it.

Our guide gives you additional help

YOUR RIGHT TO RAISE A **COMPLAINT WITH THE JERSEY OFFICE OF THE INFORMATION COMMISSIONER**

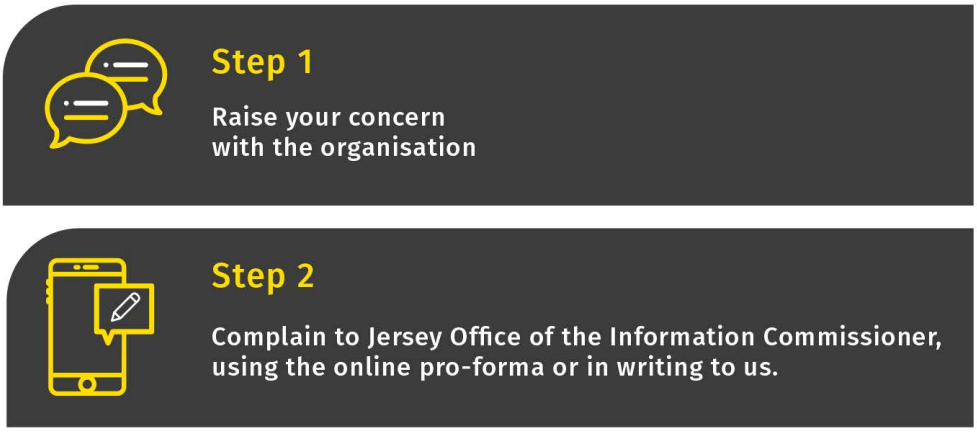
JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

In today's business world, most organisations and Government of Jersey take data protection and freedom of information very seriously, and the majority of issues are resolved without ever needing to raise a concern with us.

However, if you have contacted an organisation about an information matter and in keeping with the guidance provided in our 'Information Rights' section you are unhappy with the outcome, we may be able to help you do something about it.

You can raise the matter formally with us through our online form.

If you would just like to talk to us about a data protection or freedom of information concern please use the same form or email or telephone us. Our contact details are here.



HELPFUL
TEMPLATES

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

To help you to exercise your individual rights to secure a fair and satisfactory solution we have developed a series of template letters – one for each of your rights. Click the title to reveal the template letter.

CLICK THE TITLE TO DOWNLOAD THE TEMPLATE LETTER
The right to be informed if your personal information is being used
The right to access your personal information
The right to get your information corrected
The right to get your personal information erased
The right to limit how organisations use your personal information
The right to personal information portability
The right to object to the use of your personal information
The rights relating to decisions being made about YOU without human involvement
Your right to raise a concern with an organisation
Your right to raise a complaint with the Jersey Office of the Information Commissioner