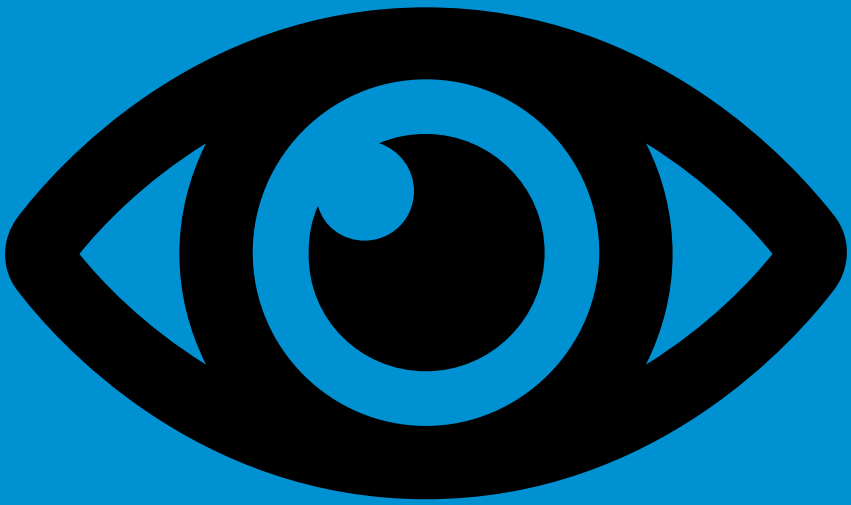
KNOW YOUR RIGHTS

Privacy and Data Protection



Irish Council for Civil Liberties

FOR ALL OUR RIGHTS. NO EXCEPTIONS.

CONTENTS

This is a general guide and not legal advice or an interpretation of the law. It contains generalisations and simplifications and is not a substitute for legislation or legal advice

GENERAL INFORMATION

Are there laws that protect my privacy and my personal data?

Yes. The Constitution protects your right to privacy. You also have the right to a private life under the European Convention on Human Rights.

The EU Charter of Fundamental Rights says that:

1.	Everyone has the right to the protection of personal data about them;
2.	Personal data must be processed fairly for specific purposes and on the basis of the consent of the person or some other legitimate basis laid down by law;
3.	Everyone has the right to access data that has been collected about them and the right to have it rectified if it is incorrect.

Data protection law, including the General Data Protection Regulation (GDPR), protects your personal data. Personal data is any information that could be used to identify you.

What should I do if I think that someone has invaded my privacy or infringed my data protection rights?

The first thing to do is consider if it is appropriate to ask the person or organisation to stop. If this does not resolve the situation, consider the following:

- Check the organisation's privacy policy. Under the GDPR you have the **right to be informed** of what personal data about you is being collected, for what purpose it is being processed and the legal basis for doing so.
- Capture any evidence you can (e.g., screenshots and emails) and keep a record of any complaints you make to the person or organisation.
- Consider who can assist you. For example, if someone shared unwanted images of you on the internet, you may want to contact the website or social media platform and make a complaint about the images being posted without your permission.
- Under the GDPR, you have a right to make a **Data Subject Access Request** to an organisation and get a copy of any personal data about you that is being processed. This is known as the right of access. This will allow you to consider if the organisation has a legal basis for processing your personal data. If you are not satisfied with the response, you can report the organisation to the Data Protection Commission (DPC).

- You should also consider further rights available to you under the GDPR. In addition to the right of access and the right to be informed, you also have the rights set out below, which all have certain limitations and restrictions:

1. **The right to have your personal data rectified** if it is inaccurate or incomplete.
2. **The right to object** to the processing of your personal data if it is being processed based on public interest, in the exercise of official authority, or based on the legitimate interests of others. The controller must stop processing your personal data unless they can show a compelling reason which overrides your rights.
3. **The right of erasure** in certain circumstances. This is sometimes known as the right to be forgotten. Such circumstances include where you withdraw consent (and there is no other legal basis for processing), your personal data is no longer needed for the purpose for which it was collected or your personal data has been unlawfully processed.
4. **The right to restrict** processing of your personal data, for example, where you have objected to the processing or claim it is not accurate. This means it can be stored by the controller, but the controller cannot do anything else with your personal data without your permission.
5. **The right to portability**. This means that in some circumstances you are entitled to obtain your personal data from a controller in an easy-to-use format and to have it transferred to another controller.
6. **The right not to be subject to a decision based on automated processing.** A decision is automated if it occurs without human intervention and produces legal consequences or significantly affects you.

- You can discuss the matter with your solicitor to see if you have a claim for damages or if you wish to seek a court order requiring the organisation to stop. However, this type of legal case can be difficult and free legal aid is not available. Under the GDPR, you have the right to an effective judicial remedy through the courts if you believe that your rights have been infringed as a result of improper processing of your personal data. You also have the right to seek a court order to oblige the DPC to act on a GDPR complaint that you have made if the DPC does not handle your complaint, or you have not been informed of the progress or outcome of your complaint within three months.

- Finally, you may want to consider if the invasion of privacy is a criminal matter which can be reported to An Garda Síochána, e.g., sharing inappropriate pictures and videos of children under 18 years of age or sharing of your intimate images without your consent.

DATA PROTECTION

What does the Data Protection Commission (DPC) do?

The Data Protection Commission (DPC) is responsible for upholding the GDPR, the Law Enforcement Directive and the Data Protection Acts. If you think your data protection rights have not been respected, you can raise a complaint with the DPC. The DPC will generally require you to have raised the matter directly with the controller before it will consider investigating.

Once you have raised a complaint with the DPC, they are obliged to provide you with an update or outcome report within three months. Where the matter goes on for longer, the DPC should update you at three-month intervals until the matter is concluded.

To contact the DPC, please see the contact details at the end of this guide.

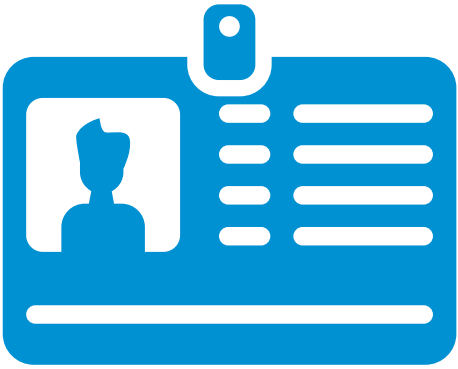
How does Data Protection Law protect my personal data?

The GDPR and the Data Protection Acts give you a number of rights. These are set out on pages **[2 and 3]**.

They also require organisations (controllers) to comply with the following principles:

1.	**Lawfulness, fairness and transparency** – your information should be used in a lawful and fair way and you should understand what information is being processed about you. There is more information below about what it means for processing to be lawful.
2.	**Purpose limitation** – your information should not be used for purposes beyond what it was collected for, without a legal basis.
3.	**Data minimisation** – an organisation should not process information it doesn't need.
4.	**Accuracy** – controllers must ensure information about you is accurate and kept up to date.
5.	**Storage limitation** – information about you should only be kept as long as it is needed for the purposes for which it was obtained.
6.	**Integrity** – organisations must ensure appropriate security is in place to protect the confidentiality of the personal data.
7.	**Accountability** – the organisation is responsible for documenting and demonstrating compliance with data protection law.

You can contact the DPC or visit its **website** for more information.



Do I have to hand over personal details if I don't want to?

It is generally your choice to give someone your personal data. However, in some situations, you must give your personal data to access services. For example, if you want to claim social welfare benefits, you must give information about yourself and your income. You must also give personal information to access services such as hospital care or schools.

In addition, you may have to give your personal data to get services from private companies, e.g. to access a service from a mobile phone company or to take out an insurance policy. But you cannot be forced to agree to any processing of your personal data that goes beyond what is required to deliver the particular services to you. You can ask a company why it needs your personal data and if you are not happy with the answer, you can contact the DPC.

The important point is that the use of your personal data must follow the principles of data protection on page **[4]**.

How can an organisation use my personal data?

To process your personal data, organisations must have a legal basis to do so. These are set out in the 'Key Words' section at the end of this guide. For more information on a legal basis, please see the **DPC website**.

Once there is a legal basis to process your personal data, the organisation must ensure that it complies with the principles of data protection found in Article 5 GDPR (see page **[4]**).

What can I do if my personal data are given to someone else?

You should be provided with a privacy notice by the organisation. This may also appear on the organisation's website. If a company or organisation shares your personal information with another organisation without your permission, general details of this should be set out in the organisation's privacy notice. If not, you can contact the organisation and ask for an explanation. If you are not happy with the response or if you have not received a response, you can make a complaint to the DPC (see the contact details at the end of this guide).

SURVEILLANCE

What is surveillance?

Surveillance involves monitoring, observing, listening to or recording the movements, activities or communications of a person or a group of people. This may involve the use of body-worn cameras, action cameras, listening devices, photography or video recording.

Body-worn cameras

Unless used for recreational reasons at home or without capturing footage of others, the person or organisation using body-worn cameras or action cameras (e.g., GoPro cameras) must comply with data protection law. As a body-worn camera is mobile, the justification for their use must be very strong. The Garda Síochána (Recording Devices) Act 2023 was signed into law in December 2023, providing for Garda use of body-worn cameras.

Online publication of recordings

If you are aware that your image or recorded footage of you has been published on a social media platform online without your consent, you can request that the social media platform remove it. If the social media platform refuses, you may need to consult with your solicitor.

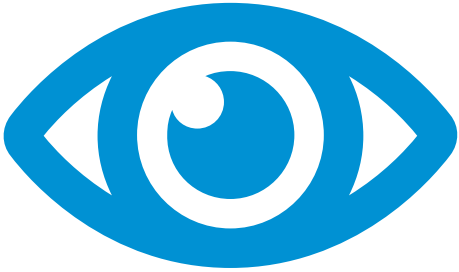
Covert filming

The use of recording mechanisms to obtain data without your knowledge is generally against the law. Covert surveillance is normally only allowed in exceptional cases e.g., by An Garda Síochána in relation to certain matters.

Law enforcement

Data processing that is carried out for law enforcement purposes falls under the Law Enforcement Directive (Part 5 of the Data Protection Act 2018) and is not covered by the GDPR. This kind of processing is carried out by a Competent Authority, such as An Garda Síochána.

However, data processing that is carried out by a Competent Authority for non-law enforcement purposes will still fall under the GDPR. Many of the same principles, obligations, and rights contained within the GDPR are also contained in the Law Enforcement Directive and Part 5 of the Data Protection Act 2018.



MEDIA

Can my picture be taken and published in the newspapers?

It depends on the circumstances. Generally speaking, a photographer is entitled to photograph and publish photographs of whomever they wish, if the photograph was taken of the person in a public place. A photographer is also entitled to photograph and publish photographs of whomever they wish in a private place where the public are admitted, subject to the terms of entry to that place.

However, this is not the case where the subject of the photograph would have a reasonable expectation of privacy. For example, someone performing at a public function can be photographed, whereas someone photographed attending a medical appointment might have a reasonable expectation of privacy.

The Press Council of Ireland has published a **code of practice** for newspapers and magazines which gives guidance to journalists, photographers and the public about when photographs can be taken and how they can be used in the press.

Under the Press Council's code of practice, journalists and photographers should not take pictures:

- under false pretences, for example, by pretending
- by deceiving people, or
- by harassing people

unless they can show that it is in the public interest, for example, that it is connected to an important news story.

Something may be 'in the public interest' if it is important and the public needs to know about it. This is not the same as something that is 'interesting to the public'. The Press Ombudsman or the Press Council will decide in each case what is in the public interest. The code also states that journalists and photographers should not take photographs of people in private places unless the people agree to it or it is in the public interest.

A photographer/journalist taking a photograph in a professional setting or for business reasons is also subject to obligations under data protection law. In particular, the photographer/journalist must have a legal basis to take and store photos. Photographs usually contain special category personal data (e.g., if it reveals the racial/ethnic origin of the person) and so the photographer will also need a lawful basis under Article 9, including, by way of example, the photographer has obtained the data subject's explicit consent to process the special category personal data, or the processing is necessary for reasons of substantial public interest (with a basis in law).

Can a newspaper publish a picture or image of a child?

The same rules apply to the taking of photographs of a child or teenager. However, children cannot give consent to their photographs being taken or published. For the purposes of the GDPR, any child under 16 cannot provide consent to their photograph being taken, so the photographer/journalist must either obtain the consent of the child's parent/guardian or rely on one of the other legal bases under the GDPR to take/store/publish the photograph. The photographer must also comply with the Press Council's code of practice. Journalists and photographers must take great care to make sure that their images are not exploited, for example, for pornography.

The media cannot publish details of a child's private life just because the child's parent is a celebrity or well known.

How do I complain about my picture being published in a newspaper or online news outlet?

If you are not happy about your picture appearing in a newspaper or you think that the behaviour of a journalist breaches the Press Council's code of practice, you can complain to the Press Ombudsman (which is part of the Press Council). The Press Ombudsman's contact details are at the end of this guide.

If you believe your picture may have been taken or published in contravention of the GDPR, you can complain to the Data Protection Commission. Their contact details are at the end of this guide.

How can I complain if I feel a television programme has affected my privacy?

You can contact Comisiún na Meán (the Media Commission), which has a complaints section (see contact details at the end of this guide). Your complaint must be made within 30 days of the programme being shown or repeated on television. You can also make a complaint to the Data Protection Commission, where relevant (see contact details at the end of this guide).

Image-based sexual abuse

Since 9 February 2021, the Harassment, Harmful Communications and Related Offences Act 2020 applies to the sharing or publication of intimate images without the consent of the person in the images. If someone records, distributes or publishes intimate images of you without your permission, or threatens to distribute or publish intimate images of you without your consent, this is a crime and should be reported to An Garda Síochána. He or she can face a maximum prison sentence of up to seven years.

CLOSED-CIRCUIT TELEVISION (CCTV)

CCTV

CCTV has legitimate uses in security, the prevention and detection of crime, and health and safety. However, it can also give rise to concerns of unreasonable intrusion into your privacy and data protection rights. The Data Protection Commission has helpful guidance here.

These are the key issues to think about when considering CCTV:

1.	**Transparency:** You have a right to be provided with transparent information about the processing of your personal data. This applies to the recording of your image by CCTV. Clear signs should be in place to advise people that CCTV recording is taking place, to explain why and to provide the contact details for the organisation.
2.	**Legal Basis:** All processing of personal data requires a legal basis under Article 6 of the GDPR. In many cases, CCTV footage may be recorded based on an organisation's legitimate interest to protect its premises and property from crime or damage, or to ensure the health and safety of staff members and the public. An organisation using a CCTV system should be able to provide you with an explanation of the legal basis on request. You can also request that the organisation provide you with a copy of CCTV footage containing your image.

Before an organisation uses CCTV cameras, it is required to carry out a Data Protection Impact Assessment to justify their use.

The use of CCTV in workplaces is dealt with in more detail in the 'Privacy At Work' section of this guide.

CCTV has been placed on my street or in community area – is this allowed?

Yes, this is allowed sometimes. Community-based CCTV systems are allowed under data protection law if they meet certain criteria, including:

- The scheme must be approved by the local authority after consultation with the joint policing committee for that administrative area;
- The scheme must comply with technical specifications issued by the Garda Commissioner and be operated in accordance with a code of practice;
- Members of An Garda Síochána must be given access at all times to the CCTV system.

It is also important that those operating the cameras, storing the images and destroying the images obey data protection law.

Under the community-based CCTV scheme, local organisations can request CCTV

schemes in their area and local authorities can apply for funding to set up community CCTV systems. You can get a code of practice for community-based CCTV systems from the Department of Justice (see contact details at the end of this guide). This code sets out how the images should be taken, stored and accessed.

If you have concerns about the use of community-based CCTV, you should contact the organisation operating it to see if it is following the code of practice. You can also contact the DPC about your concerns.

My neighbour has erected CCTV and I think the camera may point at part of my property. What can I do?

The first thing you should do is talk about your concerns with your neighbour.

If you think the CCTV is causing you harassment, you should contact the Gardaí.

You could also contact a solicitor who could advise you on your rights.

Generally speaking, if your neighbour is operating CCTV within the perimeter of their own home, this is allowed and falls outside the GDPR. However, if the CCTV system is recording neighbouring houses, driveways or individuals, your neighbour does have to comply with data protection law.

The Luas or DART line runs near my property and the CCTV is pointing at part of my house or garden – what can I do?

You should contact the company that operates the Luas or DART (see contact details at the end of this guide) and tell them about your concerns. Both the Luas and DART are subject to data protection law.

You can also contact the DPC, which may be able to help.

What about CCTV used by the Gardaí?

An Garda Síochána has the right to operate CCTV systems to protect against crime and for reasons of safety and public order. However, it must also obey data protection laws.

If you have any concerns about the operation of Garda CCTV, contact An Garda Síochána (see contact details at the end of this guide). You can also contact the DPC.

FACIAL RECOGNITION TECHNOLOGY (FRT)

Facial recognition technology (FRT) is a technology that may be used to attempt to identify or verify a person by applying it to videos (e.g., CCTV) or photographs. FRT is used to identify unknown people by comparing newly captured images of unidentified persons against images of identified persons stored in a reference database, which may also contain other information related to the identified persons.

Facial recognition involves the processing of biometric data which are classified as special category data under the GDPR and cannot be processed unless certain exemptions apply. The circumstances in which it can be used are limited and it is generally not permitted in an employment context.

The use of FRT engages many fundamental human rights including, but not limited to, the rights to human dignity, privacy, protection of personal data, non-discrimination, protest and freedom of expression, all of which are enshrined in the EU Charter of Fundamental Rights.

FRT is used in some countries by government organisations and law enforcement authorities. However, its use remains controversial and it is subject to strict restrictions. It is a source of concern for the Data Protection Commission and other data protection authorities in the EU. In Ireland, An Garda Síochána has no legal authority to use FRT but, as of August 2024, the Minister for Justice intends to introduce legislation to allow Gardaí use FRT. This is a source of considerable concern to ICCL and others.

GARDAÍ

Do the Gardaí have to obey data protection laws?

Instead of the GDPR, the Gardaí are governed by a separate piece of data protection legislation, the Law Enforcement Directive, when they process personal data for law enforcement purposes, such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Law Enforcement Directive regulates the processing of data by police and criminal justice authorities in the EU.

Individuals have similar rights to those under the GDPR. However, there is greater scope for these rights to be restricted in certain circumstances, where such restrictions are proportionate and necessary.

An Garda Síochána is also subject to the GDPR as regards the processing of data which has nothing to do with its law enforcement function (e.g., HR matters).

The Gardaí have a section on their **website** relating to data protection. You can also find more information on the Law Enforcement Directive on the Data Protection Commission's **website**.

Can the Gardaí take a picture or video of me?

If Gardaí do take pictures or video footage for law enforcement purposes, they must obey the Law Enforcement Directive. Gardaí may use the photographs or video as evidence against you. See the previous section 'Surveillance'. However, Gardaí must not harass you, follow you about in public or interfere with your private or business life unless they have a very good reason.

Can I take a photograph of a member of An Garda Síochána?

Yes. However, An Garda Síochána may confiscate (take away) your camera or device if they believe the image relates to a crime. They are not allowed to delete the image itself.

How can I find out what information the Gardaí hold about me?

You can make a Subject Access Request to the Gardaí. The form for this is available **here** on the An Garda Síochána website.

If you cannot access the form, you can also write to the Gardaí to ask for a copy of the personal information that they hold about you (please see contact details for the An Garda Síochána Vetting Unit at the end of this guide).

Your letter should include:

- your full name (including any previous name);
- your date of birth;
- your current address and former addresses (if any); and
- your signature.

When sending the form or letter, you must include an acceptable form of proof of identity, such as a copy of your passport, driving licence, birth certificate or other identification.

What is the Garda PULSE system?

This is a centralised computer database that the Gardaí use in their work. PULSE stands for Police Using Leading Systems Effectively.

If you come into contact with the Gardaí for any reason, even to report a crime, they will enter your details onto the PULSE system. The system also includes anyone who is listed on the Register of Voters.

What type of information about me can the PULSE system hold?

The PULSE system contains information about:

- recording crime;
- traffic management;
- progression of criminal cases through the courts, including the outcome;
- firearms licensing;
- driver licences;
- insurance;
- character vetting.

The PULSE system must follow data protection law. This means, for example, that information can only be put on the system for a clearly stated purpose and there must be controls over who can see the information.

What should I do if I think the information about me on the PULSE system is wrong?

First, you should ask to see what information the Gardaí hold about you. For help on how to do this, see the answer to the question 'How can I find out what information the Gardaí hold about me?' on page **[12]**.

If you check the information and it is factually incorrect, you should contact the Gardaí, explain the situation and ask them to correct the records. Individuals have a right, in accordance with the Law Enforcement Directive, to have their information amended if it is incorrect. However, this right is not absolute and can be limited in certain circumstances. If you have any queries in this regard, contact the DPC or talk to a solicitor.

What should I do if I am concerned about the personal information that is held on PULSE?

If you think that someone has viewed your personal information who shouldn't have, or if you have other data protection concerns, contact the DPC or talk to a solicitor.

If you have a complaint about a member of An Garda Síochána's use of your personal information on PULSE, you can contact the Garda Síochána Ombudsman Commission to make a complaint (additional contact details are at the end of this guide).

The Garda Síochána Ombudsman Commission is due to be replaced by Fiosrú – the Office of the Police Ombudsman. Fiosrú will be responsible for receiving and investigating complaints about An Garda Síochána.

What is the ANPR traffic system and what does it do?

ANPR stands for automatic number plate recognition. ANPR systems photograph vehicle registrations and can capture images of drivers and passengers. The net effect of an ANPR system allows a user, such as An Garda Síochána, to be able to pinpoint the date and time that a registration plate was captured at a particular location, if it was captured by an ANPR camera.

If you have a complaint about a member of An Garda Síochána's use of ANPR, you can contact the Garda Síochána Ombudsman Commission or the DPC.

When I took part in a peaceful march or protest, the Gardaí asked me for personal information. Can they do this?

You have a right to your privacy. However, in some situations, the Gardaí can ask for personal information such as your name and address. If you fail to give your name and address when a member of An Garda Síochána asks for it, you may be arrested and charged with a criminal offence.

When can Gardaí take my fingerprints?

Gardaí are entitled to take your fingerprints under certain pieces of legislation when you are detained in a Garda station.

Gardaí can also, in certain circumstances, take your fingerprints if you are not a national of the European Economic Area (EEA). For example, you must give your fingerprints if you are applying for asylum or if the Garda National Immigration Bureau (GNIB) asks for them.

What if I refuse to let the Gardaí take my fingerprints?

The Gardaí can, in certain circumstances, use reasonable force to take your fingerprints.

Do I have to allow Gardaí to carry out a DNA test?

There are detailed laws surrounding the obtaining of DNA samples by the Gardaí. You may refuse a DNA test. However, it is important to be aware that if the Gardaí ask to take a swab for a DNA test and you refuse, your refusal could be used as evidence against you in court. Furthermore, the Gardaí are entitled in certain circumstances to use reasonable force to obtain a DNA sample from you.

Do I have to give a blood or urine sample?

A blood test can only be taken if you agree to it. However, it is important to be aware that if the Gardaí ask to take a blood, pubic hair or urine sample and you refuse, your refusal could be used as evidence against you in court.

If a member of An Garda Síochána asks for a sample of your blood, breath or urine because he or she suspects you of drink driving, it is a criminal offence to refuse. This means that An Garda Síochána could arrest and charge you.

I have been charged with a criminal offence and have concerns that my privacy rights may have been breached during the investigation. Is there anything I can do?

If you have concerns about the validity of a search warrant or the collection or retention of your data by An Garda Síochána in the course of an investigation, inform your solicitor immediately (see contact details at the end of this guide).

GOVERNMENT DEPARTMENTS AND AGENCIES

What is my PPS number?

Your Personal Public Service (PPS) number identifies you so that you can access public services such as social welfare, tax services, public healthcare and education in Ireland. However, if an organisation asks for your PPS number and you feel this request is not legitimate, you should ask the organisation to explain why it needs it. If you are not satisfied with the answer, you can contact the **Data Protection Commission** (see contact details at the end of this guide).

If you have any questions about your PPS number, contact the Client Identity Services section at the Department of Social Protection (see contact details at the end of this guide).

How do I know if I have a PPS number?

You have a PPS number if:

- you were born in Ireland during or after 1971;
- you started work in Ireland after April 1979; or
- you are receiving a social welfare payment or using the Drugs Payment Scheme.

You can apply online for a PPS number **here**, if you are living in Ireland and are at least 18. More information on applying for a PPS number if you are living outside of Ireland is available **here**.

What is my PSI?

A Public Service Identity (PSI) is your PPS number along with other information such as your first name, surname, date of birth, place of birth, sex, nationality, address, all your former surnames (if any) and all the former surnames (if any) of your mother.

What is a Public Services Card?

A Public Services Card is a Department of Social Protection-issued card which establishes and authenticates your identity, assisting you in accessing a range of public services. It displays information including your name, photograph and signature.

Whilst you will be required to register for a Public Services Card if you apply for or receive a social welfare payment, the Public Services Card is not a mandatory requirement in order to access other public services.

Which government departments and agencies can use my PPS number to look at my personal information?

A wide range of public bodies are allowed to use your PPS number. These include the Department of Social Protection, the Revenue Commissioners, local authorities, the Health Service Executive and the Garda National Immigration Bureau.

You can get a full list of government departments and agencies that are allowed to use your PPS number on the Department

of Social Protection's website. If you have any doubts about whether an organisation or an individual is allowed to use your PPS number, you should contact the Client Identity Services section at the Department of Social Protection (see contact details at the end of this guide).

Can staff use my PPS number to access my personal information?

If a government department or agency is allowed to use your PPS number, then any staff member can use your PPS number to carry out their work. However, under data protection law, the department or agency must take proper security measures to make sure that staff only access your personal information when they need to.

Government departments and agencies must have an internal system in place to keep safe the personal information attached to your PPS number.

Do government departments or agencies ever give PPS numbers to others?

Sometimes government departments and agencies need other people or organisations to carry out work for them and, if so, will authorise them to have the PPS numbers.

If you have any doubts about whether someone is allowed to have your PPS number, contact the Client Identity Services section at the Department of Social Protection (see contact details at the end of this guide) or the DPC.

Does my employer need my PPS number?

Your employer will need your PPS number to pay your wages. You must give your employer your PPS number, as you could pay too much tax if you don't.

Does a government department or agency have to tell me if it loses any of my personal data (for example, if my bank details or HR information were on a laptop which was lost)?

If a government department or agency loses your personal data or if your personal data is the subject of a data breach (such as a ransomware attack), it must notify the DPC within 72 hours, unless the matter is likely to present a risk to you or other data subjects. If there is a high risk to your rights and freedoms, the department or agency must tell you 'without undue delay'. The same rules apply to private companies.

What should I do if I think that a government department or agency has lost some of my personal data?

You should contact the department or agency to find out:

- exactly what information was lost;
- when this happened;
- what steps they have taken to prevent fraud using your personal data;
- what steps they have taken to stop this happening again; and
- whether they have notified the DPC.

PRIVACY AT WORK

You have a right to privacy at work and your data protection rights apply at work as they do in any other setting. This right is balanced against your employer's rights to run their business.

Employee tracking or surveillance software is an emerging data protection issue. It is more common because of the increased number of employees working from home, but it can also be used in the office or workplace. For example, some employers use software which tracks computer activity or keystrokes.

Such tracking or software will generally be used based on the employers' 'legitimate interests'. The more intrusive the monitoring, the more difficult it will be for the employer to show that its interests in monitoring outweigh the employees' right to privacy.

Employers must be transparent about monitoring. Employees should be made aware of the tracking measures or software in place, why it is needed and what, how and when it operates.

Employers must only use the personal data collected for the purpose for which it was obtained (i.e., monitoring of work) and not for some other purpose. Any monitoring must be proportionate and can't be excessive. For example, it may be legitimate for an employer to track employees' internet usage to ensure they are not accessing inappropriate material at work but using it to find out information about an employees' private life or health issues would be excessive.

Can my employer use closed-circuit television (CCTV) at work?

CCTV images or footage from which people can be identified are personal data. The use of CCTV in the workplace could infringe data protection law, for example, if the CCTV is not necessary, if it is disproportionate, if there is no signage, or if information about how the CCTV footage will be used is not provided. Using CCTV to monitor employees is very intrusive and would need to be justified by special circumstances. However, there may be good reasons for using CCTV in a workplace, such as preventing theft or protecting employees, for example, from a threat of physical harm.

Your employer must consider if using CCTV is reasonable and necessary. It is best practice if employers and employees reach an agreement about the use of CCTV before it is put in place, including whether there are any alternatives. Employers can only use CCTV footage for the reason for which it was installed. For example, if they installed CCTV to monitor for theft but instead use it to monitor employee behaviour or performance, that would be a breach of data protection law.

Employers must carry out a data protection impact assessment before installing CCTV. It must consider the following points:

- What will they use the CCTV system for?
- Is it necessary or is there another way to achieve the same purpose that does not affect employees' privacy?

- Will they tell employees the purpose of the CCTV before it is set up?
- Will there be clear signs in the areas that are monitored by CCTV? And how will they provide people with relevant information required under transparency obligations?
- Is there a system in place to give copies of the images to an employee who asks for them?

CCTV should not be set up in areas where an employee would expect to have privacy, such as a cloakroom or changing area.

If you have concerns or questions about CCTV in your workplace, you can contact your employer's data protection officer or one of the organisations listed at the end of this guide.

Can my employer search me?

You have the right to bodily integrity. This includes the right not to have anyone touch your body without your permission. Body searches should only be used as a last resort and with good reason. Generally, only a member of An Garda Síochána can carry out a body search and only if they have a reasonable suspicion that you were involved in a crime. In all other situations, including at work, you can only be searched if you agree to it.

Your employer may ask you to agree to a body search. However, your consent must be real. This means it must be fully optional and that your employer must not treat you any differently if you do not agree to a body search.

Body searches may be included in the terms and conditions of your employment, for example in your employment contract or staff handbook. If this is the case, your employer can only search you in the way described in your contract or staff handbook.

If your employer has said that you must agree to a body search or if you have concerns or questions about body searches, you should consult with your HR department or contact one of the organisations or people listed at the end of this guide.

Can my employer check my phone calls, internet access or emails?

Your employer should give you their policy on email and internet usage in the workplace. This is sometimes known as an 'acceptable use policy' and should explain how much you can use company devices for your own personal or private communication.

If an employer wishes to monitor your internet usage or emails, they must show that it is necessary and that there is not a less intrusive way of achieving the same thing. For example, blocking websites would be less intrusive than monitoring your internet search history.

If an employer is monitoring your phone calls, emails and internet access (for example, your use of social networking sites), they must tell you:

- Who is monitoring you;
- What they are monitoring;
- How they are monitoring you; and
- When they are monitoring you.

However, your employer must tell you beforehand that your calls, internet access or emails are being monitored, usually by way of an acceptable use policy.

If you have concerns or questions about the monitoring of your phone calls or internet use, you can contact your employer's data protection officer or the Data Protection Commission.

Can my employer use a fingerprint system or facial recognition technology to record attendance?

Generally, no. Fingerprint or facial recognition data are known as biometric data. It cannot be processed unless certain exemptions apply. Generally, facial recognition involves identification based on the comparison of newly captured images with images stored in a database, which also may be linked to other information that identifies the individual. In an employment context, it is very difficult to justify the processing of biometric data unless there is a collective agreement in place which allows it. Even if you give explicit and fully informed consent, the processing may still be illegal unless the employer gives alternatives (e.g. using a swipe card, key fob or PIN number) and you are not treated any differently if you do not agree to have your fingerprints taken.

Any fingerprint system must obey data protection law. If you have any questions or concerns about the introduction of a fingerprinting system, you can contact the DPC.

Can my employer use GPS or vehicle tracking systems?

Employees are entitled to a reasonable expectation of privacy in the workplace.

Vehicle tracking is not just collecting data about the vehicle but also the personal data of the employee using that vehicle. There may be a legal basis for the use of tracking systems (e.g., tachographs are a legal requirement for bus and truck drivers) and employers may have a legitimate interest in being able to locate the vehicle at any time. However, vehicle tracking should not be used for the general monitoring of staff and the processing of personal data must be necessary and proportionate. For example, employers should only use a tracking device to check where the vehicle is during working hours. If an employee is allowed to use a vehicle for personal use, it should be possible to disable the tracking system outside of working hours.

An employer must:

(i) show a good business reason for using a tracking system;

(ii) tell the drivers about the tracking and why it is needed; and

(iii) not use the personal data for another reason or purpose (e.g., monitoring behaviour or performance).

If you have concerns or questions about the use of vehicle tracking systems in your workplace, you can contact the DPC.

Can my employer make me carry an identity (ID) card?

Yes, your employer can require you to carry a card containing your picture and other details, if it is for a valid reason, such as security. If you have any concerns or questions about carrying an ID card, you should contact the Data Protection Commission (see contact details at the end of this guide).

Can my employer ask me to submit to a retina scan?

Generally, no. Personal data generated from a retina scan is biometric data. It cannot be processed unless certain exemptions apply. An employer would have to justify the need for retina scanning. For example, retina scanning may be acceptable in an organisation that works on secretive or highly classified issues, such as the Defence Forces.

If you have any questions or concerns about the introduction of a retina scanning system in your workplace, you can contact the Data Protection Commission.

What about other forms of checking identity such as DNA testing?

No. DNA is genetic data under the GDPR. It is special category personal data, not only about you but also your entire family. There is unlikely to be any situation in which an employer would be justified in requiring employees to undergo DNA testing.

If you have any concerns or questions, you can contact the DPC.

Do I have to agree to a drug test if my employer asks for one?

You should not be under the influence of alcohol or drugs in such a way that your health and safety or that of another person in the workplace would be at risk.

Depending on your job, an employer can require you to submit to alcohol and drug tests to make sure that you are not a health and safety risk at work. For example, if you operate machinery or work in a high-risk job, alcohol and drug tests may be acceptable.

But if your job does not threaten your or other people's health and safety, then forced alcohol or drug testing may not be acceptable. Your employer could instead deal with the problem in other ways such as a discussion with your manager or a performance review.

All testing for drugs or alcohol in the workplace should comply with the **European Guidelines for Workplace Drug Testing**.

What can I do if I feel my privacy at work has been threatened?

You should check what types of monitoring are part of your employment contract or the terms and conditions of your employment.

Your employer should discuss any monitoring or testing system with you either:

- when you take up the job; or
- when a new system is introduced in your workplace.

If you have a concern regarding your privacy at work, you can this discuss this with your employer's HR team or data protection officer. If you are not comfortable with a request from your employer, you can contact one of the following:

- the National Employment Rights Authority (NERA);
- the Data Protection Commission;
- a lawyer; or
- your union representative, if you have one.

You will find contact details for NERA and the DPC on page **[40]**.

INTERNET

Do I have the right to privacy and data protection on the internet?

Yes. Everyone has the right to the protection of personal data concerning them. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid down by law.

Before publishing personal data online, e.g., on social media sites, you should consider whether that data will be publicly available and whether you are comfortable with that. There are a number of reasons for this:

1.	It is important to remember that once you place material on the internet, you may lose control over it. Even if you delete the information, image or video, someone may have made a copy or downloaded the information before you removed it.
2.	Information posted on the internet will live on long after you may have forgotten about it.
3.	You should bear in mind that potential employers may check the internet – and social media sites in particular – before offering you a job.

Websites that process your personal data are required to comply with the seven data protection principles (please see page **[4]**). They are required to have a legal basis to process your data (please see page **[5]** and the 'Key Words' section of this guide).

If you have any concerns in relation to how a website is processing your personal data, you can contact the Data Protection Commission. See the contact details at the end of this guide.

Can I request that personal data about me is removed from the internet?

You have a number of data subject rights. These are explained on pages **[2 and 3]** and in the 'Key Words' section of this guide and include the right, in certain circumstances, to have your data rectified, deleted or erased.

You can request that inaccurate personal data about you is rectified. You can request that personal data which is no longer relevant is erased. However, these rights are subject to a number of limitations and restrictions. You can request that inaccurate personal data about you is rectified, and you can also request that personal data about you which is no longer relevant is erased. However, these rights are subject to a number of limitations and restrictions. To have your personal information rectified or erased, you should first contact the website or organisation that is processing it and request that they do so. If you have questions or concerns, you can contact the Data Protection Commission..

What about privacy statements on websites?

Websites are required to have a privacy notice (sometimes called a privacy statement). Sometimes, privacy notices are long and written in technical language. However, at the very least, you should check who the website will pass your personal data to.

It is important to be aware that even though they shouldn't, many websites track you across the internet – they track what sites you visit and what you search for, with the purpose of sending you targeted adverts. Some websites, including widely used social media platforms, will use your personal data to create a "profile" of you, meaning they can then target you with specific adverts based on that profile.

Can I ask a website for a copy of the information it holds about me?

Yes, you have the right to make a Data Subject Access Request. Your data should be provided to you free of charge, in an accessible format and the website is required to reply to your request within one month of receiving it. You are also entitled to information in relation to how your data is being used.

What if I find something on the internet that I think is illegal?

You can report any suspected illegal material to the Irish Internet Hotline (see contact details at the end of this guide). If you are not sure whether content is illegal, you should report it anyway and the analysts at the hotline will assess it.

How do I protect my privacy and personal data on the internet?

There are many ways you can protect yourself online:

- Install and regularly update security software.
- Turn off location services on your devices.
- Do not give personal data in a blog or online comments section and only provide personal data if you are sure you are visiting a trustworthy website.
- Do not reply to spam or suspicious emails or click on suspicious links.
- Don't open suspicious emails or attachments from people you don't know.
- Don't enter personal data after clicking on a link in an email.
- Read the privacy statement of websites you use regularly.
- Use strong passwords (combinations of letters and numbers that would be difficult to guess) and change them at least every three months.
- Use different passwords for your financial accounts, email and online shopping.
- Never put bank details or other sensitive personal data in an email.

What are cookies and what do they do?

Cookies are files created by websites you visit. They are stored on devices connected to the internet, including your laptop, tablet and phone.

Some cookies make your online experience easier, for example, by remembering items you previously searched for or put in your shopping cart.

However, cookies and other tracking technologies are also used to track your behaviour online, target you with adverts and sell data about you.

Most websites have a cookie banner or pop-up, which appears when you land on the website. This banner or notice will also often contain a link to a cookie policy and a privacy policy which provide further, more detailed information.

There are two types of cookies:

1.	**First-party cookies** are created by the site you visit. The site is shown in the address bar.
2.	**Third-party cookies** are created by other sites. These sites own some of the content, like adverts or images (or like or share buttons) that you see on the webpage you visit.

Under the ePrivacy Directive, websites need your consent to use cookies unless the cookie is strictly necessary to provide you with a service. Pre-ticked boxes, for example, are not permitted. Cookies are not permitted unless you are provided with clear and comprehensive information which is prominently displayed and easily accessible.

According to the ePrivacy Regulations, cookies should not last longer than 12 months but, in practice, they could remain on your device much longer if you do not take action and deactivate the cookies. You can get information on how to do this from the help section of your web browser.

What about children and young people using the internet?

The internet is a great resource for everyone, including children and young people. However, there are important issues to bear in mind when young people are using the internet.

The Irish Internet Hotline provides advice and information for parents and young people about internet use (www.hotline.ie). Webwise (www.webwise.ie), the Irish Internet Safety Awareness Centre, also has resources that deal with the safe and effective use of the internet by children and young people.

The digital age of consent in Ireland is 16. This means that in order to legally process the personal data of a child under the age of 16, a website must make reasonable efforts to obtain the consent of the child's parents.

What are common types of illegal activity online?

DEFAMATION

If you make a defamatory statement (i.e., an untrue statement which damages another person's reputation) about a person or corporation online, you are at risk of being sued for defamation. The statement must have been made to at least one other person in order for it to be defamatory.

Social media posts can be defamatory and you should be careful about what you post. If someone has made a defamatory statement about you online, you can discuss the matter with your solicitor.

IMAGE-BASED SEXUAL ABUSE

The Harassment, Harmful Communications and Related Offences Act 2020 applies to the sharing or publication of intimate images without the consent of the person in the images, or the threat of distributing or publishing intimate images without the consent of the person in the images.

If you believe that intimate images are being shared unlawfully, you should report the matter to the Gardaí. In addition, Hotline.ie provides a secure, confidential service for the public to report suspected illegal content on the internet.

FRAUD, IDENTITY THEFT AND HACKING

Cybercrime is more common than ever. This includes things like fraud, forgery and identity theft (a person making a loan application in your name without you knowing it). It also includes hacking, phishing (a form of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information) and malware.

If you believe illegal activity is occurring online, you should report the matter to the Gardaí and Hotline.ie. Any suspected data breaches involving personal data should be reported to the Data Protection Commission.

CONSUMER AFFAIRS

In December 2022, the government enacted the Online Safety and Media Regulation Act 2022, which defines harmful online content and creates a new Online Safety Commissioner to oversee the regulation of websites and online services. In addition, under the Act, the Online Safety Commissioner has the power to make binding online safety codes which will address issues such as content moderation, complaints handling and online advertising.

Electronic direct marketing

Electronic direct marketing involves organisations targeting you directly via email, text message or telephone to promote a product or service. Both the GDPR and the ePrivacy Regulations apply to such marketing in Ireland.

Many companies will incentivise you to subscribe to a mailing list, which usually requires submitting certain personal data, including your name and email address. You should always have the option to unsubscribe at any time from a mailing list.

You should not receive unsolicited emails from a company if you haven't subscribed to their mailing list, agreed to receive such emails or purchased a product or service from them. Some companies say that their 'partners' or similar third parties may send you emails if you subscribe – but this must be optional and you must opt in before receiving such emails.

The general rule is that an organisation must obtain your clear consent before sending any marketing communication to you. However, there are exceptions to this. For example, consent is not required if:

i. the organisation obtained your details in the context of a sale of a product or service to you;

ii. the product or service is of a similar kind to that supplied to you in the original sale;

iii. you are given the opportunity to opt out of receiving any more communication; and

iv. the initial communication is sent to you within 12 months of the original sale to you.

Further, direct marketing telephone calls to your mobile phone are prohibited under the ePrivacy Regulations, unless you specifically consented to receiving such calls or your consent to receiving marketing calls on your mobile phone is recorded in the National Directory Database.

For further information on the rules around electronic direct marketing, you can find a copy of the Data Protection Commission's helpful guidance note **here**.

EDUCATIONAL INSTITUTIONS

Do schools, colleges and universities have to comply with data protection rules?

Yes. Data protection law applies to schools, colleges and universities.

Can my school make me take a drug test?

Some schools use drug testing as part of their substance abuse policy. Testing for drugs takes place through blood or urine tests. If you are under the age of 18, the school must get your consent as well as the consent of your parent or guardian before it can carry out a drug test.

If you have concerns about drug testing in schools, you should contact one of the children's organisations listed at the end of this guide.

Can a teacher search me in school?

Generally, only a member of An Garda Síochána can search you and then only if they have a reasonable suspicion in relation to a crime. However, other people can search you if you agree to this. Your parents or guardian must also agree before any search is carried out. Your parent or guardian should be present during any search.

Can a teacher search my locker?

Your locker is school property, but you are entitled to privacy while the locker is assigned to you during the school year.

A teacher may search your locker if they have a valid reason for doing so. The teacher should explain the reason for the search.

Can my school, college or university take and keep my fingerprints to check attendance?

No. As explained in the 'Privacy at work' section of this guide, fingerprint and facial recognition data are known as biometric data. These should not be used by schools or other educational institutions.

What can I do if I think that a school, college or university has introduced policies that affect my privacy (or the privacy of my child)?

Children and young people have the right to take part in any decisions that affect them, including matters of privacy. If a school, college or university plans to introduce any systems of fingerprinting, drug testing or locker searching, staff should explain these clearly to students and their parents.

If you have concerns about systems of fingerprinting, drug testing or locker searching used by a school, college or university, you can contact the DPC. If a policy affects people under the age of 18 and there is disagreement about whether or not it should be implemented, when all other attempts to resolve the issue have failed, you can contact the Office of the Ombudsman for Children. See contact details at the end of this guide.

FOREIGN NATIONALS AND ASYLUM SEEKERS

I am a foreign national. Do I have to register with the immigration authorities?

If you are over the age of 16 and are a non-national of the European Economic Area (EEA), the UK or Switzerland, you must register with your local immigration office if you plan to stay in Ireland for more than three months. Please note that the European Economic Area consists of all the countries in the European Union (EU) as well as Iceland, Liechtenstein and Norway.

Registration of immigration permission for people living in Dublin is now operated by the Irish Naturalisation and Immigration Service (INIS). People living outside of Dublin must register with the Garda National Immigration Bureau (GNIB) at their local GNIB Immigration Office. Once registered with immigration you will be issued an Irish Residence Permit. This is a registration card showing that your immigration permission has been registered and the type of permission you have.

What information must I give to get my Irish Residence Permit?

At your appointment you must present your passport and give your:

- name;
- nationality;
- date of birth;
- sex;
- signature;
- fingerprints; and
- photograph.

When you receive your Irish Residence Permit, it will contain your:

- name;
- sex;
- nationality;
- signature;
- photo;
- date of birth;
- registration number;
- a description of your immigration permission including stamp number;
- a microchip with a copy of your photo, fingerprints and personal details; and
- the date on which your permission to remain in Ireland expires.

If you are on the register and have an Irish Residence Permit, it may be an offence if you do not produce the Irish Residence Permit when asked to do so by an immigration officer or member of An Garda Síochána.

Asylum seekers

Asylum seekers can apply for international protection in Ireland if they are seeking to escape persecution in their own country. If your application for asylum has been accepted, you can remain in Ireland while it is being processed. During this period, you will be issued with a Temporary Registration Certificate, which is proof that you have made an application for asylum. If your application is successful and you are granted refugee or subsidiary protection declaration or you are granted leave to remain in Ireland, you must then register your permission with your local immigration office.

Do I have to give my fingerprints?

Yes, under immigration law, you must give your fingerprints to officials at the International Protection Office (IPO), the Irish Naturalisation and Immigration Service or the Garda National Immigration Board if you are not an EEA national.

Where are my fingerprints kept?

Your fingerprints are stored on the Automated Fingerprint Identification System (AFIS). This system shares your fingerprints with the European Asylum Dactyloscopy Database (EURODAC). EURODAC contains fingerprints from all asylum seekers in the EU together with fingerprints from people who have been stopped for crossing EU borders unlawfully. Fingerprints are collected from anyone over the age of 14 years.

How long are my fingerprints kept?

If someone is caught attempting to cross an EU border without papers, their fingerprints are kept on AFIS for two years. Fingerprints from asylum seekers are held for 10 years or until the applicant becomes a citizen of an EU member state.

I am an asylum seeker and I live at an accommodation centre. Do I have the right to privacy?

Yes, you have a right to your privacy. This includes privacy with your wife or husband and your family.

Most accommodation centres are managed by private providers, but the Reception and Integration Agency (RIA) oversees this. It has published rules and a code of practice for the running of accommodation centres. You can contact the RIA for a copy of these documents (see contact details at the end of this guide).

While staying in an accommodation centre your room may be searched by the centre manager, a member of staff from the RIA, or other inspectors appointed by the RIA to ensure health and safety requirements are met.

See our *Know Your Rights*: A Guide for International Protection Applicants for more information on your rights as an international protection applicant

Can officials or staff from my accommodation centre search my personal belongings?

No, you have the right to privacy in relation to your belongings. Only a member of An Garda Síochána can carry out a search of your personal belongings and they will generally – but not always – need a search warrant to do this.

Where can I go to complain about an invasion of my privacy?

It is a good idea to try and sort out the problem with the accommodation centre manager first. If that fails, you can complain to the RIA, which has a complaints system. You should ask the accommodation centre manager for information about this system. You can also complain to the Data Protection Commission, which will require that you specify what information about you has been processed, in what circumstances.

What should I do if I think that the IPO, INIS, GNIB or another government agency has wrong information about me?

You must give accurate personal information to the authorities when you apply for asylum and register your permission to remain in Ireland. The authorities must keep this information in line with data protection laws. You have the right to ask for a copy of the information that the authorities have about you. You must ask in writing and, generally, you will receive a copy of the information within 30 days. You can then correct any mistakes. If you have a problem getting access to the information that the authorities hold about you, you should contact the DPC (see contact details at the end of this guide).

Remember, you have a right under data protection law to see the personal information that is held about you. **This will not affect your claim for asylum or permission to remain in Ireland**, which is a separate legal procedure.

KEY WORDS

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AFIS)

This is a computer database of fingerprint records used by An Garda Síochána, which is able to search and compare them to identify known or unknown fingerprints.

AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

A technology system used by An Garda Síochána to read vehicle registration plates. It includes a speed detection capability as well a video camera to record speeding and other driving offences.

BARRISTER

A specialist in litigation and advocacy. Usually, barristers are instructed by a solicitor rather than directly by the person taking the case.

BIOMETRICS

The technology of measuring and analysing human body information such as fingerprints, parts of the eye (retinas and irises), voice patterns, facial patterns and hand measurements.

CLOSED-CIRCUIT TELEVISION (CCTV)

Video cameras that provide images or recordings to help with surveillance. See also 'surveillance'.

COMMUNITY-BASED CCTV SCHEME

A scheme that gives funding to some local organisations to help them set up their own community CCTV systems.

CONSTITUTION

A document which sets out fundamental law and principles of Ireland.

COOKIES

Small text files that can be placed and stored on your computer or device by a website you have visited. They are built specifically for internet web browsers to track, personalise and save information about websites you visit.

COMPETENT AUTHORITY

A public authority which is authorised by law to exercise public authority and powers for law enforcement purposes. It includes An Garda Síochána and the Revenue Commissioners.

CONSENT

A legal basis for the processing of personal data. To be valid, it must be:

(i) *freely given* and not forced;

(ii) *informed* (you must be told what your personal data will be used for and be given certain information by way of a privacy notice);

(iii) *specific* (your consent may relate to processing of your personal data for one purpose but not another); and

(iv) based on a statement or clear affirmative action showing you consent (e.g., ticking a box).

DATA CONTROLLER

A person, company or other body that decides how and why to process a person's personal data.

DATA PROTECTION COMMISSION (DPC)

Ireland's data protection supervisory authority and regulator. It handles and investigates complaints lodged by data subjects and can take enforcement action against controllers and processors that breach data protection law.

DATA PROTECTION LAWS

The laws that govern the processing of personal data. These are the Data Protection Acts 1988-2018, the General Data Protection Regulation (GDPR), the Law Enforcement Directive and the ePrivacy Regulations.

DATA PROTECTION OFFICER (DPO)

The GDPR requires controllers and processors to appoint a DPO in certain circumstances. A controller can also voluntarily decide to appoint a DPO.

DATA SUBJECT

If an organisation is holding or using your personal data, you are a data subject.

DATA ACCESS REQUEST / DATA SUBJECT ACCESS REQUEST

You have the right to request a copy of your personal data from a controller, as well as other relevant information about how and why your personal data are being processed.

DATA SUBJECT RIGHTS

You have a number of specific rights under data protection law:

(i) to be informed if, how, and why your personal data are being processed;

(ii) to access and get a copy of your personal data;

(iii) to have your personal data corrected or updated if it is inaccurate or incomplete;

(iv) to have your data deleted or erased;

(v) to limit or restrict how your personal data are used;

(vi) to data portability;

(vii) to object to processing of your personal data; and the right not to be subject to automated decisions without human involvement, where it would significantly affect you.

These rights are subject to a number of limitations and restrictions.

DNA

A chemical found in every cell in the human body. DNA is unique to each individual, except for identical twins, and holds complex information about a person's family relationships and body.

EPRIVACY REGULATIONS

Regulations that apply to cookies and to marketing by email, post and telephone in Ireland.

EUROPEAN AUTOMATED FINGERPRINTING IDENTIFICATION SYSTEM (EURODAC)

A European computer system for comparing the fingerprints of asylum seekers and certain groups of illegal immigrants.

EUROPEAN CONVENTION ON HUMAN RIGHTS (ECHR)

This protects the human rights of people in countries that belong to the Council of Europe, including Ireland.

EUROPEAN ECONOMIC AREA (EEA)

All countries in the European Union (EU) as well as Iceland, Liechtenstein and Norway.

AN GARDA SÍOCHÁNA VETTING UNIT

A section of An Garda Síochána that checks individuals who are seeking to work with children or vulnerable adults. They check to see if the individual has any charges or convictions. The Vetting Unit gives this information to the relevant employer or organisation.

GENERAL DATA PROTECTION REGULATION (GDPR)

The EU law that applies to the processing of personal data. It does not apply to the processing of personal data by an individual for 'purely personal or household' activities or law enforcement processing.

IDENTITY OR ID CARD

An ID card is used to confirm your identity. It may contain your name, address, date of birth, photograph, PPS number or biometric information.

LAW ENFORCEMENT DIRECTIVE

Where personal data are processed by competent authorities (e.g., An Garda Síochána) for law enforcement purposes (such as preventing or detecting crime), the Law Enforcement Directive (and Part 5 of the Data Protection Act 2018) applies and not the GDPR.

LEGAL ADVICE

Professional advice given by a solicitor or barrister.

LEGAL AID

Legal assistance and advice to people who are unable to afford legal representation by a solicitor or barrister in court proceedings. You do not pay for legal aid

LEGAL BASIS (A LEGAL GROUND OR PROCESSING GROUND)

A legal justification for the processing of personal data. A valid legal basis is required for all processing of personal data. There are six legal grounds for processing personal data (Article 6 of the GDPR):

- consent;
- contractual necessity;
- compliance with a legal obligation;
- protecting vital interests;
- performance of an official or public task; and
- legitimate interests (where the interest is not outweighed by the data subject's).

The processing of "special category" personal data is prohibited except in limited circumstances. Special category personal data, as per Article 9(1) of the GDPR, is personal data which reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Article 9(2) outlines ten exceptions where "special category" data may be permitted. These are if:

- the data subject has given explicit consent;
- the data has been made public by the data subject;
- processing is carried out by a not-for-profit body as part of its legitimate activities;
- processing is necessary to protect the vital interests of the data subject;
- processing is necessary for legal claims and judicial acts, or if courts are acting in their judicial capacity;

Processing may also be permitted if necessary (with a basis in law):

- for social security, employment and social protection purposes;
- for health or social care purposes;
- for reasons of substantial public interest;
- for reasons of public health;
- for archiving, research and statistical purposes.

LEGISLATION

Law made by the TDs and Senators in the Oireachtas.

PERSONAL DATA

Any information about a living person where that person is identified or could be identified. It can include many different types of information, such as name, date of birth, email address, CCTV image, phone number, address, physical characteristics, or location data – once it is clear who the information relates to, or it is reasonably possible to find out.

PERSONAL PUBLIC SERVICE NUMBER (PPS NUMBER OR PPSN)

A number that identifies you so that you can use public services such as social welfare, Revenue services, public healthcare and education.

PROCESSING

Using personal data in any way, including collecting, storing, retrieving, consulting, disclosing or sharing with someone else, erasing, or destroying.

PROCESSOR

A person, company, or other body which processes personal data on behalf of a controller.

PRIVACY NOTICE (PRIVACY STATEMENT)

A document that describes the type of information an organisation might collect about you, how it will use the information, whether it will share the information with others and your rights regarding the information it collects.

PULSE (POLICE USING LEADING SYSTEMS EFFECTIVELY)

A computer system used by An Garda Síochána for the collection and storing of information about crimes, traffic management, firearms licensing, driver licences, insurance and character vetting.

REGISTER OF VOTERS

A list of people who have the right to vote in local, national or European elections in Ireland. The register is put together by city and county councils.

RETINA SCAN

A technique that uses the unique patterns on your retina (part of your eye) to identify you.

SOLICITOR

A lawyer who deals with the person taking the case. A solicitor can provide legal advice about your rights and advises people before they are arrested and charged. Often, a solicitor is the only lawyer you will need.

SURVEILLANCE

Monitoring, observing, listening to or recording your (or a group's) movements, activities or communications. It also includes monitoring or recording places or things.

TRACKING DEVICE

An electronic device which is used to track a person or vehicle.

TRANSPARENCY

An organisation that collects information about you must tell you the name of the organisation; the contact details for the organisation or its Data Protection Officer (DPO) if it has one; the purposes and 'legal basis' for collecting the information; who the information will be shared with; how long the information will be stored; and about your rights as a data subject. This is usually done by way of a privacy notice.

WEB BROWSER

A software programme used to display and view pages on the web, for example, Google Chrome, Safari, Brave or Microsoft Edge.

CONTACT DETAILS

ASYLUM SEEKERS AND REFUGEES

Garda National Immigration Bureau (GNIB)

The Garda National Immigration Bureau (GNIB) is the section of An Garda Síochána that deals with immigration issues. It carries out deportations, border control checks and investigations relating to illegal immigration and human trafficking.

13/14 Burgh Quay
Dublin 2
Tel: 01 666 9130 / 01
Email: gnib_dv@garda.ie
Website: www.garda.ie

The Immigrant Council

The Immigrant Council of Ireland is a national, independent non-governmental organisation that promotes the rights of migrants.

7 Red Cow Lane,
Dublin, D07 XN29
Tel: 01 674 0202
Immigration Helpline: 01 674 0200
Email: admin@immigrantcouncil.ie
Website: www.immigrantcouncil.ie

International Protection Accommodation Services (IPAS)

International Protection Accommodation Services (IPAS) is responsible for the provision of accommodation and related services to people in the International Protection ('asylum') process.

Department of Children, Equality, Disability, Integration and Youth
Miesian Plaza
Lower Baggot Street
Dublin 2
Email: ipasinbox@equality.gov.ie
Website: https://www.gov.ie/en/campaigns/d9f43-international-protection-accommodation-services-ipas/

International Protection Office (IPO)

The International Protection Office (IPO) processes applications for international protection under the International Protection Act 2015. It also considers whether applicants should be given permission to remain.

Timberlay House
78-83 Lower Mount Street
Dublin 2
Tel: 01 602 8000
Email: info@ipo.gov.ie
Website: www.ipo.gov.ie

Irish Refugee Council

This non-governmental organisation advocates on behalf of refugees and asylum seekers.

Second Floor
Ballast House
Aston Quay
Dublin 2
Tel: 01 764 5854
Email: info@irishrefugeecouncil.ie
Website: www.irishrefugeecouncil.ie

Reception and Integration Agency (RIA)

This government agency manages the accommodation of people seeking asylum in Ireland. It also coordinates the provision of services at accommodation centres.

Block C
Ardilaun Centre
112-114 St Stephen's Green
Dublin 2
Tel: 01 418 3200
Email: RIA_inbox@justice.ie
Website: www.ria.gov.ie

United Nations High Commissioner for Refugees (UNHCR) Office

This UN agency coordinates efforts to protect refugees and resolve challenges facing refugees.

Merrion House
Suite 4
1-3 Lower Fitzwilliam Street
Dublin 2
Tel: 01 631 4613
Website: www.unhcr.ie

Refugee Legal Services

This is a specialised office of the Legal Aid Board. It provides confidential and independent legal services to people applying for asylum and on immigration and deportation matters.

DUBLIN:
48/49 North Brunswick Street
Georges Lane
Dublin 7
Tel: 01 646 9600
Email: dublinrls@legalaidboard.ie

Timberlay House
79/83 Lower Mount Street
Dublin 2
Tel: 01 631 0800
Email: dublinrls@legalaidboard.ie

CORK:
North Quay House
Popes Quay
Cork
Tel: 021 455 4634
Email: corkrls@legalaidboard.ie

GALWAY:
Seville House
New Dock Road
Galway
Tel: 091 562 480
Email: rlsgalway@legalaidboard.ie

CHILDREN AND YOUNG POEPLE

Children's Rights Alliance (CRA)

The Children's Rights Alliance (CRA)is a coalition of non-governmental organisations working to secure the rights of children in Ireland by campaigning for the implementation of the United Nations Convention on the Rights of the Child. You can contact the Alliance if you have any questions about your rights as a child or young person.

4 Upper Mount Street
Dublin 2
Tel: 01 662 9400
Email: info@childrensrights.ie
Website: www.childrensrights.ie

National Parents Council

This group represents parents with children in early, primary and post-primary education.

12 Marlborough Court,
Marlborough Street, Dublin 1
Tel: 01 887 4034
Email: info@npc.ie
Website: www.npc.ie

Office of the Ombudsman for Children

This office advises the government on children and young people. It conducts research and also handles complaints.

Millennium House
52-56 Great Strand Street
Dublin 1
Tel: 01 865 6800 / 1800 202 040
Email: oco@oco.ie
Website: www.oco.ie

CCTV AND TRANSPORT ISSUES

Bus Éireann

Bus Éireann is a State-owned bus and coach operator providing services throughout Ireland, with the exception of Dublin and the Greater Dublin Area, where bus services are provided by Dublin Bus.

Bus Éireann
Broadstone
Dublin 7
D07 X2AE
Tel: 0818 836 611
Website: www.buseireann.ie.

DART

The DART is the rail line running along the coast of Dublin and north Wicklow. It is run by the national rail company, Iarnród Éireann (Irish Rail).

DART Customer Relations Department
Pearse Station
Westland Row, Dublin 2
Tel: 01 703 3504
Website: www.irishrail.ie

Dublin Bus

Dublin Bus is an Irish State-owned bus operator providing services in Dublin.

Dublin Bus
59 Upper O'Connell Street
Dublin 1
D01 RX04
Tel: 01 873 4222
Website: www.dublinbus.ie

Iarnród Éireann

Iarnród Éireann, or Irish Rail, is the operator of the national railway network of Ireland.

Connolly Station
Amiens Street
Dublin 1
D01 V6V6
Tel: 01 836 6222 / 0818 366 222
Website: www.irishrail.ie

Luas

The Luas is the light rail transport system in Dublin. It operates along two routes: the green line and the red line.

Veolia Transport Customer Care
Department Luas Depot
Red Cow Roundabout
Clondalkin
Dublin 22
Tel: 01 461 4910 / 1800 300 604
Email: info@luas.ie
Website: www.luas.ie

COMPLAINTS ABOUT SURVEILLANCE

Complaints Referee

If you have a complaint about suspected surveillance activities, you can contact the complaints referee.

Judge Dara Hayes
Complaints Referee
Four Courts
Dublin 7

CRIMINAL JUSTICE

An Garda Síochána

An Garda Síochána is the Irish police service.

An Garda Síochána Headquarters
Phoenix Park
Dublin 7
Tel: 01 666 0000
Garda Confidential Line: 1800 666 111
Emergencies: 999 / 112
Website: www.garda.ie

An Garda Síochána Vetting Unit

A section of An Garda Síochána that checks individuals who are seeking to work with children or vulnerable adults to see if they have any charges or convictions. .

An Garda Síochána Vetting Unit
Racecourse Road
Thurles
Co. Tipperary
Tel: 050 427 300

Courts Service of Ireland

The Courts Service manages the courts, maintains court buildings, provides support services for judges and gives information on the court system to the public.

15-24 Phoenix Street North
Smithfield
Dublin 7
Tel: 01 888 6000
Website: www.courts.ie

Garda Síochána Ombudsman Commission (GSOC)

The Commission deals with complaints made by the public about the conduct of Gardaí.

150 Abbey Street Upper
Dublin 1
Tel: 01 871 6727 / 1890 600 800
Email: info@gsoc.ie
Website: www.gardaombudsman.ie

Office of the Director of Public Prosecutions (DPP)

Office of the Director of Public Prosecutions (DPP) is in charge of prosecutions on behalf of the State and the people of Ireland.

14-16 Merrion Street
Dublin 2
Tel: 01 678 9222
Website: www.dpp.ie

DATA PROTECTION

Data Protection Commission (DPC)

The Data Protection Commission is responsible for upholding the data protection rights of people and holding to account organisations that breach those rights.

Dublin office:
21 Fitzwilliam Square South
Dublin2
D02 RD28

Portarlington office:
Canal House
Station Road
Portarlington
Co. Laois
R32 AP23
Tel: 01 765 0100 / 1800 437 737
Website: www.dataprotection.ie

EMBASSIES

If you need to contact your embassy or consular office in Ireland, the best thing to do is to contact the Department of Foreign Affairs, where you will get information about your embassy or consular office.

Department of Foreign Affairs
Consular Section
69-71 St Stephen's Green, Dublin 2

For the Munster area:
Consular Services
Department of Foreign Affairs
1A South Mall, Cork

Tel: 01 408 2308 / 01 408 2585 /
01 408 2302
Website: www.dfa.ie

EMPLOYMENT

Workplace Relations Commission (WRC)

The Workplace Relations Commission (WRC) provides information to employees and employers on employment rights and makes sure that employment law is obeyed.

O'Brien Road, Carlow
R93 E920
Tel: 059 917 8990 / 0818 80 80 90
Website: www.workplacerelations.ie

GOVERNMENT

Citizens Information Board

This national agency gives information and advice on social services and money matters. It also provides advocacy services. Information is available through Citizens Information Services in person, by phone or on the website.

There are 268 Citizens Information Services around the country. Call the telephone helpline or visit the website to find the one closest to you.

Tel: 1890 777 121
Website: www.citizensinformation.ie

Department of Justice

This government department deals with a broad range of issues including access to justice, crime, community safety, immigration, security and victims' supports.

51 St Stephen's Green, Dublin 2
D02 HK52
Tel: 01 602 8202 / 1800 221 227
Email: info@justice.ie
Website: www.justice.ie

Department of Education and Skills

This government department oversees the education system in Ireland.

Marlborough Street
Dublin1
Tel: 01 889 6400
Website: www.education.ie

Department of Foreign Affairs

This government department deals with diplomatic issues and Ireland's interests abroad.

69-71 St Stephen's Green
Dublin 2
Tel: 01 478 0822 / 1890 426 700
Website: www.dfa.ie

Department of Social Protection

This government department is responsible for providing social insurance and social assistance schemes, for example Child Benefit, Unemployment Benefit and the State pension.

Áras Mhic Dhiarmada
Store Street
Dublin 1
Tel: 01 704 3000
Website: www.welfare.ie

Client Identity Services
Social Welfare Services
Shannon Lodge
Carrick-on-Shannon
Co. Leitrim
Tel: 1890 927 999
Email: cis@welfare.ie

Other government departments

To get information about other government departments, contact Citizens Information Services.

You can also find a list of all government departments and agencies on www.gov.ie.

LEGAL MATTERS

Bar Council

This is the representative and regulatory body for barristers. If you are looking for a barrister or have a complaint about your barrister, you can contact the Bar Council.

Bar Council Administration Office
Four Courts
Dublin 7
Tel: 01 817 5000
Email: barcouncil@lawlibrary.ie
Website: www.barcouncil.ie

Free Legal Advice Centres (FLAC)

This non-governmental organisation works towards achieving social justice. It also provides some basic, free legal services to the public.

13 Lower Dorset Street
Dublin 1
Tel: 01 874 5690
Information and Referral Line:
1890 350 250
Website: www.flac.ie

Law Society of Ireland

This is the representative and regulatory body for solicitors. If you are looking for a solicitor or have a complaint about your solicitor, you can contact the Law Society.

Blackhall Place
Dublin 7
Tel: 01 672 4800
Email: general@lawsociety.ie
Website: www.lawsociety.ie

Legal Aid Board

The board provides legal aid for people who cannot afford legal representation. Legal aid is only for civil issues such as suing for personal injury or applying for asylum. The board does not deal with criminal issues.

Kerry office
Quay Street
Cahirciveen
Co. Kerry
Tel: 066 947 1000 / 1890 615 200

Dublin office
47 Upper Mount Street
Dublin 2
Tel: 01 644 1900
Email: info@legalaidboard.ie
Website: www.legalaidboard.ie

IMMIGRATION

Department of Justice

The Immigration Service Delivery function delivers frontline immigration services on behalf of the government.

Immigration Service Delivery
Department of Justice
13-14 Burgh Quay
Dublin 2
D02 XK70
Website: www.irishimmigration.ie

Immigrant Council of Ireland

The Immigrant Council of Ireland is a non-governmental organisation that promotes the rights of migrants through information, legal advice, advocacy, lobbying, research and training. The Council is also an independent law centre.

2 St Andrew Street
Dublin 2
Tel: 01 674 0202
Email: admin@immigrantcouncil.ie
Website: www.immigrantcouncil.ie

MEDIA

Coimisiún na Meán

Coimisiún na Meán is the independent regulator for broadcasters and online media in Ireland.

2-5 Warrington Place
Dublin 2
Tel: 01 644 1200
Email: info@cnam.ie
Website: www.cnam.ie

Office of the Press Ombudsman

The Press Ombudsman investigates complaints against members of the press.

1-3 Westmoreland Street
Dublin 2
Tel: 1890 208 080
Email: info@pressombudsman.ie
Website: www.pressombudsman.ie

Press Council of Ireland

The Press Council has developed a code of practice for those working in newspapers and periodicals. The Council appoints the Press Ombudsman, makes decisions in complex cases and decides on appeals from the Press Ombudsman.

1-3 Westmoreland Street
Dublin 2
Tel: 01 648 9130
Email: info@presscouncil.ie
Website: www.presscouncil.ie

PRISONS

Irish Penal Reform Trust

The Irish Penal Reform Trust campaigns for the rights of people in prison and for prison reform.

Fourth Floor
Equity House
16-17 Upper Ormond Quay
Dublin 7
Tel: 01 874 1400
Email: info@iprt.ie
Website: www.iprt.ie

TRADE UNIONS

Association of Secondary Teachers Ireland (ASTI)

This trade union represents second-level teachers in community colleges, comprehensive schools and voluntary secondary schools.

Thomas McDonagh House
Winetavern Street
Dublin 8
Tel: 01 604 0160 / 1850 418 400
Email: info@asti.ie
Website: www.asti.ie

Fórsa

Fórsa is the second largest union on the island of Ireland.

Nerney's Court
Dublin 1
D01 R2C5
Tel: 01 817 1500
Website: www.forsa.ie

Irish National Teachers Organisation (INTO)

This trade union represents Irish national teachers.

35 Parnell Square, Dublin 1
D01 ET35
Tel: 01 804 7700
Email: info@into.ie
Website: www.into.ie

Irish Congress of Trade Unions (ICTU)

The Irish Congress of Trade Unions (ICTU) represents 800,000 workers and is affiliated with 44 unions across Ireland and Northern Ireland.

31/32 Parnell Square, Dublin 1
Tel: 01 889 7777
Email: congress@ictu.ie
Website: www.ictu.ie

Mandate Trade Union

This trade union represents the retail and bar trade.

O'Lehane House
9 Cavendish Row
Dublin 1
Tel: 01 874 6321 / 2 / 3
Website: www.mandate.ie

National Union of Journalists (NUJ)

This trade union represents people working in media and publishing.

Spencer House
Spencer Row
Off Store Street, Dublin 1
Tel: 01 817 0340
Email: info@nuj.ie
Website: www.nuj.org.uk

Services, Industrial, Professional and Technical Union (SIPTU)

Head Office
Liberty Hall
Dublin 1
Tel: 01 858 6300
Email: genpres@siptu.ie
Website: www.siptu.ie

Teachers' Union of Ireland (TUI)

73 Orwell Rd
Rathgar
Dublin 6
Tel: 01 492 2588
Email: tui@tui.ie
Website: www.tui.ie

TRANSLATION AND INTERPRETATION

Association of Translators and Interpreters Ireland (ATII)

The Association of Translators and Interpreters Ireland represents translators and interpreters. If you are looking for a translator or interpreter, you could contact them for advice.

Trinity Centre for Literary and Cultural Translation
Trinity College Dublin
36 Fenian Street
Dublin 2
Email: info@atii.ie
Website: www.atii.ie

OTHER

Equality Authority

This government-funded body works to prevent discrimination in both employment and access to goods and services.

Birchgrove House, Roscrea
Co. Tipperary

Dublin office:
2 Clonmel Street
Dublin 2

Tel: 1890 245 545
Email: info@equality.ie
Website: www.equality.ie

Irish Human Rights and Equality Commission (IHREC)

Ireland's national human rights and equality institution.

16-22 Green Street
Dublin 7
D07 CR20
Tel: 01 858 9601
Email: info@ihrec.ie
Website: www.ihrec.ie

Irish Internet Hotline

This organisation provides an anonymous reporting service to members of the public who accidentally uncover illegal content on the internet, particularly child pornography or activities relating to the sexual exploitation of children.

ISPAI Service
Unit 24 Sandyford Office Park
Dublin 18
Tel: 1890 610 710
Email: info@hotline.ie
Website: www.hotline.ie

KNOW YOUR RIGHTS Privacy and Data Protection

Know Your Rights is a public information project of the Irish Council for Civil Liberties (ICCL), designed to inform people in clear and accessible language about their rights under various key areas of the law in Ireland.

This is the 9th guide in the Know Your Rights series. This, and other guides in the Know Your Rights series, are also available for print and download free of charge on our webpage: **https://www.iccl.ie/your-rights/**.

This guide provides information about your privacy and data protection rights. This guide was researched and written by Aidan Healy and Charlotte Burke of DAC Beachcroft.

ICCL would like to thank all who contributed to this guide.

Irish Council for Civil Liberties

FOR ALL OUR RIGHTS. NO EXCEPTIONS.

Irish Council for Civil Liberties,
First Floor, Castleriver House,
14/15 Parliament Street,
Dublin 2, D02 FW60, Ireland
Phone: +353-1-9121640
Email: info@iccl.ie
www.iccl.ie