ÁRAS NUA-EALAÍNE
NA hÉIREANN
IRISH MUSEUM OF
MODERN ART

+353 1 612 9900
imma.ie

IMMA

DATA PROTECTION POLICY

Ospidéal Ríoga
Cill Mhaighneán
Baile Átha Cliath 8
D08 FW31, Éire

Royal Hospital
Kilmainham
Dublin 8
D08 FW31, Ireland

IMMA

Table of Contents

IMMA

This data protection policy is written to ensure that the General Data Protection Regulations as of 25 May 2018 are implemented and relevant to how IMMA and its subsidiaries will be responsible when dealing with the personal data of its employees, visitors, patrons, clients, business partners and service providers.

IMMA is committed to reviewing and auditing its policies and procedures through due diligence in its commitment to securing personal data, sensitive personal data, other sensitive data and general data. This Policy has been ratified by the Board of IMMA and will be reviewed every May.

IMMA

THE POLICY

The purpose of this policy document is to provide concise information regarding the Data Protection obligations of the Irish Museum of Modern Art (IMMA) and its subsidiary the Royal Hospital Kilmainham (t/a RHK) when dealing with the personal data of its employees, visitors, patrons, business partners clients and service providers. IMMA is committed to adhering to the regulations as required by the General Data Protection Regulations (GDPR) and other relevant legislation that governs obtaining, storage and disposal of personal data as defined by European and Irish legislation.

IMMA makes no distinction between its employees and those who are not and acknowledges all rights of data subjects & entities and commits to treating all equally under this policy.

The scope of this policy covers both personal and sensitive personal data that may be provided by individuals or entities or is obtained during the course of its business, that relates to data subjects and is managed or stored electronically or in a manual data filing system.

All personal data and sensitive personal data will be treated with care and retained securely. IMMA is committed to ensuring that all personal data held by the museum is accurate, relevant and is retained no longer than is permitted by the original permissions under which it was provided and in any case in compliance with the Data Protection Regulations.

Personal Data will be securely controlled within the organisation and will not be shared with third parties unless Data Subjects have consented to this at the time of providing the data,
or
where data is processed on behalf of IMMA by a third party organisation on its behalf that in each case there is a formal written contract with the processor outlining their obligations in relation to the personal data, the specific purposes for which they are engaged and the agreement that they will process the data on behalf of IMMA in compliance with the European and Irish Data Protection Regulations.

Irish Museum of Modern Art (IMMA) – Data Controller
During the course of the museums operational activities, IMMA may acquire, process and store personal data in relation to:

- Employees of IMMA
- Visitors and users of IMMA Services
- Commercial clients and activities of the RHK
- Third party service providers
- Collection archives and loan agreements
- Exhibition archives and agreements
- Educational and learning activities and programs

This policy identifies that during the course of the museum's activities, personal data will be provided to IMMA for use solely for the purposes that it was provided. IMMA is committed to ensuring that all staff are made aware, through regular training, of the guidelines under the Data Protection Regulations on how personal data must be managed and to be able to identify where a data protection issue may arise that could be contrary to the regulations. Should an issue be identified, all staff are instructed to notify and seek advice from the Data Protection Officer so that personal data is dealt with correctly and/or appropriate corrective action is taken.

Data Storage
When you give your personal details to IMMA, as an organisation we are committed to keeping these details private, safe and in a secure data storage system. IMMA is committed to ensuring that all personal data and non-personal data is securely stored and managed using the latest state of the art technology available, as required by the Data Protection Regulations. The security and capability of the data storage systems will be reviewed and integrity tested on a regular basis.

Data Breach or Data Loss
IMMA is committed to complying with the Data protection regulations and all recommendations set by the Data Protection Commissioner. As Data Controller, in the event of any loss or breach of security, or protocols that relate to a subject's data being compromised IMMA undertakes to:

- Notify the data subject of any incident where their data may be lost or compromised.
- Report the loss/compromise to the Data Protection Commissioner immediately and in case within 72 hours.
- Take all steps necessary to recover/erase the data and commence a full investigation as directed by the Data Protection Commissioner.
- Conduct an open and transparent investigation in accordance with this policy.

IMMA Protocol for action in the event of a breach or loss of data
Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller will give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, the data controllers will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions, etc.

All incidents of loss of control of personal data, in manual or electronic form, by a third party contracted data processor will be reported to the IMMA Data Protection Officer as soon as the data processor becomes aware of the incident and to the Data Protection Commissioner and in any case within 72 hours.

IMMA Protocol for action by third party data processor in the event of a breach or loss of data.
Contact will be immediately made with the Data Protection Officer within IMMA.

Where the data concerned is encrypted or protected by technological security measures that make it unintelligible to any person who is not authorised to access it, IMMA may conclude after investigation that due to the security measures in place that there is no risk to the data being opened/read/utilized. Any loss of control has been contained and/or the data erased and put beyond use. This would mean that there is no need to inform the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the security measures (such as encryption) were of a high standard.

However, where such an incident does occur, IMMA is committed to inform the data subject of the events.

Where it is clear that the personal data has been lost or compromised and cannot be recovered or controlled the IMMA Data Protection Officer will gather a small team of trained staff to assess the potential exposure/loss. This team will assist with the practical matters associated with this investigation.

IMMA Procedure in the event of loss or control personal data
The IMMA investigation team, under the direction of the Data Protection Officer, will give immediate consideration to informing all data subjects who may be affected. At the direction of the Data Protection Officer, the team shall:

Make initial contact with the data subjects concerned to advise them that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.

As soon as practicable, the data subjects will be advised of:

- The nature of the data that has been potentially exposed/compromised
- The level of sensitivity of this data and
- The steps IMMA intends to take by way of containment or remediation or recovery.
- That IMMA has contacted other organisations including the Office of the Data Protection Commissioner.
- That where the data subjects express a particular concern with respect to the threat to their personal data, consideration must be to advise the relevant authority e.g. Gardaí etc.
- Where the data breach is suspected to be criminal or has caused the data to be "damaged" (e.g. as a result of hacking), the Data Protection Officer shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
- IMMA shall notify the insurance company which the Museum is insured and advise them that there has been a personal data security breach.

IMMA will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate.

By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.

Where data has been "damaged" (as defined in the Criminal Justice Act, 1991, e.g. as a result of hacking), the matter will be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011.

Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act, 2011 as discussed above.

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner and the data subject within 72 hours of the incident. Contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data.

Where IMMA has contracted a third party service such as a data storage facility or data processor the contractor will report a data breach directly to the primary IMMA contact as a matter of urgent priority. This requirement will be clearly set out in the supplier contract. On receipt of any such breach by or affecting a 3rd party data processor, the above breach procedure will commence.

IMMA

Data Subjects - Access Requests
You have the right to data protection when your details or personal data is:

- Stored on a computer or other digital format.
- Held on paper or other manual form as part of a filing system
- Made up of photographs or video recordings of your image or recordings of your voice.

You have the right to ensure that the information IMMA manages or is stored about you is:

- Factually correct.
- Only available to those who should have it. That it is protected and access to the data restricted.
- Only used for stated purposes. That IMMA cannot share your data without your permission.

Your rights as a Data Subject
You have a range of rights on how your data is obtained and managed. IMMA is committed to upholding those rights. You have the right to have your details used in line with Data Protection Regulations.

As a data controller who holds information about an individual, IMMA must:

- Get and use the information fairly, be honest in seeking information. IMMA must have your permission, we can't assume it.
- Keep it for only one or more clearly stated and lawful purposes. We have to tell you exactly what we want it for.
- Use and make known this information only in ways that you have given permission for. We can't share it.
- Keep the information safe. We have to store/manage your data using up to date technology. Restrict access to it.
- Make sure that the information is factually correct and up-to-date. We will ask you at regular periods, or you can ask to see and check the data is correct yourself.
- Make sure that there is enough information – but not too much - and that it is relevant. If it's not relevant we can't keep it.
- Keep the information no longer than it is needed & only for the reason stated. Once that reason no longer exists, we must delete it.
- Give you a copy of all your personal information that IMMA has when you ask for it.

Information we must give you when we seek to obtain your data
As a data controller, when IMMA seeks to obtain personal information we must, at a minimum, give you:

- The reason why IMMA wants or needs your details;
- How we plan to use that data and,
- Any other information that you may need to make sure that we are handling your details fairly – for example, the details of other organisations or people to whom we may share your personal data with.

When this information is sought from you in person, you must be given the name of the person collecting the information and the IMMA department they are collecting the information for.

Right to access your personal data retained by IMMA
You can ask for a copy of all your personal details held by IMMA on a computer or in manual form by writing to the Data Protection Officer (See How do I get Access to My Data below)

You should also be informed of, and given the chance to object to, any decisions about you that are automatically generated by a computer without any human involvement.

Data Portability
You have the right to have personal data transmitted to another data controller without hindrance, where technically feasible. This is only possible in relation to personal data given with consent, and does not apply to data generated by IMMA. When we receive a request from a data subject to transfer personal data to another entity we will comply with that request.

Data Profiling
Data profiling is defined as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work; economic situation; health; personal preferences; interests; reliability or behaviour; location or movements “.

As a data subject you have the right not to be the subject of any decision based solely on automated processing, except where you have explicitly agreed or the profiling forms part of a contract.

International Data Transfers
Data transfers outside the EEA are prohibited unless the receiving country ensures appropriate safeguards to secure personal data and it is retained in compliance with the regulations. IMMA will not transfer any personal data outside of the EEA unless that country is approved by the Irish Data Protection Commissioner and only then if we have the permission of the data subject and that they have consented/requested the data transfer.

Data Privacy Impact Assessments
Data Privacy Impact Assessments (DPIAs) are obligatory impact assessments that must be undertaken at the early stages of any organisational changes involving

'high risk' to the data rights of individuals, but only where the organisation or change involves:

- Large-scale processing of sensitive data
- Large-scale monitoring of a public area
- Processing of data related to criminal convictions

The Data Protection Commissioner is to produce guidelines for the requirements surrounding DPIAs.
IMMA is committed to complying with this principle and undertakes to carry out a DPIA on all new projects of data processing in particular using new technologies that could result in a high risk to the rights of data subjects. A copy of all DPIAs undertaken will be available and contained as part of the Data Protection Register.

Changes to consent for data collection
Consent to the collection and processing of personal data must now involve affirmative action. You must be required to directly opt in. Automatic opt-in, pre-ticked boxes or inactivity are no longer acceptable means of acquiring consent from data subjects.

Consent is defined as:
"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"
In addition to specifically opting-in to processing, as a data subject you must be advised of the reasons your data will be processed, including 'legitimate interests' processing. Legitimate interests include:

- Prevention of fraud
- Direct marketing
- Ensuring security
- Reporting possible criminal acts
- Necessary transmission of data within an organisation

IMMA is committed to this requirement and will actively assess and change its current and future means of communication with our audience.

Privacy by Design, Privacy by Default
Privacy by design and default is a new concept that IMMA, as a data controller, is required to embed into our organisational processes, projects and changes. We are committed to:

- Embedding data privacy into our operational processes.
- Use appropriate technical and organisational measures to ensure your privacy.
- Employ pseudonymisation – the renaming of identifying data fields in databases.
- Implement data minimisation – by default collecting only directly relevant data. If we don't need it, we don't ask.
- Security will be fundamental to database design and data processing.
- Personal Data will only be processed for the specific purpose it was obtained.

- Access to your data will be controlled and limited.
- Data retrieval, erasure and portability measures will be included in data processing design and policy.

Demonstrating Accountability
IMMA is registered with the Office of the Data Protection Commissioner and as such will be able to demonstrate, on request, our compliance with the GDPR regulations. We will achieve this by:

- Maintaining records of how data is acquired by us and processed.
- Being able to provide those records and policies to the supervisory authority on request.
- Being able to demonstrate that consent was requested, received and correctly recorded.
- Maintaining records of measures taken to address non-compliance by us and any third-party data processor contracted to IMMA.
- Reviewing our data protection policies to ensure that they clearly demonstrate compliance which promotes confidence.

Expansion of the Data Protection Principles under GDPR
The principles applied, retained and expanded upon with GDPR are below:

The right of access to personal data	All requests will be complied with as outlined in this policy without fail even though it is no longer a specific principle, but is retained and covered separately in the regulations.
Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data

	is processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.
One-Stop-Shop	IMMA will now be able to deal with a single supervisory data protection authority, for us it is the Office of the Data Protection Commissioner.

Data Processors and GDPR
Third party data processors are used by IMMA but are strictly controlled through contracts of agreement for the processing of data obtained on our behalf. The data processors face new restrictions and obligations under GDPR. Specific obligations under GDPR include:

- Obtain IMMA (data controller) permission before using any sub-contracted data processors.
- Process data, only in accordance with IMMA (data controller) instructions.
- Maintain data processing records and making them available to the supervisory authority.
- Take appropriate security measures and notifying the data controller of any breaches. (see our data breach procedures)
- Comply with overseas data transfer rules.

Roles and Responsibilities within IMMA
The concept of accountability is a significant new addition that imposes additional obligations on data controllers and processors as per the below:

Chairman and IMMA Board	The Chairman and IMMA Board have ultimate responsibility for overseeing the implementation and management of the IMMA Data Protection Policy through regular reviews, audits and reports. The Director will present monthly reports for the Board which will confirm that the policies and procedures are in place and that IMMA as an organisation is complying with the requirements and regulations of the Data Protection Act.
IMMA Director	Is responsible for ensuring that all departments within IMMA are adhering to the Data Protection Regulations through policy implementation, internal audits and regular updates with a view to compliancy, including all

	requests for data access, which will be overseen by the Data Protection Officer. The Director will confirm to the IMMA Board through report that all data within the control of IMMA is obtained, used & retained securely in compliance with the Data Protection Act and where necessary report all breaches when they occur.
Data Protection Officer	Is responsible for the development and implementation of the IMMA Data Protection Policy, overseeing compliancy, internal audits and data access requests as required by GDPR. They are responsible for reporting and investigation all data breaches to the Director and Data Protection Commissioner.
Human Resources	The Human Resources Department within IMMA will ensure that the requirements of the Data Protection Policy and GDPR are communicated to all new staff through induction. They will also ensure that staff awareness is constant through staff reviews and regular policy updates.
Heads of Department (Line Managers)	Responsible for ensuring compliance with the IMMA Data Protection Policy within their departments. They will ensure staff in their departments are aware of the policy and receive regular updates through organisation or departmental training processes. As data controllers they are responsible for ensuring the collection, use, retention and disposal of data within their control is secure and used in compliance with GDPR.
Staff	Have a personal responsibility for ensuring compliancy with all the principles of the Data Protection Act, to follow the IMMA Data Protection Policy ensuring that all personal data is used within the controls of the Data Protection Regulations.

How Do I get Access to My Data?
If you think that IMMA is holding some of your personal details or information about you, you can ask us to confirm this. You should apply in writing to the Data Protection Officer at IMMA. The written request for the information can be by postal letter, email or a letter handed in to the Museum, but it must be in writing. All applications must be accompanied by photographic identification, such as passport/driving licence/European identity card plus a recent utility bill or Government letter. Copies of the original documents will suffice.

On receipt of the application the Data Protection Officer will provide you with an acknowledgement of the request. This will be followed with a copy of all the data we have on you within 21 days. We must tell you which details we hold and the reason why we are holding this information. This information free of charge.

There may be occasions when the data we hold may be in a manual archival system that needs to be physically searched for your data references as the data may be have been obtained prior to May 2018. If this is the case we will let you know in writing and give an estimated time period that it will take to retrieve the information for you.

Please see the section on ***Accessing Your Information from the Data Protection Commissioner*** at the end of this policy.

Right to change or remove your details
If IMMA is legally retaining data about you that is not factually correct, you can ask us to change or, in some cases, remove these details.

Similarly, if you feel that IMMA does not have a valid reason for holding your personal data or that they we have taken these details in an unfair way, or they are being used in a manner that is exceeds the reasons for which they were obtained or retained, then you can also ask us to change or remove the data.

In both cases, you can write to the Data Protection Officer, explaining your concerns and outlining what data is incorrect. You should apply in writing to the Data Protection Officer at IMMA. The written request for the information can be by postal letter, email or a letter handed in to the Museum, but it must be in writing.

On receipt of the application, the Data Protection Officer will provide you with an acknowledgement of the request. This will be followed by a confirmation that a copy of all the data we have on you has been corrected as requested or removed/deleted from retention within the IMMA data storage systems. We must do this within 40 days or explain why we have been unable do so.

There may be occasions when IMMA is required, on a legal basis, to retain personal data on a data subject. In response to the request to change or remove your retained data we must explain fully the legal basis under which we are required to retain that data. Such examples could be for pension/revenue purposes. Either way you will be fully informed.

There may be occasions when the data we hold may be in a manual archival system that needs to be physically searched for your data references as the data may be have been obtained prior to May 2018. If this is the case we will let you know in writing and give an estimated time period that it will take to retrieve the information for you. IMMA is committed to keeping you fully informed during any application for data information.

Right to remove your details from a direct marketing list
IMMA uses MailChimp as our marketing automation platform. By signing up to our emailing list(s) you acknowledge that the information you provide will be transferred to MailChimp for processing in accordance with their Privacy Policy and Terms.
If IMMA holds personal data about you for direct marketing purposes, you can ask us to remove your data. You can do this by writing to the Data Protection Officer. The written request for removal can be by postal letter, email or a letter handed in to the museum, but it must be in writing.

On receipt of the application the Data Protection Officer will provide you with an acknowledgement of the request.

This will be followed by a confirmation that the request for removal has been complied with. IMMA undertakes to comply with the request as soon as possible and in any case within 40 days.

How do I contact the IMMA Data Protection Officer to request access to my details?
You can contact the IMMA Data Protection Officer by writing to:

IMMA Data Protection Officer
Irish Museum Of Modern Art
Royal Hospital
Military Road
Kilmainham
Dublin
D08 FW31

Or by emailing dataprotection@imma.ie

IMMA is committed to protecting the data rights of its staff, visitors, patrons, business partners and service providers. With this in mind we have published some further guidelines below from the Office of the Data Protection Commissioner. These guidelines are incorporated into the Data Protection Policy above along with the seven key principles of the IMMA Data Protection Guidelines. The guidelines will also assist you in preparing a written application. Please remember to include as much detail as possible in all data requests, this will help facilitate all applications.

General Data Protection Regulation (GDPR) and the Data Protection Acts 1988 and 2003 imposes obligations on data controllers to process personal data entrusted to them in a manner that respects the rights of data subjects. Data controllers are under a specific obligation to take appropriate measures to protect the security of such data.

The Seven Key Principles outlined by the Office of the Data Protection Commissioner

GDPR relies on seven 'principles' contained in Article 5, which will regulate the processing of personal data. We have incorporated these principles into the policy above, in the section ***Expansion of the data protection principles under GDPR***

In summary these are:

1. Lawful, Fair and Transparent Processing
Processing personal data needs to be based on one or several lawful processing conditions (see below). The Data Subject should have full and transparent knowledge of the identity of the parties to the processing, the purposes of the

processing, the recipients of personal data, the existence of Data Subject rights and freedoms, and how to contact the Controller.

2. Specified and Lawful Purpose
Personal data must be processed only on the basis of one or several specified purposes. Organisations should not collect any piece of data that does not fit the collection purpose.

3. Minimisation of Processing
Processing of personal data should be adequate, relevant and restricted to what is necessary. Not only will this relieve the organisation of the burden of performing actions on personal data, which are not required or necessary, but it will also reduce the overall risk of data breaches. Businesses collect and compile data for various reasons such as understanding behaviour and patterns. Based on this principle an organisation must ensure they are only collecting the minimum amount of data required for their purpose.

4. Accuracy
Personal data shall be accurate, kept up to date and fit for purpose. Organisations should rectify any incorrect data and erase any data, which is known to be erroneous or obsolete.

5. Storage Limitation or Retention
Personal data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. Anonymisation or deletion is encouraged in order to minimise the length of time that personal data is held by the organisation. Some identifiable data may be kept for statistical, scientific or historical research purposes. It may also be in the public interest to keep such data. This includes implementing and enforcing data retention policies and not allowing data to be saved in multiple locations. Users should not save data to local devices or move data to an external device. Having multiple copies of the same data significantly reduces the organisations ability to comply with GDPR.

6. Security and Confidentiality
Appropriate technical and organisational measures should be implemented to ensure a level of security appropriate to the volume and format of the data, its sensitivity, and the risks associated with it. Technical measures such as password protection on files and encryption should be used as necessary.

7. Liability and Accountability
The Data Controller and the Data Processor will be required to demonstrate their compliance with the GDPR. GDPR requires that organisation respond to data requests from data subjects regarding what data is available about them. An organisation must be able to promptly correct or erase that data if desired (the ‘right to be forgotten’). Organisations not only need to have a process in place to manage the request but also need to have a full audit trail to support data requests.

What is the role of the Data Protection Commissioner?
The Data Protection Commissioner aims to make sure that your rights are being upheld and that data controllers respect data protection rules. If you think that an organisation or person is breaking these rules and you are not satisfied with their response to your concerns, you can complain to the Commissioner.

Accessing Your Personal Information - How can I see what information a body or company holds about me?
Under Section 3 of the Data Protection Acts, you have a right to find out, free of charge, if a person (an individual or an organisation) holds information about you. You also have a right to be given a description of the information and to be told the purpose(s) for holding your information.

You must make the request in writing. The person must send you the information within 21 days.

Under Section 4 of the Data Protection Acts, 1988 and 2003, you have a right to obtain a copy, clearly explained, of any information relating to you kept on computer or in a structured manual filing system or intended for such a system by any entity or organisation. All you need to do is write to the organisation or entity concerned and ask for it under the Data Protection Acts.

Your request could read as follows:

Dear ...
I wish to make an access request under Section 4 of the Data Protection Acts 1988 and 2003 for a copy of any information you keep about me, on computer or in manual form in relation to.... (Fill in as much information as possible to assist the organisations to locate the data that you are interested in accessing e.g. customer account number, staff number, or PPS number (if you are writing to a public sector organisation such as the Revenue Commissioners or the Department of Social Protection)).

You should also include any additional details that would help to locate your information - for example, a customer account number or staff number. You may be asked for evidence of your identity. This is to make sure that personal information is not given to the wrong person. When requesting some types of record, such as credit history or Garda records, it may also be useful to provide a list of previous addresses, previous names and your date of birth. You may be asked to pay a fee, but this cannot exceed €6.35.

Once you have made your request, and paid any appropriate fee, you must be given the information within 40 days (most organisations manage to reply much sooner).

Right to object
A data controller may intend to use your details for official purposes, in the public interest or for their own interests. If you feel that doing so could cause you unnecessary damage or distress, you may ask the data controller not to use your personal details.

This right does not apply if:

- you have already agreed that the data controller can use your details;
- a data controller needs your details under the terms of a contract to which you have agreed;
- election candidates or political parties need your details for electoral purposes; or
- a data controller needs your details for legal reasons.

You can also object to use of your personal details for direct marketing purposes if these details are taken from the electoral register or from information made public by law, such as a shareholders' register. There is no charge for objecting.

Right to freedom from automated decision making
Generally, important decisions about you based on your personal details should have a human input and must not be automatically generated by a computer, unless you agree to this. For example, such decisions may be about your work performance, creditworthiness or reliability.

Right to refuse direct marketing calls or mail
If you do not want to receive direct marketing telephone calls, you should contact your service provider. They will make a note of your request in the National Directory Database (NDD) 'opt-out' register. It is an offence to make direct marketing calls to any phone number listed in the NDD. If you have not included your phone number in this register, you can also refuse such calls by simply asking the caller not to phone you again.

An organisation must get your permission before they contact you by fax machine or automated dialling for direct marketing purposes.

An organisation must also get your permission before they send marketing emails to your computer or before they send marketing text messages to your mobile phone.

How do I make a complaint to the Commissioner?
To make a complaint, simply write to or email the Data Protection Commissioner explaining your case. In your letter or email, you should:

- name the organisation or person you are complaining about;
- describe the steps you have taken to have your concerns dealt with;
- give details of any response which you have received; and
- provide copies of any letters or emails exchanged between you and the organisation or person.

The Commissioner will investigate your complaint and try to resolve the matter in the best way possible. If this is not possible, you may ask the Commissioner to make a formal decision on whether the data controller has violated your rights. However, the Commissioner cannot award you compensation. If the Commissioner agrees with your complaint, he will try to make sure that the data controller obeys the law and puts matters right. If the Commissioner rejects your complaint, he will let you know in writing. If you are not happy with the Commissioner's decision, you can appeal the decision in the Circuit Court.

When should I contact the Data Protection Commissioner?
If you are not happy with how your details are being used, you should contact the organisation in question. If you believe that the organisation or individual is still not

respecting your data protection rights, you should contact the Office of the Data Protection Commissioner to ask for help. www.dataprotection.ie