Public: Privacy Policy

Policy Name:	GDPR Privacy Policy
Policy No:	MHC-GDPR-04
Division (if applicable):	Corporate Operations - GDPR
File location:	CorporateServices/GDPR/Policies-MasterCopies/MHC-GDPR-04PrivacyPolicyAll
Date Implemented:	May 2018
Policy Updated:	8 October 2019
Revision Date:	8 October 2020
Policy Owner:	Information Governance Unit
Approved by MHC:	Version 2: Approved by SMT 8 October 2019

CONTENTS

PRIVACY POLICY

1. What does this Privacy Policy cover?

This Privacy Policy explains how the Mental Health Commission ('we', 'us' or the MHC) use Personal Data which we collect about individuals. The MHC is an independent body established under the *Mental Health Act, 2001* (the 2001 Act). The MHC's functions under the 2001 Act are to promote, encourage and foster high standards and good practices in the delivery of mental health services and to protect the interests of people who are detained in approved centres pursuant to the 2001 Act and regulations made thereunder and any other legislation relating to the performance of these functions (Mental Health Legislation).

In December 2015, the *Assisted Decision Making Capacity Act, 2015* (the 2015 Act) was passed. This resulted in the establishment of the Office of the Decision Support Services (DSS). This Privacy Policy will be updated in due course with details of how the DSS processes Personal Data.

Personal Data is defined as information about living individuals. We use the words 'Personal Data' to describe information that is about you or another, and from which you or they are identifiable.

Special Categories of Personal Data refers to Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning an individual's sex life or sexual orientation. The MHC routinely processes Personal Data relating to physical or mental health but, from time to time, other Special Categories of Personal Data may be processed, as explained in this Privacy Policy. We may also process data relating to criminal offences and convictions as set out in this Privacy Policy.

Our aim is responsible handling of Personal Data and this Privacy Policy describes how we use Personal Data that we collect as part of our functions. This Privacy Policy may be supplemented by other privacy notices tailored to our specific relationships with you. This is to make sure you have a full picture of how we collect and use your Personal Data.

The Personal Data we may hold about you and other individuals may differ depending on the function(s) carried out. Personal Data provided by you, or in relation to you, by way of the MHC's statutory forms and/or other forms required by the MHC must be provided as they relate to a statutory requirement under the Mental Health Legislation. Such information is necessary for the performance of our functions or we otherwise require such Personal Data for the purposes of entering into, or performing a contract, with you.

In the event that you engage with our Corporate Operations as a supplier or are applying for a position with the MHC, you must provide certain Personal Data, as outlined below, for contractual purposes. Panel Members must provide Personal Data requested by the MHC for both statutory and contractual purposes, further details of which are set out in our Privacy Policy for Panel Members. Failure to furnish any of this Personal Data may result in the MHC being unable to engage further with you.

The MHC is comprised of the following departments:

Office of the Inspector of Mental Health Services (the Inspectorate team)

Standards and Quality Assurance (the S&QA team)

Mental Health Tribunals team (that constitute and support the operation of a Mental Health Tribunal)

Corporate Operations of the MHC

Decision Support Service (DSS)

2. Office of the Inspector of Mental Health Services

2.1 Functions

The functions of the Office of the Inspector of Mental Health Services (the Inspectorate team) are set out in Section 51(2) of the *Mental Health Act, 2001*.[1] These functions enable the Inspectorate team to examine and take copies of, or extracts from, any record or other document on any Approved Centre (i.e. a hospital or other in-patient facility for the care and treatment of persons suffering from mental illness or a mental disorder) or any other premises where mental health services are being provided (Mental Health Services). The Inspectorate team may also require the production or provision of information from persons in such Mental Health Services. Certain records or information may include Personal Data and the obtaining of such Personal Data is in accordance with data protection legislation.[2]

2.2 Categories of Personal Data

The categories of Personal Data examined (processed) by the Inspectorate team include the following:

Resident Data

(a) Extracts from a resident's files and medication records copied as evidence of compliance with Mental Health legislation, relevant rules, regulations or codes of practice which are identified in the course of an inspection. The resident's name is redacted from these copies before they are uploaded to the MHC file for the applicable Mental Health Services. In order to maintain an audit trail, the resident's initials and date of birth or medical record number (MRN) are not redacted to enable the Inspectorate team to follow up. Copies of documents that contain the resident's name are not retained by the team.

(b) Mental Health Services are requested to redact any records that are sent directly by such a centre to the MHC Inspectorate in line with the above protocol.

(c) Notes from interviews conducted with residents in the course of an inspection – only the Mental Health Service's resident IDs and date of birth (or the MRN) is recorded on the interview notes.

---

[1] For further information on these functions, please see **http://www.mhcirl.ie/Inspectorate_of_Mental_Health_Services/**

[2] See, for example, Data Protection Act, 2018 and General Data Protection Regulation, 2018.

Personnel Data

(a) Notes from interviews with staff in the course of an inspection (e.g. to confirm whether they have received the requisite level of training);

(b) Training records of staff members; and

(c) Garda vetting records.

Other

From time to time, the Inspectorate team may also receive Personal Data in the context of receiving a protected disclosure during the course of an inspection.

Members of the public or those who are treated or work in a Mental Health Service, their representatives or members of advocacy groups may contact the Inspectorate team directly by phone, letter or email in the event they wish to submit an issue of concern relating to a Mental Health Service. Please see Section 5 below in the context of a protected disclosure

The MHC does not record phone calls but notes of the call or a copy of the relevant correspondence will be retained on the file for the relevant Mental Health Service. This may contain the name and contact details and other Personal Data of a service user, a member of staff of a service or that of a third party depending on the nature of the communication.

The Child and Family Agency (Tusla), the Health Information and Quality Authority (HIQA) or other regulatory body may refer matters (including Personal Data) to the MHC for consideration and action (if this also comes within the remit of the MHC).[3]

2.3 **How does the Inspectorate Team use Personal Data and how is it shared?**

The Inspectorate team will use Personal Data to assist them in determining compliance by an Approved Centre with the applicable Mental Health Legislation, the rules, regulations and codes of practice and to assess the quality of care and treatment of residents in Mental Health Services (in so far as same are relevant). No Personal Data is included in the reports that are compiled by the Inspectorate team for these Mental Health Services.

The Standards and Quality Assurance team (S&QA) in the MHC has access to the data (including the clinical and/or Personal Data) held by the Inspectorate team for the Mental Health Services and, where relevant, use this data to follow up on incidents of non-compliance, for ongoing monitoring and for registration decisions for Approved Centres.

[3] There is a Memorandum of Understanding (MOU) between HIQA and the MHC. This will be updated to ensure any disclosure of personal data (where necessary) is compliant with data protection legislation as regards disclosing only personal data that is necessary and thereafter ensuring it is sent securely and only to the appropriate recipient within the MHC (not to a general email address).

The Inspectorate team may identify serious matters of non-compliance which will be referred to the Senior Management Team in the MHC for a decision as to whether to refer the matter to the relevant regulatory body for the applicable healthcare professional/s (e.g. Medical Council, etc.). This may require the disclosure of Personal Data, where necessary.

2.4 **How long does the Inspectorate team retain Personal Data?**

The current policy of the MHC is to retain copies of records relating to inspections for six years (two registration cycles) and during the following seventh year arrangements will be made to confidentially shred and/or delete all relevant materials containing Personal Data (to the extent technically feasible).

3. Standards and Quality Assurance

3.1 Function

The Standards and Quality Assurance team (S&QA) function is part of the regulatory function of the MHC. It is responsible for registering Approved Centres, developing and monitoring compliance with regulations, rules and codes of practice and enforcement where there is non-compliance. The S&QA team works in collaboration with the Inspectorate in reviewing other Mental Health Services. The Director of S&QA may, pursuant to Part 5 of the 2001 Act, requires applicants for registration of an Approved Centre or a registered proprietor of an Approved Centre to furnish the MHC with such information as the MHC considers necessary for the purpose of its functions under the Mental Health Legislation. This may include Personal Data (please see 3.2 below for details).

3.2 **Categories of Personal Data**

The categories of Personal Data processed by the S&A team include the following:

(a) Personal Data contained in notifications from Approved Centres in relation to the quality and safety of services (e.g. child admission, restrictive practices). The S&QA team will receive Approved Centre resident IDs, dates of birth, gender, legal status, diagnosis and a brief description of medical treatments and interventions for residents (or medical reference number (MRN));

(b) Name, address, contact details and employment status of the registered proprietor;

(c) Name, Medical Council reference number (where applicable) and contact details for the Clinical Director and the Senior Management Team of an Approved Centre;

(d) Details of the resident profile of a facility to determine whether the facility is operating as an Approved Centre, resident IDs, initials of the resident's names and date of birth, diagnoses and name of treating consultant;

(e) Name and contact details of members of the public who may wish to make submissions on consultations (e.g. guidance documents, frameworks, rules and codes of practice, etc.);

(f) On an ongoing basis, the S&QA team conducts monitoring and enforcement of rules, regulations and codes of practice. In order to perform its functions, and follow up on issues of concern, the S&QA team may require Approved Centres to furnish the MHC with extracts from the relevant resident's clinical file and/or care plan to ensure that the rights and needs of the resident are being appropriately addressed. Approved Centres are requested to redact the relevant residents' names from any records furnished by the Approved Centre to the S&QA team leaving only the Approved Centre resident's IDs, initials of the resident's names and date of birth (or MRN).

3.3 **How does the S&A team use Personal Data and how is it shared?**

When the S&QA team processes Personal Data, it can do so for the following purposes:

(a) To inform the registration process for Approved Centres;

(b) To monitor compliance and conduct enforcement;

(c) To develop a 'risk profile' for Approved Centres;

(d) To investigate issues of serious concerns (including those raised by the Inspectorate team);

(e) To refer any safety or compliance concerns around the care and treatment of a resident to the Inspectorate team if an inspection is deemed necessary;

(f) Reporting on quality and safety notifications (including the use of electro-convulsive therapy, seclusion and restraints, deaths, child admissions, etc.);

(g) Conducting a census type survey on Approved Centres (e.g. to verify transfers and patients on section 26 leave);

(h) To monitor individual cases of concern on care and treatment and monitoring the handling of incidents in Approved Centres (including incidents involving staff and/or other residents); and

(i) To inform improvements in future.

3.4 **How long does the S&QA team retain Personal Data?**

The current policy of the MHC is to retain copies of records relating to inspections for six years (two registration cycles) and during the following seventh year arrangements will be made to confidentially shred and/or delete all relevant materials containing Personal Data (to the extent technically feasible).

4. Mental Health Tribunals

4.1 Function

The MHC is responsible for constituting Mental Health Tribunals for patients of Approved Centres who have been involuntary detained, within 21 days of the detention.[4] [5] The MHC's role in constituting and supporting a Mental Health Tribunal requires that Personal Data is processed as follows:

4.2 Categories of Personal Data

(a) Personal Data contained in statutory forms which are completed in cases of involuntary detention, these contain details of:

(i) the patient's name, address, a brief description of his/her mental condition and whether the individual poses a risk to himself/herself or to others or otherwise, the purpose of the recommendation of the detention, date of birth or age and gender; [6]

(ii) name and contact details of the applicant and relationship or any connection with the patient; and

(iii) name and Medical Registration Number (MRN) of the General Practitioner and name and MRN of the Responsible Consultant Psychiatrist attending the patient.

(b) Personal Data of all five Panel Members (name, address, contact details (see also Section 4.1(c) in respect of Personal Data held by MHC Corporate Services);

(c) Personal Data of the legal representative and the independent consultant psychiatrist for the patient (see also Section 4.1(d) in respect of Personal Data held by MHC Corporate Services);

(d) Event notes of phone calls or copies of correspondence received from a patient or family member;

(e) The decision of the Mental Health Tribunal (i.e. whether or not the person is suffering from a mental health disorder together with the reasons and a full record of the proceedings of the Tribunal and any notes of the members);

(f) In a limited number of cases, the MHC may hold Personal Data relating to criminal offences (e.g. detailed patient assessments from the Central Mental Hospital);

---

[4] In section 3, the policy refers to patients rather than residents to comply with the provisions of the Mental Health Act 2001.

[5] For further information, please see http://www.mhcirl.ie/for_the_public/Mental_Health_Tribunals/.

[6] The statutory forms will be updated to remove the reference to PPS number in accordance with current practice. Currently, the PPS number is not filled in on the Forms.

(g) Apart from Personal Data relating to physical or mental health, other Special Categories of Personal Data or data relating to criminal offences or convictions may be contained in a report prepared by the independent consultant psychiatrist (see 4.3.(c) below) should he or she deem it relevant; and

(h) The MHC maintains a contact list (including names and contact numbers) for consultant psychiatrists and Mental Health Administrators in Approved Centres, compiled from the MHC's own records or from Approved Centres for the MHC's own internal purposes.

4.3 **How does the MHC use Personal Data and how is it shared in the context of constituting and supporting a Mental Health Tribunal?**

(a) The MHC will convene a Tribunal which comprises of three members from the relevant panels, each of whom are contractually bound to comply with data protection and confidentiality obligations and who will have access to the relevant records received by the MHC in respect of the patient for the purpose of the Tribunal.

(b) The MHC will assign a legal representative to assist the patient and copies of the statutory forms containing the Personal Data set out above are shared with the legal representative.

(c) The MHC will also appoint an independent consultant psychiatrist to examine the condition of the patient and prepare a report for the Tribunal. The independent consultant psychiatrist's report is sent to the MHC and this report is forwarded to the legal representative, the Tribunal panel convened for that individual and the Mental Health Act administrator, the liaison person at the relevant Approved Centre (on behalf of the responsible consultant psychiatrist). It is important to note that the MHC does not have a copy of the medical chart for the patient but this is accessed by the independent consultant psychiatrist, the legal representative and the Tribunal Panel in the Approved Centre. Extracts from a medical file are only received by the MHC in exceptional circumstances where a specific concern has been raised or if there are legal proceedings.

(d) Access to Tribunal files is limited within the MHC to those staff members who work on the Tribunal team, members of the Corporate Services team who may require to assist with payments/payment queries and members of the Senior Management Team of the MHC who are consulted on specific matters (e.g. serious incident or data breach).

(e) Access by the five Panel Members as referred to above, Tribunal Members, the legal representative and the independent consultant psychiatrist are provided by way of a secure service (save in exceptional circumstances and in those cases by way of email with the relevant documents being password protected).

(f) Legal aid for Tribunals is automatically provided and the documentation forms part of the case file for each tribunal hearing.

Appeals to the Circuit Court

(i) In the event that a patient wishes to appeal a decision of the Mental Health Tribunal, the Notice of Appeal is filed in Court and the application for legal aid is made to the Chief Executive Officer (CEO) of the MHC.

(ii) In the event of an appeal, the file containing the statutory forms, the independent consultant psychiatrist report, the decision of the Tribunal, any transfer orders in respect of a transfer to another Approved Centre and any relevant correspondence that was considered by the Tribunal is forwarded to the MHC's legal advisors in a secure manner;

(iii) The name, contact number and email address of the patient's Responsible consultant psychiatrist and contact details of the patient's legal representative is also furnished to the MHC legal team.

4.4 How long does the MHC retain copies of Tribunal files?

The retention of Tribunal files is addressed in the MHC's retention policy and will be for a maximum of 8 years from the date the last case was closed by the tribunal team. [7]

5. MHC Corporate Services

The Corporate Services team supports the functions of the MHC in relation to Finance, IT, HR and other matters including general statutory compliance matters related to its functions.

5.1 Categories of Personal Data

The categories of Personal Data processed by the Corporate Services team include:

(a) Personal Data of employees;

(b) Personal Data of candidates for employment including name, address, contact details, professional qualifications and educational background, work experience, references and any other information furnished by the candidate to the MHC;

(c) Personal Data of members of the Mental Health Tribunal panel, including name, contact details, professional qualifications, work experience (where relevant), character references, PPSN, results of Garda vetting;

[7] A 'case' is created on receipt of an admission order or a renewal order (or proposal to transfer to the Central Mental Hospital or proposal to perform psychosurgery). That case is closed once the Tribunal has reviewed the order or, where applicable, the order has been revoked and the time period for the patient to seek a review of the revoked order has expired.

(d) Personal Data of legal representatives on the Mental Health Tribunal panel, professional qualifications, practising certificate, confirmation of professional indemnity insurance and copy of tax clearance certificates;

(e) Names and contact details of contact persons within supplier organisations or contract workers, PPSN for individual suppliers;

(f) Personal Data of persons who contact the MHC with queries with respect to, for example, Freedom of Information and data protection;

(g) Details of car insurance for processing mileage expense claims; and

(h) Bank details for processing all payments.

5.2 **How does the MHC Corporate Services use Personal Data and how is it shared?**

The MHC Corporate Services team processes Personal Data for the following purposes:

(a) Hiring of staff members and administering employment and benefits;

(b) Services required to appoint persons to the panel of Tribunal members including Garda vetting and processing expense claims;

(c) Processing expense claims to legal representatives and witnesses in court proceedings;

(d) Dealing with supplier organisations which provide services to the MHC;

(e) Dealing with queries from government authorities such as the Revenue Commissioners and Department of Social Protection; and

(f) Electronically stored Personal Data is transferred to, or is otherwise accessible by our IT service providers and hard copy data are secured and tagged before it is transferred offsite to our storage providers.

5.3 **How long does MHC Corporate Services retain copies of Personal Data?**

MHC Corporate Services generally retain Personal Data for 7 years after termination of the MHC's contractual relationships with the categories of individuals referred to above. More detailed information on the retention periods can be found in the MHC's Data Retention Policy. Personal Data may be retained for a longer period where required in the context of an ongoing legal claim or legal proceedings.

6. **Protected Disclosures**

6.1 The Director of Standards and Quality Assurance or the Inspector of Mental Health Services are the persons designated to receive protected disclosures pursuant to Part 9A of the Health Act 2004 (as inserted by the Health Act, 2007 and amended by the

Protected Disclosures Act 2014) and the CEO of the MHC is responsible for receiving protected disclosures under the Protected Disclosure Act, 2014.[8]

6.2 In the normal course, protected disclosures do not contain Personal Data and we ask that persons making a protected disclosure confine the disclosure to the relevant issue and to not disclose any Personal Data unless expressly requested by the Director of S&QA, the Inspectorate or the CE (as relevant) to do so. In the event that Personal Data is disclosed in the context of a protected disclosure, this shall be processed by the Director/Inspector/CE for the purposes of complying with the legal obligations associated with the receipt of the protected disclosure, performance of statutory functions (including the regulatory function) and shall be retained for 7 years after the completion of the relevant investigation, unless it is required to be retained for longer in the context of a legal claim or proceedings.

7. Legal justification for our use of Personal Data

To comply with the law, we need to tell you the legal justification we rely on for using your Personal Data for our purposes.

First, the MHC has a statutory function under section 33 of the 2001 Act 'to promote, encourage and foster the establishment and maintenance of high standards and good practices in the delivery of mental health services and to take all reasonable steps to protect the interests of persons detained in approved centres.' The powers and obligations of the MHC under Mental Health Legislation have been explained in the relevant sections of this Privacy Policy and are required for the performance of our statutory functions.

While the law provides several legal justifications, this section describes the main legal justifications that apply to our purposes for using Personal Data:

7.1 Justification for processing Personal Data

(a) Compliance with our legal obligations (as set out in the Mental Health Legislation or other applicable legislation, court orders or Ministerial orders to which we may be subject or ministerial orders);

(b) Performance of tasks carried out in the public interest or in the exercise of official authority (whether by reference to our statutory functions); and

(c) Where necessary for the performance of a contract with you or for taking steps prior to entering into a contract with you (e.g. suppliers or candidates for employment).

7.2 Special Categories of Personal Data

We only process Special Categories of Personal Data in the context of performing our functions by reference to the following legal grounds:

[8] For further information on protected disclosures, please see http://www.mhcirl.ie/for_H_Prof/Protected_Disclosures/

(a) where necessary and proportionate for the performance our functions, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of individuals;

(b) to protect the vital interests of the resident in question or of another individual;

(c) where necessary for the purpose of providing or obtaining legal advice or for the purposes of, or in connection with, the establishment, exercise or defence of legal claims, prospective legal claims, legal proceedings or prospective legal proceedings or whenever courts are acting in their judicial capacity. Such processing is also necessary in the context of constituting a Mental Health Tribunal and dealing with any appeals to the Circuit Court);

(d) where necessary for the purposes of establishing, exercising or defending legal rights; and

(e) processing is necessary for reasons of public interest in the areas of public health on the basis of our statutory functions including ensuring high standards of quality and safety of health care in mental health facilities.

8. **Criminal Data**

Processing of Personal Data relating to criminal convictions and offences or related security measures shall be carried out only in the context of the MHC performing its functions and when the processing is authorised by EU or Irish law providing for appropriate safeguards for the rights and freedoms of data subjects. Such data may be processed by the MHC in the context of conducting Garda vetting or in the course of the MHC processing and storing Personal Data on behalf of a Mental Health Tribunal or Inspectorate (e.g. when such data are included by a consultant psychiatrist in a report to a Mental Health Tribunal or an extract taken by the Inspectorate Team from a resident's file). Such processing may be carried out where necessary for the purpose of: (a) providing or obtaining legal advice or for the purposes of, or in connection with, the establishment, exercise or defence of legal claims, prospective legal claims, legal proceedings or prospective legal proceedings; and (b) in the exercise of our official authority in the context of a Mental Health Tribunal hearing (where applicable) or the exercise of our regulatory functions.

9. **Security of Personal Data**

The MHC uses appropriate technical, legal and organisational measures, which comply with data protection laws to keep Personal Data secure.

As most of the Personal Data we hold is stored electronically we have appropriate IT security measures to ensure this Personal Data is kept secure. For example, we may use anti-virus protection systems, firewalls, secure messaging services for transmission of certain files in the context of Tribunals and, where appropriate, data encryption technologies. We do not transfer Personal Data outside the European Union. We have procedures in place to keep any hard copy records physically secure. We also train our staff on data protection and information security.

When MHC provides Personal Data to a third party (including our service providers or to Tribunal panel members and other relevant parties in the context of a Mental Health Tribunal)

or engages a third party to collect Personal Data on our behalf, the third party will be required to use appropriate security measures to protect the confidentiality and security of Personal Data and will assume certain responsibilities under data protection law for looking after the Personal Data that they receive from us.

Unfortunately, no data transmission over the Internet or electronic data storage system can be guaranteed to be completely secure. If you have reason to believe that your interaction with us is no longer secure (e.g. if you feel that the security of any Personal Data you might have sent to us has been compromised), please notify us immediately.

10. **Retention of Personal Data**

We will keep Personal Data for as long as is necessary for the purposes for which we collect it or by reference to any statutory obligation to retain Personal Data in specific circumstances. Please see Sections 1.4, 2.3, 3.3, 4.3 and 5 of this Privacy Policy for further guidance on our retention periods.

In all cases, Personal Data may be retained for a longer period where required in the context of an ongoing legal claim or legal proceedings.

11. **Personal Data Rights?**

The following is a summary of the data protection rights available to individuals in connection with his/her Personal Data. These rights may only apply in certain circumstances and are subject to certain legal exemptions set out in data protection legislation.

Description	When is this right applicable?
Right of access to Personal Data You have the right to receive a copy of the Personal Data we hold about you and information about how we use it.	This right is applicable at all times when we hold your Personal Data (subject to certain exemptions).
Right to rectification of Personal Data You have the right to ask us to correct Personal Data we hold about you where it is incorrect or incomplete.	This right is applicable at all times when we hold your Personal Data (subject to certain exemptions).
Right to erasure of Personal Data This right entitles you to request that your Personal Data be deleted or removed from our systems and records. However, this right only applies in certain circumstances.	Examples of when this right applies to Personal Data we hold include (subject to certain exemptions): • when we no longer need the Personal Data for the purpose we collected it; • if you withdraw consent to our use of your information (in circumstances where we have sought consent) and no other legal justification supports our continued use of your information;

	• if we have used your Personal Data unlawfully; and • if the Personal Data needs to be erased for compliance with law.
Right to restrict processing of Personal Data You have the right to request that we suspend our use of your Personal Data. Where we suspend our use of your Personal Data, we will still be permitted to store your Personal Data, but any other use of this information will require your consent, subject to certain exemptions.	You can exercise this right if: • you think that the Personal Data we hold about you is not accurate but this only applies for a period of time that allows us to consider if your Personal Data is in fact inaccurate; • the processing is unlawful and you oppose the erasure of your Personal Data and request the restriction of its use instead; • we no longer need the Personal Data for the purposes we have used it to date but the Personal Data is required by you in connection with legal claims.
Right to object to processing of Personal Data You have the right to object to our use of your Personal Data for the performance of our statutory functions where your objection is based on grounds particular to your situation. However, we may continue to use your Personal Data, despite your objection, where we can demonstrate compelling legitimate grounds for the processing which override your objection or where need to use your Personal Data in connection with any legal claims.	
Right to withdraw consent to processing of Personal Data Where we have relied upon your consent to process your Personal Data, you have the right to withdraw that consent.	This right only applies where we process Personal Data based upon your consent.
Right to complain to the relevant data protection authority If you think that we have processed your Personal Data in a manner that is not in accordance with data protection law, you can make a complaint to the data protection authority. If you live or work in an EEA member state, you may complain to the data protection authority in that state.	This right applies at any time.

If you wish to exercise your rights, please contact us using the details below.

12. Who to contact about your Personal Data

If you have any questions or concerns about the way your Personal Data is used by us, you can contact us by e-mail at: dpfoi@mhcirl.ie.

This Privacy Policy was created in May 2018. We review this Privacy Policy regularly and reserve the right to make changes at any time to take account of changes in our functions, legal requirements, and the manner in which we process Personal Data.