Public: Privacy Policy

Policy Name:	GDPR Privacy Policy
Policy No:	MHC-GDPR-04
Division (if applicable):	Corporate Operations – Information Governance Unit
File location:	Corporate Operations - 2022 Version - Checked out to (sharepoint.com)
Date Implemented:	May 2018
Policy Updated:	28 February 2023
Revision Date:	As required but at least every two years
Policy Owner:	Information Governance Unit
Approved by MHC:	16 March 2023

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. The 2015 Act established the Decision Support Services (DSS). The DSS is part of the MHC but has a new and separate role. The duties of the DSS include, but are not limited to, the registration and supervision of decision support arrangements, to maintain a panel of experts who will act as decision-making representatives, special and general visitors, and to investigate complaints made under the 2015 Act.

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 and Assisted Decision-Making Capacity 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

2.1.1 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 registered with the MHC 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]

2.2.1 Categories of Personal Data

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

Resident Data

1. 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.

[1] For further information on these functions, please see Office of Inspector of Mental Health Services | Mental Health Commission (mhcirl.ie)

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

2. 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.

3. 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.

Personnel Data

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

2. Training records of staff members; and

3. Garda vetting records.

Other

From time to time, the Inspectorate team may also receive Personal Data in the context of a protected disclosure received by the MHC.

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 7 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]

2.3.1 **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). The Inspectorate Team may also use Personal Data to assist them in their inspection of mental health services which are not approved centres as deemed appropriate under

[3] Existing Memoranda of Understanding and Data Sharing Agreements are published on the MHC website, see: https://www.mhcirl.ie/freedom-information-publication-scheme/service-level-agreements-and-memoranda-understanding

Section 51(1)(a) of the Mental Health Act 2001. 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.

The Inspectorate team may identify serious matters of non-compliance which will be referred to the Senior Leadership 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.

2.4.1 **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). Certain records such as those pertaining Reports are kept on a permanent basis.

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, require 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).

3.2.1 Categories of Personal Data

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

1. 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));

2. Name, address, contact details and employment status of the registered proprietor;

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

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

5. 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.);

6. 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 and date of birth (or MRN).

3.3.1 How does the S&QA 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:

1. To inform the registration process for Approved Centres;

2. To monitor compliance and conduct enforcement;

3. To develop a 'risk profile' for Approved Centres;

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

5. 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;

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

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

8. 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

9. To inform improvements in future.

3.4.1 **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). Certain records such as those pertaining to Statutory Notifications, Reports and Statistics are kept on a permanent basis.

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:

4.2.1 Categories of Personal Data

1. Personal Data contained in statutory forms which are completed in cases of involuntary detention, these contain some or all of the following details:

   (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.

2. Personal Data of all five Panel Members (name, address, contact details) (see also Section 5.1.3 in respect of Personal Data held by MHC Corporate Operations);

3. Personal Data of the legal representative and the independent consultant psychiatrist for the patient (see also Section 5.1.4 in respect of Personal Data held by MHC Corporate Operations);

4. Event notes of phone calls or copies of correspondence received from a patient or family member;

5. 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);

6. 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 have been updated to remove the reference to PPS number in accordance with current practice. Currently, the PPS number is not filled in on the Forms.

7. 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

8. 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.

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

1. 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.

2. 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.

3. 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).

4. During Covid 19, Mental Health Tribunals had to be held remotely. As a result of this the patient medical file for each Hearing, which was previously only available to the Panel Members, Independent Consultant Psychiatrists and Legal Representatives as a physical file at the Approved Centre, was scanned and sent by the Approved Centre to the MHC via CIS. The MHC then made the file available via CIS to the Panel Members, Legal Representative, and Independent Consultant Psychiatrist. This practice continues to be the case. Patient records are scanned by the staff of the approved centre the afternoon before a hearing is due to take place and sent to the MHC via CIS. The MHC then sends the Patient File to the Tribunal Panel Members and the Legal Representative. The Tribunal Members and the Legal Representative are also entitled to view the original chart on the day of the hearing. If an order is revoked before the date of the hearing a patient file is not required. Should a patient wish to exercise their right under s28 of the Mental Health Act to proceed with a Mental Health Tribunal despite the order having been revoked, a patient file is requested as per normal procedure. Certain measures have been put in place to ensure that confidentiality is maintained, and that data protection requirements are met. All documents labelled as "Patient Records" are automatically deleted from CIS one day after a hearing to which the document is attached has been closed.

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

6. 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).

7. 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 or reports that were 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 or their secretary and contact details of the patient's legal representative is also furnished to the MHC legal team.

4.4.1 **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]

Notwithstanding the above, when a patient's medical file is received as per circumstances outlined in 4.3 (c) above the medical file is permanently deleted from CIS 1 day after the closure of the associated case.

[7] A 'case' is created on receipt of an admission order, a renewal order or an additional review of a renewal order that shall not exceed 6 months (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 under s28 of the Mental Health Act 2001 has expired.

5. MHC Corporate Operations

The Corporate Operations 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.

5.1.1 Categories of Personal Data

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

1. Personal Data of employees;
2. 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;
3. Personal Data of members of the Mental Health Tribunal and Decision Support Service panels, including name, contact details, professional qualifications, work experience (where relevant), character references, PPSN, results of Garda vetting;
4. 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;
5. Names and contact details of contact persons within supplier organisations or contract workers, PPSN for individual suppliers;
6. Personal Data of persons who contact the MHC with queries with respect to, for example, Freedom of Information and data protection;
7. Details relating to the vehicle and journeys undertaken by panel members for processing mileage expense claims; and
8. Bank details for processing all payments.

5.2.1 How does the MHC Corporate Operations use Personal Data and how is it shared?

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

1. Hiring of staff members and administering employment and benefits;
2. Services required to appoint persons to the panel of Mental Health Tribunals or the Decision Support Services including Garda vetting and processing expense claims;
3. Processing expense claims to legal representatives and witnesses in court proceedings;
4. Dealing with supplier organisations which provide services to the MHC;
5. Dealing with queries from government authorities such as the Revenue Commissioners and Department of Social Protection; and

6. 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.

5.3.1 **How long does MHC Corporate Operations retain copies of Personal Data?**

MHC Corporate Operations 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. Decision Support Services

The Decision Support Service was founded under *Assisted Decision Making Capacity Act,* 2015. Its primary goal is to promote the rights and interests of people who may need support with decision-making.

6.1 Categories of Personal Data

The categories of Personal Data processed by the Decision Support Services include:

1. Full name, Date of birth, Residential address, Postal address (if different), Phone number, Alternative contact number, Email address, PPSN, Gender, Ethnicity for Relevant Person and Supporter

2. Marital status, Relevant condition/impairment, Communication needs/accessibility needs, Medical card, Healthcare instructions, Employment status, Assets details, Healthcare instructions for the Relevant Person.

3. Full name, email address, Relationship to the Relevant Person for the supporter and Witness / Notice Party

4. Where such matters require the request for Decision Making Representative then the following data is provided to the Courts Service:

    (a) Mandatory: Case Reference, Name of Person who requires DMR or Court Friend

    (b) Optional: Address, DOB, Special Needs of Person who requires DMR or Court Friend

5. Full name, Residential address, Postal address (if different), Phone number, , Email address and Professional Registration Documents for Panel members such as Special and General Visitors (The Court Friends panel has yet to commence at the time of writing),

6. The Decision Support Services will process complaints received under the Assisted Decision Making (Capacity) Act 2015. The complaints will contain the identifiers of the complainant and any other information the complainant deems relevant.

7. Persons who wish to review the register of Co- Decision-Making Arrangements, Decision Making Representation Orders, or Enduring Powers must apply to do so with the Director of the Decision Support Services. They will be asked to provide personal details that would allow the Director of the Decision Support Services to verify their identity and that they meet the requirements of "Legitimate Interest"[8] as per the Legitimate Interest Policy.

8. Professionals making capacity statements will be asked to provide Identifiers, professional registration documents, and credentials. (For example. General Practitioners or Social Workers).

9. During the course of investigation, the Decision Support Services may encounter data from anyone that is relevant to that investigation.

Where such matters are appealed to the court the MHC will store appeal documentation and outcomes as per the "Legal" section of the Data Retention Policy.

6.2.1 **How does the Decision Support Services use Personal Data and how is it shared?**

The DSS team processes Personal Data for the following purposes:

1. To set up DSS Accounts and, if the person has a PPSN, verify same with MyGovID.

2. To provide information on decision support arrangements to persons entitled to receive them.

3. Data shared with 3rd party provider to process payment and payment waivers.

4. To process objections to decision support arrangements.

5. To consider reports provided from panel members.

6. To submit details to a relevant authority if there are sufficient grounds for concern. The matter may be referred to An Garda Siochana, the Courts Service or HSE Safeguarding and Protection Teams, whichever body is deemed most appropriate in relation to the concern and provided that appropriate safeguards for data transfers are in place

7. To facilitate the investigation and resolution of complaints. The matter may be referred to An Garda Siochana if the complaint relates to a criminal offence.

8. To facilitate the calling of relevant witnesses

9. To register a person or organisation as an "approved entity". This is prescribed by regulations made by the Minister.

[8] The term "Legitimate Interest" refers to Sections 25, 45 and 72 of the Assisted Decision-Making (Capacity) Act 2015 and not Article 6 Section 1(f) of the GDPR Regulations. All mentions of "Legitimate Interest" in this policy are the same.

10. To facilitate selection of appropriate panel members per case.

11. To facilitate a court request for a Decision-Making Representative or Court Friend.

12. To process applications by the public to view registrations as per the Legitimate Interest Policy. Applicants from outside Ireland may be registered as per the Legitimate Interest Policy as they cannot be an approved body.

13. Data may need to be transferred to bodies outside the EEA, in those instances the DSS shall rely on at least one of the appropriate safeguards set out in Articles 45 – 50 of the GDPR Regulations.

6.3.1 **How long does Decision Support Services retain copies of Personal Data?**

Depending on the Data Type the DSS may retain a document for anywhere between 12 months to 25 years. Some data is kept indefinitely (for example data pertaining to property that is likely to be under the ownership of the relevant person for the duration of their life).

7. Protected Disclosures

A protected disclosure is a disclosure of information by a worker which, in the reasonable belief of the worker, tends to show one or more relevant wrongdoings, which came to the attention of the worker in a work-related context and is disclosed in one of the ways prescribed in the 2014 Act.

The Mental Health Commission has two Protected Disclosure Policies. One of them refers to Internal Workers and is available here. The other policy refers to External Workers and is available here.

7.1 Internal Workers

7.1.1 The staff member responsible to receive protected disclosures is referred to as the "Designated Person" (DP) in the Protected Disclosures Policy. The DP may delegate any of their functions where appropriate. Disclosures in relation to the Senior Leadership Team should be made to the Chief Executive and disclosures relating to the Chief Executive should be made to the Chairperson of the Mental Health Commission.

The Protected Disclosures Act of 2014 allows a person to make Protected Disclosures to an external body in certain circumstances, these may be another responsible person, a prescribed person, the Protected Disclosures Commissioner, a Minister of Government or a legal adviser.

7.2.1 A persons can make a protected disclosure in writing or verbally. To submit a protected disclosure in writing they should use the form the link to which is embedded in section 9.1 of the Protected Disclosure Policy, or you can write to the DP directly at protecteddisclosures@mhcirl.ie. To make a verbal submission a person can contact the Mental Health Commission at 353(1) 636 2400. Their call may be recorded, or it may be transcribed to a written record which will be made available to the caller to

confirm that they agree that the record created reflects the call to which it refers. They should not disclose any additional Data unless expressly requested by the DP, the CE or Chairperson (as relevant) to do so.

7.3.1 In the event that Personal Data is disclosed in the context of a protected disclosure, this shall be processed by the DP 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)

7.4.1 In accordance with these provisions, the Commission may, in certain circumstances, refuse to provide certain personal data as part of a response to a data subject access request. These circumstances include where, if the personal data were provided, it would hinder making disclosures, or impede or frustrate follow-up or investigations, or would reveal the identity of the reporting person. Any person whose response to their data subject access request has been affected by this restriction may bring a complaint to the Data Protection Commissioner

7.5.1 Personal Data disclosed in the context of a Protected Disclosure shall be retained for 7 years unless it is required to be retained for longer in the context of a legal claim or proceedings.

7.2 External Workers

7.6.1 For the purposes of the 2014 Act, the Protected Disclosure (External Workers) policy applies to workers for whom the Commission is not the employer under the 2014 Act. Before making a disclosure or reporting a concern, the Commission generally encourages workers to use the internal mechanism for making protected disclosures provided for by their own organisation. However, it is recognised that circumstances may arise where a worker wishes to make a disclosure external to their own organisation without recourse to that organisation's internal procedures for making disclosures. In these circumstances the worker should contact the DP, the Inspector, or the Chief Executive, in accordance with the subject matter of the concern relevant to the 2004 Act as referred in section 4.1 of the Protected Disclosure (External Workers) policy.

7.7.1 A disclosure should ideally be in writing, preferably through completing the form the link to which is enclosed in section 4.2.1 of the Protected Disclosure Policy (External Workers) or via email to protecteddisclosures@mhcirl.ie . Disclosures will also be accepted orally and should include all relevant dates and other details necessary to enable a full and proper consideration and investigation of the disclosure.

8. 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.'

In addition, the remit of the MHC was extended by the Assisted Decision-Making (Capacity) Act 2015 to establish the function of the Decision Support Service (DSS). The role of the DSS is to register the new decision support arrangements and supervise the individuals who are providing a range of supports to people with capacity difficulties.

The powers and obligations of the MHC under Mental Health Legislation and Assisted Decision-Making 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:

8.1.1 **Justification for processing Personal Data**

1. Compliance with our legal obligations (as set out in the Mental Health Legislation, Assistant Decision-Making Legislation or other applicable legislation, circulars, court orders or Ministerial orders to which we may be subject or ministerial orders);

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

3. 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).

8.2.1 **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:

1. 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;

2. to protect the vital interests of the resident in question or of another individual;

3. 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);

4. where necessary for the purposes of establishing, exercising or defending legal rights; and

5. 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.

9. **Criminal Data**

Processing of Personal Data relating to criminal convictions and offences, or related security measures shall be carried out only in one of two contexts:

1. The Law Enforcement Directive and as per Part 5 of the Data Protection Act 2018 or,

2. Under GDPR - When the MHC is performing its functions and/or when the processing is authorised by EU or Irish law providing for appropriate safeguards for the rights and freedoms of data subjects.

The Mental Health Commission is a "competent authority" as defined under Section 69(1)(a) of the Data Protection Act 2018 which designates a competent authority as "a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security,"

The Mental Health Commission is a competent authority by virtue of the Mental Health Act 2001 which sets out several offences relating to approved centres which the Commission may decide to prosecute. Examples of this include (but are not limited to):

- Section 63 states that a person is guilty of an offense if they carry on a centre that is not registered as an "Approved Centre" or that the person in question is not the registered proprietor.

- Section 64(8)(b) states that under part (a) the Mental Health Commission may request from the applicant of the registration of an Approved Centre any information it deems necessary to allow it to carry out its functions under Section 64 and that it is an offense to furnish information to the MHC that is false or misleading unless the person submitting it can demonstrate that what they submitted was correct to the best of their knowledge.

- Section 64(13) states that a registered proprietor of an Approved Centre may be guilty of an offense if they contravene a condition attached to the registration of the Approved Centre.

In any of the above scenarios the LED may apply to data processing activities provided that:

1. The purposes of processing the data conform to Section 70(1)(a) of the Data Protection Act 2018, which is "the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or…the execution of criminal penalties,"

2. The processing activity occurs in the course of an activity that falls within the scope of the law of the European Union (as per Section 70(2) of the Data Protection Act 2018).

If the Law Enforcement Directive applies to a data processing activity the MHC should have regard to Article 10 of the Law Enforcement Directive which addresses the processing of Special Category data which includes, among other things, data concerning the health of the data subject. Special Category data is only to be processed under the Law Enforcement Directive where strictly necessary and subject to appropriate safeguards. In addition, processing is to be carried out provided one of the below applies:

(a) Where the processing is authorised by Union or Member State law;

(b) Processing is necessary to protect the vital interests of the data subject or of another natural person; or

(c) Where such processing relates to data which are manifestly made public by the data subject.

In addition to the above, the MHC will need to clearly distinguish between the following four data subjects and treat them separately.

1. Suspected Offenders,
2. Convicted Offenders,
3. Victims
4. Other witnesses.

Data Subject Rights "may be restricted, if proportionate and necessary, to

1. Avoid obstructing official or legal investigations or procedures
2. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
3. Protect public or national security
4. Protect the rights and freedoms of other persons."[9]

If the LED does not apply (i.e. – The purposes of processing the data does not conform to Section 70(1)(a) of the Data Protection Act 2018), then Data Processing may take place under GDPR. In that instance, 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 Tribunals, Decision Support Services or the 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), a Case under the Decision Support Service or the exercise of our regulatory functions.

[9] Source: https://www.citizensinformation.ie/en/government_in_ireland/data_protection/legislation_relating_to_the_general_data_protection_regulation.html

If the Mental Health Commission engages in the processing of personal data which falls under the scope of the Law Enforcement Directive, and where this processing is not occasional, this should be duly reflected in the Record of Processing Activities.

10. 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 have procedures in place to keep any hard copy records physically secure. We also train our staff on data protection and information security.

When the MHC provides Personal Data to a third party (including our service providers or to Panel Members assigned in the context of Mental Health Tribunal hearings or Decision Support Services cases) 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 the DPO at dpfoi@mhcirl.ie immediately.

11. Transfers of personal data outside of the European Economic Area

The MHC will not transfer the personal data of its data subjects outside of the European Economic Area unless there is a statutory, legal, or contractual basis for that transfer, or the consent of the data subject is provided for that transfer. In addition, unless there are adequate data protection measures in place for the data transfer as set out in the Data Protection Acts, the transfer will not take place. All such proposed transfers will be notified to the Information Governance Unit prior to the transfer of the data and such transfers are only permitted upon receipt of written approval from the Information Governance Unit and the Legal Department.

12. 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 2.4, 3.4, 4.4, 5.3 and 6.3 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.

13. 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 we 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 exclusively 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 exclusively 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.

14. 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.

We 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.