Panel Members: Privacy Policy

Policy Name:	GDPR Privacy Policy – Panel Members
Policy No:	MHC-GDPR-06
Division (if applicable):	Corporate Operations – Information Governance Unit
File location:	MHC - Data protection policies - All Documents (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 FOR PANEL MEMBERS

1. **What does this Privacy Policy cover?**

This Privacy Policy explains how the Mental Health Commission ("**we**", "**us**" or the "**MHC**") uses Personal Data which we collect about Panel Members for Mental Health Tribunals and the Decision Support Services.

Personal Data is information about living individuals.

We use the words Personal Data to describe information that is about you or another individual, and from which you or they are identifiable. Our aim is responsible handling of Personal Data and this Privacy Policy describes how we use Personal Data that we collect in the course of hiring Panel Members. This includes Personal Data obtained from a variety of sources including:

1.1. Panel Member applications online or on paper;

1.2. Panel Member files which will include details of education, employment history and professional qualifications;

1.3. Garda vetting database;

1.4. Protected disclosure under the Protected Disclosures Act 2014 or pursuant to the MHC Protected Disclosures Policy;

1.5. Current and/or previous employers and/or government department or agencies.

Personal Data may be provided to us by you directly or by a third party.

2. **Panel Members as data subjects**

All Panel Members are independent contractors of the MHC as follows:

<u>Mental Health Tribunals</u>:

(a) Solicitors – Legal Representatives;

(b) Solicitors / Barristers – Chairpersons of Tribunals;

(c) Consultant Psychiatrists – who sit on Tribunals;

(d) Members of the Public with an interest in mental health, known as 'Lay Members' – who sit on the tribunals; and

(e) Independent Consultant Psychiatrists who provide reports pursuant to Section 17 of the Mental Health Act 2001. These panel members do not sit on Tribunals.

Decision Support Services

(a) Decision Making Representative- Appointed by the Courts to a Relevant Person if the court decides that said person is unable to make certain decisions. The Courts will select a Decision-Making Representative from our panel only in the absence of a suitable candidate that is known and trusted by the Relevant Person under consideration.

(b) General Visitors – They may visit a Relevant Person and their Decision-Making Representative to ensure that an arrangement is working how it should. They are required to provide a report to the DSS after every visit.

(c) Special Visitors – They may visit a person and their Decision-Making Representative to assess the person's capacity to make certain decisions. They are required to provide a report to the DSS after every visit.

(d) Court Friend – Section 100 of the Assisted Decision-Making (Capacity) Act 2015 is the legal basis by which the Court Friend panel operates. Please note at the time of the drafting of this policy this panel was on hold. This policy will be updated once this panel has become active.

3. **How we use Personal Data**

We use Personal Data to carry out our statutory functions and administer the operation of the MHC on a day to day basis. These include:

1. Under section 33(1) of the Mental Health Act, 2001 (the "**Act**") the principal functions of the MHC are to promote, encourage and foster the establishment and maintenance of high standards in the delivery of mental health services and to take all reasonable steps to protect the interests of persons detained in approved centres under the Act.

2. Under section 48 of the Act, the MHC can establish Mental Health Tribunals (known as Tribunals) and such Tribunals shall determine matters referred to it pursuant to section 17 of the Act.

3. In December 2015, the MHC's remit was extended to include the establishment of the Decision Support Service (DSS) under the provisions of the Assisted Decision Making (Capacity) Act, 2015. Its core function is to support decision-making by and for adults with capacity difficulties.

We may use the Personal Data to:

3.1 Assess your application for appointment to a panel and, if successful, to enter into a contract with you;

3.2 As part of the vetting process;

3.3 Process payment of professional fees and where applicable expenses;

3.4 Provide training or instruction;

3.5 Communication in relation to the establishment of a Mental Health Tribunal or a case created under the Decision Support Services

3.6 Review details of any incident or complaint made by a third party;

3.7 All other relevant matters arising out of your application and appointment to a panel and the carrying out of services to your contract for services.

3.8 Ensure that there is an adequate gender balance in the constituting of a Mental Health Tribunal panel where possible.

4. Personal Data

Personal Data we may hold and process includes:

Type of Personal Data	Examples
Contact information	Name, address, email and telephone number(s)
General information	Gender, date and place of birth (from passport) Vehicle registration number and insurance (for the purpose of processing expense claims).
Proof of identity, proof of address	Proof of identity and proof of address are required for the Garda vetting process for Panel Members. This may include a copy of a passport and utility bill.
Education and employment information	Educational background (and where required supporting documentation), employer details and employment history, skills and experience and references. Professional memberships and affiliations and any other relevant information (e.g. employment status).
Government and other official identification numbers (to include professional registration numbers)	PPS number, passport number, tax identification number, driver's licence number, professional registration numbers or other government issued identification number. Any other relevant documentation (e.g. work permit).
Financial information and account details	Bank account number, or other financial account number and account details, other financial information for processing wages
Information held for members of Legal Representatives Panel	Application forms, name, firm address, office number, work mobile number, practicing certificate, professional indemnity cover, tax clearance and tax access numbers, and any other relevant correspondence.
Information held for members of other Panels	This may include data from and with the Application form submitted for the Panel, contract numbers, details of firm/hospital s/he is working at, Medical Council requirements (e.g. for members of the Medical Profession as applicable), , tax clearance and tax access numbers, vetting requirements.
Information held for members of Decision-	This may include data pertaining to registration with a regulated professional governing body, professional indemnity cover, tax clearance and access numbers, garda

Making Representative Panel	vetting details, application form. Professional bio provided for case allocation purposes.
Criminal data	Details of any past criminal offences or proceedings in respect of offences may be included in a Garda vetting report for a Panel Member for the Mental Health Tribunals and/or the Decision Support Service. Vetting is conducted before successful applicants are admitted to the panel. In the event any criminal offences are disclosed, these are considered by the MHC as to whether they are of a nature so as to disqualify the candidate from admission to either of the panels.

5. **Responsibility for Personal Data**

The MHC is responsible for looking after your Personal Data in accordance with this Privacy Policy, our internal standards and procedures and the requirements of data protection law.

The MHC shall apply suitable and specific safeguards which are designed to ensure that the requirements of data protection legislation are applied to our processing operations.

6. **Sharing of Personal Data**

In connection with the purposes described above, we may need to share your Personal Data with third parties (this may involve third parties disclosing Personal Data to us and us disclosing Personal Data to them). Such information shall only be disclosed where necessary and not otherwise. These third parties may include the following

Type of third party	Examples
Our service Providers	External third party service providers, such as security professionals, accountants, auditors, experts, lawyers and other professional advisors; travel assistance providers; IT systems, support and hosting service providers; banks and financial institutions that service our accounts; pay roll providers; document and records management providers; and other third party vendors and outsourced service providers that assist us in carrying out our activities.
Government authorities and third parties involved in court action	We may also share Personal Data with: (a) government or other public authorities (including, but not limited to, courts, regulatory bodies, law enforcement agencies, tax authorities and criminal investigations agencies); and (b) third party participants in legal proceedings and their accountants, auditors, lawyers, and other advisors and representatives, as we believe to be necessary or appropriate. The Office of the Comptroller and Auditor General may access files of the MHC relating to its agents.

7. **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 (e.g. we may use anti-virus protection systems, firewalls, and data encryption technologies). We have procedures in place at our premises to keep secure both soft and hard copy records. Access to such documents is restricted to relevant personnel. We also train our staff regularly on data protection and information security.

When the MHC provides Personal Data to a third party (including our service providers) 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 100% 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 immediately notify us.

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 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."*

Second, under the provisions of the Assisted Decision Making (Capacity) Act, 2015, MHC's remit was extended to include the establishment of the Decision Support Service (DSS). Its core function is to support decision-making by and for adults with capacity difficulties.

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

(a) Consent (where appropriate);

(b) Performance of a contract to which you are subject;

(c) Compliance with legal obligations; and

(d) Performance of our tasks carried out in the exercise of official authority and performance of our statutory functions.

9. **Special Categories of Personal Data**

These more sensitive or "special" categories of Personal Data include Personal Data revealing 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.

We only process data concerning health where required (e.g. to assess your fitness to serve as a Panel Member and to ensure your safety during the provision of such services). Such data may also be processed in the context of legal proceedings or claims.

We will rely on any one or more of the following categories in processing your sensitive Personal Data:

(a) your explicit consent;

(b) to protect your vital interests in circumstances where you are physically or legally incapable of giving consent; and

(c) where necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.

10. **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:

(a) The Law Enforcement Directive and as per Part 5 of the Data Protection Act 2018 or,

(b) 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 Law Enforcement Directive shall 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.

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. This is permitted in accordance with the National Vetting Bureau (Children and Vulnerable Persons) Act 2012 as may be amended from time to time. The Law Enforcement Directive (LED) shall not apply to the above as data is not being processed for the purposes as set out in Section 70(1)(a) of the Data Protection Act 2018.

11. 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 a Protected Disclosure Policy for "Internal Workers", that is, workers who are employed by the Mental Health Commission. This policy is available here.

11.1 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.

11.2 A person 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.

11.3 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)

11.4 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

11.5 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.

12. Monitoring communications

We reserve the right to monitor electronic communications (e.g. emails) to protect you, our organisation and IT infrastructure, and relevant third parties including by:

(a) identifying and dealing with inappropriate communications; and

(b) looking for and removing any viruses, or other malware, and resolving any other information security issues.

13. Retention of Personal Data

We will keep Personal Data for as long as is necessary for the purposes for which we collected it. The retention period for each type of data is documented in the MHC Data Retention policy.

Where we hold Personal Data to comply with a legal or regulatory obligation, we will keep the information for at least as long as is required to comply with that obligation.

For further information about the period of time for which we retain your Personal Data, please contact us using the details below.

14. Personal Data Rights?

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 as outlined in the legislation).
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	Examples of when this right applies to Personal Data we hold include (subject to certain exemptions):

systems and records. However, this right only applies in certain circumstances.	• when we no longer need the Personal Data for the purpose we collected it; • if you withdraw consent to our use of your information and no other legal justification supports our continued use of your information; • if you object to the way we use your information and we have no overriding grounds to continue using it; • if we have used your Personal Data unlawfully; and • if the Personal Data needs to be erased.
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; or • you have objected to our processing of the Personal Data and we are considering whether our reasons for processing override your objection.
Right to data portability This right allows us to obtain your Personal Data in a format which enables you to transfer that Personal Data to another organisation. You may have the right to have your Personal Data transferred by us directly to the other organisation, if this is technically feasible.	This right will only apply: • to Personal Data you provided to us; • where we have justified our use of your Personal Data based on: o your consent; or o the fulfilment by us of a contract with you; and • if our use of your Personal Data is by electronic means.

Right to object to processing of Personal Data You have the right to object to our use of your Personal Data in certain circumstances on grounds that are particular to your situation. However, we may continue to use your Personal Data, despite your objection, where there are compelling legitimate grounds to do so or we need to use your Personal Data in connection with any legal claims.	This right will only apply to Personal Data processed by us in the performance of our statutory functions and/or exercise of official authority.
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 Commission (DPC) If you live or work in an EEA member state, you may complain to the regulator in that state.	This right applies at any time.

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

15. **Your obligations in relation to Personal Data**

You should keep your Personal Data up-to-date by informing us of any significant changes to your Personal Data.

16. **Your obligations in relation to other persons Personal Data**

When processing Personal Data in the course of performing your duties as a Panel Member, it is your duty to abide by all applicable laws and/or MHC policies, standards and procedures, as may be amended from time-to-time, relating to the processing of Personal Data. In particular, you must not access or use Personal Data for any purpose other than in connection with, and to the extent necessary for, your work with us. Any breaches of security of Personal Data in your possession or of which you become aware must be notified without undue delay in accordance with our Personal Data Security Breach Procedure for Panel Members.

Your obligation to keep the Personal Data of others confidential continues after the termination of your relationship with the MHC.

Any proven breach of data protection laws and/or internal policies, standards and/or procedures may result in the termination of your appointment to the relevant MHC panel.

17. **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 the Data Protection Officer (DPO) by email at dpfoi@mhcirl.ie