MHT Panel Members: Data Security Breach Procedure

Policy Name:	GDPR Personal Data Security Breach Procedure for MHT Panel Members
Policy No:	MHC-GDPR-01
Division (if applicable):	Corporate Operations – GDPR
File location:	CorporateServices/GDPR/Policies-MasterCopies/MHC-GDPR-01PersonalDataSecurityBreachProcedureforPanelMembers
Date Implemented:	May 2018
Policy Updated:	28 August 2019
Revision Date:	28 August 2020
Policy Owner:	Information Governance Unit
Approved by MHC:	Version 2 : Approved by SMT 10 September 2019

CONTENTS

Important Notice

It is crucial for all MHT Panel Members to immediately report any potential or suspected Data Breach (as defined in this Procedure) to the Data Protection Officer by phone and email – contact details are set out in paragraph 5 of this Procedure.

If unsure whether an incident is a Data Breach or not please refer to the guidance set out in this Procedure and consult with the Data Protection Officer.

1. Introduction

The Mental Health Commission ("**MHC**") is a Data Controller[1] for the purposes of the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**"). The GDPR imposes obligations on Data Controllers and processors to process Personal Data (as defined below) in a manner that ensures the security, confidentiality and integrity of the Personal Data by implementing appropriate technical and organisational measures. In the event of a Data Breach (as defined below) that is likely to cause a risk to individuals the GDPR requires mandatory notification to the Data Protection Commission (the "**DPC**") and, in some cases, an additional communication to the affected individuals. This Personal Data Security Breach Procedure (the "**Procedure**") describes the process for identifying, escalating, reporting and recording suspected or actual Data Breaches involving Personal Data in accordance with the MHC's GDPR obligations.

The purpose of this Procedure is to ensure that the MHC manages and contains any Data Breach quickly so that the impact of the Data Breach can be minimised and any legal obligation to report the Data Breach to a regulator and/or any individual(s) affected by the Data Breach (in accordance with the GDPR) can be complied with in good time. This Procedure is also intended to enable the MHC to take appropriate measures to reduce the risks for affected individuals.

2. Who does this Procedure apply to?

This Procedure applies to Mental Health Tribunal (MHT) Panel Members and independent consultant psychiatrists appointed by the MHC in the context of a Tribunals established under the Mental Health Act, 2001 (together they will be referred to in this Procedure as 'Panel Members). All Panel Members should read and familiarise themselves with the contents of this document.

3. What is Personal Data?

Personal Data is any information relating to an identifiable living individual. A person is identifiable if s/he can be identified directly or indirectly (e.g. by reference to an identifier such as a name, address, date of birth, Medical Registration Number (MRN), telephone number, job title, photo, IP address and so forth). If in doubt as to whether any specific information or data may constitute Personal Data, please consult the Data Protection Officer (DPO).

4. What is a Personal Data Breach?

4.1 The GDPR defines a *'personal data breach'* as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise process"* ("**Data Breach**"). A Data Breach occurs when there is any unauthorised or accidental disclosure, loss, or any other form of unauthorised, accidental, or unlawful collection, use, recording, storing or distributing (each being a form of "**Processing**") of Personal Data. Examples of Data Breaches may include, but are not limited to:

[1] ***'Data Controller" or "Controller'*** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(a) loss, theft or misplacement of IT equipment or devices, if any nature, containing Personal Data (e.g. smartphone, laptop, USB key, etc.).

(b) loss, theft or misplacement of a folder, briefcase or any other container with Personal Data in physical hardcopy form.

(c) human error resulting in email or post containing Personal Data being sent to an unintended recipient.

(d) unauthorised access to automated or manual Personal Data as a result of a break-in to the MHC's business premises or to any premises where Panel Members have, or have stored, Personal Data.

(e) unauthorised access to Personal Data as a result of a breach of access controls

(f) an attack by a hacker, i.e. unauthorised access to the MHC's computer network, which may consist of a deliberate interruption to IT network services or penetration of the IT network or system, by an unauthorised party with the intention of obtaining information, destroying data or preventing access to data.

(g) unforeseen circumstances such as a flood or fire, in particular where Personal Data is not accessible either temporarily or permanently.

(h) unauthorised access to Personal Data where information is obtained by deception.

(i) in certain circumstances where there is a loss of access to or availability of Personal Data (temporarily or permanently) (e.g. where Personal Data has been deleted either accidentally or by an unauthorised person and the data cannot be restored).

4.2 Whether the data incident giving rise to the suspected Data Breach involves Personal Data must be determined on a case-by-case basis. If a Data Incident does not involve Personal Data, it is not a Data Breach. Furthermore, not all Data Incidents involving Personal Data will be Data Breaches.

(a) the Personal Data is securely encrypted or anonymised such to make the Personal Data unintelligible; and/or

(b) there is a full, up-to-date back-up of the Personal Data (in cases of accidental destruction).

The matter should be notified to the DPO as outlined in this Policy and it will be a matter for the DPO to determine if the Data Incident is a Data Breach or not.

5. **Panel Members obligation to report Data Incidents to the Data Protection Officer**

5.1 It is vital that all Data Incidents are immediately reported to the MHC's DPO as soon as they are identified. It is the role of the DPO to ascertain whether the Data Incident is in fact a Data Breach. The DPO contact details are as follows:

Name	Ruth-Blandina Quinn
Email	dpfoi@mhcirl.ie

Phone	01 636-2400

5.2 Prompt reporting of any Data Incidents to the DPO is crucial to ensure compliance with the GDPR, which contains a number of action points that must be put into immediate effect when the MHC is alerted or notified of a suspected or potential Data Breach. Panel Members will be required to co-operate with the DPO in determining the full facts surrounding the breach, any mitigation that might be necessary and any subsequent investigation.

5.3 The DPO will investigate the Data Incident to assess whether it is a Data Breach and the level of risk to the affected individuals, consider containment measures and determine whether: (i) a notification to the DPC; and/or (ii) a communication to the affected individuals is required.

5.4 While it is important to note that not all Data Incidents will necessarily involve Personal Data, and will not require notification to the DPC, all Panel Members should note that all loss, theft, or misplacement of IT equipment should be reported to the Director of Corporate Operations as soon as possible.

5.5 The failure to report any Data Incident or to report any Data Incident within the timeline provided could impact on the indemnity provided by the MHC to Panel Members and/or could lead to termination of the Panel Members contract for service.

6. Outsources Activities

The GDPR requires that all Data Breaches must be reported to the relevant Data Controller without undue delay[2] as soon as the Data Processor[3] becomes aware of the incident. The MHC requires any Data Incident to be notified to it immediately and no later than 24 hours from the time the incident occurred. Should a Panel Member receive a notice of Data Breach from any of the MHC's service providers, s/he is asked to please contact the DPO immediately so that the DPO can follow up directly with the service provider.

7. Making a Report to the Data Protection Commission

The MHC's DPO is responsible for making reports to the DPC in accordance with the Data Breach Response Plan and will act as the relevant point of contact in relation to requests for detailed written reports or any subsequent investigation by the DPC. Please note that the DPC may wish to contact the Panel Member directly, seek information or a report from the Panel Member. Panel Members are required to fully co-operate with the MHC and the DPC in relation to any such requests.

8. Record of Personal Data Security Breaches in Data Breach Log

The MHC's DPO is responsible for keeping a written record of all potential or suspected Data Breaches that are notified to him/her (including those that are not notified to the DPC or the affected individuals).

[2] Article 33(2) GDPR

[3] "Data Processor" or 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.