PERSONAL INJURIES ASSESSMENT BOARD
DATA PROTECTION CODE OF PRACTICE

ADOPTED ON 23rd May 2018

TABLE OF CONTENTS

Section *Page*

1. **Introduction**

1.1 The Personal Injuries Assessment Board (PIAB) is a statutory body which provides independent assessment of personal injury compensation for victims of workplace, motor and public liability accidents.

1.2 The principal function of PIAB is to make assessments of compensation for personal injuries without the need for legal proceedings. The Board is also obliged to prepare and publish a Book of Quantum, cause a cost benefit analysis to be made of the legal procedures and associated processes for awarding compensation for personal injuries, collect and analyse data in relation to amounts awarded or settlements made of personal injuries actions and such other functions as may be conferred on the Board as the Minister for Business, Enterprise and Innovation specifies. In performing its functions, PIAB is required to process significant amounts of "Personal Data" within the meaning of the Data Protection Acts 1988 and 2003 ("DPA"). PIAB respects the privacy rights of those whose Personal Data we process and we are conscious of our obligations under the DPA. PIAB is aware of and complies with the General Data Protection Regulation (GDPR), effective from 25 May 2018 and with Irish legislation based on the GDPR, including the Data Protection Act 2018.

1.3 The purpose of this Code of Practice is to disclose in a transparent way how PIAB obtains and processes Personal Data so that all those who provide us with Personal Data will clearly understand our practices and procedures. This Code also sets out our approach to dealing with Data Subject Access Requests under relevant legislation.

1.4 This Code of Practice was originally formally approved by the Data Protection Commissioner under the terms of the Data Protection Acts 1988 and 2003, and has been updated in the context of the GDPR

2. **Glossary**

2.1 Appendix 1 contains a Glossary of the key terms used in this Code of Practice.

3. **Types of Personal Data held by Us**

3.1 PIAB has been registered as a Data Controller with the Office of the Data Protection Commissioner under relevant legislation. While not applicable under the GDPR, PIAB keeps in contact with the Office of the Data Protection Commissioner and ensures it is aware of guidelines and decisions of the Office.

3.2 PIAB would typically retain and process the following types of Personal Data, as more particularly set out in the Board's Application Form:

(a) *Regarding Claimants*: Name, address, gender, date of birth, occupation (this information is required in the Claimant Application Form). Claimants may also provide contact information regarding their next of kin or other family members.

(b) *Regarding Respondents*: Claimants will also provide name and contact details for the party/parties they believe were responsible for their injuries ("Respondents") as well as details of the Respondent's insurance policies, car registration numbers etc.

(c) *Other:* Contact details of witnesses, medical experts, solicitors etc.

3.3 PIAB also processes Sensitive Personal Data relating to the medical condition of a Claimant. This Sensitive Personal Data would usually emanate from the Claimant him/herself and be in the form of medical report from the Claimant's treating Doctor or from a medical professional engaged by PIAB as part of the Assessment of the claim. When claimants submit an application for loss of earnings processing of financial details including wages and taxation details and Personal Public Service Numbers (PPSNs) will occur.

3.4 PIAB also processes information in relation to its staff, including contact details, names, and other personal information relating to Board members and employees of the Board.

4. **Obligations of PIAB**

4.1 PIAB controls the contents and use of certain Personal Data provided to it in the course of any Assessment. PIAB will usually perform its functions itself. When PIAB engages third parties to process personal data on its behalf it will ensure in its contracts that such third parties will also be subject to the data protection obligations set out in the DPA. PIAB specifically complies with the principles in the GDPR including: Lawful, fair and transparent processing; Purpose limitation; Data minimization; Accurate and up-to-date processing; Right to have data corrected (Rectified); Confidential and secure, appropriate security safeguarding; Accountability; Right of access and reporting of breaches; Data protection by design.

5. **What we do with Personal Data**

5.1 PIAB processes Personal Data provided to us only for the purposes of complying with our obligations under the Personal Injuries Assessment Board Acts 2003 and 2007 (as may be amended from time to time). These obligations include:

(a) efficiently and expeditiously processing applications for compensation arising from a personal injury;

(b) assisting Claimants and Respondents in the process;

(c) assessing how much (if any) compensation is due to injured parties;

(d) reducing the amount of time it takes to finalise a claim for compensation;

(e) contacting the parties to an assessment (and, where applicable, their nominated representatives) in connection with the Assessment and responding to any communications received.

6. **Collection, processing, keeping, use and disclosure of personal data**

PIAB is obliged to comply with the data protection principles set out in relevant Data Protection legislation including the Data Protection Act implementing the GDPR. These obligations mean the Personal Data we hold must meet the following criteria:

(a) Must be obtained and processed fairly

I. As most Personal Data obtained by us is provided directly by the Claimants and Respondents (or their nominees) PIAB will regard such data as having been fairly obtained. Reference to this Code and details on how to request/view a copy will be provided on our website and notifications of our data protection policies will be on claim forms as provided to all claimants and respondents. As PIAB only processes Personal Data in fulfilment of its obligations under the Personal Injuries Assessment Board Acts 2003 and 2007, it also considers that it fulfils its obligations with regard to fair processing. Under section 26 of the PIAB Act 2003 PIAB may request any person to furnish to them records, documents or other information for the purpose of verifying any item of loss alleged by a Claimant. Under section 28 of the PIAB Act 2003, by virtue of having made an Application, a Claimant is deemed to have consented to the Revenue Commissioners furnishing to PIAB information in relation to the income of a Claimant for the purpose of verifying any item of financial loss alleged by a Claimant.

II. PIAB bases its Assessment of a claim on the Application Form received from the Claimant, the medical report submitted by the Claimant's treating doctor and, where required, independent medical report(s) as arranged by the Board.

III. The level of information contained in a Claimant's medical report is determined not by PIAB but by the Claimant's treating doctor who includes such information as he/she thinks is appropriate and relevant to the claim. PIAB is not in a position to exercise editorial discretion in relation to this information, however, see (d) IV below. We must therefore rely upon the Claimant's treating doctor to take care to omit any irrelevant data from the medical report. If Claimants submit details of their medical history in or with their Application Form, PIAB will presume that the Claimant is doing so because this information is relevant to the injuries alleged to have been sustained. To assist in this regard, PIAB has produced a guidance document for Claimants for the assistance of their treating doctor when completing such reports.

(b) Shall be accurate, complete and kept up to date

All Claimants are required to sign a declaration on their Application Form that the information they have provided is true and accurate in every respect. In addition, any Claimants or Respondents who fail to provide complete or accurate information to PIAB may prejudice the outcome of their case. PIAB manages the data provided to it on its centralised, secure IT system. All telephone calls or other case information is updated on this system as and when it is received. PIAB will also comply with any data rectification requests received under Section 4 of the DPA in accordance with Section 12 below. Accordingly, PIAB ensures that Personal Data processed

by it is accurate, complete and up to date. Data received from Claimants and entered into PIAB's system is cross checked by file handlers to ensure accuracy and completeness.

(c) Shall have been obtained only for one or more specified, explicit and lawful purposes

PIAB processes Personal Data that it holds only for the purposes of complying with our obligations under the Personal Injuries Assessment Board Act 2003 (as may be amended from time to time). Further details regarding how we process Personal Data are set out in this Code of Practice. PIAB has a legitimate basis to process data for the purposes of its statutory duties under the PIAB Act 2003 as amended and other subsequent legislation dealing with our functions, and to transfer data to other parties for the purposes of its statutory duties.

(d) Must not be further processed for incompatible purposes

I. PIAB does not process Personal Data for purposes otherwise than in compliance with and in discharge of its functions.

II. PIAB is obliged to notify the Respondent of the nature of the claim and the Respondent has to reply within 90 days stating whether or not he/she consents to the making of the assessment.

III. PIAB will disclose the Claimant's Application and medical reports to Respondents in order for Respondents to consider the extent of their involvement or exposure to the claim submitted and whether they wish to consent to the assessment of the claim by the Board.

IV. In exceptional circumstances, where the claim is not appropriate for assessment (such as where the injuries are wholly psychological or there is overlap of injuries between a number of accidents) the medical report will not be provided to the Respondent. In addition, where the **medical report** contains information that is particularly sensitive, such as in relation to sexual abuse, the **medical report** will not be provided to the Respondent.

V. PIAB may commission an independent medical report for the purposes of assessing a claim. Where such a report is commissioned a copy of the report will be issued with the assessment to the Claimant and their advisor (if any) and to the Respondent or their advisor (if any) so that they can consider acceptance.

VI. PIAB will not disclose Personal Data to third parties unless the Data Subject has consented to this disclosure (example: the claimant's solicitor) or unless the disclosure to the third party is necessary for the Board's functions (in such circumstances, the third party is bound by similar data protection requirements). However, PIAB will disclose Personal Data to third parties if we believe in good faith that we are required to disclose it in order to comply with any applicable law, a summons, a search warrant, a court or regulatory order or other statutory requirement. PIAB may also notify the Motor Insurers' Bureau of Ireland of motor claims where a Respondent's insurers are unknown or unidentified.

VII. Under Section 86 of the PIAB Act 2003, PIAB may disclose certain Personal Data to a central database relating to personal injuries claims but only if the database is maintained in accordance with the DPA. Any plans to implement such a system will be conducted in consultation with the Data Protection Commissioner. Nothing has been implemented in relation to this, to date.

VIII. Under Section 73 of the PIAB Act 2003 it is an offence, other than with the consent of the Board, for a member of the Board, a member of the staff of the Board, a member of a committee of the Board or an advisor or consultant to the Board, to disclose confidential information, including information that would identify a Claimant or a Respondent or to make known the amount of an assessment that has been made in a particular claim.

IX. Under Section 54(1)(d) of the PIAB Act 2003, the Board of PIAB is also obliged "to collect and analyse data in relation to amounts awarded on foot of, or agreed in settlement of, civil actions to which this Act applies". Such data will be sought from the Courts Service, individual insurers/relevant parties, Insurance Ireland and from such other sources as from time to time may be deemed appropriate.

X. In a limited number of cases, PIAB processes Personal Public Service Numbers (PPSNs) for example for purposes such as -- verifying loss of earnings, assessing damages in cases of fatal injuries, or recovery of payments made by the Department of Social Protection. This process is in line with our statutory role and duty. We only process this data where needed and PPSN data is then deleted in line with our data retention policy, following assessment/closure of claims.

(e) Shall be adequate, relevant and not excessive for those purposes

PIAB only requires Personal Data which is relevant to the performance of its duties under the Personal Injuries Assessment Board Acts 2003 and 2007. It does not seek, nor does it wish to receive, excessive levels of data which are not relevant to these duties. The guidance note produced for Claimants Treating Doctors will also assist in this regard.

(f) Shall be kept for no longer than is necessary

I. PIAB case files are ordinarily archived for a period of seven years from the last action on a file for data held in electronic form and for 26 months from the date of receipt of data held in manual form. This allows PIAB to recall the information in the event of subsequent litigation. PIAB will retain statistical factual information about cases indefinitely, but such data will not be "personal data" as defined in the DPA or GDPR.

II. Data collected from other sources in relation to amounts awarded or agreed will be retained for 7 years.

(g) Must be kept secure against unauthorised access, alteration or destruction

PIAB uses a robust IT case management system with restricted access to ensure that only those who have a need to access Personal Data can do so. PIAB's Manual Data is stored in a secure site. Access to the case management system is by authorised personnel with password restricted entry to the system.
The Board has established appropriate security provisions to ensure that: -

1. Access to the Board's computers is restricted to PIAB authorised staff or external processors authorised by PIAB.
2. Access to the information is restricted to PIAB IT Authorised staff or external processors authorised by PIAB.
3. The Board's systems are password protected.
4. The Board has comprehensive back up procedures in operation.
5. All waste papers, printouts, etc are disposed of securely.
6. **Back-up Data.** Back-up data are data held specifically for the purpose of recreating a file in the event of the current data being destroyed. In accordance with our security obligations under the DPA, PIAB's electronic case management system is regularly backed-up so as to avoid the loss or compromise of data. Back-up data will not ordinarily be provided in response to a Data Subject Access Request. The tapes are taken regularly and stored offsite at a secure location which only authorised PIAB Personnel have access to.
7. Access to the computer and communications room is restricted to PIAB IT authorised personnel by manual lock and keys which are located in a locked store room which authorised PIAB IT Personnel have access to.
8. PIAB is aware of and fully compliant with the notification timelines for data breaches. We have a data breach policy and have integrated that into data breach procedures.

7. Right of Access

7.1 Under relevant legislation, Data Subjects, such as Claimants or Respondents, are entitled to the following information from PIAB and PIAB has processes in place to provide that information:

a) confirmation as to whether we keep Personal Data relating to them;
b) a description of the categories of Personal Data processed;
c) a copy of such Personal Data in intelligible form;
d) a description of the purpose(s) behind the processing of the Personal Data;
e) the identity of those to whom we have disclosed (or currently disclose) the data; and
f) the source of the Personal Data (unless this is contrary to the public interest)

7.2 Access requests under GDPR apply to Personal Data held by PIAB in both a computerised and manual form. However, where a document

exists in duplicate, e.g. where correspondence is scanned into our case management system, two copies of the same document will not be provided in response to a request.

7.3 **The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989):** The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) provide that health data relating to an individual should not be made available to the individual, in response to a Data Subject Access Request, if that would be likely to cause serious harm to the physical or mental health of the Data Subject. This provision would not normally apply in the case of Assessments administered by PIAB but in the event that a medical professional issues an opinion that these Regulations apply, the health data in question will not be provided to the Data Subject. Such opinion will, however, be furnished to the Data Subject's own medical practitioner.

8. **Formalities for Data Subject Access Requests**

8.1 Data Subject Access Requests must meet certain formalities:

(a) they must be in writing;

(b) PIAB will make reasonable enquiries to satisfy ourselves about the identity of the person making the request to ensure we are not disclosing Personal Data to a party who is not entitled to it under the DPA;

(c) data requests must include a reasonable level of appropriate information to help us to locate the information required. (However no reason for the request needs to be provided);

8.2

a) Where a Data Subject Access Request does not specify otherwise, it is to be assumed, subject to Parts 9 and 10 below, that a copy of all Personal Data held by PIAB about the Data Subject is to be disclosed.

b) Data Subject Access Requests will be complied with within one month of receipt of the request. Where reasonable additional information is required to substantiate the request as described in paragraph 7.1(b) and (c), the time frame for responding runs from receipt of the additional information.

c) If we receive a very general Data Subject Access Request, e.g. "please give me everything you have on me", legislation allows us to seek more detailed information on the nature of the request, such as the approximate

date of a particular incident, our case record number, the identity of the other party etc. However, this will be assessed on a case by case basis.

9. **Information Which Will not be Provided**

9.1 PIAB will not normally disclose the following types of information in response to a Data Subject Access Request:

(a) **Information about other People**

A Data Subject Access Request may cover information which relates to one or more people other than the Data Subject. The information about the other person may be Personal Data about that person, to which the usual data protection rules under the DPA, including the restrictions on disclosure, apply.

In such circumstances we will not grant access to the information in question unless either:

(i) the other person has consented to the disclosure of their data to the Data Subject; or

(ii) in all the circumstances it is reasonable to make the disclosure without that person's consent.

If the person's consent is not forthcoming and it is not reasonable to make the disclosure without consent, we will make available as much Personal Data as we can without revealing the identity of the other person (for example by excluding the person's name and/or other identifying particulars).

(b) **Opinions given in Confidence**

Where we hold Personal Data about the Data Subject in the form of an opinion given in confidence we are not required to disclose such opinions in response a Data Subject Access Request in all cases.

(c) **Repeat Requests**

The DPA provides an exception for repeat requests where an identical or similar request has been complied with in relation to the same Data Subject within a reasonable prior period. The Board will consider that if a further request is made within a period of six months of the original request and where there has been no significant change in the personal data held in relation to the individual, it will be treated as a repeat request. Accordingly, where Personal Data has recently been provided to the Data Subject or his/her legal representative, PIAB will not normally provide a further copy of the same data in response to a Data Subject Access Request. The Board will not consider that it is obliged to provide copies of documents that are in the public domain.

(d) **Privileged Documents**

Where a claim of privilege could be maintained in proceedings in a court in relation to communications between an individual and his or her professional legal advisers (or between those advisers) any privileged information which we hold need not be disclosed pursuant to a Data Subject Access Request.

9.2 Where PIAB refuses a Data Subject Access Request, we will do so in writing and we will set out the reasons for our refusal.

10. **Exceptions to Right to Data**

10.1 Relevant legislation provides that individuals do not have a right to see information relating to them where any of the following circumstances apply. While these circumstances would not ordinarily apply to PIAB, they are set out below for the sake of completeness:

(a) If the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing/collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities;

(b) If granting the right of access would be likely to impair the security or the maintenance of good order in a prison or other place of detention;

(c) If the information is kept for certain anti-fraud functions; but only in cases where allowing the right of access would be likely to impede any such functions;

(d) If granting the right of access would be likely to harm the international relations of the State;

(e) If the information concerns an estimate of damages or compensation in respect of a claim against the organisation, where granting the right of access would be likely to harm the interests of the organisation. This would only apply in respect of data relating to a claim against PIAB, not other claims administered by PIAB;

(f) If the information would be subject to legal professional privilege in court;

(g) If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.

11. **Format of the Response**

11.1 The DPA provides a right of access to a permanent copy of the Personal Data that is held about the Data Subject unless this is not possible or would involve

disproportionate effort. The information must be communicated to the Data Subject in an intelligible form. Usually this will mean that a photocopy or printout of the Personal Data will be provided to the Data Subject. However, where a Data Subject agrees, information can be provided in electronic format e.g. by email or on disk.

12. **Rectification or Erasure**

12.1 If a Data Subject seeks to have any of his or her Personal Data rectified or erased, this will be done within one month of the request being made provided there is reasonable evidence in support of the need for rectification or erasure.

13. **Disclosures of Personal Data Outside of the EEA**

13.1 PIAB will not ordinarily transfer Personal Data to countries outside the European Economic Area (EEA) (unless, for example, we are corresponding with a Claimant or Respondent who resides outside of the EEA). If any data is processed outside of the European Economic Area (EEA), PIAB will ensure there are measures in place in association with the processor to ensure this is consistent with GDPR. PIAB will comply with its obligations under data protection legislation to ensure such transfers are lawful.

14. **Changes to this Code**

14.1 The latest version of this Code will be published on our website.

15. PIAB has designated a Data Protection Officer (DPO) in line with the GDPR and data legislation in Ireland. The DPO can be contacted via enquiries@injuriesboard.ie or by telephone at 01 463 4018 or by post at PIAB, Grain House, Exchange Hall, Belgard Square North, Tallaght, Dublin 24.

PERSONAL INJURIES ASSESSMENT BOARD

23rd May 2018

Appendix 1
Glossary

Personal Data: The DPA applies only to Personal Data as defined in Section 1 of the DPA:
Personal Data: means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This includes Personal Data held in a computerised or manual (paper) form.

Sensitive Personal Data: There is a second sub-category of Personal Data referred to as Sensitive Personal Data.
Sensitive Personal Data: means Personal Data as to racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; physical/mental health; biometric information, sexual life; commission or alleged commission of offences; or criminal convictions/proceedings.

Data Subject: A Data Subject is the individual who is the subject of the Personal Data. Only a Data Subject is entitled to make a Data Subject Access Request.

Data Subject Access Request: A Data Subject Access Request is a request made in writing to PIAB by a Data Subject pursuant to Section 4 of the DPA or under the General Data Protection Regulation (GDPR) and data protection legislation to implement the GDPR.

Processing: Processing is extremely broadly defined and includes practically all imaginable acts of collection, access, use, storage and deletion of data.

Data controller: Data controller means a person who, either alone or with others, controls the contents and use of personal data.

Data Processor: Data processor means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.

Relevant data protection legislation: This means the Data Protections Acts in force in Ireland up to May 2018 and the Data Protection legislation introduced Ireland under the GDPR.