IHPBA POLICY ON GDPR

Purpose

The purpose of this document is to outline the
International Hepato-Pancreato-Billiary Association's policy on GDPR.

1) Awareness

IHPBA is aware of the GDPR Regulations and the Executive Director has undertaken an audit of the personal information and data stored and has put measures in place to ensure compliance with the new regulations.

2) Information held

IHPBA has prepared a document which details personal data held by the Association. The document also details where the information comes from, why the information is held, the lawful basis this is held (consent), how this is updated and if this is shared with any other parties. This document also ensures compliance with the accountability principle, which requires organisations to be able to show how they comply with the data protection principles for example by having effective policies and procedures in place.

3) Communicating privacy policy

IHPBA has a privacy notice and the necessary changes have been made to this to ensure compliance.

The privacy policy states:

- The identity of IHPBA
- How the information is intended to be used
- The lawful basis for processing the data
- The data retention period
- The individual's right to complain to the ICO if they think there is a problem with the way the data is being handled

4) Individuals' rights

The GDPR includes the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object; and
- The right not to be subject to automated decision making including profiling

IHPBA understands these rights and has updated processes to ensure compliance.

5) Subject access requests

The Association has the processes in place to ensure access requests can be met within 40 days and free of charge**.**

6) Lawful basis for processing personal data

The Association has identified the lawful basis for processing personal data and this is included in the document referred to in point 2 above.

7) Consent

The Association understands that consent must be freely given, specific, informed and unambiguous.

8) Children

The Association does not collect, process or store any data on children.

9) Data breaches

Should a data breach occur in the Association, the Association's Board will report and investigate the breach. Depending on the nature of the breach the Board will determine if the individuals and/or the ICO will be notified.

10) Data Protection by Design and Data Protection Impact Assessments

The business of the Association has been assessed and it was deemed not necessary to carry out a Data Protection Impact Assessment. The data processing within the Association is minimal and not high risk.

11) Data Protection Officers

The Association has considered the need to appoint a DPO and have decided that due to the size and nature of the organisation this is unnecessary.

12) International

The Association operates in more than one EU member state. The lead data protection authority is the UK as this is where the main business/establishment is conducted.