INTERNATIONAL POLICE ASSOCIATION IRELAND

Data Protection Policy Document.

INDEX.

INTERNATIONAL POLICE ASSOCIATION IRELAND
Data Protection Policy

1. Introduction
IPA Ireland treats data protection and privacy with utmost importance.

As per the Data Protection Act 1998-2003 and the General Data Protection Regulation (GDPR), IPA Ireland is a data controller.

All personal data that comes into the possession of IPA Ireland will be processed and stored in accordance with the above regulations.

2. Purpose of personal data collection by IPA Ireland
IPA Ireland collects personal data of its members and non-members in order to facilitate the following activities, which IPA Ireland collectively refers to as “IPA Business”:

1. Identity and membership verification of members of IPA Ireland and members of other IPA Sections worldwide.
2. Membership based services via postal, email and text based notifications.
3. IPA National Treasury payments.
4. IPA Travel facilities.
5. IPA Accommodation facilities.
6. IPA Supplies, Hobby and Memorabilia facilities.
7. Professional Seminar facilities.
8. Participation in IPA Prize Draws.
9. Delivery of IPA Publications.
10. IPA Police Exchange/Police Placement Programmes.
11. IPA Language Based and Other Scholarships.
12. Other Regional, National and International based Social, Cultural and Professional IPA Events and Activities.

3. IPA Ireland's principles of personal data collection.

Following the national and international best practice, IPA Ireland will collect personal data in accordance with the following eight Data Protection principles:

1) Obtain and process personal data fairly, and in accordance with the law.
2) Keep it only for one or more specified, explicit and lawful purposes.
3) Use and disclose only in ways compatible with these purposes.
4) Keep personal data safe and secure.
5) Keep personal data accurate, complete and up-to-date.
6) Ensure personal data is adequate, relevant and not excessive.
7) Retain personal data for no longer than is necessary.
8) Give a copy of his/her personal data to that individual, on request.

4. Responsibility for Proper Use of Personal Data

The overall responsibility for ensuring compliance with Data Protection legislation rests with the National Executive Committee of IPA Ireland.

All employees, NEC members, Regional Secretaries, Regional Travel Officers and any other persons duly delegated by IPA Ireland to collect, control, process and use personal data shall be considered "Facilitators" for the purposes of Data Processing and shall carry individual responsibility for their personal compliance with the Data Protection legislation.

Personal data controlled by IPA Ireland will be used only in relation to IPA Business, as defined in Section 2 of this Policy.

All operations conducted on personal data on behalf of IPA Ireland will be carried out with strict adherence to the principles listed in Section 3 of this Policy.

The Association's Data Protection Coordinator is the President of the Section, then in Office.

The Data Protection Coordinator shall co-ordinate the provisions of assistance, advice and training within IPA Ireland and together with the National Executive Committee, shall ensure that the organisation is in a position to comply with all relevant legislation.

The National Executive Committee may appoint another Member of the NEC to assist the Data Protection Coordinator with those responsibilities.

Each Regional Committee Secretary and Travel Officer shall be appointed as an IPA Facilitator in his/her respective Region.

5. Personal data processing by IPA Ireland employees, National Executive Committee, Regional Committees *and IPA Facilitators.*

The only persons authorised to access and process personal data will be those appointed to do so on behalf of IPA Ireland.
Such data shall be accessed/processed only in relation to IPA Business, as defined in Section 2 of this Policy.

Data cannot be shared informally, whether within IPA Ireland or with third parties.

IPA Ireland will provide training to all employees and IPA Facilitators to help them understand their responsibilities when handling personal data.

IPA Ireland employees and IPA Facilitators should keep all data secure, by taking precautions and following the guidelines below in terms of data security:

1. Passwords and login credentials cannot be shared.
2. Only encrypted storage media can be used for storing personal data.
3. Backups of data must be performed when necessary, always onto encrypted storage media.
4. Personal data cannot be disclosed to unauthorised persons, either within IPA Ireland or outside.
5. Personal data cannot be shared by email in plain text.
6. When transmitted as attachments, personal data files can be sent only to authorised parties, and only when fully encrypted and password protected.
7. No personal data can be saved onto personal computers by IPA Ireland employees or IPA facilitators.
8. Data should be reviewed and updated regularly to ensure that it is not out of date.
9. When no longer required, data should be deleted in adherence to the IPA Ireland Data Deletion Policy.
10. IPA Ireland employees and IPA Facilitators should request the help of the Data Protection Coordinator when unsure about any aspect of data protection. Decisions made by the Data Protection Coordinator are final.

6. Storage of Personal Data

The following rules shall be adhered to by IPA Ireland personnel for the safe keeping of personal data within IPA Ireland.

1. When personal data is stored in any format on any paper layout, such paper records shall be kept securely and in such a way as to prevent unauthorised access to such records.

2. Printouts/paper records containing personal data shall be shredded and disposed of securely when no longer required. The responsibility for the safe disposal of large volumes of paper data shall rest with the Data Protection Coordinator, who will make appropriate arrangements for such safe disposal.

3. When personal data is stored electronically, the hardware used for the storing of such data shall be equipped with adequate encryption and up-to-date digital security measures. Adequate passwords, firewalls, anti-virus software, etc. shall be used to ensure unauthorised access, accidental deletion and hacking attempts. This shall be achieved in line with provisions of Section 5 of this Policy.

4. Uploading data onto private or third party storage media, servers, cloud storage services or other means shall be strictly regulated by this Policy Document and carried only when authorised by the IPA Data Protection Coordinator.

5. Data shall be backed up frequently, as per Section 5 of this Policy.

7. Access Requests / Withdrawal Of Consent

Access Requests:

1. Data Protection Policy & Consent Withdrawal Forms are located/available to download on the Member's area of the Association's website for the information/use of IPA members.

2. Information is carried on the home page of the IPA website advising non IPA Members of the availability of the Data Protection Policy Document and Consent Withdrawal Forms at the Association's Office, with necessary address details.