IACP Data Protection Policy

Purpose

The General Data Protection Regulation (GDPR) (EU)2016/679) governs the controlling and processing of personal data in the European Union.

GDPR was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the IACP processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

The purpose of this policy is to ensure that the IACP meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individual's best interest.

The data protection laws include provisions that promote accountability and governance and as such the IACP has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

The purpose of gathering data include, but is not limited to, the validation and accreditation of members, course accreditation, complaints, organisation and administration of seminars, research activities, the recruitment and payment of staff and compliance with statutory obligations.

Policy scope

This policy applies to all staff within the IACP *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in Ireland or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

This policy covers all personal information including both member and employee information generated in all IACP locations. It applies to all personal data collected and stored at all IACP locations. This policy applies to both soft and hard copy data held on all IACP systems, on

network share drives, email, intranet sites, end user applications microfiche, voice recordings and CCTV.

Where data is being transferred to any third party it is the responsibility of the organisation to ensure contractual agreements are in place covering security and retention of data.

GDPR Principles

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storagelimitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Subject Access Requests

Under Article 15 of the GDPR, an individual has the right to obtain from the controller, confirmation as to whether personal data concerning them is being processed. The IACP have dedicated processes in place for providing data subjects with access to their personal information. Where a data subject asks the IACP to confirm whether we hold and process personal data concerning him or her and requests access to such data this is referred to a Subject Access Request (SAR).

SAR's are passed to the Data Protection Officer as soon as received, will be completed within 30- days, and provided free of charge. Please contact:

Data Protection
Officer
IACP
First Floor, Marina
House 11-13
Clarence Street
Dun Laoghaire
County Dublin

Or hannah@iacp.ie/ any staff member to send a Subject Access Request.

Please Note:

1. Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received.
2. In order for us to protect the security of personal data, it may be necessary for you to provide proof of your identity before release of data is authorised.

Taking Photo's / Video's at Events

The IACP uses photograph, video and audiotape at its events without the expressed written permission of those included. Clear signs are displayed at events which will advise data subjects of the data being captured. An announcement will be made at IACP events informing individuals that photos/videos will be taken at the event and advising of their right not to participate.

This data may be used in publications, including but not limited to, brochures, journals, invitations, books, newspapers, magazines, television, websites. If an individual prefers not to be photographed/ videoed they must advise the photographer/videographer at the event. If a data subject features in material and would like this removed, they should contact the IACP, and where possible, material will be deleted.

Correspondence Sent via Email

The IACP sends correspondence to members via email as this is the organisations main and preferred method of communication. Much of this correspondence is essential to inform and update the membership on IACP requirements and to ensure members are aware of contractual obligations.

Secondary to this, the IACP send communication which is not essential to receive as outlined above. In the case an individual does not wish to receive such emails, they must click unsubscribe at the bottom of the email and will be removed from the mailing list.

Data Retention Schedule

The IACP recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation. The purpose of a Data Retention Schedule is to ensure that IACP have clear and enforceable instructions around how long data is retained.

The objective of this policy is to ensure that:

- Guidance exists so that retention limits can be set for data which complies with GDPR legislation;
- Once retention limits are reached, the data is either automatically destroyed or reviewed for destruction;
- Retained data is held securely;
- All data marked for destruction is comprehensively and securely destroyed;
- All relevant staff are sufficiently trained to comply with Data Retention Schedule

Considerations necessary prior to implementation of this schedule

- If under investigation or if litigation is likely, retain files as they may be used as evidence.
- On-going legislative requirements.

Record Retention Limits

<table>
<tr><th>Type of Record</th><th colspan="2">Retention Period</th><th>Responsibility</th></tr>
<tr><td>Current and Ex Employee Data</td><td colspan="2"><table>
<tr><th>Category of personal Data</th><th>Retention Period</th></tr>
<tr><td>Terms and conditions of Employment (includes contracts of employment and all related documentation)</td><td>7 years from the termination or expiration of the contract of employment</td></tr>
<tr><td>Working time records (includes working hours, leave, name/address of employee etc.)</td><td>3 years from the date of creation</td></tr>
<tr><td>Payslips</td><td>3 years from the date of their making</td></tr>
<tr><td>Employee payroll and Tax records</td><td>7 years from the end of the financial year following termination of employment, or to the end of any enquiry by the Revenue Commissioners</td></tr>
<tr><td>Medical records</td><td>6 years from the Termination or Expiration of the Contract of Employment</td></tr>
</table></td><td>Operations Manager</td></tr>
<tr><td>Applications & Interview Notes</td><td colspan="2">6 months after notifying unsuccessful candidates</td><td>Operations Manager</td></tr>
<tr><td>Member Softcopy Data</td><td colspan="2">7 years from the date the individual’s membership has lapsed</td><td>Administration Officer</td></tr>
<tr><td>Member’s Hardcopy Data</td><td colspan="2">1 year from the date the individual’s membership has lapsed</td><td>Administration Officer</td></tr>
<tr><td>Unsuccessful Application Data</td><td colspan="2">1 year from date the application is deemed unsuccessful</td><td>Accreditation Supervisor</td></tr>
<tr><td>Incomplete Application Data</td><td colspan="2">1 year from date applicant was last contacted by IACP</td><td>Administratio n Officer</td></tr>
<tr><td>Withdrawn Application Data</td><td colspan="2">1 year from date the applicant submitted</td><td>Administratio n Officer</td></tr>
<tr><td>Deceased Members Data</td><td colspan="2">1 year from the date IACP are notified of the death</td><td>Administration Officer</td></tr>
<tr><td>Payment Information</td><td colspan="2">No card details are to be stored on hardcopy. Payment details should be inputted to the secure online payment facility at point of purchase</td><td>All Staff</td></tr>
</table>

Complaints	7 years from the date the complaint is finalised	Complaints Secretary

Minutes of Meetings – Board of Directors **Minutes of Meetings – Committees**	Indefinitely 10 years	Board PA Administration Officer for relevant Committee
Garda Vetting	Hardcopy approved applications are kept for 1 year after individual's membership has lapsed Unsuccessful applications are kept for a 7 year period Submissions for review by Garda Vetting Decision Maker are kept for 1 year after individual's membership has lapsed Unsuccessful Appeals are kept 7 years from the date they have been finalised Successful Appeals are kept for 7 years after individual's membership has lapsed.	Accreditation Supervisor Accreditation Supervisor Accreditation Supervisor Accreditation Supervisor Accreditation Supervisor
Hardcopy Course Accreditation Applications	Applications are destroyed once the new application has been approved. Unsuccessful applications are destroyed after a one-year period After a course is no longer accredited with the IACP, data will be kept for 1 year.	Accreditation Supervisor Accreditation Supervisor Accreditation Supervisor
Softcopy Course Data	1 year after the course is no longer accredited with the IACP Course details remain in the register of previously accredited courses (IACP Website)	Accreditation Supervisor Accreditation Supervisor
Subject Access Requests/Data Protection Breaches	7 years after the request/breach	Data Protection Officer
Email	Emails to and from IACP members / members of the public are kept in MS Outlook for no longer than 3 years Emails to and from vendors / suppliers / contractors are kept in MS Outlook for no longer than 3 years after the contract / business relationship ends	All Staff

Email Accounts	Email accounts for IACP employees, no longer than 1 year after staff members have left.	Operations Manager
MS Teams Chat	Chat messages are deleted 2 months after being posted.	Operations Manager

Erasure

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the IACP recognise that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies:*

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data must be erased in order to comply with a legal obligation;
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and the IACP receive a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Protection Officer in conjunction with any department manager to ensure that all data relating to that individual has been erased.

Data Storage & Access of Records and Data

Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependant on their purpose and actiontype.

Destruction Policy

The destruction of records will take place as part of a managed process. The responsibility for destruction of data is listed in the data retention schedule above.

Training and Awareness

The management of records involves all employees; therefore, all employees must be made aware of the impact of the Data Retention Schedule on their day-to-day interaction with records/ member information.

Definitions

As with any legislation, certain terms have particular meaning. The following are some useful definitions:

Data means information in a form which can be processed. It includes both automated data and manual data.

Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

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 can be a very wide definition depending on the circumstances.

Processing means performing any operation or set of operations on data, including: – obtaining, recording or keeping data, – collecting, organising, storing, altering or adapting the data, – retrieving, consulting or using the data, – disclosing the information or data by transmitting, disseminating or otherwise making it available, – aligning, combining, blocking, erasing or destroying the data.

Data Subject is an individual who is the subject of personal data. Data Controllers are those who, either alone or with others, control the contents and use of personal data.

Data Controllers is a body that, either alone or with others, controls the contents and use of personal data. It can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as G.P.'s, pharmacists or soletraders.

Data processor is 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/her employment. Again, individuals such as G.P.'s, pharmacists or sole traders are considered to be legal entities.

Data security breach occurs when there is unauthorised access to, collection, use, disclosure or disposal of personal information. This type of breach can occur for a number of reasons including:

- Loss or theft of data or equipment on which dataisstored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human Error;
- Unforeseen circumstances such as a flood orfire;
- A hacking attack;
- Access where information is obtained by deceiving the organisation that holdsit.

A record is defined under the Freedom of Information Acts 1997 and 2003 as "any memorandum, book, plan, map, drawing, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (within the meaning of the Data Protection Act, 2018) are held, any other form (including machine-readable form) or device in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form of any of the foregoing or is a combination of two or more of the foregoing" (Freedom of Information Act, 1997, 2003).

DATA SECURITY BREACH GUIDELINES

As a data controller, IACP processes significant amounts of personal data and appropriate measures require to be taken against the unauthorised or unlawful processing and accidental loss, destruction of or damage to personal data. It is, therefore, essential that in the event of a data security breach, appropriate action is taken by IACP to minimise any associated risks as soon as possible.

The purpose of these guidelines is to set out the processes that represent best practice in the event of a data security breach involving personal data or sensitive personal data. These guidelines are a supplement to IACP's Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with GDPR & Data Protection legislation.

Responding to a Potential Data Security Breach

In line with best practice, these guidelines outline five stages to managing a response to a breach:

Stage 1: Identification and Classification

If an IACP staff member considers that a data security breach has occurred, this must be reported immediately to the IACP Data Protection Officer and to the staff member's line manager (where applicable).

Stage 2: Containment and Recovery

Containment involves limiting the scope and impact of a data security breach. If a breach has occurred, appropriate action will be taken by the relevant IACP staff to minimise any associated risks which may include:

- establishing who within IACP needs to be made aware of the breach and ensuring relevant staff are informed what is required to assist in the containment exercise;
- establishing whether there are any actions which may recover losses and limit the damage the breach can cause;
- where appropriate, informing the Gardaí

Stage 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant IACP staff are required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided by the individual reporting the breach can assist with this stage.

Stage 4: Notification of Breaches

Where applicable, the Supervisory Authority will be notified of the breach no later than 72 hours after the IACP becoming aware of it.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

If informing the data subject of the breach involves disproportionate effort, the IACP reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

Stage 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the Data Protection Officer and Management will occur to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Potential Data Security Breach Report

Please complete the following questions in order to ascertain if a data security breach has occurred and return the completed form to the Data Protection Officer or your line manager.

What type of data is involved?	
Does it fall under the definitions of personal data and/or special category information as outlined in the Data Protection Policy?	
If so, the following information must be provided	
Details of the breach	
Date and time incident occurred (if known)	
Date and time incident detected	
Name of person reporting incident	
Details on how the data was held, e.g. laptop, memory stick, personal digital assistant etc.	
Details of safeguards (e.g. encryption), if any, that would mitigate the risk if data has been lost or stolen	
Are there any reasons to suspect that the passwords used to protect the data may have been compromised? (e.g. password stored with mobile device or weak password used)	
Details of the number of individuals whose information is at risk, i.e. how many individuals' personal data are affected by the breach?	
Who are the individuals whose data has been breached - are they staff, students, suppliers, third parties etc?	
What could the data tell a third party about the individual?	
Any other information	