IAP

DATA PROTECTION POLICY

SEPTEMBER 2019

INTERNATIONAL ASSOCIATION OF PROSECUTORS

DATA PROTECTION POLICY

SEPTEMBER 2019

Index

página

DATA PROTECTION POLICY

SEPTEMBER 2019

Role of the IAP

The **International Association of Prosecutors (IAP)**[1] is an independent, non-governmental and non-political organisation and the only worldwide professional association for prosecutors.

The IAP has over 180 organisational members, including prosecuting agencies, associations of prosecutors and crime prevention agencies. Together with individual members, this represents over 350,000 prosecutors in more than 177 countries and territories around the world.

The IAP is committed to both setting and raising standards of professional conduct and ethics for prosecutors worldwide; promoting the rule of law, fairness, impartiality and respect for human rights and improving international cooperation to combat crime.

The managing and administrative body of the IAP is the Executive Committee which is subject to the authority of the General Meeting, the governing body of the Association. The Association elects a President, up to nine Vice-Presidents and up to 21 other ordinary members constituting the Executive Committee. The membership of the Executive Committee reflects the regions of the world in which the Association has members.

The Executive Committee appoints a Secretary-General who is the Chief Executive of the Association and manages its day to day affairs and a General Counsel who is the legal counsellor and manager of the professional programme and project work of the Association. The Executive Director is responsible for membership relations and recruitment and for the Association's network development and facilitation.

Location of the IAP Secretariat

The IAP Secretariat is located at:
Hartogstraat 13
2514 EP The Hague
THE NETHERLANDS

The European Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data is commonly referred to as the **General Data Protection Regulation (GDPR)**.

[1] The **International Association of Prosecutors(IAP)** is based on the *Foundation Treasury International Association of Prosecutors*, a non-profit foundation (Stichting) established under Dutch law.

The regulation came into force in May 2018 and replaced the existing data protection framework under the EU Data Protection Directive.

The regulation is designed to protect people's privacy. It confers rights on individuals in relation to the privacy of their personal data, as well as responsibilities on individuals and organisations holding and processing that data.

Because the IAP processes personal data it has certain obligations under the regulation. This policy explains what those obligations are and how the IAP will comply with them. It does not deal with every possible situation and it does not give legal advice.

What is personal data?

Personal data is any information about an identified or identifiable person, also known as a data subject. Personal data includes information such as their:

- Name;
- Address;
- ID card/passport number;
- Income;
- Cultural profile;
- Internet Protocol (IP) address;
- Data held by a hospital or doctor (which uniquely identifies a person for health purposes)

Special categories of personal data

Special categories of personal data are defined as:

- Personal data revealing racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- The processing of genetic data;
- Biometric data for the purposes of uniquely identifying a natural person;
- Data concerning health or data concerning a natural person's sex life or sexual orientation

Under the GDPR, the processing of special categories of personal data is prohibited unless at least one of the conditions in Article 9 is met. Special categories of data held by the IAP are likely to be limited, if they exist at all.

Where special categories of personal data are proposed to be processed, the relevant conditions must be met before processing commences.

What is processing?

The processing of personal data means an operation or a set of operations which is performed on personal data whether or not by automated means, such as, collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

During processing, personal data can pass through various different companies or organisations. Within this cycle there are two main profiles that deal with processing data:
• The data controller;
• The data processor

Who is the controller?

The controller is the agency which alone or jointly with others, determines the purposes and means of the processing of personal data. The IAP is the data controller and is based in The Hague, the Netherlands in the European Union.

Who is a processor?

A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Some of the work of the IAP is undertaken by external processors. All such processors are required to act only on the instructions of the IAP and are obliged to fulfill their obligations in relation to the use of personal data under the regulation.

The GDPR principles

When personal data is being processed, the following data protection principles must be adhered to:

a) The data shall be processed lawfully and fairly;
b) The data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes;
c) The data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed;
d) The data shall be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
e) The data shall be 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;
f) The data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The lawfulness of processing

Personal data should not be processed unless it is lawful to do so. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose;
b) Contract: the processing is necessary for a contract with the individual, or because they have asked you to take specific steps before entering into a contract;
c) Legal obligation: the processing is necessary for you to comply with the law;
d) Vital interests: the processing is necessary to protect someone's life;

e) Legitimate interests: the processing is necessary for the legitimate business interests of the organisation;
f) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

The IAP uses multiple platforms including database management systems, websites, event registration systems, members only networks and manual systems to hold and process data.

In most instances the IAP collects and uses personal information by relying on the legitimate interest legal basis. When, for example, a member requests services or products from the IAP, the IAP has a legitimate organisational interest to use their personal information to respond and there is no overriding prejudice to the member in using their personal information for this purpose. In some circumstances the IAP will rely on consent for the use of personal information.

Personal data access requests

Any individual whose personal data is being processed by the IAP has a right to know:
- Why the data is being processed;
- The categories of personal data being processed;
- The third parties, if any, to whom data has been disclosed;
- How long the data will be kept by the IAP.

If any individual wishes to know about their personal data, they can make a Subject Access Request. An individual is only entitled to their own personal data, and not to information relating to other people.

Any individual making such a request must provide the IAP Secretariat with such information as is necessary to satisfy the Secretariat of the identity of the individual and to locate any relevant personal data or information.

Where any such request for personal data is manifestly unfounded or excessive the IAP may charge a reasonable fee or refuse to act on the request.

Right to information

The right of access gives individuals the right to obtain a copy of their personal data as well as other supplementary information, which largely corresponds to the information set out in the IAP Privacy Statement on the IAP website.

Right to rectification, erasure and restriction of processing

Under the GDPR individuals have the right to have inaccurate personal data rectified. An individual has the right to request restriction of the processing of their personal data where they contest its accuracy and the IAP is checking it. The IAP can refuse to comply with a request for rectification if it is manifestly unfounded or excessive.

Retention

Personal data should not be kept for longer than it is needed and retention is subject to periodic review by the Secretariat.

Restrictions on the exercise of the data subjects' rights

A controller may restrict, wholly or in part, the exercise of a right of a data subject where certain criteria are met. The restrictions are set out in Chapter III of the GDPR.

Where a controller restricts the exercise of a right of a data subject, the controller shall create and maintain a record in writing of the factual or legal basis for the decision to restrict the right. This record shall be made available to the supervisory body upon request.

The data subject may lodge a complaint with the supervisory body arising out of the decision to apply restrictions to the data subject's rights.

Record of personal data processing activities

A record should be kept of each category of personal data processing activity in line with the requirements of the GDPR. This should be updated and maintained where processing activities change and can be made available to the supervisory body upon request for examination.

Transfers of data to third countries and international organisations

The GDPR primarily applies to controllers and processors located in the European Economic Area (the EEA) with some exceptions.

The EEA countries consist of the EU member states and the EFTA States. The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. The EFTA states are Iceland, Norway and Liechtenstein.

The GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

The work of the IAP occasionally requires the transfer of personal data to a country outside of the EEA. This is referred to as a restricted transfer under the GDPR. A restricted transfer may be made where:

The restricted transfer is covered by an EU Commission adequacy decision. This decision is a finding by the Commission that the legal framework in place in that country, territory, sector or international organisation provides adequate protection for individuals' rights and freedoms for their personal data.

Adequacy decisions made prior to GDPR remain in force unless there is a further Commission decision which decides otherwise. You can view an up to date list of the countries which have an adequacy finding on the European Commission's data protection website.

If there is no adequacy decision about the country, territory or sector, the transfer may still take place subject to appropriate safeguards, which are listed in the GDPR. These appropriate safeguards ensure that both parties involved in the transfer are legally required to protect individuals' rights and freedoms for their personal data.

If the transfer is not covered by an adequacy decision, nor an appropriate safeguard, then the transfer may still take place if it is covered by one of the exceptions set out in Article 49 of the GDPR. These are known as derogations for specific situations and include the data subject explicitly consenting to the proposed transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

Data protection breach

All data protection breaches must be reported to the IAP Secretariat immediately. This includes breaches identified by processors of the IAP.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

The Secretary-General must report a notifiable breach to the supervisory body without undue delay, and not later than 72 hours after becoming aware of it. If notification takes longer than this, the report must give reasons for the delay.

The report must provide a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- a contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Secretariat will inform those concerned directly and without undue delay.

Obligations of IAP staff

All IAP staff should be familiar with the contents of the IAP Data Protection Policy, the IAP Privacy Statement and data protection principles generally. Staff should be aware of their obligations to keep personal data safe, secure, accurate and up to date and to only process personal data for the purpose for which it was obtained in compliance with data protection principles.

IAP staff should take particular care when they remove personal data belonging to the IAP from IAP business premises, ensuring that electronic data is stored on encrypted hardware or encrypted USB key and that paper files are kept secure at all times. When transferring electronic personal data to other parties they should ensure that the methods used are secure and compliant with the GDPR.

IAP staff should comply with any instructions issued in respect of the storage of personal data within the IAP network.

Supervisory body

The IAP Secretariat is based in The Hague and is subject to any relevant national data protection legislation of the Netherlands.

The supervisory body of the Netherlands is:

Autoriteit Persoonsgegevens
Bezuidenhoutseweg 30
PO Box 93374, 2509 AJ Den Haag
Website: https://autoriteitpersoonsgegevens.nl/en