INGRAPH LTD
GDPR POLICY

1 PURPOSE

This policy establishes an effective, accountable, and transparent framework for ensuring compliance with the requirements of the GDPR.

2 SCOPE

This policy applies to all INGRAPH LTD employees and all third parties responsible for the processing of persona data on behalf of INGRAPH LTD.

3 POLICY STATEMENT

INGRAPH LTD is committed to operating the INGRAPH platform in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of INGRAPH LTD employees and third parties in relation to the collection, use, retention, transfer, disclosure, and destruction of any personal data belonging to INGRAPH LTD contact (i.e. the data subject).

Personal data is any information (including opinions and intentions) that relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organizations may process personal data. An organization that handles personal data and makes decisions about its use is known as a Data Controller. INGRAPH LTD, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose INGRAPH LTD to complaints, regulatory action, fines, and/or reputational damage.

INGRAPH LTD leadership is fully committed to ensuring continued and effective implementation of this policy and expects all INGRAPH LTD employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanctions.

3.1. Governance

3.1.1. Data Protection Officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, INGRAPH LTD has appointed a Data Protection Officer. The Data Protection Officer operates with independence and is supported by suitability skilled individuals granted all necessary authority. The Data Protection Officer reports to INGRAPH LTD management board members. The Data Protection Officer's duties include:

- Informing and advising INGRAPH LTD and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of INGRAPH LTD current or intended personal data processing activities;

- Making and keeping current notifications to one or more DPAs as a result of INGRAPH LTD current or intended personal data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing senior management board members and officers INGRAPH LTD of any potential corporate, civil and criminal penalties which may be levied against INGRAPH LTD and/or its employees for violation of applicable data protection laws.

Ensuring the establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides personal data to an INGRAPH LTD service/entity
- receives personal data from an INGRAPH LTD service/entity
- has access to personal data collected or processed by INGRAPH LTD

3.1.2. Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems of the INGRAPH platform or processes, each of them must go through an approval process before continuing. Each INGRAPH LTD service/entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the company management board for review and approval.

3.1.3. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all INGRAPH platform services/entities in relation to this policy, the Data Protection Officer will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with the policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
  - ✓ Raising awareness.
  - ✓ Training of employees.
- The effectiveness of data protection related operational practices, including:
  - ✓ Data subject rights.
  - ✓ Personal data transfers.
  - ✓ Personal data incident management.
  - ✓ Personal data complaints handling.
  - ✓ The level of understanding of data protection policies and privacy notices.
  - ✓ The currency of data protection policies and privacy notices.
  - ✓ The accuracy of personal data being stored.
  - ✓ The conformity of data processor activities.
  - ✓ The adequacy of procedures for redressing poor compliance and personal data breaches. The Data Protection Officer, in cooperation with the company management board will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored, and shared by the INGRAPH LTD management board.

3.2. Data Protection Principles

INGRAPH LTD has adopted the following principles to govern its collection, use, retention, transfer, disclosure, and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, INGRAPH LTD must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means INGRAPH LTD must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed on the INGRAPH platform and for the protection of the platform user's copyrights. This means INGRAPH LTD must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means INGRAPH LTD must have in place processes for identifying and addressing out-of-date, incorrect, and redundant personal data.

Principle 5: Storage Limitation. Personal 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 is processed. This means INGRAPH LTD must wherever possible store personal data in a way that limits or prevents identification of the data subject, without compromising the operation of the platform and legal obligations of the company.

Principle 6: Integrity & Confidentiality. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage. INGRAPH LTD must use appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for, and be able to demonstrate compliance. This means INGRAPH LTD must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3. Data collection

3.3.1. Data Sources

Personal data should be collected only from the data subject unless one of the following applies:

- There are reasonable doubts about the truthfulness of the provide information or if the data is collected under the relevant company AML policy.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent violation of platform user copyrights.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following applies:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of the personal data.
- The data was collected for the purpose of the company AML policy.

3.3.2. Data subject consent

Each INGRAPH LTD service/entity will obtain personal data only by lawful and fair means. Where a need exists to request and receive the consent of an individual prior to the

collection, use, or disclosure of their personal data, INGRAPH LTD is committed to seeking such consent. The Data Protection Officer, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

3.3.3. Data subject Notification

Each INGRAPH LTD service/entity will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following applies:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.3.4. External Privacy Notices

The platform website provided by INGRAPH LTD will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

3.4. Data Use

3.4.1. Data processing

INGRAPH LTD uses the personal data of its contacts for the following broad purposes:

- The general running and administration of the INGRAPH platform services/entities.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

INGRAPH LTD service/entity will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, INGRAPH LTD will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When deciding as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

- In any circumstance where consent has not been gained for the specific processing in question, INGRAPH LTD will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between the data subject and the Data Controller.
- The possible consequences of the intended further processing for the data subject.

3.4.2. Special Categories of Data

INGRAPH LTD will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise, or defense of legal claims.
- The processing is specifically authorized or required by law, including the applicable AML policy of the company.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data, or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question.

3.4.3. Children's Data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility for the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

3.4.4. Data Quality

Each INGRAPH LTD service/entity will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject. The measures adopted by INGRAPH LTD to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
    - ✓ a law prohibits erasure.
    - ✓ erasure would impair the legitimate interests of the data subject.
    - ✓ the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

3.4.5. Profiling & Automated Decision Making

INGRAPH LTD will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorized by law.

3.4.6. Digital Marketing

As a general rule INGRAPH LTD will not send promotional or direct marketing material to an INGRAPH LTD Contact through digital channels such as mobile phones, email, and the Internet, without first obtaining their consent. Any INGRAPH LTD service/entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the data subject must first have it approved by the Data Protection Officer.

3.5. Data Retention

To ensure fair processing, personal data will not be retained by INGRAPH LTD for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which INGRAPH LTD services/entities need to retain personal data is set as 5 years.

3.6. Data Protection

INGRAPH LTD will adopt physical, technical, and organizational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorized alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorized persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorizations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified, or removed without authorization.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on, or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

3.7. Data Subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure. If an individual makes a request relating to any of the rights listed above

INGRAPH LTD will consider each such request in accordance with all applicable data protection laws and regulations.

3.8. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of personal data is necessary for any of the following purposes:

- The prevention or detection of crime or violation of copyrights of the platform user.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.
- Application of money laundering prevention measures.

If INGRAPH LTD processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

3.9. Data Protection Training

All INGRAPH LTD employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training.

3.10. Data Transfers

INGRAPH LTD may transfer personal data to internal or third-party recipients located in another country where that country is recognized as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. INGRAPH LTD may only transfer personal data where one of the transfer scenarios lists below applies:

- The data subject has given consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise, or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

3.11. Complaints handling

Data subjects with a complaint about the processing of their personal data should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through the competent court of Great Britain.

3.12. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail, by calling,

or by using the independent whistleblowing line. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred.

4 ROLES AND RESPONSIBILITIES

4.1 Implementation

The management team of INGRAPH LTD must ensure that all INGRAPH LTD employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, INGRAPH LTD will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by INGRAPH LTD.

4.2 Support, Advice, and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer on _____ or email the Data Protection Officer _____

5 REVIEW

This policy will be reviewed by the Data Protection Officer every three years unless there are any changes to regulations or legislation that would enable a review earlier.

6 RECORDS MANAGEMENT

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognized INGRAPH LTD recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

7 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions, and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures outlined in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

personal data: any information related to a natural person or ‘data subject’, that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Subject Access Right: also, known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

8 RELATED LEGISLATION AND DOCUMENTS

- 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, and repealing Directive 95/46/EC (General Data Protection Regulation)

- The General Data Protection Regulation (**GDPR**) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU.

- UK Data Protection Act 2018 (DPA 2018)