GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

For use in conjunction with GDPR Procedures.

Table of Contents

INTRODUCTION

This document lays out Research4Insights GDPR policy.

PURPOSE

This Policy expresses the strong commitment of Research4Insights to respect and protect the privacy and Personal Data of its employees, suppliers, customers, business partners, Clients, and their respective end customers. This Policy will provide appropriate safeguards when Research4Insights processes Personal Data.

SCOPE

This Policy applies to Research4Insights parent company, related affiliates/subsidiaries, and third parties who process Personal Data on behalf of those entities whenever those entities process Personal Data from Data Subjects who reside in the European Economic Area.

DEFINITIONS

Consent of the Data Subject: Any freely given, specific, informed, and unambiguous indication of will, whereby the Data Subject agrees to the Processing of Personal Data about and/or relating to him or her. Consent shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of the Data Subject by an agent specifically authorized by the Data Subject to do so.

Controller: A person or organization who alone or jointly with others determines the purposes and means of Processing of Personal Data.

Data Subject: An individual whose Personal Data is Processed.

Filing System: Any structured set of personal data which are accessible according to specific criteria, in such a way that specific information relating to a particular person is readily accessible.

GDPR: EU Regulation 2016/679.

Information and Communications System: A system for generating, sending, receiving, storing or otherwise Processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted, or stored and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.

Personal Data: Any information relating to an identified or identifiable data subject who can be identified, directly or indirectly, from that information.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Processor: Any person (other than the staff of the Controller) or organization that Processes Personal Data on behalf of a Controller. A group company that Processes Personal Data for the Controller will be a Processor.

Processing, Process, Processed, or Processes: Any operation or any set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.

Special Category of Personal Data: Refers to Personal Data:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;
2. About an individual's health, education, genetic, or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings.

ENFORCEMENT

Policy Compliance: Research4Insights expects all directors, executives, employees, and agents will comply with this Policy.

Monitoring: Research4Insights ensures that all requirements contained in this Policy are properly implemented by:

1. Providing evidence of compliance on an annual interval to Harsha Vats;
2. Reviewing submitted evidence to determine whether submitted evidence complies with this Policy; and
3. Auditing Steps 1 and 2 at least once a year.

Sanctions: Non-compliance is defined as any one or more of the following:

1. Any act that infringes on this Policy whether by negligence or willful misconduct;
2. Unauthorized Processing of Personal Data;
3. Using hardware, software, communication networks and equipment, or Personal Data for illicit purposes which may infringe local laws or regulations; or
4. Acts exposing Research4Insights to actual or potential monetary loss, regulatory censure, or reputational damage.

Any infringement of this Policy may be treated as serious misconduct. Sanctions may include termination of employment or other contractual arrangement, and civil or criminal prosecution in accordance with applicable laws and regulation.

TRAINING

Research4Insights will provide regular privacy and data protection training to its employees who Process Personal Data or develop tools used to Process Personal Data. Such training will raise awareness about this Policy and requirements contained herein.

GENERAL PRIVACY PRINCIPLES

Generally, the requirements in this section will apply to Research4Insights whenever it Processes Personal Data.

Principles Related to Research4Insights Processing of Personal Data: Whenever Research4Insights Processes Personal Data, Personal Data will be:

1. Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes;
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which the Personal Data is Processed;
4. Accurate and kept up to date when necessary. If Research4Insights retains Personal Data that is inaccurate, and the purpose for gathering the document requires accuracy, Research4Insights will take timely and reasonable steps to erase or rectify the inaccurate Personal Data;
5. Kept in a form which permits identification of Data Subjects for no longer than is necessary when taking into consideration the purpose for which the Personal Data is Processed; and
6. 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, using appropriate technical or organizational measures.

Research4Insights must be able to demonstrate compliance with the six principles above.

Lawfulness of Processing: Research4Insights will only Process Personal Data lawfully. The following lays out the scenarios wherein Processing is lawful:

1. The Data Subject has given consent to the Processing of their Personal Data for one or more specific purposes;
2. Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
3. Processing is necessary for compliance with a legal obligation to which Research4Insights is subject;
4. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Research4Insights; and
6. Processing is necessary for Research4Insights to pursue its legitimate interest. Research4Insights will not rely on this lawful basis for Processing if a Data Subject's interests or fundamental rights and freedoms override Research4Insights legitimate interests.

Determining Whether Processing Exceeds the Initial Purpose for Processing Personal Data: When Research4Insights needs to determine whether additional Processing exceeds the purpose of initial Processing, Research4Insights will weigh the following:

1. Any link between the purpose for collecting Personal Data and the purpose for additional Processing;
2. The context in which the Personal Data has been collected while weighing the relationship between Data Subjects and Research4Insights;
3. The nature of the Personal Data; including, whether the Personal Data is a Special Category of Personal Data or Personal Data regarding criminal convictions;
4. The consequences of additional Processing; and The existence of appropriate safeguards such as encryption or pseudonymization.

Consent: When the purpose for Processing is based on consent, Research4Insights will demonstrate that the Data Subject consented to Processing his or her Personal Data. The consent must be presented by Research4Insights to the Data Subject separate from other matters, in an easily accessible form, and in clear and plain language. Pre-ticked boxes or silence do not constitute valid consent. Research4Insights will allow consenting Data Subjects to withdraw their consent to Process Personal Data at any time in a manner that is as easy to exercise as it was to give consent in the first place. Consent should only be used as a basis for Processing where no other basis is applicable.

Consent from Children: Whenever Research4Insights Processes Personal Data from a Data Subject who is below the age of 16 on the basis of consent, Research4Insights will get consent to Process from such Data Subject's parent or legal guardian. Research4Insights will take reasonable efforts to verify such parent or legal guardian has or holds parental responsibility over the Data Subject.

Processing Special Categories of Personal Data: Research4Insights may Process Special Categories of Personal Data when:

1. The Data Subject has given explicit consent for one or more specified purposes;
2. Processing is necessary for the purposes of carrying out Research4Insights or Data Subject's specific rights for employment, social security, or social protection;
3. Processing is necessary to protect the Data Subject's vital interests or of another natural person where the Data Subject is physically or legally incapable of giving consent;
4. Processing is carried out while engaging in legitimate activities with appropriate safeguards by a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that Personal Data will not be disclosed outside that body without consent from the Data Subjects;
5. Processing relates to Personal Data which the Data Subject made public;
6. Processing is necessary for the establishment, exercise, or defense of legal claims or upon an order from a court;
7. Processing is necessary for a substantial public interest and based on laws in the European Economic Area or its member states' laws;
8. Processing is necessary for preventive or occupational medicine, for assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services based on laws in the European Economic Area or its member states' laws or pursuant to a contract with a health professional. Processing in this instance may be Processed under the responsibility of a professional subject to the obligation of professional secrecy pursuant to laws in the European Economic Area or its member states' laws;
9. Processing is necessary for reasons of public interest in the area of public health; or
10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes pursuant to laws in the European Economic Area or its member states' laws.

These conditions for Processing Special Categories of Personal Data are generally set out in more detail in each EU member state's national laws.

Processing Personal Data Relating to Criminal Convictions and Offences: Research4Insights will only Process Personal Data relating to criminal convictions and offences under the control of an official authority or when Processing is authorized by the laws of the European Union or its member states'.

Processing Which does not Require Identification: If Research4Insights Processes information which does not require the identification of a Data Subject, Research4Insights does not need to maintain, acquire, or Process additional information to identify a Data Subject. If Research4Insights cannot identify a Data Subject, Research4Insights will inform the Data Subject accordingly. In such instances, a Data Subject's right to access, rectification, erasure, restriction of Procession, notification regarding rectification or erasures, and data portability do not apply.

CONTROLLER REQUIREMENTS

Whenever Research4Insights acts as a Controller of Personal Data, the requirements in this section will apply.

General Responsibilities: Taking into account the nature, scope, context, and purposes of Processing Personal Data as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, Research4Insights will implement appropriate technical and organizational measures to ensure and demonstrate that Processing is performed in accordance with the GDPR. Research4Insights will review and update those measures when necessary.

Notice and Transparency Requirement: Whenever Research4Insights Processes Personal Data, it will provide Data Subjects with a notice. Research4Insights will provide this notice at the time they obtain the Personal Data from the Data Subject. If Research4Insights obtains the data from a source other than the Data Subject, Research4Insights will provide this notice to the Data Subject no later than one month after obtaining the Personal Data. Such notice will include:

1. Research4Insights identity and contact details and where applicable, its representative;
2. The contact details for Research4Insights data protection officer, where applicable;
3. The purpose and legal basis for Processing the Personal Data;
4. Where applicable, the legitimate interests pursued by Research4Insights or a third party;
5. Where the Personal Data was obtained from a source other than the Data Subject, the categories of Personal Data;
6. A list of recipients or categories of recipients who receive Personal Data, if any;
7. Where applicable, Research4Insights intent to transfer Personal Data to a third country or international organization and the following:
    a The existence of an adequacy decision by the European Commission, or
    b References to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
8. The period for which the personal data will be stored, or if that is not possible the criteria used to determine that period;
9. The existence of the right to request access to and rectify or erase Personal Data, or restrict Research4Insights Processing of Personal Data;
10. Where Processing is based on consent, the existence of the right to withdraw consent at any time;
11. The right to lodge a complaint with a supervisory authority;

12. Whether the provision of Personal Data is statutory or a contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequence of failure to provide such data;
13. The existence of automated decision-making, including profiling, where decisions are made solely on automated processing and where the decision has a legal effect or similarly significant effect. If either such methods are used to Process Personal Data, Research4Insights will provide the Data Subject with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject; and
14. If Research4Insights intends to Process Personal Data for purposes that extend beyond the initial purpose for Processing Research4Insights will provide the information above before additional Processing takes place.

Where the Data Subject is a child, the notice should be written in clear and plain language that a child will understand.

Data Protection by Design and Default: Research4Insights will, at the time of determining how it will Process Personal Data and at the time of Processing such data implement appropriate technical and organizational measures designed to implement data-protection principles.

Data Protection Impact Assessments: Research4Insights will carry out a Data Protection Impact Assessment prior to any new Processing. Research4Insights will implement appropriate technical and organizational measures to ensure that, by default, only the Personal Data that are necessary for each specific purpose are Processed.

The Data Protection Impact Assessment will ensure Research4Insights:

1. Implements appropriate technical and organizational measures for ensuring, by default, it only Processes Personal Data necessary for a specific purpose. This requirement applies to the amount of Personal Data collected, the extent of Processing, retention periods, and to the Personal Data;
2. Ensures, by default, Personal Data is not accessible without an individual's intervention with a natural person;
3. Describes the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by Research4Insights;
4. Assesses the necessity and proportionality of the Processing operations in relation to its purpose;
5. Assesses the risks to the rights and freedoms of Data Subjects; and
6. Measures the envisaged Processing to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the GDPR.

Wherever a Data Protection Impact Assessment reveals proposed Processing may create a high risk to the rights of Data Subjects in the European Economic Area, Research4Insights will revise the proposed Processing until it no longer creates a high risk to such individuals.

Where a type of Processing that uses new technologies may result in a high risk to the rights and freedoms of natural persons residing in the European Economic Area, Research4Insights will, before Processing, conduct a Data Protection Impact Assessment to assess the impact of the Processing. Research4Insights will seek out the advice of its data protection officer, if applicable, when carrying out the Data Protection Impact Assessment.

While Research4Insights should carry out a Data Protection Impact Assessment prior to any new Processing as outlined above, the Data Protection Impact Assessment is required when:

1. Research4Insights systematically and extensively evaluates personal aspects relating to natural people with an automated Process, including profiling, wherein decisions with legal effects are produced;
2. Processing on a large scale of Special Personal Data or criminal convictions or offenses; or
3. Systematic monitoring of a publicly accessible area on a large scale.

Joint Controllers: When Research4Insights is a Controller with one or more other Controllers, they will determine and document their respective responsibilities for compliance under the GDPR, including when a Data Subject wishes to exercise their privacy rights. Research4Insights must be able to explain the above arrangement to Data Subjects. Data Subjects may exercise their rights against each Controller.

Research4Insights Representatives in the European Economic Area: Research4Insights will designate a representative in a European Economic Area member state. Such representative must be located where at least one of the Data Subject's, whose Personal Data is Processed in relation to the offering of goods or services to them, or whose behavior is monitored, resides.

Purpose Limitation and Data Minimization Requirement: Personal Data must be collected for specific and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later Processed in a way compatible with such declared, specified, and legitimate purposes only.

Personal Data must be Processed fairly and lawfully.

Personal Data must be accurate, relevant, and—where necessary for purposes for which it is to be used—kept up to date. Research4Insights must rectify, restrict Processing, supplement, or destroy inaccurate or incomplete Personal Data.

Research4Insights will only keep Data Subjects' Personal Data so long as it is necessary for the purpose for which the data was originally Processed.

Research4Insights will only keep Personal Data for as long as is necessary:

4. For the fulfillment of the declared, specified, and legitimate purpose, or when the Processing is relevant to the purpose has been terminated;
5. For the establishment, exercise, or defense of a legal claim; or
6. For legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

Research4Insights will dispose or discard Personal Data in a secure manner that prevents further Processing, unauthorized access, or disclosure.

Research4Insights will not keep Personal Data in perpetuity in contemplation of a possible future use yet to be determined.

Research4Insights may keep Personal Data in a form which does not permit identification of Data Subjects for longer than is necessary for a declared, specified, and legitimate purpose.

Processing Procedures Requirement: Research4Insights will implement and review:

1. A procedure for the collection of Personal Data, including procedures for obtaining consent, when applicable;

2. Procedures that limit the Processing of Personal Data to ensure Processing is only to the extent necessary for the declared, specified, and legitimate purpose;
3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems;
4. Policies and procedures for Data Subjects to exercise their rights under local law or regulation; and
5. A data retention schedule, including timeline or conditions for erasure or disposal of records.

Data Quality and Proportionality Requirement: Research4Insights will Process Personal Data in a manner ensuring data quality and appropriate privacy and security safeguards. Inaccurate or incomplete Personal Data must be rectified, restricted from further Processing, supplemented, or destroyed.

Data Processing Contracts: Research4Insights may engage Processors to Process Personal Data on its behalf if:

1. The Processor provides sufficient guarantees to implement appropriate technical and organizational measures to protect the rights of Data Subjects and comply with the GDPR.
2. The Processor agrees not to engage another Processor without prior specific or general written authorization from Research4Insights. In such instances, the Processor must tell Research4Insights about any changes and give Research4Insights an opportunity to object to such changes.
3. Research4Insights and Processor enter into a contract setting out:
    a. What categories of Personal Data will be Processed;
    b. The duration of Processing;
    c. The nature and purpose of Processing;
    d. The type of Personal Data;
    e. The categories of Data Subjects involved; and
    f. Research4Insights rights.

    Such contract must also stipulate that the Data Processor:

    a. Only Processes Personal Data with Research4Insights instructions, including with regard to transfers of Personal Data to a third country or an international organization;
    b. Ensures that persons who will Process Personal Data on the Processor's behalf have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
    c. Implement security measures consistent with the GDPR;
    d. Will apply all the requirements from this section, **Data Processing Contracts**, to other Processors;
    e. Assists Research4Insights when a Data Subject makes a request to exercise his or her rights;
    f. At Research4Insights choice, deletes or returns all Personal Data to Research4Insights when the Processor no longer provides services to Research4Insights; and
    g. Will make available information necessary to demonstrate compliance, and contribute to audits or inspections from Research4Insights or Research4Insights designee. Processor may inform Research4Insights if, in its opinion, an instruction infringes the GDPR or other law from the European Union or one of its member states' laws.

Processing under the Authority of Research4Insights: Processors and any person acting under the authority of the Research4Insights or the Processor, who have access to Personal Data, can only Process data with instructions from Research4Insights.

Record of Processing Activities: Research4Insights, and, where applicable, its representative in the European Economic Area, will maintain records describing its Processing activities. Records will include:

1. Research4Insights name and, where applicable, the name of the joint Data Controller, Research4Insights representative, and Research4Insights data protection officer;
2. Information about the purpose of the Processing of Personal Data, including any intended future Processing or data sharing;
3. A description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data (including statements about whether the Personal Data transfers to a third country or an entity outside the European Economic Area) that will be involved in the Processing;
4. General information about the data flow within the organization, from the time of collection, Processing, and retention, including the time limits for disposal or erasure of Personal Data;
5. The time limits for erasing categories of Personal Data; and
6. A general description of the organizational, physical, or technical security measures in place.

Notifications about Automated Processing: Whenever Research4Insights automatically Processes information and that Processing is the sole basis for making a decision about a Data Subject, and when the decision would produce legal effects or otherwise significantly affect the Data Subject, Research4Insights will provide the following notice.

1. The notification will include the following information:
   a. The purpose for Processing;
   b. Categories of Personal Data to undergo Processing;
   c. Category or categories of Data Subjects;
   d. Consent forms or manner of obtaining consent from Data Subjects;
   e. The recipients or categories of recipients to whom the data are to be disclosed;
   f. The length of time the data are to be stored;
   g. Methods and logic utilized for automated Processing;
   h. Decisions relating to the Data Subject that would be made on the basis of Processed data or that would significantly affect a Data Subject's rights and freedoms; and
   i. The name and contact details for Research4Insights compliance or data protection officer.

Cooperation with Supervisory Authorities: Research4Insights will cooperate, on request and when applicable, with supervisory authorities while administering this policy.

Security of Processing: Research4Insights security program will evaluate, where appropriate, the following:

1. The nature, scope, context, and purpose of Processing; and
2. Risks (such as unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed), varying likelihoods, and severity of an impact on the freedoms of natural persons residing in the European Economic Area should a risk occur.

Research4Insights technical and organizational measures will implement, where appropriate to the risk, the following:

1. Psuedonymization and encryption of Personal Data;
2. The ability to protect the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services;
3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident and
4. A Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of Processing.

Notification of a Data Breach to Supervisory Authorities: In the event of a Personal Data Breach, Research4Insights will—within 72 hours after having become aware of it—notify the appropriate supervisory authority unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons residing in the European Economic Area. If a notification to the supervisory authority is not made within 72 hours, Research4Insights will explain the reason(s) for delay.

Research4Insights notification will at least:

1. Describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and proximate number of Personal Data records concerned;
2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. Describe the likely consequences of the Personal Data Breach; and
4. Describe the measures taken or proposed to be taken by the Research4Insights to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects.

Research4Insights may provide information to supervisory authorities in phases without undue delay.

Research4Insights will document any Personal Data Breaches, list the facts related to it, its effects, and remedial action taken.

Communication of a Personal Data Breach to the Data Subject: When a Personal Data Breach is likely to result in a high risk to the rights and freedoms of a natural person residing in the European Economic Area, Research4Insights will communicate the Personal Data Breach to the Data Subject without undue delay.

The communication to the Data Subject will, in clear and plain language, explain the nature of the Personal Data Breach and:

1. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
2. Describe the likely consequences of the Personal Data Breach; and
3. Describe the measures taken or proposed to be taken by Research4Insights to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects.

Research4Insights is not required to make the communication discussed above if any of the following conditions are met:

1. Research4Insights has implemented appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular those that render the Personal Data unintelligible to any person not authorized to access the Personal Data, such as encryption;
2. Research4Insights has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialize; or
3. It would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby Data Subjects are informed in an equally effective manner.

Data Protection Officer Requirement: Research4Insights will designate an individual or individuals as the data protection officer ("DPO") in any case where:

1. The Processing is carried out by a public authority or body;
2. The core activities of Research4Insights consist of Processing operations which require regular and systematic monitoring of Data Subjects on a large scale; or
3. The core activities of Research4Insights consist of Processing on a large scale either Special Categories of Personal Data or Personal Data related to criminal offenses.

Research4Insights will designate a DPO based on the individual's expert knowledge of data protection laws and practices and their ability to fulfill the tasks in the following section.

Research4Insights may designate a staff member as the DPO, or may fulfill the tasks assigned to the DPO via service contract. If a staff member, the DPO may fulfill other tasks and duties, so long as Research4Insights ensures that these tasks and duties do not result in a conflict of interest. Positions such as CEO or senior roles in IT, Marketing, Finance or Human Resources will likely lead to conflicts.

Research4Insights will publish the contact details of the DPO and communicate those details to the supervisory authority.

The DPO, and his or her agents, or representatives will operate and hold Personal Data under strict confidentiality if the Personal Data is not intended for public disclosure. These obligations will continue even after such person ends their employment with Research4Insights. Research4Insights will incorporate orientation or training programs for such agents or representatives regarding privacy or security policies.

Autonomy of Data Protection Officer: Research4Insights will ensure that the DPO reports directly to the highest management level of Research4Insights and that the DPO does not receive any instruction in exercising the tasks in the following section. The DPO will not be dismissed or penalized by Research4Insights for performing their tasks.

Research4Insights will support the DPO in performing the tasks described in the following section by providing the resources necessary to carry out those tasks, the required access to Personal Data, and opportunities to maintain their expert knowledge.

Research4Insights will ensure that the DPO is involved properly, and in a timely manner, in all issues related to the protection of Personal Data.

Data Protection Officer Tasks: The DPO will be Research4Insights point of contact for all Data Subject issues related to the Processing of Personal Data or the exercise of rights under the GDPR.

The DPO will, at a minimum, perform the following tasks, taking into account the risk of Processing operations and the nature, scope, context, and purposes of Processing:

1. Inform and advise Research4Insights and its employees of their Processing obligations under the GDPR and other European Union or member state data protection provisions;
2. Monitor Research4Insights compliance with the GDPR, EU or member states data protection provisions, and Research4Insights policies in relation to protection of Personal Data. Under this monitoring, the DPO will assign data protection responsibilities, train and raise awareness for the staff involved in Processing operations, and conduct the necessary audits;
3. Provide advice related to Data Protection Impact Assessments, as requested, and monitor the performance of Data Protection Impact Assessments;
4. Cooperate with the supervisory authority(ies); and
5. Act as the contact point for the supervisory authority on issues relating to Processing, and consult with the supervisory authority as required on any other matter.

International Data Transfers Requirements: Research4Insights will ensure that any transfer of Personal Data to a third country outside the European Economic Area or an international organization does not undermine the level of protection guaranteed by the GDPR.

The transfer of Personal Data to a third country or an international organization may only take place where:

1. The European Commission has decided that a third country or organization's protections provide an adequate level of protection (including Privacy Shield);
2. Research4Insights has provided appropriate safeguards and enforceable rights and effective legal remedies are available to Data Subjects;
3. The supervisory authority has approved binding corporate rules; or
4. The GDPR permits a specific exemption. Specific exemptions include:

    a. The data subject has explicitly consented to the transfer;
    b. The transfer is necessary for the performance of a contract between the Data Subject and Controller;
    c. The transfer is necessary for important reasons of public interest; or
    d. The transfer is not repetitive, concerns only a limited number of Data Subjects, is necessary for the purposes of compelling legitimate interests pursued by the Controller, and the Controller has provided suitable safeguards with regard to the protection of Personal Data.

International Data Transfers via Appropriate Safeguards: Research4Insights may only transfer Personal Data to a third country or international organization under this article if Research4Insights provides appropriate safeguards and on the condition that enforceable rights and effective legal remedies are available to Data Subjects.

Appropriate safeguards may be provided by contractual clauses between Research4Insights and the recipient of the Personal Data in the third country or international organization, subject to authorization from the competent supervisory authority.

Appropriate safeguards may also be provided via one of the following:

1. A binding, enforceable instrument between public authorities or parties;
2. Binding corporate rules;

3. The use of standard data protection clauses adopted by the European Commission or the supervisory authority;
4. Use of a code of conduct approved by associations or other bodies representing Processors; or
5. Use of an approved data protection certification mechanisms.

Research4Insights will use contractual or other reasonable means to provide comparable levels of protection of Personal Data while being Processed by a Personal Data Processor or third party.

Research4Insights will designate an individual or individuals who are accountable for its compliance with local privacy laws and regulations. The identity of such individuals will be made known to Data Subjects upon a Data Subject's request.

PROCESSOR REQUIREMENTS

Whenever Research4Insights acts as a Processor, the following Requirements will apply:

Controller-Processor Relationship Requirement: Research4Insights will comply with local privacy laws and regulations, contractual privacy obligations with the Controller, or other legal acts with a Controller.

Processing under the Authority of a Data Controller: Any person acting under the authority of the Research4Insights can only Process data with instructions from the Controller.

Data Processing Contracts: Research4Insights may engage Processors to Process Personal Data on its behalf if:

1. The Processor provides sufficient guarantees to implement appropriate technical and organizational measures to protect the rights of Data Subjects and comply with the GDPR.
2. The Processor agrees not to engage another Processor without prior specific or general written authorization from Research4Insights. In such instances, the Processor must tell Research4Insights about any changes and give Research4Insights and opportunity to object to such changes.
3. Research4Insights and Processor enter into a contract setting out:
    a. What categories of Personal Data will be Processed;
    b. The duration of Processing;
    c. The nature and purpose of Processing;
    d. The type of Personal Data;
    e. The categories of Data Subjects involved; and
    f. Research4Insights rights.

Such contract must also stipulate that the Processor:

a. Only Processes Personal Data with a Controller's instructions, including with regard to transfers of Personal Data to a third country or an international organization;
b. Ensures that persons who will Process Personal Data on the Processor's behalf have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
c. Implement security measures consistent with the GDPR;
d. Will apply all the requirements from this section, **Data Processing Requirements**, to other Processors;
e. Assists Research4Insights when a Data Subject makes a request to exercise his or her rights;
f. At Research4Insights choice, delete or returns all Personal Data to Research4Insights when the Processor no longer provides services to Research4Insights;
g. Make available information necessary to demonstrate compliance, and contribute to audits or inspections from Research4Insights or Research4Insights designee. Processor

may inform Research4Insights if, in its opinion, an instruction infringes the GDPR or other law from the European Union or one of its member states' law.

Cooperation with Supervisory Authorities: Research4Insights will cooperate, on request and when applicable, with supervisory authorities while administering this Policy.

Security of Processing: Research4Insights security program will evaluate, where appropriate, the following:

1. The nature, scope, context, and purpose of Processing; and
2. Risks (such as unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed), varying likelihoods, and severity of an impact on the freedoms of natural persons residing in the European Economic Area should a risk occur.

Research4Insights technical and organizational measures will implement, where appropriate to the risk, the following:

1. Psuedonymization and encryption of Personal Data;
2. The ability to protect the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services;
3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
4. A Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of Processing.

Record of Processing Activities: Research4Insights and, where applicable, its representative in the European Economic Area, will maintain records describing its Processing activities. Records will include:

1. Research4Insights name, Research4Insights representative, and Research4Insights data protection officer;
2. The name, representative and data protection officer of each Controller on behalf of which Research4Insights is Processing Personal Data.
3. Categories of Personal Data being Processed on behalf of each Controller;
4. Whether the Personal Data transfers to a third country or an entity outside the European Economic Area) that will be involved in the Processing and if so the country in question and the safeguards in place; and
5. A general description of the organizational, physical, or technical security measures in place.

Notification of a Personal Data Breach to the Controller: When Research4Insights acts a Processor and it discovers a Personal Data Breach, it will notify the Controller without undue delay after becoming aware of the Personal Data Breach.

Research4Insights notification will at least:

1. Describe the nature of the Personal Data Breach including where possible the categories and approximate number of Data Subjects concerned and the categories and proximate number of Personal Data records concerned;

2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. Describe the likely consequences of the Personal Data Breach; and
4. Describe the measures taken or proposed to be taken by the Research4Insights to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects.

Research4Insights may provide information to Controllers in phases without undue delay. Research4Insights will document any Personal Data Breaches, list the facts related to it, its effects, and remedial action taken.

DATA SUBJECTS' RIGHTS

After verifying a Data Subject's identity, Research4Insights will take appropriate measures to provide any information referred to in this section using concise, transparent, intelligible, and easily accessible form, using clear and plain language.

Research4Insights will provide information when a Data Subject requests to exercise their rights listed in this section without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Research4Insights will inform the Data Subject of any such extension within one month of receipt of the request.

If Research4Insights does not take action on the request of the Data Subject, Research4Insights will inform the Data Subject without delay and at the latest within one month of receiving the Data Subject's request of the reasons for not taking action and inform the Data Subject that they may lodge a complaint with a supervisory authority.

Research4Insights will not charge Data Subjects for receiving information for exercising their rights in this section, but when a Data Subject makes manifestly unfounded or excessive requests, Research4Insights may charge a reasonable fee; or refuse to act on the request.

Right of Access Requirement: Upon the request of a Data Subject, Research4Insights will confirm whether Personal Data concerning the Data Subject is being Processed, and where that is the case, Research4Insights shall give the Data Subject access to their Personal Data and the following information:

1. The purpose of the Processing;
2. Contents of Processed Personal Data and the categories of Personal Data concerned;
3. The recipients or categories of recipients to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organizations;
4. Where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
5. The existence of the right to request from the controller rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;
6. The right to lodge a complaint with the supervisory authority;
7. Where the Personal Data is not collected from the Data Subject, any available information as to its source;

8. The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
9. Where Personal data is transferred to a third country or to an international organization, Research4Insights will inform the Data Subject of the safeguards used to protect the transferred Personal Data;
10. Date when the Data Subject's Personal Data was last accessed and modified; and
11. The designation, name, and address of the Controller.

Research4Insights will provide the information described above to the Data Subject within 30 days of receipt of the request. If, because of the complexity of the request, Research4Insights is unable to comply within 30 days, Research4Insights will inform the Data Subject of the need for an extension within 30 days of receipt of the request. The extension may be for up to two months.

If the Data Subject makes the request by electronic form, Research4Insights will provide the information by electronic means if possible, unless otherwise requested by the Data Subject. Research4Insights will include a copy of the Personal Data undergoing Processing in answering a request.

Rectification Requirement: Research4Insights will allow Data Subjects to rectify inaccuracies or errors in the Data Subject's Personal Data.

The Data Subject also has the right, taking into account the purposes for Processing, to have incomplete Personal Data completed, including by means of providing a supplementary statement.

Research4Insights will suspend, withdraw, or order the blocking, removal, or destruction of the Data Subject's Personal Data from Research4Insights filing system upon discovery and substantial proof that the Personal Data is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes, or are no longer necessary for the purposes for which they were collected.

When the Data Subject's Personal Data is corrected, Research4Insights will allow the Data Subject to access the new and retracted Personal Data and provide the Data Subject with receipts of the new and retracted Personal Data. Research4Insights will communicate any rectification of Personal Data to each third-party recipient to whom the Personal Data has been disclosed. Research4Insights will inform the Data Subject of these third-party recipients if the Data Subject requests it.

Erasure or Blocking Requirement: Data Subjects will have the right to obtain from the Controller the erasure of their Personal Data from Research4Insights filing system without undue delay if one of the following applies:

1. A Data Subject's Personal Data is no longer necessary for the purposes for which that Personal Data was collected;
2. A Data Subject withdraws consent, where Processing is on the basis of consent, or objects to Research4Insights Processing of the Data Subject's Personal Data and where there is no other legal ground for Processing;
3. The Data Subject objects to the Processing on the basis of automated decision making or direct marketing purposes and there are no overriding legitimate grounds for Processing;
4. Research4Insights Processing of a Data Subject's Personal Data is unlawful;
5. The Personal Data has to be erased for compliance with a legal obligation in the European Economic Area or the laws of one if its member states to which the controller is subject;
6. The Personal Data has been collected in relation to the offer of information society services to an individual under the age of 16.

If Research4Insights has made the Personal Data subject to erasure public, Research4Insights shall take reasonable steps, including technical measures, to inform controllers which are Processing the Personal Data that the Data Subject has requested the erasure of any links to or copies of their Personal Data.

Research4Insights will communicate any erasure of Personal Data to each third-party recipient to whom the Personal Data has been disclosed. Research4Insights will inform the Data Subject of these thirdparty recipients if the Data Subject requests it.

Right to Restrict Processing: A Data Subject has the right to restrict Research4Insights Processing if one of the following applies:

1. The accuracy of the Personal Data is contested by the Data Subject, for a period enabling Research4Insights to verify the accuracy of the Personal Data;
2. The Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;
3. The controller no longer needs the Personal Data for the purposes of the Processing; or
4. The Data Subject has objected to Processing on the basis of automated decision making, and the determination of whether the legitimate grounds of the controller override those of the Data Subject is pending.

If Processing is restricted based on one of the above grounds, such Personal Data shall only be Processed with the Data Subject's consent, for the exercise defense of legal claims, for the protection of the rights of another, or for public interests reasons.

If a Data Subject has successfully obtained a restriction to Process their information, Research4Insights will notify the Data Subject before Processing restricted information.

Data Portability Requirement: Data Subjects will have the right to obtain from Research4Insights the Personal Data that they have provided to Research4Insights in a structured, commonly used, and machine-readable format. The Data Subjects will also have the right to transmit this data to another controller without hindrance from Research4Insights.

This data portability requirement only applies if the Processing is based on consent or a contractual obligation and the Processing is carried out by automated means.

Right to Object Requirement: When the legal basis for Processing is for the public interest or necessary for Research4Insights legitimate interests, a Data Subject can object to Research4Insights Processing. Research4Insights will notify Data Subjects of this right to object, at the latest, at the time of their first communication with the Data Subject.

If the Data Subject exercises their right to object, Research4Insights will no longer Process the Personal Data unless they demonstrates compelling legitimate grounds for Processing which overrides the rights of the Data Subject.

Where the Personal Data is Processed for direct marketing purposes, the Data Subject can object at any time. Where the Data Subject objects to Processing for direct marketing purposes, Research4Insights will no longer Process their Personal Data for such a purpose.

Automated Individual Decision-Making, Including Profiling: Data Subjects have the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning the Data Subject. The foregoing does not apply if the decision based solely on automated processing:

1. Is necessary for entering into, or performance of, a contract between Research4Insights and the Data Subject;
2. Is authorized by the European Union or the laws of one of its member states; or
3. Is based on the Data Subject's explicit consent.

When Research4Insights uses automated processing to make a decision, it will implement suitable measures to safeguard the Data Subject's rights and freedoms and preserve the right to obtain human intervention so that Data Subject may contest the decision.

Research4Insights will not use automated processing on special categories unless the Data Subject has provided explicit consent or there is a substantial public interest.

EFFECTIVE DATE

This Policy shall take effect on **05/24/2023**. All previous issuances of this Policy that are inconsistent with the whole or any part of this policy are revoked and superseded.

ADMINISTRATION

This Policy will be administered by Harsha Vats.

Harsha Vats shall retain the right to amend, revoke, withdraw, or nullify the whole or any part of this Policy as it may deem necessary.