

GivingInsight

Data Security and Privacy Policy

Introduction

GivingInsight is committed to protecting the privacy of our clients and their donors. This policy outlines our practices concerning the collection, use, and protection of personal data.

Data Controller

The Trustee for Nourish Analytics Unit Trust ABN 465 0314 8115

Trading as: GivingInsight

Responsible Contact Person

David Pettigrew

CEO and Founder

Address

c/o 43 Fletcher Street

Essendon Victoria, 3040

Australia

Email Address:

info@givinginsight.com

Personal Data Collection

From Client CRMs:

GivingInsight interfaces with our clients' Customer Relationship Management (CRM) systems through an API. The only personal data collected from these systems is a unique identifier number, which is necessary for matching donor/customer records within our system with those in our clients' databases. This unique identifier is used strictly for providing analytics and insights to our clients and is not used for any other purpose.

Direct Collection from Individuals:

For sales, marketing, and customer communication purposes, GivingInsight may collect the following categories of personal data directly from individuals:

- Contact details, such as name, email address, telephone number, and postal address.
- Professional details, such as job title, department, and company name.

- Interaction data, such as email communication responses, website interactions, and feedback provided directly to GivingInsight.
- Account details, for individuals who have created an account with GivingInsight, which may include login credentials and usage data.

This personal data is collected:

- Directly from individuals when they express interest in our services, sign up for an account, subscribe to our newsletters, download content from our website, or engage in communication with us.
- From public sources or third-party services, in accordance with their privacy policies and GDPR compliance.

The data collected is essential for:

- The establishment of a business relationship.
- Providing information on our services and offers.
- Customer account management.
- Responding to inquiries, support requests, or feedback.
- Marketing and sales analysis to improve our service offerings.

Legal Basis for Processing

GivingInsight processes personal data under the following legal bases as defined by the General Data Protection Regulation (GDPR):

For Data Pulled from Client CRMs:

- **Performance of a Contract:** The processing of the unique identifier numbers from client CRM systems is necessary for the performance of the service agreement between GivingInsight and our clients. This processing facilitates the delivery of analytics and insights that our clients use to make informed decisions and strategies regarding their operations.

For Direct Collection from Individuals for Sales and Marketing:

- **Consent:** Individuals have given their clear consent for GivingInsight to process their personal data for specific purposes. These purposes include receiving newsletters, marketing materials, product updates, and other communications. Consent is obtained through explicit opt-in mechanisms, and individuals are informed that they have the right to withdraw their consent at any time.
- **Legitimate Interests:** The processing is necessary for the purposes of the legitimate interests pursued by GivingInsight or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects. Our legitimate interests include:
 - Developing and enhancing our service offerings to provide value to our clients.

- Conducting market research and analysis to understand the market and ensure our services meet client needs.
- Communicating with clients and prospects to provide service information, support, and to maintain our business relationship.
- Improving the user experience on our digital platforms.

For Customer Communication and Account Management:

- **Performance of a Contract:** Processing personal data of clients for account management and support is necessary for the performance of the service agreement and to fulfil our contractual obligations, such as providing customer support and service notifications.
- **Legal Obligation:** Processing personal data may also be necessary for compliance with a legal obligation to which GivingInsight is subject, such as tax laws and other regulatory requirements.

Transparency and Data Subject Rights:

- GivingInsight is committed to ensuring transparency in our processing of personal data. Data subjects are informed about the processing activities and their rights under the GDPR.
- Data subjects have the right to access their personal data, rectify inaccuracies, erase data, restrict processing, object to processing, and exercise their right to data portability.
- Requests to exercise these rights can be directed to GivingInsight's designated contact point, and will be addressed promptly in accordance with GDPR requirements.

GivingInsight will continue to monitor and evaluate our processing activities to ensure they align with the legal bases outlined here and will make adjustments as necessary in response to regulatory guidance, legal precedent, or changes in our business practices.

Data Protection Measures

GivingInsight is dedicated to upholding the highest standards of data security and has implemented comprehensive technical and organisational measures to protect the personal data of our clients and their customers against unauthorised or unlawful processing, accidental loss, destruction, or damage. Our data protection strategy includes but is not limited to the following measures:

Technical Measures:

- **Encryption:** Personal data is encrypted during transit and while at rest using industry-standard encryption protocols to prevent unauthorised access.

- **Access Controls:** Strict access controls are enforced to ensure that only authorised personnel have access to personal data, based on their role and the necessity to access data for the performance of their duties.
- **Data Minimisation:** We adhere to the principle of data minimisation, ensuring that only the data required for specific, legitimate purposes is processed.
- **Regular Audits:** Regular security audits and assessments are conducted to identify and remediate any potential vulnerabilities in our systems.
- **Incident Response Plan:** A well-defined incident response plan is in place, which includes procedures for responding to data breaches or potential data security incidents swiftly and effectively.
- **Secure Development:** Our software development practices include security considerations at every stage of development to ensure that data protection is an integral part of our systems.

Organisational Measures:

- **Data Protection Policies:** Comprehensive data protection policies and procedures govern all our operations and are regularly reviewed and updated.
- **Staff Training:** Regular training on data protection and security is provided to all staff members to ensure they understand the importance of data protection and how to handle personal data securely.
- **Vendor Assessment:** Any third-party vendors or partners are carefully assessed to ensure they meet our data protection standards before any data processing occurs.
- **Data Processing Agreements:** Contracts with clients and third-party service providers include data processing agreements that outline the responsibilities and data protection obligations of each party.

Commitment to Continuous Improvement:

- GivingInsight is committed to continuously improving our data protection measures and staying abreast of the latest security technologies and best practices.
- We engage with data protection experts and IT security professionals to ensure our measures meet or exceed industry standards.

Compliance:

- GivingInsight complies with relevant data protection legislation, including the GDPR, and cooperates with supervisory authorities as required.
- We are prepared to demonstrate our data protection measures to clients and regulatory bodies upon request and provide all necessary documentation to support our compliance efforts.

Our commitment to data protection is at the core of our service delivery, and we take pride in the trust our clients and their customers place in us. GivingInsight's proactive approach to data security ensures that personal data is protected at all levels of our operations.

Data Retention

Data Retention for Client CRM Data:

In accordance with the General Data Protection Regulation (GDPR), GivingInsight adheres to a strict data retention policy to ensure the privacy and protection of personal data. For the data pulled into the GivingInsight platform from our clients' CRM systems, retention is governed by the following principles:

- The data is retained only for the duration of the active agreement between GivingInsight and the client.
- Upon the termination of the agreement, for any reason, all personal data obtained from the client's CRM will be erased or destroyed in a secure manner that renders the data non-retrievable, following a standard and documented data destruction process.
- GivingInsight will also provide clients with confirmation of the data erasure or destruction upon request.
- No copies of the data will be retained by GivingInsight once the agreement has concluded, unless required by law or for legitimate business purposes, such as audit requirements. In such cases, the data will be retained in a secure environment and access will be restricted to authorised personnel only.

Data Retention for Sales, Marketing and Clients:

- Personal data of prospects, clients, and any other individuals that engage with GivingInsight will be retained as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.
- Data used for marketing or communication purposes will be kept until an individual opts out or requests to be removed from our communication lists. When an opt-out request is received, we will remove the individual's personal data from our distribution lists promptly and confirm the removal to the individual.
- We maintain a suppression list to ensure that individuals who have opted out are not inadvertently contacted in the future.
- Personal data that is no longer required will be deleted or anonymised in a secure manner that complies with GDPR requirements.

Review of Data Retention Periods:

- GivingInsight regularly reviews data retention periods and adjusts them where necessary. The criteria used to determine retention periods include the purpose for

which data is collected, legal obligations to retain data for a certain period, statute of limitations for legal claims, and guidelines issued by relevant data protection authorities.

- Clients and individuals will be informed of any changes to our data retention policy through updates to this policy, which will be made available on our website.

GivingInsight remains committed to upholding the data rights of our clients and their customers and adheres to best practices for data retention and destruction to ensure compliance with GDPR and other applicable data protection laws.

Your Rights

Under the GDPR, individuals have rights concerning their personal data, including the right to access, rectify, erase, restrict processing, object to processing, and the right to data portability. Individuals can exercise these rights by contacting GivingInsight directly. We will provide mechanisms for individuals to consent to the processing of their data and to withdraw that consent at any time.

Use of Personal Data

GivingInsight uses the personal data collected from client CRMs and directly from individuals under the following purposes, aligned with the GDPR:

From Client CRMs:

- **Analytics and Insights:** The unique identifier numbers collected from our clients' CRM systems are used solely for matching donor/customer records in our system to those in the client's CRM. This data enables us to provide precise analytics and insights, helping our clients understand the impact of their operations and make data-driven decisions to improve their strategies and activities.
- **Service Improvement:** Data from client CRMs is also used to enhance the functionality and efficiency of GivingInsight's platform, ensuring that our services remain effective and responsive to our clients' needs.

Direct Collection from Individuals:

- **Marketing Communications:** Personal data collected directly from individuals, such as contact details and professional information, is used to send newsletters, promotional materials, and information about new features or services. This communication is aimed at keeping our clients and potential clients informed and engaged with our offerings.
- **Customer Support and Relationship Management:** We use personal data to manage our clients' accounts, respond to inquiries, and provide support. This includes sending important service notifications, assisting with technical issues, and ensuring that our clients receive a high level of service.

- **Market Research and Development:** By analysing interaction data and feedback from users, GivingInsight can improve existing products and develop new services that meet the evolving needs of our market. This research helps us to stay competitive and responsive to industry trends.
- **Sales Initiatives:** Personal data is also used to support sales initiatives, including direct outreach to potential clients. We utilise contact information to initiate discussions regarding our services and to tailor our outreach based on the recipient's professional role and interests.

General Business Operations and Compliance:

- **Legal Compliance:** We process personal data as necessary to comply with legal obligations, such as regulatory requirements, tax laws, and audit necessities.
- **Internal Record-Keeping:** Personal data is used for internal operations, including troubleshooting, data analysis, testing, research, and for statistical and survey purposes, all aimed at enhancing the security and usability of our services.

Data Security and Fraud Prevention:

- **Security Measures:** We use personal data in the monitoring and maintenance of the security of our services, including the prevention of unauthorised access to or use of our systems, and the prevention of potential threats to data security.

Each use of personal data is carefully considered to ensure that it aligns with our legal obligations and the expectations of our clients and their customers. GivingInsight is committed to handling all personal data responsibly and in accordance with the best practices for data protection.

Legal Basis for Processing

Legitimate Interests

GivingInsight processes the unique identifier numbers of donors/customers based on the legitimate interests of our clients to:

- Analyse and understand the effectiveness of their fundraising activities, enabling them to make informed decisions about future initiatives and strategies.
- Enhance the experience of their donors/customers by tailoring their outreach and engagement strategies based on the insights derived from the data.
- Improve the efficiency of their operations by utilising data-driven insights to streamline processes and reduce costs.
- Maintain accurate records of fundraising activities and donor/customer engagement to ensure compliance with other regulatory requirements.
- Conduct internal research and development to improve our service offerings and to introduce new features that benefit our clients.

To safeguard the privacy and rights of the donors/customers, GivingInsight:

- Ensures that the processing is strictly limited to the stated purposes that are necessary for the interests of our clients.
- Implements strict access controls and security measures to prevent unauthorised access to the data.
- Provides clear information to clients regarding the processing activities, ensuring transparency.
- Maintains a minimal data footprint by only processing the necessary data (i.e., unique identifiers).
- Regularly reviews the processing activities to ensure they remain necessary and proportional to the legitimate interests pursued.
- Allows data subjects the opportunity to object to the processing, taking into consideration any objections raised.

Clients are advised to conduct their own balancing tests to confirm that their interests are not overridden by the interests, rights, or freedoms of the data subjects prior to utilising GivingInsight's services.

Data Sharing and Transfer

GivingInsight adheres to strict guidelines regarding the sharing and transfer of personal data, ensuring compliance with GDPR and safeguarding the privacy of our clients and their customers.

Data Sharing:

- **With Third Parties:** GivingInsight does not share personal data obtained from client CRMs or directly from individuals with any third parties, except as explicitly authorised by our clients or as required by law. In cases where client authorisation is given, it will be documented and executed in accordance with the specific terms outlined in our data processing agreements.
- **Contractual Requirements:** Any necessary sharing of data with authorised third parties is conducted under strict contractual terms that ensure the data is processed for limited and specified purposes consistent with the consent provided by the data subjects, and that the confidentiality and integrity of the data are preserved.

Data Transfer to Clients:

- **Client Data Returns:** The only transfers of data are those back to our clients, involving the data initially pulled from their CRMs. This transfer is strictly governed by our service agreements and is performed to fulfill our contractual obligations.
- **Secure Transfer Methods:** When transferring data back to clients, GivingInsight uses secure, encrypted channels to ensure the integrity and security of the data during

transit. We employ industry-standard security measures, such as SSL/TLS, to safeguard data from unauthorised access or breaches.

International Transfers:

- **Within the EU/EEA:** As GivingInsight operates within the EU/EEA, all data transfers occur within this region, adhering to the GDPR regulations without the need for additional safeguards.
- **Outside the EU/EEA:** Should any transfer of data to countries outside the EU/EEA be required, it will only be carried out with the explicit consent of our clients and in full compliance with the GDPR's requirements on international data transfers. This includes ensuring that the country to which data is transferred provides an adequate level of data protection, as determined by the European Commission, or under the protection offered by legally binding and enforceable instruments between public authorities or bodies.

Safeguards for Data Transfers:

- **Data Processing Agreements:** GivingInsight ensures that all data transfers are covered by robust data processing agreements that meet the requirements of the GDPR. These agreements stipulate the responsibilities of all parties involved in the processing of the data and ensure that all parties adhere to the highest standards of data protection.

By strictly controlling the circumstances under which data is shared and transferred, GivingInsight maintains the trust of our clients and ensures compliance with applicable data protection laws. We are committed to transparency and will continue to monitor and adjust our data sharing and transfer practices in response to legal requirements and best practices.

Data Security

At GivingInsight, we prioritise the security of the personal data we handle, both that of our clients and their customers. We implement a range of technical and organisational measures designed to protect data against unauthorised access, alteration, disclosure, or destruction. Our comprehensive data security protocols ensure compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws.

Technical Measures:

- **Encryption:** All sensitive data, including personal data transmitted between our clients' systems and ours, is encrypted using industry-standard encryption technologies such as TLS (Transport Layer Security). Data at rest is also encrypted to prevent unauthorised access.

- **Access Control:** Access to personal data is strictly controlled and limited to employees who need access to perform their job functions. We use robust authentication and authorisation mechanisms to enforce access controls.
- **Data Masking and Anonymisation:** Where possible, data is anonymised or pseudonymised to reduce the risks to the data subjects in the event of a data breach.
- **Security Audits:** Regular security audits are conducted to ensure the effectiveness of our security measures. These audits are performed by both internal teams and external experts to identify and mitigate potential vulnerabilities.
- **Network Security:** Our network infrastructure is protected using firewalls, intrusion detection systems, and anti-malware software to guard against unauthorised access and cyber threats.

Organisational Measures:

- **Data Security Policies:** We have established comprehensive data security policies and procedures that are communicated to all employees. These policies are regularly reviewed and updated to reflect new security practices and technologies.
- **Employee Training:** All employees receive training on the importance of data security and the specific measures they must follow to protect personal data. This training is provided upon hire and periodically refreshed.
- **Incident Response Plan:** We maintain a formal incident response plan to deal with any data security breaches. This plan includes procedures for internal reporting, assessment, containment, and mitigation as well as legal compliance and communication with affected individuals and regulatory authorities.
- **Vendor Management:** We carefully select and monitor third-party service providers who may have access to personal data, ensuring they comply with strict data protection and security standards.

Commitment to Continuous Improvement:

- **Monitoring and Evaluation:** We continuously monitor our data security systems and practices and evaluate their effectiveness. We adapt our security measures in response to new security challenges and technological developments.
- **Feedback Loop:** We encourage feedback from our clients and security experts on our data security practices. This feedback is used to make continual improvements.

GivingInsight is committed to maintaining the highest standards of data security. By implementing these measures, we aim to protect the data integrity and privacy of our clients and their customers, thereby fostering trust and ensuring compliance with applicable laws.

Data Retention

GivingInsight is committed to retaining personal data only for as long as necessary to fulfill the purposes for which it was collected, in accordance with our data retention policies and applicable legal, tax, and regulatory requirements.

Data Retention for Client CRM Data:

- **Client Data:** Data pulled from our clients' CRM systems, such as unique identifier numbers, is retained only for the duration of our agreement with the client. This ensures we provide the analytics and insights necessary for our clients to effectively manage and understand their operations.
- **Post-Contract Data Handling:** Upon termination of a client agreement, all personal data obtained from the client's CRM will be securely erased or destroyed within a predefined period, which will not exceed 30 days, unless legal requirements dictate otherwise. This process includes the secure deletion of any backups containing the data.

Data Retention for Direct Collection from Individuals:

- **Prospect and Client Data:** Personal data collected directly from prospects and clients for sales, marketing, and communication purposes will be retained as long as it is necessary for the continuation of our relationship, for as long as an individual is a user of our services, or until the individual opts out or requests deletion of their data. Following an opt-out or deletion request, personal data will be immediately removed from active systems and any further processing will cease.
- **Compliance and Legal Obligations:** Personal data may also be retained for longer periods if required by tax, audit, and other regulatory requirements, or to protect our interests in the event of litigation or regulatory investigations.

Retention Periods Review:

- **Regular Reviews:** GivingInsight regularly reviews the data retention periods associated with different categories of personal data to ensure they are in line with our operational requirements and legal obligations. Adjustments to these periods are made based on changes in legal requirements, contractual obligations, and our business needs.
- **Minimisation of Data Retention:** We employ data minimisation techniques to ensure that we retain the minimum amount of personal data necessary for our legitimate business purposes and to comply with legal obligations.

Secure Disposal of Data:

- **Data Disposal Procedures:** At the end of the retention period, personal data is securely disposed of using methods that prevent data from being reconstructed or read. This includes the use of certified data destruction methods and secure erasure software for digital data.

GivingInsight's data retention policies are designed to ensure that we meet our legal obligations and manage our operational needs effectively while respecting the privacy rights of individuals. Our commitment to data minimisation and secure data disposal helps to protect the personal data of our clients and their customers against unauthorised access and potential data breaches.

Your Rights

GivingInsight is committed to ensuring that you are fully aware of your rights under the General Data Protection Regulation (GDPR). Here are the rights you have regarding the personal data we process, whether it is obtained from client CRMs or collected directly from you:

Right to Access: You have the right to request access to your personal data that GivingInsight processes. You can ask for copies of your data and for information about how it is being used.

Right to Rectification: If you believe that any personal data we hold about you is incorrect or incomplete, you have the right to request that we correct or complete it.

Right to Erasure ('Right to be Forgotten'): You have the right to request that GivingInsight erase your personal data, under certain conditions, such as when the data is no longer necessary for the purpose for which it was collected, or you withdraw consent and no other legal basis for processing exists.

Right to Restrict Processing: You have the right to request that GivingInsight restrict the processing of your personal data, under certain conditions, such as if you contest the accuracy of the data or have objected to our use of the data, and we are considering whether our legitimate grounds override yours.

Right to Object to Processing: You have the right to object to GivingInsight's processing of your personal data, under certain conditions, particularly if we are processing your data on the basis of legitimate interests or for direct marketing purposes.

Right to Data Portability: You have the right to request that GivingInsight transfer the data that we have collected to another organisation, or directly to you, under certain conditions. This right only applies to data you have provided to us, where the processing is based on your consent or for the performance of a contract, and when processing is carried out by automated means.

Right to Withdraw Consent: Where we rely on your consent to process personal data, you have the right to withdraw that consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

Right to Lodge a Complaint: You have the right to lodge a complaint with a supervisory authority if you believe that our processing of your personal data infringes the GDPR.

How to Exercise Your Rights:

To exercise any of these rights, please contact us using the details provided in this policy. GivingInsight will respond to any requests without undue delay and within one month of receipt. If the request is particularly complex or you have made a number of requests, we may extend this period by a further two months and will inform you of this extension and the reasons for the delay.

GivingInsight takes your privacy seriously and is committed to protecting your rights and handling your data transparently, fairly, and legally. Should you have any concerns about how your personal data is handled, please do not hesitate to get in touch with us.

Changes to This Policy

We may update this policy from time to time by publishing a new version on our website.

Contact Information

If you have any questions about this policy or our treatment of your personal data, please contact us at:

GivingInsight

info@givinginsight.com

Applicable Laws

In the context of this document, "applicable laws" refers to the legal and regulatory requirements that GivingInsight must comply with in relation to the processing of personal data. These include, but are not limited to, the following:

General Data Protection Regulation (GDPR): As a principal regulation, the GDPR governs the processing of personal data of individuals within the European Union. It sets out the principles for data management and the rights of the individual, and provides strict guidelines on how personal data should be processed transparently, securely, and in compliance with the law.

Local Data Protection Laws: In addition to the GDPR, GivingInsight adheres to the specific data protection laws of the countries in which we operate or where our clients and their customers are located. These laws can provide additional requirements and protections beyond those stipulated in the GDPR.

Consumer Protection Laws: Depending on the nature of the services provided by GivingInsight, certain consumer protection laws may apply, particularly those relating to electronic communications, marketing, and transactions.

Cybersecurity Laws: These laws include regulations and standards that apply to the technical and organisational measures we implement to protect personal data against security breaches and cyber threats.

Sector-Specific Regulations: For certain sectors like financial services, healthcare, or education, specific regulatory requirements may govern how personal data related to these sectors must be handled.

International Data Transfer Regulations: When personal data is transferred across borders, especially outside the EU/EEA, international data transfer regulations such as the EU-U.S. Privacy Shield Framework or Standard Contractual Clauses (SCCs) must be complied with to ensure the protection of data outside the European Union.

Employment Laws: When processing employee data, GivingInsight complies with employment laws relevant to the jurisdictions in which it operates, which can dictate how employee data is collected, stored, and processed.

Compliance with Court Orders and Legal Requests: GivingInsight is also bound to comply with law enforcement requests and court orders which might require disclosure of personal data under specific circumstances as dictated by law.

Audit and Record-Keeping Requirements: Various laws require the maintenance of records in a particular manner and for specified durations for accountability and transparency in the event of audits or inspections.

By referring to "applicable laws," we commit to adhering to all these regulatory frameworks, ensuring that data protection practices at GivingInsight are compliant, robust, and up to date. Our policies and procedures are regularly reviewed and revised to align with any changes in these laws, thereby safeguarding the personal data under our stewardship against misuse or unauthorised access.