Global Tuna Alliance – Data Confidentiality and Privacy Policy

version: 1.0

Date: 28 August 2025

Introduction and Purpose

The Global Tuna Alliance (GTA) is committed to protecting the confidentiality of all supply chain data entrusted to us by our partners. This standalone policy outlines how GTA and its partners (retailers and their suppliers) handle confidential supply chain information – including volumes, fisheries, and supplier-specific data – in a secure and legally compliant manner. The purpose of this policy is to ensure all parties understand their obligations and rights regarding data confidentiality, and to foster trust that sensitive business information will be protected at all times. This policy is not tied to any specific contract; it applies broadly to GTA's operations and collaborations with partners across multiple jurisdictions.

Scope and Applicability

Geographical Scope: This policy applies to GTA and all data-sharing partners in the United States, United Kingdom, European Union, and South Africa. We adhere to the data privacy and confidentiality laws and regulations of each of these jurisdictions, including but not limited to the EU's General Data Protection Regulation (GDPR), the UK Data Protection Act (DPA) 2018 (and UK GDPR), the California Consumer Privacy Act (CCPA) in the US, and South Africa's Protection of Personal Information Act (POPIA).

Parties Covered: All GTA employees, contractors, and authorized personnel who process partner data are bound by this policy. Likewise, all partner organizations (retailers and their downstream suppliers) that share data with GTA are expected to understand and respect the confidentiality provisions herein. Third-party service providers who handle the data on GTA's behalf (such as our platform host) are also required to comply with equivalent confidentiality and data protection standards as described in this policy.

Information Covered: This policy covers all supply chain data submitted to GTA by partners or generated through GTA's systems. This includes, for example, sourcing volumes, details of fisheries, supplier identities and performance data, and any associated personal information (such as contact details of partner personnel or suppliers, if provided). All such information is considered "Confidential Information" under this policy. It will be handled with strict confidentiality and in compliance with applicable privacy laws, regardless of whether it is business-sensitive data or personal data relating to identified individuals or entities.

Legal and Regulatory Compliance

GTA recognizes and abides by the key data protection and confidentiality laws in the regions where we and our partners operate. In particular, GTA's data practices are aligned with the following frameworks and requirements:

- EU and UK – GDPR / Data Protection Act: We comply with the GDPR (and the UK's equivalent DPA 2018) which govern how personal data must be collected, processed, and protected. GTA ensures there is a lawful basis for any processing of personal information, such as consent or legitimate interests, and that only data necessary for specified purposes is collected. We uphold principles like transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity/confidentiality as set out in these laws. For example, in line with GDPR requirements, if a data breach involving personal data occurs, GTA will notify the appropriate supervisory authorities (and affected individuals when required) within 72 hours of becoming aware of the breach.

- United States – CCPA (California): For partners or data subjects under the jurisdiction of CCPA, GTA's practices ensure transparency in how personal information is collected, used, and shared. Although the supply chain data we handle is primarily business-related (and often not directly consumer personal data), if any personal information of California residents is included, we will honor CCPA rights such as the right to know, delete, or opt-out of sale (noting that GTA does not sell any personal data). We do not discriminate against any individual for exercising their privacy rights under CCPA. Clear mechanisms are in place for any data subject to contact GTA regarding their data, and our privacy notices will reflect the requirements of CCPA as applicable.

- South Africa – POPIA: GTA complies with South Africa's POPIA when handling personal information of South African partners or individuals. POPIA's conditions for lawful processing (such as accountability, purpose specification, further processing limitation, information quality, openness, security safeguards, data subject participation, etc.) are embedded in our data management processes. Notably, POPIA extends protection to information about juristic persons (companies) as well as natural persons, meaning GTA treats even business supply chain data as confidential information. Any third-party operator processing data for GTA (e.g., our IT contractor) is legally bound to treat personal information as confidential and not disclose it without authorization, and must report data breaches to GTA immediately. GTA in turn will notify the South African Information Regulator and affected parties of breaches as required by POPIA.

GTA constantly monitors changes in privacy legislation and ensures ongoing compliance. All data processing agreements with partners or service providers reflect the requirements of these laws, and where necessary (for example, in cross-border data transfers from the EU), we implement appropriate safeguards such as Standard Contractual Clauses or rely on adequacy decisions to ensure data is protected in transit and storage.

Roles and Responsibilities

To maintain clarity on how confidential data is handled, the following roles and their key responsibilities are defined:

- Global Tuna Alliance (GTA): GTA acts as the data custodian (and in many cases the "data controller" or "responsible party" under data protection law) for the supply chain data collected. GTA is responsible for implementing and enforcing this confidentiality policy across the organization. GTA will determine the purposes for which the data is used (limited to alliance objectives) and ensure compliance with all applicable laws. GTA staff are trained on confidentiality obligations and data protection best practices. All GTA personnel with access to partner data must adhere to strict non-disclosure obligations, using the information only for authorized purposes and protecting it with the utmost care. GTA also designates an Information Security/Data Protection Officer (or equivalent responsible official) to oversee compliance, handle any questions or requests regarding data, and manage incident response including breach notifications.

- Data Partners (Retailers and Suppliers): Each partner providing data retains ownership of their own supply chain information. Partners serve as the source of data and are considered "data subjects" or even co-controllers for certain datasets (particularly where they determine what data to submit). Partners are expected to only share data that they have the right to disclose and that is accurate to the best of their knowledge. They should also comply with any obligations under privacy laws (for instance, providing any required notices to their own staff or suppliers if personal data is included in what they share). Partners have the right to expect that their data will be kept confidential and secure by GTA, and they may request access to or deletion of their data from GTA's systems at any time, consistent with applicable law. Partners also agree not to attempt to access data of other partners and to respect the confidentiality of any aggregated results or reports provided to them through GTA (i.e. not attempt to disaggregate or misuse any information that could be considered sensitive business data of others).

- Web Labs Ltd (Hosting and IT Service Provider): Web Labs Ltd is a UK-based contractor engaged by GTA to develop, host, and support the GTA Partner Dashboard platform. Web Labs acts as a data processor (or "operator" under POPIA) processing data on GTA's behalf. Per our Master Services Agreement, Web Labs is bound by a comprehensive Non-Disclosure Agreement (NDA) and Service Level Agreement (SLA). Under these agreements, Web Labs must: hold all GTA and partner data in strict confidence, not disclose it to any unauthorized party, and use it solely for the purposes of providing the contracted services. Web Labs is required to implement robust security controls (aligned with ISO 27001 standards) including encryption in transit and at rest, access controls, and other measures to safeguard data. Web Labs personnel accessing the data are limited to those with a legitimate need and are themselves bound by confidentiality obligations equal to those of GTA staff. In the event of any security incident or breach on their side, Web Labs must promptly inform GTA so that we can take appropriate action. GTA's contract with Web Labs also affirms that all data processed remains the property of GTA or our

partners (as applicable), and Web Labs has no rights to such data beyond providing the service.

- Other Third Parties: GTA does not routinely share partner confidential data with any third parties besides Web Labs. If in the future GTA engages any additional service providers or advisors who need access to partner data (for example, an analytics consultant or an auditor), such parties will only be engaged under strict confidentiality agreements and with obligations equivalent to those outlined in this policy. They would act only on GTA's instructions and for the limited purposes defined, in line with applicable data protection laws (similar to the role of a data processor). GTA will maintain a list of any such authorized processors and make it available to partners upon request.

Data Collection and Use Practices

Data Collection: GTA collects supply chain data from partners through secure means (e.g., an online portal, encrypted file transfers, or secure forms). The types of data we collect are limited to what is necessary for GTA's mission of improving tuna sustainability and supply chain transparency. This may include data such as: total tuna volumes (by product or species), source fisheries and their locations, certifications or sustainability ratings, details of supply chain participants (like processors or vessels), and related compliance information. Whenever personal data might be incidentally collected (for example, contact names or emails of individuals filling out forms, or names of small supplier businesses considered as juristic persons under POPIA), GTA will collect such data in compliance with consent requirements or other lawful bases and will clearly inform the partner of the purpose at the time of collection.

Purpose of Use: All collected data is used exclusively for the legitimate purposes of the Global Tuna Alliance, namely: to measure and report on progress towards sustainable tuna commitments, to provide partners with insights and benchmarking, and to facilitate collaborative efforts to improve supply chain practices. GTA will not use partner data for any other purpose outside of our stated mission – for example, we do not use or share partner data for commercial marketing, and we do not sell or monetize any partner-provided information. Each party's confidential data will only be used for the benefit of that party and the broader alliance objectives in an aggregated, anonymized manner. In no event will GTA or its contractors use a partner's data for any purpose that is incompatible with the purpose for which it was collected without obtaining the partner's prior written consent. This limitation extends to ensuring that if a new use of the data arises (e.g. a research project or case study), GTA will either anonymize the data or reach out to the partner for permission.

Data Minimization: GTA follows the principle of data minimization under GDPR and similar laws – we request and retain only the minimum data necessary to achieve the intended outcomes. Partners will not be asked to provide irrelevant or excessive data. The data collection forms and templates are designed to avoid collection of sensitive personal data unless absolutely required (currently, GTA does not foresee collecting special categories of personal data). If any such sensitive data is ever collected, it will be handled with additional safeguards per legal requirements.

Confidentiality and Access Controls

Partner data is not accessible to GTA Board members or the Partner Advisory Group (PAG). Access is limited solely to assigned GTA employees and contracted technical service providers with a specific need-to-know basis. This is a deliberate design choice to preserve confidentiality and avoid any perception of competitive or political influence.

Internal Access: Access to confidential partner data within GTA is strictly limited to authorized personnel who need the information to perform their duties. GTA operates on a role-based access control model – for instance, only designated GTA program managers or analysts who work on the supply chain project will have access to the raw data, and then only to the data of the partners that they manage (if applicable). All GTA employees and contractors with access sign confidentiality agreements as part of their employment or engagement terms. They are educated on the importance of protecting partner information and are obligated to handle it with care equivalent to how GTA protects its own confidential business information. Internally, we treat partner data as highly sensitive: it is labeled and stored in restricted-access systems, and any misuse or unauthorized access by an employee is a serious disciplinary matter.

Partner Access: Each data partner will have access to their own data through the GTA portal (or via reports provided to them). Partners will not be able to access other partners' submissions or confidential details. The system is designed with tenant isolation, meaning a retailer can log in and see their data and aggregated benchmarks, but cannot drill down into any other specific retailer's data. This protection is fundamental to our alliance – it ensures that competitive or sensitive information (like exact volumes or sources) remains known only to the providing partner and GTA administrators. Any comparative reports that are shared (e.g., benchmarking performance) will be anonymized and averaged among peer groups so that no individual company is identifiable. For example, a partner might be shown that they are performing in the top quartile of participants on a certain metric, or that "firms of similar size" have certain averages, but no individual company's data point or identity will be disclosed without consent. This approach ensures confidentiality is maintained even in the context of alliance-wide insights.

Third-Party Access: Aside from the partner themselves and authorized GTA staff, the only other party with regular access to the raw data is Web Labs Ltd (the hosting provider) as needed for maintenance and support. Web Labs' access is governed by contractual confidentiality obligations (NDA) that require them to keep all data secret and secure. They operate under GTA's instructions and do not independently access data unless necessary to resolve a technical issue. Any other third-party that might come to handle the data (such as a data backup storage service or cloud provider, if used indirectly by Web Labs) is similarly bound by strong confidentiality and security terms through subcontracting agreements. GTA does not grant access to any government, law enforcement, or regulatory agency unless required by law; if we receive a legal demand for a partner's data, we will notify the affected partner (unless legally prohibited) and will only disclose what is lawfully mandated.

Non-Disclosure Assurance: Every person or entity with access to partner confidential data is required to hold it in strict confidence and not disclose it further. This is reinforced by NDAs, employment agreements, and this policy itself. The obligations of confidentiality continue even if an employee leaves GTA or if the partnership with a company ends, until such information properly enters the public domain through no fault of GTA or until the partner agrees to disclosure. GTA's standard is to apply at least the same degree of care in

protecting partner data as we do for our own confidential information, and in any case no less than a reasonable standard of care in the industry.

Data Sharing and Disclosure Restrictions

No Sharing Between Partners: GTA explicitly guarantees that one partner's supply chain data will never be shared with or disclosed to any other partner without permission. Each partner's data is siloed and confidential. Partners can feel confident that sensitive details like volumes sourced, specific suppliers, or any competitive information will not be divulged to others in the alliance. Even within GTA, as noted, data is handled on a need-to-know basis to further ensure this segregation.

Aggregate Reporting: From time to time, GTA may produce industry-wide reports or aggregate analyses (for example, to highlight overall progress of the alliance or trends in sustainable sourcing). These reports will only use data in an anonymized and aggregated format. No individual company or supplier will be identifiable from such publications. We take care to ensure that aggregation is done in a way that a reasonably knowledgeable person cannot reverse-engineer the identity or value of a single partner's contribution. For instance, we might report "X% of GTA partners have achieved a certain sourcing target" or provide average metrics by region or segment, but we would not publish a list comparing companies by name without their consent. Prior to releasing any aggregated data publicly, GTA will double-check that confidentiality is maintained. If there is any doubt, we will seek consent from the relevant partner(s) before release.

External Disclosure Prohibitions: GTA will not disclose partner-provided confidential data to any external entity except in very limited circumstances: (a) if required by law or legal process (and then only to the extent strictly necessary, and with partner notification where permissible), (b) if the partner explicitly requests or consents to a disclosure, or (c) to the third-party processors under contract as described (who are bound to confidentiality). We do not consider it acceptable to share or sell partner data to consultants, NGOs, other alliances, or any third parties without a clear basis in consent or legal obligation. In the event an external party (e.g., an auditor or funder) requests data for verification or oversight reasons, GTA would either refuse or ensure the data is sufficiently anonymized, unless the partner has agreed otherwise in advance.

Data Processing by Web Labs: Web Labs Ltd's role as a data host has been addressed above, but reiterating here: Web Labs will not share or sub-process the data beyond what is needed to host the platform. They have no ownership or independent rights over the data, and all processing they do is strictly on behalf of GTA and under GTA's control. The SLA in place ensures they maintain uptime and security, but does not grant them any license to use the content of the databases except for fulfilling their service obligations. Web Labs also cannot subcontract any portion of the data handling to another party without GTA's approval, and any approved subcontractor would need to sign equivalent confidentiality commitments.

Data Security and Storage Measures

GTA takes the security of confidential data very seriously. We employ a combination of organizational and technical measures to protect data from unauthorized access, alteration, loss, or disclosure, in line with industry best practices and legal requirements:

- Secure Hosting: All partner data is stored in secure servers managed by Web Labs Ltd in the UK. These servers are protected in certified data centers with strong physical security controls. The hosting environment complies with relevant standards such as ISO 27001 for information security management. This means that formal risk assessments are conducted and controls are in place covering access control, encryption, backup, and network security. The system is also designed with high availability and regular backups to prevent data loss.

- Encryption: Data is encrypted during transmission and at rest. When partners upload data to the GTA portal, Transport Layer Security (TLS) is used to encrypt the data in transit (HTTPS). Within the database and storage, sensitive fields are encrypted at rest so that even if storage media were compromised, the data remains unreadable without proper keys. Encryption keys are managed securely and rotated periodically. Web Labs follows encryption protocols recommended by ISO 27001 and related standards to ensure confidentiality and integrity of data.

- Access Controls: Both GTA and Web Labs enforce strict user access controls. User accounts in the portal have role-based permissions (e.g., a Contributor at a partner can only enter or view certain forms, an Organization Manager at the partner has full access to their organization's submissions, while GTA Portal Administrators have oversight access across the system). Each user's access is protected by strong authentication (unique accounts and passwords, with two-factor authentication enabled where possible). Internally, administrative access to servers or databases is limited to a handful of authorized personnel from GTA's tech team and Web Labs, each using secure login methods. All access to data is logged and audit trails are maintained, so any access or changes to the data can be traced.

- Secure Development and Testing: Changes to the GTA data portal are developed and tested in secure environments. No live confidential data is used in non-production (testing) environments without masking or anonymization. Web Labs as the developer adheres to secure coding practices and the platform is tested for vulnerabilities. Regular security assessments (including penetration tests or vulnerability scans) are conducted to identify and address any weaknesses.

- Monitoring and Prevention: GTA and Web Labs implement monitoring tools to detect unusual activities or potential intrusions. Firewalls, intrusion detection systems, and anti-malware protections are in place to guard the network and systems containing partner data. If any suspicious activity is detected, our teams will investigate immediately and take action to prevent any breach.

- Employee and Contractor Training: Technical measures are complemented by ensuring all people handling the data are trained in data security. GTA conducts periodic training on phishing prevention, secure data handling, and confidentiality obligations. Web Labs similarly trains its staff under its ISO 27001-aligned policies. Only staff who have completed necessary training and have a need-to-know are

granted access to the systems.

- Compliance and Audits: GTA's data handling processes are periodically reviewed to ensure compliance with this policy and legal standards. We may conduct internal audits or engage independent auditors to verify that data is being managed securely and confidentially. Findings from such reviews are used to continually improve our security posture. Partners may request a summary of our security measures or audit certifications, and GTA will provide relevant information (under appropriate confidentiality) to assure partners of our controls.

Data Ownership and Intellectual Property

Each GTA partner retains ownership over the supply chain data that they provide to GTA. By submitting data to GTA, partners are not transferring ownership of that data; rather, they are granting GTA the right to use and process the data for the purposes outlined in this policy and in any participation agreements. GTA acknowledges that partner data may include proprietary information (trade secrets or competitively sensitive details), and partners remain the proprietors of such information.

GTA itself claims no intellectual property rights over raw data contributed by partners. Any aggregated data compilations, analyses, or reports that GTA produces (which combine multiple sources and may include GTA's own intellectual contributions) are owned by GTA only in their aggregated form. However, these aggregated insights will never reveal a partner's confidential information without consent, as stated. If any report or publication were to indirectly allow identification of a partner (even in aggregate), GTA would consider that the partner's data and would not release it without permission.

On the other hand, GTA maintains ownership of the platform and database structure, and any software or methodologies used to collect and process data. The data that partners provide, however, remains their data. Partners are free to use their own data independently of GTA, and may request extraction of their data from the GTA system at any time if needed (for example, to use it for their internal purposes or to verify what GTA has on file).

In summary, data ownership is as follows: each partner owns its submitted data; GTA is a steward and custodian of that data, with a license to use it for alliance objectives; and no party (including other partners, GTA's contractors, or GTA itself beyond the alliance scope) may sell or exploit another partner's data without explicit permission. GTA's agreements with Web Labs and any other processors reinforce that all data is the property of GTA or the partners – service providers have no rights to the information. If a partner leaves the alliance or ceases to participate, their data remains confidential and will be handled per the Retention and Destruction section below.

Data Breach Notification and Incident Response

Despite robust safeguards, GTA acknowledges the possibility of data breaches or security incidents. A "data breach" means any unauthorized access, acquisition, disclosure, or loss of partner data. GTA has an Incident Response Plan that outlines steps to take in the event of a suspected or confirmed security incident. Key points of our breach response and notification protocol include:

- Immediate Containment: Upon detection of a potential breach, GTA (and Web Labs, if the incident occurs on the platform side) will immediately work to contain the incident. This may involve isolating affected systems, revoking compromised credentials, or shutting off certain functions to prevent further unauthorized access. Our first priority is to stop any ongoing data leakage and secure the environment.
- Investigation: GTA will promptly investigate the scope and root cause of the incident. We will determine what data may have been compromised, which partners are affected, and how the incident occurred. Web Labs will assist in this technical investigation if the breach is related to the platform. This investigation is done urgently and thoroughly, leveraging logs, forensic tools, and expert support as needed.
- Partner Notification: If any partner's confidential data is suspected to have been accessed or disclosed by an unauthorized party, GTA will inform that partner without undue delay. We recognize our responsibility to keep partners informed of issues with their data. In line with regulatory requirements (such as GDPR's 72-hour notification rule for personal data breaches), GTA will also notify relevant authorities within the required timeframe when a breach involves personal information. The notification to partners will include information about the nature of the breach, the data concerned (to the extent known), and any immediate steps GTA has taken to mitigate harm. We will also provide recommendations for the partner if any action is required on their side to protect their interests (for example, if credentials need changing or if they need to alert any of their own impacted stakeholders).
- Authority Notification: Depending on the jurisdictions involved and the nature of the data, GTA will handle regulatory notifications. For instance, if EU personal data is affected, GTA (as controller) will notify the relevant Data Protection Authority within 72 hours as required. If South African data is involved, we will notify the Information Regulator and, if necessary, the affected data subjects in accordance with POPIA. Web Labs, as a processor, is contractually required to promptly notify GTA of any breach on their side, and they are aware that GTA must then notify partners and possibly authorities. In the case of US data, if personal information (like certain identifiers) is involved, state breach notification laws (such as California's) may require notices to individuals; GTA will comply with all such laws. We maintain a prepared template and process for notifying all required parties efficiently.

- Remediation and Follow-up: After a breach, GTA will take steps to remediate any vulnerabilities and prevent similar incidents. This may include patching software, changing processes, enhancing monitoring, or providing additional training if human error was a factor. We will also offer support to affected partners – for example, if the breach could lead to any risk for the partner, we will coordinate on public communications or other responses as appropriate. All breaches and near-misses are reviewed by GTA leadership and the security team to learn lessons and strengthen our confidentiality safeguards. Partners will be informed when the incident is fully resolved and any further actions completed.
- Documentation: GTA documents all incidents, responses, and notifications in an internal breach register. This documentation is important for legal compliance and continuous improvement. Partners can request a report on an incident affecting

their data for transparency.

By adhering to these steps, GTA strives to handle any incident responsibly, quickly, and transparently. Our goal is to prevent breaches entirely, but if one occurs, we are prepared to mitigate harm and keep our partners' trust through honest communication and effective action.

Data Retention and Destruction

GTA manages data retention in line with the principle that data should not be kept longer than necessary for the purposes for which it was collected. Our retention and destruction practices are as follows:

- Retention Period: Supply chain data collected from partners will be retained for as long as the partner remains a member of the GTA initiative and the data is needed to fulfill the alliance's objectives. This typically means we keep historical data to allow year-on-year comparisons, trend analysis, and to track progress on sustainability commitments. However, even during partnership, if certain data is no longer needed (for instance, an outdated data field that is phased out), GTA will either delete or anonymize that information. We periodically review the data held to ensure we are not retaining anything beyond its useful life.
- End of Participation: If a partner leaves the alliance or discontinues its participation in the data-sharing program, GTA's policy is to securely delete or return that partner's data upon request. By default, upon a partner exiting, we will archive their data for a short grace period (e.g. 3-6 months) in case the partner reconsiders or for any necessary administrative closure, but we will not actively use it. After that period (or immediately upon the partner's request), the partner's data will be purged from our live systems and backups, or anonymized if retained for statistical aggregate purposes. If the partner prefers the data to be returned to them before deletion, we can export the data and provide it, then proceed to deletion. GTA will provide written confirmation to the partner once their data is fully removed from our systems, as required under our confidentiality commitments.

- Ongoing Programs: For active partners, we retain submitted data throughout the duration of the program to enable longitudinal analysis. In compliance with legal requirements, personal data that is part of the supply chain data (if any) will not be kept indefinitely. We set retention schedules for different categories of data. For example, raw survey/form inputs might be kept for X years, whereas aggregated metrics might be kept longer without personal identifiers. When personal data is no longer necessary, we either delete it or irreversibly anonymize it. Anonymized data (which no longer can be linked to an individual or company) may be retained for research or historical analysis, since confidentiality concerns would no longer apply once data is truly anonymized.

- Secure Destruction: When data is deleted, GTA ensures it is done in a secure manner. For digital records, "secure deletion" means using methods that prevent recovery – e.g., data is permanently erased from databases and any associated files

are expunged or overwritten. Backups are managed such that expired data is also removed from backup storage within a reasonable timeframe. For any physical records (if any were ever printed, though GTA tries to keep everything digital), secure shredding or incineration is used. GTA will document the destruction of confidential data when it occurs, especially for a departing partner's data (providing confirmation as noted). These practices align with obligations to securely destroy confidential information upon request or end of need.

- Legal Holds: If a law or regulation requires GTA to retain certain data for a longer period (for example, if there is an ongoing investigation or if specific records must be kept for audit/tax purposes), GTA will secure the data until the hold is lifted, even if it surpasses normal retention. During such a hold, the data remains protected under this policy and will be destroyed once it is legally permissible to do so.

By enforcing retention limits and secure destruction, GTA reduces the risk associated with storing data longer than necessary and demonstrates respect for our partners' information. Partners may inquire about the retention period for their specific data, and GTA will be transparent in communicating those details.

Accountability and Enforcement

GTA's leadership and all employees are accountable for ensuring that this Confidentiality Policy is followed. The GTA Executive Director (or equivalent roles) oversee the implementation of and compliance with this policy. We have internal procedures and oversight (including board-level oversight if applicable) to enforce these rules. If any GTA personnel or contractor is found to have violated the confidentiality policy – for example, by unauthorized disclosure or mishandling of data – GTA will take appropriate action, which may include disciplinary measures up to termination of employment or contract, and legal action if warranted.

Each partner also has a responsibility to report to GTA if they suspect any misuse of their data or if they become aware of any incident that could indicate a breach. GTA will treat such reports with high priority and investigate as described in the breach section. We encourage an open dialogue with partners on data protection matters – questions or concerns can be addressed to our Data Protection Officer at any time.

This policy is provided to all partners to assure them of our commitments. It is a publicly available document that can be shared with stakeholders to demonstrate GTA's adherence to confidentiality and privacy standards. While this policy itself is not a contract, its provisions may be reflected in binding agreements between GTA and partners. GTA stands behind this policy and will update it as needed to remain current with legal requirements and best practices.

While this policy is standalone, it is directly referenced in the Global Tuna Alliance Charter and forms a binding condition of participation. Partners affirm their agreement to this policy when joining GTA and when accessing the GTA portal.

Policy Review and Updates

This confidentiality policy will be reviewed at least annually, or more frequently if required by changes in law or the scope of GTA's activities. Updates will be made to ensure continuous alignment with the latest data protection regulations and security standards. If material changes are made to the policy (for example, changes that affect how partner data is used or shared), GTA will notify all partners in advance and provide the updated policy. Partners will always have the opportunity to ask questions or seek clarifications on any new policy terms.

By maintaining this policy and keeping it up to date, GTA reaffirms our dedication to safeguarding our partners' sensitive information. We understand that trust is the foundation of our alliance, and we will do everything in our power – legally, technically, and organizationally – to justify that trust by keeping data confidential and secure.

Contact Information

In the event of a concern or suspected breach of confidentiality, partners may contact GTA's Data Protection Officer (DPO) directly at privacy@globaltunaalliance.org. GTA commits to escalating all legitimate concerns to its Executive Director within 24 hours and convening a response review if warranted.

For any questions about this policy, or to report a potential issue, please contact GTA's data protection lead:

Executive Director/DPO – Global Tuna Alliance

Email: privacy@globaltunaalliance.org (for example)

Address:

Transpolispark

Siriusdreef 17-27

Hoofddorp

2132 WT, Netherlands

Partners can reach out to the DPO for requests such as data access or deletion, to obtain copies of relevant data processing agreements, or to discuss any confidentiality concerns. GTA is committed to responding promptly to any such inquiries.