ATNi
NUTRITION
MARKETS
IMPACT

DATA PROTECTION POLICY

February 2026

TABLE OF CONTENTS

1 DATA PROTECTION POLICY

1.1 INTRODUCTION

ATNF is committed to protecting the privacy and security of personal data entrusted to us by our donors, partners, employees, and other stakeholders. This Data Protection Policy outlines our approach to data protection and our commitment to compliance with applicable data protection laws and regulations in all jurisdictions where we operate.

1.2 SCOPE

This policy applies to all personal data collected, processed, stored, or transmitted by ATNF in our operations worldwide, regardless of the format or medium in which it is stored.

1.3 PRINCIPLES

ATNF adheres to the following principles regarding the processing of personal data:

- **Lawfulness, Fairness, and Transparency**: We process personal data lawfully, fairly, and transparently, in accordance with applicable data protection laws and regulations.
- **Purpose Limitation**: We collect and process personal data only for specified, explicit, and legitimate purposes, and we do not process personal data in a manner incompatible with those purposes.
- **Data Minimization**: We collect and process only the personal data that is necessary for the purposes for which it is being processed.
- **Accuracy**: We take reasonable steps to ensure that personal data is accurate, complete, and up to date.
- **Storage Limitation**: **Employee personal data** (such as identification documents, work permits, visa information, payroll and employment records) is retained for up to 7 years, as required by Dutch tax and employment legislation. **Applicant data** (such as resumes and application materials of unsuccessful candidates) is retained for no longer than 12 months, unless a longer retention period is required or consent is obtained.
- **Integrity and Confidentiality**: We have implemented appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data. We use Homerun for job applicants and Creatio as our CRM database.
- **Accountability**: We take responsibility for compliance with this policy and applicable data protection laws and regulations.

1.4 PERSONAL DATA COLLECTION AND PROCESSING

- We collect personal data only for specified, explicit, and legitimate purposes, and we inform individuals of those purposes at the time of collection.

- We collect personal data directly from individuals whenever possible and only with their consent. When collecting personal data from third parties, we ensure that the data was obtained lawfully and that individuals are aware of the processing.
- We process personal data only if one or more of the following conditions apply: the individual has given consent, processing is necessary for the performance of a contract, processing is necessary for compliance with a legal obligation, processing is necessary to protect the vital interests of the individual or other persons, processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or processing is necessary for the legitimate interests pursued by ATNF or by a third party. The purpose of our Privacy Statement is to explain how we collect, use, and protect personal data, ensuring transparency and compliance with relevant data protection laws.
- We do not process sensitive personal data (e.g., information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation) unless one of the specific conditions for processing sensitive personal data applies and appropriate safeguards are in place.
- We provide individuals with clear and transparent information about the processing of their personal data, including the purposes of processing, the categories of personal data processed, the recipients or categories of recipients of personal data, the period for which personal data will be retained, and their rights with respect to their personal data.

1.5 DATA SECURITY

- We implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- We restrict access to personal data to authorized personnel who need to know the information for their duties.
- We ensure that any third party that processes personal data on our behalf (e.g., service providers, contractors) provide sufficient guarantee of compliance with data protection laws and regulations and implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data.

1.6 DATA SUBJECT RIGHTS

We respect the rights of individuals with respect to their personal data, including the right to access, rectify, erase, restrict processing, object to processing, and data portability, as provided by applicable data protection laws and regulations. We provide individuals with mechanisms to exercise their rights with respect to their personal data and respond to requests from individuals in a timely manner and in accordance with applicable laws and regulations.

1.7 DATA BREACH NOTIFICATION

In the event of a data breach, the Head of MEL & Data will assess without undue delay whether the breach is likely to result in a risk to the rights and freedoms of individuals. Where required under the GDPR, we will notify the competent supervisory authority, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If the personal data breach is likely to result in a high risk to the rights and freedoms of affected individuals, we will inform those individuals without undue delay. In addition, for transparency, where we have confirmed that a personal data breach has occurred, Head of MEL & Data may decide to inform affected individuals even where such notification is not strictly required. For more information about how to handle a breach, see Annex 1.

1.8 TRAINING AND AWARENESS

We provide training for our employees - and, when necessary, consultants and service providers - on their responsibilities regarding data protection and privacy. Additionally, we actively raise awareness among our stakeholders about their rights and obligations under applicable data protection laws and regulations.

1.9 COMPLIANCE AND ENFORCEMENT

We monitor compliance with this policy and applicable data protection laws and regulations and take appropriate measures to address any breaches or violations thereof. Employees and service providers who violate this policy or applicable data protection laws and regulations may be subject to disciplinary action, up to and including termination of employment or contract.

1.10 REVIEW AND UPDATE

We review and update this policy annually to ensure it remains accurate, relevant, and effective due to changes to our operations or applicable data protection laws and regulations.

1.11 CONTACT INFORMATION

For questions, concerns, or complaints regarding the processing of personal data by ATNF, please contact ATNF at info@atni.org.

ATNF is committed to protecting the privacy and security of personal data and to complying with applicable data protection laws and regulations. By adhering to the principles and practices outlined in this Policy, we aim to ensure that personal data is processed lawfully, fairly, and transparently, and that individuals' rights with respect to their personal data are respected and upheld.

2 ANNEX: DATA BREACH NOTIFICATION

In case of data breach, it is crucial to follow a structured and prompt response plan to mitigate risks and comply with legal requirements. Here are the necessary steps ATNF will take in the event of a data breach:

2.1 IDENTIFY AND CONTAIN THE BREACH

- Detection: Recognize that a data breach has occurred through monitoring systems, user reports, or notifications from third parties.
- Containment: Immediately contain the breach to prevent further unauthorized access, loss, or damage. This may involve isolating affected systems, changing passwords, or temporarily shutting down certain operations.

2.2 ASSESS THE BREACH

- Scope and impact: Determine the nature and extent of the breach. Identify the data affected, the number of individuals impacted, and the potential harm.
- Data types: Classify the types of data compromised (e.g., personal data, financial information, sensitive personal data).
- Root cause: Investigate the cause of the breach to understand how it occurred and prevent future incidents.

2.3 NOTIFY RELEVANT PARTIES

- Immediate reporting (suspected breaches): Any suspected personal data breach must be reported without delay to the Head of MEL & Data, if unavailable to the Operations Manager. Where there is any doubt, employees must err on the side of caution and escalate the incident.
- Internal notification (confirmed data breaches) inform the Head of MEL & Data and Management about the breach.
- The Head of MEL & Data will lead the investigation and report to the supervisory authority if required and will take the lead in the steps mentioned in paragraph 7 (Post-Breach Analysis).
- When requited, regulatory Notification: Notify the relevant supervisory authority (e.g., the Autoriteit Persoonsgegevens in The Netherlands or the Data Protection Commission in the EU) within the required timeframe, usually within 72 hours of becoming aware of the breach, if it poses a risk to individuals' rights and freedoms.
- Affected individuals: Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms. For transparency, even where a high risk is not strictly identified, the Head of MEL & Data may also choose to notify affected individuals of a confirmed breach. Provide clear information about the breach, its potential impact, and steps they can take to protect themselves.
- Third parties: Inform any third parties, such as partners, service providers, or insurers, as required.

- For low- and medium-risk breaches, the Management Team, decides whether to inform the Board Audit committee.
- For high-risk breaches (i.e., likely to result in a significant impact on individuals' rights and freedoms, regulatory obligations, or the organisation), the Board Audit Committee must be informed; about the breach and the steps taken to address it, and outline measures to prevent similar incidents in the future.

2.4 MITIGATION AND REMEDIATION

- Immediate actions: Take swift steps to mitigate the impact of the breach, such as securing affected systems, removing malicious software, or restoring data from backups.
- Long-Term measures: Address vulnerabilities that led to the breach by updating security protocols, enhancing encryption, and providing additional staff training.
- Policy review and updates: We will review and update this data protection policy and related procedures annually to strengthen our defenses and prevent future breaches.

2.5 DOCUMENTATION

- Record keeping: Document all details of the breach, including the cause, impact, actions taken, and decisions made. This includes maintaining an incident log with timelines and communications.
- Breach report: Prepare a detailed breach report that can be reviewed by internal stakeholders and regulatory authorities if required.

2.6 COMMUNICATION AND SUPPORT

- Staff support: Provide support to affected staff, including guidance on how to protect themselves from potential consequences of the breach (e.g., changing passwords, monitoring credit reports).
- Public Relations: Head of Policy & Communication will take the lead on managing public communication to address any concerns from stakeholders and the media, maintaining transparency and trust.

2.7 POST-BREACH ANALYSIS

- Root cause analysis: Conduct a thorough investigation to understand the root cause of the breach and identify any gaps in security.
- Lessons learned: Analyze the incident to identify lessons learned and areas for improvement.
- Report to Management: Present findings and recommendations to senior management to ensure they are informed and can support necessary changes.

2.8 REGULAR REVIEWS AND DRILLS

- Policy reviews: Regularly review and update this Data Protection Policy.
- Security drills: Conduct regular security drills and simulations to ensure readiness and improve response times for future incidents.
- Regular training: Implement ongoing training programs for staff to stay updated on data protection best practices and emerging threats.
- Third-party risk management: Regularly assess and manage risks associated with third-party vendors and service providers.

DATA PROTECTION POLICY ATTESTATION FORM

To be completed and signed by Staff members, Board, consultants and other stakeholders who have a contractual relationship with ATNF.

[ ] I have reviewed and understood the Data Protection Policy of the Access to Nutrition Foundation and agree to abide by it; (This box must be checked by all.)

Name: _____

Position: _____

Signature: _____

City: _____

Date: _____

ATNi (Access to Nutrition initiative)
Arthur van Schendelstraat 650
3511 MJ Utrecht
The Netherlands
+31 (0)6 429 51 655
info@atni.org
www.atni.org