GAIN DATA PROTECTION POLICY

MARCH 2019

1. INTRODUCTION

The protection of individuals in relation to the processing of personal data is a fundamental right. Whilst data protection legislation is not new in the European Union (the "EU"), the General Data Protection Regulation ("GDPR")[1] has entered into effect on 25th of May 2018. The objective of GDPR is to give citizens more control over their personal data, increase corporate accountability while reducing their reporting burden and strengthen the role of data protection authorities. Even if the seat of the Global Alliance for Improved Nutrition ("GAIN", "We", "Us", the "Foundation") is based in Switzerland (which is not part of the European Union), GAIN shall be GDPR compliant due to the material and territorial scope of application described below. Furthermore, the current Swiss Federal Law on data protection is currently being revised to integrate and implement the requirements of GDPR.

1.1 Material scope (Art 2 GDPR): GDPR applies to the processing of personal data wholly or partly by automated means (i.e. computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or is intended to for part of a filing system.

1.2 Territorial scope (Art 3 GDPR): GDPR will apply to all controllers that are established in the EU who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

GAIN is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations. We hold personal data about our employees, consultants, partners, board members, suppliers and other individuals for a variety of business purposes as detailed in the definition section.

The objective of this Data Protection Policy (the "**Policy**") is to set out how GAIN processes personal data.

2. DEFINITIONS

All terms relevant to the GDPR are defined under Article 4 GDPR.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN

BUSINESS PURPOSES	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include (but is not limited to) the following: • Compliance with our legal, regulatory and corporate governance obligations and good practices. • Provide information to our donors when and to the extent necessary for the purposes of the legitimate interest pursued (i.e. seeking to ensure it is working with appropriately qualified individuals). • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests. • Ensuring business policies are adhered to (such as policies covering email and internet use). • Operational reasons such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking. • Investigating complaints. • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments. • Monitoring staff conduct, disciplinary matters. • Marketing our business. • Improving services.
DATA CONTROLLER [2]	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided by Union or Member State law.
DATA PROCESSOR [3]	Means a natural or legal person, public authority, agency or other bodies which processes personal data on behalf of the controller.
PERSONAL DATA [4] **(ART 14.1)**	Means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data we gather may include individuals' phone number, email address, educational background, financial and payment details, details of certificates and diplomas, education and skills, marital status, nationality, pictures and CV.
PROCESSING [5]	Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
SPECIAL CATEGORIES OF PERSONAL DATA [6]	Include information revealing an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings, and genetic and biometric information — any use of special categories of personal data should be processed in accordance with Article 9 of GDPR.
SUPERVISORY AUTHORITY [7]	This is the national body responsible for data protection. It varies from country to country. • For EU countries, please access the following link: https://edpb.europa.eu/about-edpb/board/members_en • In Switzerland the Federal Data Protection Commissioner will exercise its competencies in the context of the Swiss Federal law.
CONSENT [8]	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has been fully informed of the intended processing and has agreed to it. • Consent given shall be "specific, granular, clear, prominent, opt-in, and properly documented". • Consent shall be freely given and can't be inferred from –a non-response to a communication.

[2] Article 4.7 GDPR

[3] Article 4.8 GDPR

[4] Article 4.1 GDPR

	• The data subject shall have the right to withdraw his or her consent at any time. Such withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.

3. SCOPE

GDPR and the policy focus on processing data pertaining to individuals, not to companies. This policy applies to the personal data pertaining to staff members, individual consultants and members of GAIN's Board and Partnership Council, who must be familiar with this policy and comply with its terms.

Partners and any third parties working with or for GAIN, and who may or may have access to personal data, will be expected to have read, understood and to comply with this Policy.

This Policy is an integral part of GAIN's internal control policy framework and shall be read and applied in conjunction with the GAIN Code of Conduct. It supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time which will be circulated to the persons covered by this Policy.

This Policy will be reviewed regularly.

4. THE PRINCIPLES

All processing of personal data must be conducted in accordance with the data protection set out in Article 5 of the GDPR (the "**Principles**"). GAIN's policies and procedures are designed to ensure compliance with the Principles listed below:

4.1. Lawful, fair and transparent processing

- Lawful [9]: it is possible to satisfy the requirement of "lawful processing" by relying on either consent or the legitimate interest grounds.

  There are also other grounds which may be applicable in some instances – for example, where processing is necessary for compliance with a legal obligation to which GAIN is subject or processing which is necessary for the performance of a contract with the data subject.

  For special categories of data, legitimate interest is not a valid ground for processing and consent would be required unless other more limited grounds are met (such as the public interest). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

- Fair and transparent [10]: for processing to be fair and transparent, GAIN has to provide certain information to the data subject in an intelligible form using clear and plain language.

  GAIN shall maintain a register of all systems in which personal data is processed by the Foundation. The processing purpose will be clearly mentioned in the register.

[5] Article 4.2 GDPR
[6] Article 9 GDPR
[7] Article 4.21 GDPR
[8] Article 7 GDPR
[9] Article 6 GDPR
[10] Articles 12, 13 and 14 GDPR

4.2 Personal data must be processed in a manner that ensures appropriate security of the personal data

Personal data can only be collected for a specific purpose and shall not be used for a different purpose.

4.3 Data minimisation

GAIN shall ensure that any personal data collected from a data subject is adequate, relevant and limited to what is necessary to the purpose of processing.

4.4 Accuracy and kept up to date

- The data we hold must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
- GAIN shall ensure that the data subject covered by this policy is trained in the importance of collecting accurate data and maintaining it.
- The data subjects are responsible for ensuring that the personal data they provide to GAIN is accurate and up-to-date.
- GAIN will review annually the personal data maintained in its register and will identify personal data that is no longer required in the context of the purpose it was collected for in order to delete it.

4.5 Personal data must be kept in a form which permits identification of data subject for no longer than is necessary for the purpose for which it was collected

GAIN cannot store data longer than necessary for the purpose it was collected for. GAIN may keep the personal data for a longer period for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of measures in accordance with GDPR.

4.6 Personal data must be processed in a manner that ensures appropriate security of the personal data

- The personal data we hold will be kept processed securely by means of appropriate technical and organisational measures and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- Access to personal data shall be limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information.
- GAIN shall use encryption and/or pseudonymisation where it is appropriate to do so.
- GAIN shall ensure it has appropriate back-up solutions in place in order to restore access to personal data in the event of an incident.

5. RESPONSIBILITIES

GAIN is a data controller and/or data processor under the GDPR. Where GAIN engages a third party to process personal data (i.e. payroll), an agreement GDPR compliant shall be set up with the supplier/service provider. GAIN must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

5.1 GAIN's responsibilities

- Regularly review the register and only retain personal data relevant to the purpose it was provided for.
- Documenting in a register the type of personal data we hold, the processing purposes and the lawful basis for processing.
- Comply with data protection principles as detailed in section 4.

- Enable the data subjects to exercise their rights as described in section 6.
- Ensure GAIN's staff receives appropriate training on data protection matters.
- Implementing and reviewing procedures to detect, report and investigate personal data breaches.
- Store data in safe and secure ways.
- Assess the risk that could be posed to individual rights and freedoms should data be compromised.

5.2 Responsibilities of GAIN's staff and consultants

- Read the Policy and comply with its terms.
- Check that any data processing activities you are dealing with comply with our Policy and are justified.
- Do not use data in any unlawful way.
- Treat all personal data securely and with care. i.e. lock your computer when you are not at your desk, keep any document containing personal data in a lockable room or cabinet, and use the confidential been to destroy any document containing personal data.
- Do not cause GAIN to be in breach of data protection laws and our policies through your actions.
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

To demonstrate GAIN's commitment to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations, the following steps have been taken:

- The Policy has been approved by the Senior Management Team and the GAIN Board;
- Organised training sessions to educate GAIN staff on their rights and obligations related to data protection
- Appointment of a Data Protection Officer

5.3 Who is responsible for this policy?

Firas Zuhairi, Head of IT/IS
Mobile:+44 7876 889026
Email: fzuhairi@gainhealth.org

Firas Zuhairi, GAIN's Head of IT/IS is appointed to be our data protection officer (DPO) and has overall responsibility for GAIN's data protection compliance and the day-to-day implementation of this Policy. The DPO is supported in his work by a Data Protection Advisory Group comprising the Director of Strategic Operations (Elizabeth Maddison); Legal Manager (Chloe Ribal-Vigneau) and Head of Communications (Nathalie Perroud).

6. RIGHTS OF DATA SUBJECT

Individuals have rights regarding data processing which we must respect a. We must ensure individuals can exercise their rights in the following ways:

6.1 Right to be informed[11]**:** data subjects have the right to be informed about the collection and use of their personal data.

- GAIN must provide individuals with information about how we look after the data we hold on them including the purpose for processing, retention periods, and who it will be shared with ("Privacy Information").
- Privacy Information must be provided in a concise, transparent, intelligible and easily accessible way, free of charge, and shall be written in clear and plain language, particularly if aimed at children.

[11] Articles 13 and 14 GDPR

- If data is obtained from other sources than the data subject, GAIN shall provide an individual with Privacy Information within a reasonable period of obtaining such data, no later than one month. Such communication requirement shall not apply when the individual already has the information or if it would involve a disproportionate effort for GAIN to provide it to the individuals.
- GAIN shall keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

6.2 Right to access[12]**:** the data subjects have the right to obtain from GAIN confirmation as to whether or not personal data concerning him/her has been or is being processed.

- GAIN shall enable individuals to access their personal data.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

6.3 Right to rectification[13]**:** the data subjects shall have the right to obtain from GAIN without undue delay the rectification of inaccurate or incomplete personal data concerning him/her.

- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

6.4 Right to erasure (right to be forgotten)[14]**:** the data subjects shall have the right to obtain from GAIN the erasure of personal data concerning him/her without undue delay and GAIN shall have the obligation to erase such data when:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed.
- Consent is withdrawn.
- The individual objects to processing and there is no overriding legitimate interest for continuing the processing.
- Personal data was unlawfully processed or otherwise breached data protection laws.
- To comply with a legal obligation.
- The processing relates to a child.

GAIN can refuse to delete the data in the following circumstances:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

6.5 Right to restrict processing[15]**:** the data subjects shall have the right to obtain from GAIN a restriction of processing when one of the conditions listed in Article 18 GDPR applies (i.e. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data).

[12] Article 15 GDPR
[13] Article 16 GDPR
[14] Article 17 GDPR
[15] Article 18 GDPR

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6.6 Right to data portability[16]**:** the data subject shall have the right to receive the personal data concerning him/her, which he/she has provided to GAIN, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

- GAIN must provide individuals with their data so that they can reuse it for their own purposes across different services.
- Such right allows the individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- The right only applies to information an individual has provided to GAIN.

6.7 Right to object[17]**:** the data subject shall have the right to object, on grounds relating to his/her particular situation, at any time to processing of personal data concerning him/her which is based on public interest or legitimate interest, including profiling based on those two grounds.

- GAIN must no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, exercise or defence of legal claims.
- GAIN must respect the right of an individual to object to direct marketing, including profiling.
- GAIN must respect the right of an individual to object to processing their data for scientific and historical research and statistics.
- An individual can object verbally or in writing.

6.8 Rights in relation to automated decision making and profiling[18]**:** the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her.

- GAIN must respect the rights of individuals in relation to automated decision making and profiling.
- GAIN can only carry out this type of decision-making where the decision is:
    - necessary for the entry into or performance of a contract; or
    - authorised by Union or Member state law applicable to the controller; or
    - based on the individual's explicit consent.

7. STORING DATA SECURELY

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- The DPO must approve any cloud used to store data.

[16] Article 20 GDPR
[17] Article 21 GDPR
[18] Article 22 GDPR

- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the GAIN's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software.
- All possible technical measures must be put in place to keep data secure.

8. TRANSFERING DATA INTERNATIONALLY

GAIN shall ensure that no personal data is transferred to a country, territory or international organisation outside of the European Union or the European Economic Area (EEA) unless that country, territory or international organisation ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The European Commission has set up a list of countries, territories, one or more sector within a country, or international organisations which have been assessed as procuring an adequate level of protection (the "**Adequacy Decision**") [19]. In the absence of such adequacy decision, GDPR still allows transfers subject to GAIN (as a controller or processor) providing appropriate safeguards listed in Article 46 GDPR, or in the case of derogations for specific situations as described in Article 49 GDPR.

This is a complex issue, and in order to avoid any misunderstanding or complications in the context of international transfers, as well as to allow GAIN to comply with its obligations, GAIN's staff is requested to contact the DPO to get its express permission for international transfers of personal data. The DPO shall record such requests in GAIN's files.

9. REPORTING BREACHES

Any breach of this policy or of data protection laws must be reported as soon as practically possible to the DPO, who will transmit the information to Senior Management Team if he considers it is necessary. GAIN will assess the likelihood and severity of any risk to people's rights and freedoms, following the breach. If the result of the assessment is that there is a risk, GAIN will notify the relevant authority depending on the country where the breach has occurred.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary;
- maintain a register of compliance failures;
- notify the relevant supervisory authority of any compliance failures putting at risk people's rights and freedoms.

Please refer to our DPO for further reporting procedure.

10. FAILURE TO COMPLY

We take compliance with this Policy very seriously. Failure to comply puts both you and GAIN at risk.

Failure to comply with this Policy may constitute a serious disciplinary offence and may lead to disciplinary action under our procedures, including dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

[19] Article 45 GDPR