BUILD UP

DATA PROTECTION POLICY

AUGUST 2022

1. **DEFINITIONS**

Organisations	refers to **How To Build Up, Inc**., a non-profit, non-governmental organisation registered in California, USA (registration #4206324).
GDPR	refers to the EU's General Data Protection Regulation, as codified by the European Parliament in Regulation 2016/679.
DPIA	refers to a Data Protection Impact Assessment which is used to assess the Organisation's GDPR compliance.
Data	refers to all digital information relating to an identified or identifiable natural person (an '**Individual'**) which is pulled from social media and/or other platforms that allows the Organisation to effectively assess, collect, analyse, synthesize, and take action on online engagements and sentiments directly or indirectly related to topics focusing on or derived from peace and conflict within contexts of interest.
Policy	refers to this data protection policy.
Responsible Person	refers to the Organisation's data protection focal point, holding the responsibility for ensuring this policy is complied with. This role will be carried out by the Organisation's Treasurer.

2. **JOINT POLICY**

2.1. In instances where the Organisation is in collaboration with a co-controller of the Data, an MOU between the co-controllers will explicitly define the roles each plays in controlling the Data and ensuring compliance of this Policy. In the case of any internal or external GDPR compliance assessments, including periodic DPIA's that the Organisation will have independently conducted, the MOU between co-controllers will be provided.

3. **POLICY STATEMENT**

3.1. The goal of this Policy is to protect the rights of Individuals, to ensure compliance with the GDPR and to also provide proof of compliance through the enactment and adherence to this Policy by the Organisation.

3.2. The Organisation is committed to processing the Data in accordance with its responsibilities under the GDPR. The (possible) applicability of the GDPR originates from the fact that the Organisation monitors behaviour of Individuals, including Individuals who are in the EU.

3.3. GDPR requires that personal data shall be:

DATA USE & TRANSPARENCY[1]

3.3.1. processed lawfully, fairly and in a transparent manner in relation to individuals;

3.3.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

[1] Headers added to reflect the Organisation's core data protection principles

3.3.3. eligibility determinations are never made about people
3.3.4. the Organization never discriminates or encourages discrimination
3.3.5. the Organization does not use its systems or tools for surveillance

DATA MINIMIZATION & RETENTION

3.3.6. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
3.3.7. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to ensure GDPR compliance, thus safeguarding the rights and freedoms of individuals;

DATA ACCURACY

3.3.8. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; and

DATA SECURITY

3.3.9. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.4. The Organisation has summarized these GDPR requirements into the four data protection principles as described in paragraphs 4-7.

4. DATA USE & TRANSPARENCY

4.1. The Organisation has a legitimate interest in assessing, collecting, analysing, and synthesising the Data, based on its intention to use the Data for the common good, namely objectively understanding conflict and building peace. This will be reflected in each project-defined problem statement in which the Data will be collected.

4.2. The Organisation understands that the processing of Data as described in 4.1 may entail risks for Individuals due to the sensitive nature of the engagements and sentiments posted online. Through the implementation of the data protection principles described in this Policy, the Organisation aims to limit these risks as much as possible while at the same time continue to perform meaningful conflict understanding and peace building efforts.

4.3. The Organisation will ensure that its identity shall be clearly stated with each intervention it engages in where Data will be collected (e.g. by using the https://www.facebook.com/howtobuildup/ account when intervening in an discussion on Facebook).

4.4. The Organisation will ensure transparency when it comes to how and why Data is being collected and how it is being utilized and stored through the publication of a privacy statement on its website.

4.5. Given that notifying each Data source of the intention to use the Data would undermine the intent and constitute a disproportionate or non-possible effort, the Organisation will not typically involve individual Data sources in its transparency commitment except when engaging directly with a source.

5. DATA MINIMISATION AND RETENTION

5.1. The collection of the Data will be minimised to only that which is adequate, relevant and necessary to achieve the objectives of the intervention.

5.2. The retention of personal data will be minimised by aggregating to de-identify (fully anonymise) and then removing the raw data and any personally identifiable data in processed datasets once it has served its purpose but not to exceed the period indicated below.

5.3. Raw Data will be held no longer than 6 months, with exceptional cases extending to no more than 12 months. For exceptional cases, justification for extension of retention of Data shall be articulated in writing with measures that will be taken to ensure the Data remains protected.

5.4. Raw Data will only be retained when there are direct interventions, and even in those cases names and other raw personal datapoints will be replaced with unique codes. These codes will be either reversible (=pseudonymisation) or non-reversible (=anonymisation)*. This will ensure that it is still possible to identify which data belongs to which unique individual, without knowing which individual is linked to the data. Hyperlinks will be checked regularly, and raw data removed if the content behind the hyperlink has been removed. This includes syncing the Data so that if the Individual deletes Data, that Data will automatically be deleted from the data. This will also give effect to Individuals who exercised their rights of erasure or rectification.

5.5. Each employee involved in the collection and/or use of the Data shall be responsible for ensuring the Data retention measures stipulated in this Policy are being adhered to. The twice yearly reviews, and the annual DPIA will assess compliance and instruct on corrective measures if there are failures in adherence with this Policy.

6. DATA ACCURACY

6.1. The Organisation will ensure that Data are accurate and up-to-date.

6.2. The Organisation will ensure that links to original content are retained for as long as the raw Data is retained, checking periodically to ensure the original content has not been altered or deleted. Again, this will give effect to Individuals who exercised their rights of erasure or rectification.

6.3. Whenever possible, the Organisation will only retain the link and not the raw Data.

7. DATA SECURITY

7.1. The Data will be stored in cloud platforms which are equipped with security measures based on the GDPR.

7.2. The Organization will limit access to the Data to only those directly involved in the control and/or processing of the Data. In cases where that includes clients, partners and/or co-controllers, this Policy and compliance with it, will be stipulated in a signed agreement between the Organisation and the relevant entity(ies).

8. CLIENT/STAKEHOLDER ENGAGEMENT

8.1. All clients and/or stakeholders that are engaged in processes using the Data will be briefed in writing about the Organisation's use of the Data, and the relevant aspects of this Policy that will apply.

8.2. Any clients and/or partners that will be processing or co-processing the Data in a GDPR processor role will enter into a Processing Agreement, which can be found in Annex 1 of this Policy.

9. INTERNAL AND INDEPENDENT DPIAs

9.1. Prior to each intervention involving the collection of the Data, the Organisation will conduct an assessment to ensure that the proposed measures for the project are compliant with this Policy.

9.2. For interventions that are ongoing, an assessment of the sources of the Data, including checking that the data sources are still relevant, will be conducted no less than twice per year.

9.3. The Organisation will also carry out an independent DPIA annually.

10. POLICY APPROVAL

10.1. This Policy has been reviewed by the Organisation's Board of Directors. Signature by the Board Treasurer below signifies that this Policy has been approved by the Board of Directors.

Jerry McCann
Board Treasurer

31 Aug, 2022