The purpose of The New Humanitarian’s Internal Privacy Policy ("Internal Privacy Policy"), is to describe how The New Humanitarian ("TNH"), located at rue de Varembé 3, 1202 Geneva, Switzerland, collects, processes and protects personal data of its employees, consultants, freelancers, and job applicants. In addition, this Internal Privacy Policy describes the rules applicable to the processing of such personal data within TNH, which must be observed by:

(i) each employee of TNH
(ii) each consultant who is contracted to work for TNH
(iii) freelancers who have a signed agreement with TNH
(iv) members of the Board
(all of the above are collectively referred to as “TNH Collaborators”).

For the avoidance of doubt, agreements entered into between TNH, on the one hand, and employees, consultants or freelancers, on another hand, shall include reference to this Internal Privacy Policy. Thus, the obligations contained within this Internal Privacy Policy shall be incorporated into such agreements.

It is hereby specified that nothing in this Internal Privacy Policy shall render a consultant and/or a freelancer an employee, agent, representative or partner of TNH and the consultant and/or freelancer shall not represent him or herself as such.

Each contracted employee, consultant and freelancer is required to read this Internal Privacy Policy. Any questions should be addressed to TNH’s data protection officer (“DPO”) at dpo@thenewhumanitarian.org who will provide an appropriate response and guidance.

As a general principle, TNH does not sell personal data to third parties. Communication of such data to third parties may be required only in compliance with the requirements set out in this Internal Privacy Policy.
1. PERSONAL DATA COLLECTED BY TNH

A. Types of Personal Data

1.1. TNH collects personal data, as defined in the applicable EU and Swiss data protection laws, from various categories of people, including job applicants, its employees, consultants and freelancers.

1.2. TNH only collects personal data that is required to fulfill its obligations to each of the above categories of people and some of that personal data may be considered sensitive personal data, as defined in the applicable EU and Swiss data protection laws.

1.3. In terms of sensitive personal data, TNH notably may collect health data of its employees, consultants and freelancers when they travel to high-risk areas. In the course of conducting risk assessments information may be collected regarding racial or ethnic origin, gender identity, and sexual orientation in order to assess and mitigate safety risk, and any information that may arise as a result of a Sanctions/Politically Exposed Persons Watchlist check.

1.4. TNH maintains a register of processing activities.

B. Transparency and Information

1.5. The persons concerned are informed of the collection and processing of their personal data.

1.6. In the context of its activities, TNH may collect and process personal data, including sensitive personal data, either received directly from the concerned individuals themselves, or from a third-party source, e.g. through a Sanctions and Politically Exposed Persons (PEP) Watchlist Screening executed by a third-party provider on TNH’s behalf.

C. Personal Data Collection and Legal Basis for Processing

1.7. Personal data can also be collected from multiple points such as through the TNH website, social media, online meeting platforms, through recruitment processes, through email or when interviews take place. Employee, consultant and freelancer personal data is notably collected through the contracting process, during performance reviews, staff surveys, and through disciplinary discussions.

1.8. Where personal data is collected in relation to a contract, the basis of such processing is the execution of such contract.

1.9. With regards to sensitive personal data, the processing of employees' sensitive personal data is also based on their employment contract, while the processing of consultants’ and freelancers’ sensitive personal data is based on their explicit consent. In the absence of any other legal basis for processing, personal data shall be processed on the basis of the concerned person's consent, which must furthermore be explicit in the event that sensitive personal data is processed.

1.10. Where applicable and in conformity with applicable law, the concerned persons have the right to withdraw their consent to the processing of their personal data, including sensitive personal data, at any moment.
D. Minimization of Personal Data

1.11. In compliance with the minimization principle, TNH collects and stores only personal data which are necessary in relation to the purpose for which the personal data are collected.

2. PERSONAL DATA PROCESSING BY TNH

A. IT Systems

2.1. TNH’s practice is to store and process personal data which it requires for its normal operating activities with its cloud-based service providers, such as Dropbox, Slack, Microsoft Office 365, Google Workspace, Recruitee and Trello, or on its internal website, stored on a server located in the European Union.

B. TNH Collaborators’ Obligations

2.2. TNH follows a “Bring Your Own Device” policy for its employees and consultants. Wherever possible, personal data must only be saved and stored using TNH’s IT service providers, such as Dropbox, Microsoft Office 365, Recruitee, Google Workspace, Slack and Trello.

2.3. TNH may specify at any time devices or software which are not allowed when processing personal data in relation to the performance of professional activities.

2.4. Access by employees and consultants to TNH’s IT services is provided through authorized user ID’s and associated passwords. Rules governing the issue and use of such user ID’s and passwords are specified and maintained in TNH’s internal policies and employees and consultants must comply with these.

2.5. All TNH Collaborators shall segregate any personal data collected and stored for TNH purposes from any of their own private data.

2.6. All TNH Collaborators cannot store personal data related to their professional activities in physical and cloud storage systems others than those provided by TNH.

2.7. All TNH-issued user ID’s and passwords must never be shared with any other person outside of TNH.

3. USE OF PERSONAL DATA BY TNH

A. Use for Internal and Security Purposes

3.1. TNH uses employees’, and to a lesser extent, consultants’ and freelancers’ personal data, for contract management purposes, notably to honor TNH’s remuneration and social security obligations, for administrative personnel management purposes and for the purpose of organizing the work to be executed.

3.2. Personal data can only be used internally (for instance for statistical purposes) if the anticipated use meets the purpose for which the personal data has been collected or if the data has been appropriately anonymized.
3.3. TNH may also, on the legal basis of its legitimate interest, use personal data if necessary for security purposes, to investigate possible fraud or other violations of this Internal Privacy Policy and/or attempts to harm other owners of personal data.

B. Sanctions and Politically Exposed Persons (PEP) Watchlist Screening Information

3.4. For job applicants applying to work at TNH as either an employee, consultant or freelancer, TNH conducts a Sanctions and Politically Exposed Persons (PEP) Watchlist Screening with a third-party provider, NameScan, based in Australia, which is conducted prior to the signature of a contract. TNH conducts such screening of job applicants in order to comply with its contractual obligations with private foundations and governmental donors. The legal basis for such processing is TNH’s legitimate interest, and in the case of potential employees, the legal provision of art. 328b of the Swiss Code of Obligations.

C. TNH Collaborators’ Obligations

3.5. All TNH Collaborators shall use only personal data that are necessary in relation to the tasks he or she is responsible for and for the purpose for which the personal data are collected. These purposes must comply with this Internal Privacy Policy.

3.6. With regards to the Sanctions and Politically Exposed Persons (PEP) Watchlist Screening conducted in relation to candidates, TNH will uphold the highest standards of data protection and confidentiality when processing the information resulting from such screening. Thus, members of TNH responsible for conducting the screening will notably: (i) only disclose screening information with relevant individuals directly involved in the recruitment and/or due diligence process, and (ii) any exchange of the screening information through email or other electronic correspondence shall be anonymized and/or encrypted. Once the result of the screening has been evaluated and the relevant decision to retain the candidate, or not, has been taken, such result is deleted.

4. ACCESS TO PERSONAL DATA BY THIRD PARTIES

A. Contractual Partners and Cross-Border Transfers of Personal Data

4.1. In order to conduct its normal operational activities, TNH may share personal data of its contracted employees, consultants and freelancers with 3rd party service providers, such as IT services, insurance companies (e.g. for travel or pension fund contributions), Employer of Record Providers and other companies located in or outside Switzerland and/or the European Union (EU).

4.2. TNH will only share such personal data with 3rd parties who are subject to the same personal data protection laws in Switzerland and the EU. To the extent that TNH shares data with contracted 3rd parties who are not subject to Swiss or EU data protection laws, and which do not have an adequate level of protection of personal data compared with that provided in Switzerland or the EU, TNH seeks to enter into the appropriate contractual agreements with such 3rd parties, which ensure an adequate level of protection of the personal data, including sensitive personal data.

B. Legal Disclosures

4.3. It is possible that TNH will need to disclose personal data of those covered by this policy when required by law, such as with government social security and taxation authorities, or if that disclosure is necessary to (i) investigate, prevent, or take action regarding suspected or actual illegal activities or to assist government enforcement agencies; (ii) enforce agreements with third-parties such as providers, (iii) investigate and defend itself against any third-party claims or
allegations, (iv) protect the security or integrity of its IT systems (such as by sharing with companies facing similar threats); or (v) exercise or protect the rights and safety of personnel, or others.

4.4. TNH will notify those concerned about any legal demands for their personal data when appropriate and technically feasible, unless prohibited by law or court order or when the request is for an emergency.

5. MANAGEMENT OF PERSONAL DATA BY TNH

A. Protection of Personal Data

5.1. TNH shall implement the appropriate technical and organizational measures to guarantee the integrity of the personal data and appropriate access to such data. Sensitive personal data is notably stored separately with further restricted access.

5.2. TNH shall exercise all commercially reasonable efforts to prevent unauthorized exposure or disclosure of personal data. TNH implements and maintains technical and organizational measures for managing unauthorized disclosure or exposure of personal data, particularly sensitive personal data.

5.3. In the event of unauthorized exposure or disclosure of personal data (i.e. a data breach), TNH will (i) make best efforts to promptly notify the people concerned, where legally required and technically feasible, and (ii) cooperate with them to investigate and resolve the data breach, including without limitation by providing reasonable assistance to them in notifying any 3rd parties who may have been adversely impacted. TNH will give them prompt access to such records related to a data breach as them may reasonably request; provided such records shall be TNH’s confidential information, and TNH shall not be required to provide them with records belonging to, or compromising the security of, other users.

5.4. In the event of a data breach, or in the event that TNH suspects a data breach, TNH will in addition notify the competent authorities in accordance with applicable law.

TNH Collaborators’ Obligations

5.5. In the event a TNH Collaborator suspects a data breach, he or she must inform the TNH Data Protection Officer immediately.

5.6. All TNH Collaborators shall exercise all reasonable efforts to prevent unauthorized exposure or disclosure of personal data and assist TNH in case of a data breach.

B. Access to and Correction of Personal Data, and Opposition to Processing

5.7. Whilst TNH will make reasonable efforts to ensure that all personal data, including personal data of all contracted employees, consultants and freelancers remains accurate and up-to-date, any contracted employee, consultant or freelancer may request changes to their personal data to the TNH DPO who will ensure that any such change is acted upon whilst ensuring any contractual obligations are maintained.
5.8. All persons concerned (including employees, consultants and freelancers) may object to the processing of the personal data if such processing is based on public interests or TNH’s legitimate interests. Such objection may be raised by sending an email to the TNH DPO.

**TNH Collaborators’ Obligations**

5.9. Should any TNH Collaborator receive a request for access to or change of personal data other than their own, he or she shall immediately inform the TNH DPO.

5.10. All TNH Collaborators shall take reasonable steps to ensure that personal data is kept accurate and up-to date for the purposes for which it was collected.

C. **Retention of Personal Data**

5.11. TNH retains personal data as long as these data are required to meet the purposes for which they have been collected and in order to comply with any legal or accounting obligations.

D. **Deletion of Personal Data, Restriction of Processing and Data Portability**

5.12. Every person concerned may request the deletion of his or her personal data at any time, provided that these data are no longer required in relation to the performance of contractual obligations and subject to any retention obligations imposed on TNH.

5.13. Upon request made within 30 days after the request for deletion of personal data, TNH will make the personal data available to the person concerned for export or download in a commonly accepted format. TNH remains free not to accept any specific format required by the person concerned for the export or download of his or her personal data or to accept any such format at his or her cost.

5.14. After such 30-day period, TNH will have no obligation to maintain or provide any personal data, and will thereafter delete or destroy all copies of the personal data in its systems or otherwise in its possession or control.

5.15. TNH may retain de-personalized (anonymous) information after the deletion of personal data.

5.16. In accordance with applicable law, the persons concerned may request that the processing of their personal data be restricted.

5.17. In accordance with applicable law, the persons concerned may also request to receive the personal data which they provided to TNH, from TNH in a structured, commonly used and machine-readable format, and/or may request that such personal data be transferred directly from TNH to another data controller (as defined by the applicable data protection laws).

**TNH Collaborators’ Obligations**

5.18. In the event that a TNH Collaborator receives a request for deletion, restriction of processing or data portability, they will immediately inform and transfer the request to the DPO.

6. **AMENDMENT OF THIS INTERNAL PRIVACY POLICY**
6.1. TNH may change this Internal Privacy Policy at any time and without prior notification by making available the revised version of this Internal Privacy Policy through appropriate channels.

6.2. The new version will become effective on the date it is posted, which will be listed at the top of the Internal Privacy Policy as the new effective date.

7. QUESTIONS AND COMPLAINTS

7.1. Should an employee, consultant, or freelancer have any questions or complaints in relation to the present Internal Privacy Policy, they can contact the TNH DPO at the email address provided at the beginning of the Internal Privacy Policy. They can equally reach TNH by post, at The New Humanitarian, rue de Varembé 3, 1202 Geneva, Switzerland.

7.2. Employees, consultants or freelancers also have the right to lodge a complaint with the competent supervisory authority, should they consider that the personal data is not processed in accordance with the present Internal Privacy Policy or in compliance with applicable laws.