STOCKHOLM

INFORMATION SECURITY STANCE

CYBER SECURITY WHITE PAPER

This document summarises the STOCK of Humanitarian Organisations Logistics Mapping (STOCKHOLM) platform's Information Security and Privacy programs and policies. This document is to inform users and organisations interested in the platform, about the way in which we protect our systems and data.

DATA SECURITY AND PRIVACY INFORMATION

HOSTING

Tonkin + Taylor Group (T+T) are project developers, developing the application, named STOCKHOLM, for German NGO Welthungerhilfe (WHH). The STOCKHOLM platform is hosted via WHH's Microsoft Azure cloud platform. All data resides in the WHH Azure tenancy.

There are two hosting servers, one located in France and the other in Germany. As with all Microsoft Azure data centres, these are ISO27001 certified. T+T does not physically store any data captured via the STOCKHOLM platform at their premises.

All data is transmitted utilising HTTPS using TLS 1.2.

SECURITY AND PRIVACY PROGRAM DETAILS

The STOCKHOLM platform adheres to the General Data Protection Regulation (GDPR), Europe's data privacy and security law.

Key aspects of how the platform adheres to the GDPR include the following.

Lawfulness, fairness and transparency

- All data is processed in a lawful, fair and transparent manner, as laid out in the Terms of Use and Privacy Policy.

Purpose limitation

- Data is only processed for the legitimate purposes specified in the Terms of Use. All users must agree to these terms to access the platform.

Data minimisation

- Only the data necessary for the purposes specified in the Terms of Use is collected and processed.

- If users wish to opt out and request their profile be deleted, then their personal information is permanently removed from the system.

Accuracy

- Notification systems are in place to assist users and humanitarian organisations in identifying data that has not been updated recently to encourage accurate data collection in the platform.
- User login dates are tracked to allow regular deletion of inactive users after a series of escalated notifications if the inactivity continues.

Storage limitation

- Personally identifying data is kept to a minimum and is only stored for as long as necessary for the purposes laid out in the Terms of Use and Privacy Policy. The databases are encrypted to GDPR standards. Personal identification data is not available to any users other than the relevant Super Admins and Admin Geographical Area users within their own Organisation.
- Only registered users who have accepted the Terms of Use and Privacy Policy can access the platform. There is an approval process managed by administrative members of the platform to maintain oversight of users granted access and check validity of registrations.

Integrity and confidentiality

- Data processing on the platform uses encryption to ensure appropriate security, integrity and confidentiality as per the Privacy Policy.

Additional information

As the company powering the STOCKHOLM platform, T+T has an established security program which is aligned to the NIST Cybersecurity Framework. The framework allows T+T to reduce business risk by enacting controls across six key areas: Govern, Identify, Protect, Detect, Respond and Recover. The NIST framework is one of a number of broadly equivalent Cybersecurity standards, including ISO27001, NZISM, Australian ISM, and to a lesser extent the more basic Australian “Essential 8”. T+T is audited internally and externally on a regular basis to ensure the framework is successfully implemented.

SECURITY CONTROLS

The following controls are currently used to maintain information security and privacy:

- Enforcing all users agree to the Terms of Use and Privacy Policy before being granted access to the website.

- An approval process for new user registrations (administrators have to approve new users allowing the opportunity to first follow up if the email address, job role, reasons for requesting access, or connection to the humanitarian sector are uncertain).
- All Azure portal accounts are Multi-Factor Authentication enabled.
- Microsoft and Google authenticator are used to secure logins. As a result, STOCKHOLM does not store passwords and shared accounts are not permitted.
- Data encryption for encryption and decryption:
  - Advanced Encryption Standard (AES) and base64 encoding, as used by the US government to protect classified information.
- Independent penetration testing every 12-24 months by certified third parties to check for any data security risks or improvements that can be made.
- Maintenance and use of a User Acceptance Testing (UAT) environment to test any coding changes or platform upgrades independently of the Live database and users.
- Deployment processes for any new developments on the platform to ensure stringent testing is completed prior to deploying new features or updates.
- Contractual terms with all developers and contractors that work on the platform, covering compliance and adherence to all relevant policies, processes and procedures for:
  - Information security
  - Data governance, and
  - Privacy.
- Processes and procedures to ensure that security incidents are discovered in a timely manner and dealt with effectively. Logs of suspicious activities are reviewed through Azure Insights and T+T also has its own separate monitoring system.
- Regular internal review of security threats the platform could be exposed to, and consideration of these factors with all new feature developments.
- A change management process to ensure that all changes to networks, systems, and processes are appropriately reviewed.
- Azure Front Door is used for security and traffic management.

- Policies are updated to reflect changes in processes and security requirements on a regular basis, annually by T+T with independent third-party audits.

SECURITY AND PRIVACY POLICIES, STANDARDS AND FRAMEWORKS

T+T security and privacy policies include:

- An overarching Information Security policy
- Privacy policy
- Data Governance, classification and handling standards
- IT user standard (IT Acceptable use)
- Asset and Vulnerability Management
- Identity and Access management
- Device Configuration and Management standard
- Business Continuity, Incident management, Data breach and Disaster Response processes
- Risk management frameworks
- Compliance with laws and regulations

PRIVACY POLICY SPECIFICS

Access to personal information is restricted to those of the platform members and third parties who need to know that information for the purposes set out in the Terms of Use and Privacy Policy. Where an external service provider is engaged to work on the platform, reasonable steps are taken to ensure that the information will not be held, used, or disclosed by the service provider inconsistently with applicable data protection and privacy laws (to at least the standard required by GDPR).

Only the minimum personal information required by the platform is collected, with the extent of the usage detailed in the Terms of Use and Privacy Policy.

Personal information is not held for longer than is required for the purpose(s) for which the information was collected.

Physical, electronic and procedural safeguards are maintained to protect your personal information from misuse, unauthorised access or disclosure, and loss or corruption by computer viruses and other sources of harm.

Software code peer reviews are undertaken, as well as external testing to highlight any areas for vulnerability. These areas of concerns are then remediated.

The T+T and WHH legal teams ensure we meet our compliance against applicable industry and governmental regulations.

PARTNER SECURITY PROGRAM

T+T has a selected team responsible for reviewing service providers and subcontractors to ensure they sufficiently protect the security and privacy of sensitive information and systems. To manage third party risk, T+T group have a “T+T third party risk management standard” that defines the process, and an online portal to manage the questionnaire, responses and assessments. Contracts with relevant third parties require them to adequately protect the privacy and security of all confidential information they may get access to during the partnership.

DATA BACKUP

There are three environments (Dev, UAT and Live). The database is backed up in UAT and Live periodically via the Microsoft Cloud Azure Backup Services. The backups are stored for up to one year. The UAT database is restored monthly with the Live database testing purposes.

In addition, a summary of the stock quantities in STOCKHOLM are exported and archived monthly.

DATA SECURITY TRAINING

All T+T employees must complete annual data security and cyber security training through our quality management system. Two key e-learnings have been developed that speak to ‘Protecting Privacy’ and ‘Cyber Security Essentials’. There are also other trainings on personal data protection which employees are asked to complete on an ad-hoc basis. Some of these are compulsory.

THIRD PARTIES ACCESS TO STOCKHOLM

STOCKHOLM shares data with third parties (such as the LogIE platform from the Global Logistics Custer) via API. However, the data is aggregated at regional level and cannot be identified as belonging to a particular organisation or facility.

The third parties do not have access to the environment that is storing/processing/transmitting data. Only T+T and WHH have access to the hosting environment.

CODE OF CONDUCT AND CONFIDENTIALITY

T+T’s Code of Conduct sets out the key standards of ethical conduct and behaviour by the T+T group of companies and of each of our people and suppliers. To fulfil T+T's purpose and strategy and live our values, we commit to doing the right thing and acting with integrity. Our Code of Conduct governs

the way we do business and how we conduct ourselves with our clients, our colleagues, our suppliers, and the communities we operate in. It provides a framework for ethical decision making to help us successfully navigate issues and to do the right thing, consistent with our values.

There are various e-learnings and trainings within T+T's quality management system that train our staff on our Code of Conduct.

All T+T employees are also bound by a confidentiality clause in their employment contract.

CONTACT
For further information, please email esups@welthungerhilfe.de.