Data security statement

I. Introduction

Ituran Location and Control Ltd. (''**Ituran**'' or ''**the company**'') values and respects the privacy of the website's users and customers. Hence, it uses appropriate and customary means to secure the personal data collected and stored in its systems.

Ituran maintains the appropriate standards of security and has in place robust technical and organizational measures for the protection of personal data, primarily to protect the website and its customers, as possible, from attacks and unauthorized access, and to reasonably secure personal data against loss, falsification or unauthorized access by third parties. These measures are also taken to properly and reasonably secure personal data transfers via the internet and/or other communication means.

The measures are evaluated and updated from time to time to address new threats and challenges, as well as new legal requirements.

II. Data security implementation

1. Risk management

1.1. The Company constantly works to locate information security risks in its systems to maintain the integrity, confidentiality, privacy of the data. In addition, the Company periodically conducts vulnerability tests and penetration tests (PT) in all its systems contains data, to examine the possible risks and changes, and acts to correct them as required.

1.2. The company also maps its database systems and maintains an updating list of all its technological structure in order to identify and map future risks to the personal data within its database.

2. Security and access control to data processing systems

2.1. The company grants access to its databases to a limited number of people and only to authorized people on a need to know basis.

2.2. The Company also restricts the entry of suppliers and employees into certain work areas according to their access authorizations. The company monitors and documents the access to its databases and updates periodically the access rights to these work areas.

2.3. The company separates its systems in a manner that personal data is segmented from other systems, and by relevant access controls. The company also uses logical security mechanisms to prevent unauthorized access to personal data.

3. Identification and authentication

3.1. The company allows access to the databases only for authorized people according to their access controls and authorizations.

3.2. In order to access the databases, one can only use his personal identification, and his personal complex password. When needed, it will be based on physical means under the exclusive control of the authorized person (according to the sensitivity of the data).

3.3. The company updates its granted authorizations and passwords periodically.

4. Employees

4.1. Ituran implements measures and policies to ensure that all its personnel are trained and fully aware to security and privacy-related topics and makes sure that only relevant personnel have access to the needed areas within its databases.

5. Documentation

5.1. The company logs all authorized/ unauthorized entries to its sensitive databases, and all exceptional attempts to access its systems are documented, insofar as possible, and treated accordingly.

6. Network and web transfers security

6.1. Network Security - In order to prevent unauthorized intrusion into Company's databases, the Company has implemented a network security system.

6.2. Transfers of data from Company's database - the Company monitors and secures the transfer of data from its systems to external entities by documenting and encrypting all information transmission.

6.3. Internet - the Company ensures adequate data security, using logical and/or physical separation between the Internet network and the internal company network, in accordance with Directive ISO / IEC 27001: 2013.

6.4. Remote connection - Remote connection to the Company's databases are made only by those who are authorized to do so, and under strong identification based on MFA (Multi Factor authentication).

7. Security and Encryption

7.1. The Company uses standard security or encryption methods to secure the personal data contained in its databases. Moreover, the company encrypts: all network traffic using

conventional protocols; external and remote access to the company's systems; password files and sensitive business information; other communication lines, etc.

8. Backups

8.1. The company backups the data within its systems and protects it, using both logical and physical measures, insofar as possible, from accidental destruction or loss.

8.2. The Company regularly performs restoration drills for backups, to ensure its ability to restore data.

9. Portable devices

9.1. The company restricts the use of laptops only to employees who are required to do so. In the end of employment, the computer will be returned to The Company.

9.2. The computers are reasonably hardened, encrypted and secured by the company's anti-virus tools.

10. Audits

10.1. The Company conducts a comprehensive periodic review of management procedures, updates its authorized personnel, and ensures the existence of up-to-date data security policies, in order to locate data security risks, reduce irrelevant authorizations, and ensure, as possible, that there is no surplus data in its databases.

11. Data security events

11.1. The Company holds a comprehensive data breach policy and procedures. In addition, the Company has a DRP recovery plan designed to prevent, insofar possible, interference with the Company's ongoing operations and aims to protect data from destruction, disruption, deletion, copying or leakage in the Company's physical and logical information systems.

12. Periodic updates

12.1. The Company updates its procedures, policies, land access controls, in accordance to technological changes, risks to data and by the results of internal tests, in order to ensure the security of the data in its systems.