1. ’s management demonstrates commitment to data protection by creating the policy and associated requirements, assigning specific roles and responsibilities, continuously developing a good data protection culture, and allocating appropriate resources.
2. is responsible for compliance with:
    a. General Data Protection Regulation (GDPR, 2016/679);
    b. Cyprus National Law Providing for the Protection of Natural Persons with Regard to the Processing of Personal Data and for the Free Movement of Such Data (Law No. 125(I)/2018);
    c. other applicable laws concerning privacy and personal data protection.
3. understands its roles and responsibilities in data processing.
4. Personal data in are:
    a. processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);
    b. collected for specified, explicit and legitimate purposes (purpose limitation);
    c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
    d. accurate and, where necessary, kept up to date (accuracy);
    e. stored no longer than is necessary for the purposes for which the personal data are processed (storage limitation);
    f. processed in a secure manner that ensures the confidentiality, integrity and availability of personal data.
5. is able to demonstrate compliance with this statement (accountability).
6. respects the rights of the data subjects (the right to be informed, the right to access, the right to rectification, the right to erasure (right to be forgotten), the right to restrict processing, the right to data portability, the right to object, the rights in relation to automated decision making and profiling) and guarantees their observance.
7. understands and assesses potential risks to the rights and freedoms of natural persons. If necessary, a data protection impact assessment (DPIA) is conducted.
8. has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    a. the encryption of personal data;
    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c. the ability to restore the availability and access to personal data in a timely manner in the event of incidents;
    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

9. has a Data Protection Officer. The Data Subjects can contact him/her at any time and receive additional information. Contacts: info@holdi.com.
10. The Data Subjects have the right to file a complaint with a lead supervisory authority. Please follow this link to lodge a complaint: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1i_en/page1i_en?opendocument.
11. The Privacy Policy is subject to periodic assessment, revision and updating every two years or, if necessary, at shorter time intervals to reflect changing conditions.