Leptos Group

Data Privacy Policy

Contents

Document Control			
Document Title	Data Privacy Policy	Revision	0.1
Document Owner	Leptos Group	Placement	
Location	Cyprus	Effective Date	May 2019
Department	Data Protection Office	Review Frequency	Annual

Authorization		
Prepared By	Reviewed By	Approved By
EY		
Signature / Date	Signature / Date	Signature / Date
EY / May 2019		

Revision History				
Revision No.	Effective Date	Prepared By	Approved By	Description
0.1	May 2019	EY		

1. Introduction

Leptos Group and affiliated entities (here after “company acronym”, “we”, “our”, “us”, “the Company”) endeavours to meet leading standards for data protection and privacy. This Privacy policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

While our reasons are founded in ethical and corporate responsibility, our privacy practices as outlined in this policy facilitate the establishment of the following:

- Competitive Advantage: Our emphasis on protecting the privacy of customers, vendors, and employees distinguishes us from our competitors.
- Good Corporate Citizenship: A sound privacy policy is emblematic of reliable corporate citizens that respect data subjects’ privacy.
- Business Enablement: Since Leptos Group uses significant volumes of personal information, privacy notices become a prerequisite to building enduring business relationships.
- Legal Protection: Appropriate privacy notices offer an opportunity to eliminate allegations of unlawful usage of personal information.
- Comply with the General Data Protection Regulation (GDPR): failure to comply with the provisions of the GDPR may expose Leptos Group to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher.

This document (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

2. Purpose

This Policy defines requirements to help ensure compliance with laws and regulations applicable to Leptos Group collection, storage, use, transmission, disclosure to third parties and retention of Personal and special categories of personal data (also referred to as personal and sensitive personal information respectively in this policy).

3. Scope

This policy is applicable to all Leptos Group employees, contractors, vendors, interns, customers, and business partners who may receive personal information from Leptos Group, have access to personal information collected or processed by or on behalf of Leptos Group, or who provide information to Leptos Group.

This policy covers the treatment of personal information gathered and used by Leptos Group for lawful business purposes. This policy also covers the personal information we share with authorized Third Parties or that Third Parties share with us.

4. Objective

The main objectives of the Data Privacy Policy are:

- To ensure that all the personal information in Leptos Group custody is adequately protected against threats to maintain its security.
- To ensure that Leptos Group employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches.
- To limit the use of personal information to identified business purposes for which it is collected.
- To create an awareness of privacy requirements to be an integral part of the day to day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy.
- To make all the employees aware about, the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal information.
- To ensure that all third parties collecting, storing and processing personal information on behalf of Leptos Group provide adequate data protection.
- To ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal information are adhered to.

5. Accountability and Management

5.1. A Data Privacy Policy shall be developed and maintained to document the privacy principles and practices followed by Leptos Group. (Refer: Appendix A – Privacy principles)
5.2. A privacy organization shall be defined for governance of data privacy initiatives. (Refer: Appendix B – Privacy organization structure)
5.3. A Data Privacy Officer (DPO) shall be appointed (or DPO function) to process complaints and requests for information related to Leptos Group privacy practices.
5.4. Implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
5.5. Establish procedures for the identification and classification of personal information.
5.6. Leptos Group Privacy Policy statement shall be made available on Leptos Group internal portal.
5.7. The Data Privacy Policy shall be communicated to Leptos Group internal personnel.
5.8. Procedures shall be established for disciplinary and remedial action for violations of the Data Privacy Policy.
5.9. Changes or updates to the Data Privacy Policy shall be communicated to Leptos Group internal personnel when the changes become effective.
5.10. Establish procedures for performing mandatory registration with regulatory bodies.
5.11. Risk Assessment is to be carried out on a periodic basis to ensure risks to personal information are identified and mitigated.
5.12. The potential impact on data privacy is assessed when new processes involving personal information are implemented, or when significant changes are made to such processes. (Refer: Appendix C – Privacy Impact Assessment guidelines)

6. Privacy Notice and Transparency

6.1. Appropriate notice shall be provided to data subjects at the time personal information is collected.
6.2. When Leptos Group is the Data Controller for PII data it must provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent,

intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.3. The privacy notice or policies and other statements to which they are linked shall provide as full information as is reasonable in the circumstances to inform an individual how their personal information will be used so that Leptos Group use is fair and lawful. The following information should be considered for inclusion in a notice (as is appropriate in individual circumstances):

6.3.1. Purposes for which personal information is collected, used and disclosed;

6.3.2. Choices available to the individual regarding collection, use and disclosure of personal information, wherever applicable;

6.3.3. Period for which personal information shall be retained as per identified business purpose or as mandated by regulations, whichever is later;

6.3.4. That personal information shall only be collected for the identified purposes;

6.3.5. Methods employed for collection of personal information, including 'cookies' and other tracking techniques, and third party agencies;

6.3.6. That an individual's personal information shall be disclosed to Third Parties only for identified lawful business purposes and with the consent of the individual, wherever possible;

6.3.7. That an individual's personal information may be transferred within Leptos Group entities, globally as per requirement, for business purposes with adequate security measures required by law or as per guidance of provided by industry leading practices;

6.3.8. Consequences of withholding or withdrawing consent to the collection, use and disclosure of personal information for identified purposes;

6.3.9. Data subjects are responsible for providing Leptos Group with accurate and complete personal information, and for contacting the entity if correction of such information is required;

6.3.10. Process for an individual to view and update their personal information records;

6.3.11. Process for an individual to register a complaint or grievance with regard to privacy practices at Leptos Group;

6.3.12. Contact information of person in charge of privacy practises and responsible for privacy concerns with address at Leptos Group;

6.3.13. Process for an individual to withdraw consent for the collection, use and disclosure of their personal information for identified purposes; and

6.3.14. That explicit consent is required to collect, use and disclose personal information, unless a law or regulation specifically requires or allows otherwise.

6.4. Data subjects shall be provided a Privacy Notice in case any new purpose is identified for using or disclosing personal information before such information is used for purposes not previously identified.

6.5. When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7. Choice and Consent

7.1. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

7.2. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.
7.3. If Consent is given in a document which deals with other matters, then the Consent must be explicit from those other matters.
7.4. A Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.
7.5. Consent may need to be refreshed if there is intention to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.
7.6. Explicit consent shall be obtained from data subjects at the time of collection of personal information or as soon as practical thereafter.
7.7. Explicit consent shall be obtained from data subjects for the collection, use and disclosure of their personal information, unless a law or regulation specifically requires or allows otherwise. A record is maintained of explicit consent obtained from data subjects.
7.8. Consent shall be obtained from data subjects before their personal information is used for purposes not previously identified.
7.9. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.
7.10. Leptos Group must maintain evidence on types of Consent and keep records of all Consents captured so that the Company can demonstrate compliance with Consent requirements.
7.11. Requests for consent should be designed to be appropriate to the age and capacity of the data subject to consent for themselves and to the particular circumstances (e.g. children who are not older than 16th, vulnerable data subjects unable to understand and consent for themselves).
7.12. Organisation should establish communication guidelines to notify other data controllers (with whom PII was shared) for rectification/deletion/restricting of personal data of data subject.
7.13. Organisation should document guidelines for managing directories of subscribers to electronic services which include the following:
- Guidelines for obtaining consent from the end users.
- What information is to be provided to the data subject at the time of data collection (purpose, search functions, right to object and information how personal data can be rectified or deleted).

8. Collection of Personal Information

8.1. The collection of personal information shall be limited to the minimum requirement for lawful business purposes.
8.2. The GDPR allows Processing for specific purposes, some of which are set out below:
a. The Data Subject has given his or her Consent;
b. The Processing is necessary for the performance of a contract with the Data Subject;
c. To meet our legal compliance obligations;
d. To protect the Data Subject's vital interests;
e. To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data

Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices; or

f. [OTHER GDPR PROCESSING GROUNDS]: identify and document the legal ground being relied on for each Processing activity [in accordance with the Company's guidelines on Lawful Basis for Processing Personal Data].

8.3. Methods of collecting personal information shall be reviewed by management to ensure that personal information is obtained:
- 8.3.1. Fairly, without intimidation or deception, and
- 8.3.2. Lawfully, adhering to laws and regulations relating to the collection of personal information.

8.4. Management shall confirm that Third Parties from whom personal information is collected:
- 8.4.1. Use fair and lawful information collection methods, and
- 8.4.2. Comply with the Leptos Group Data Privacy Policy and their contractual obligations with respect to the collection, use and transfer of personal information on behalf of Leptos Group

8.5. Data subjects shall be notified if additional information is developed or acquired about them.

9. Data Minimization

9.1. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

10. Limiting Use, Disclosure and Retention

10.1. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

10.2. Personal information retention shall be only for the duration necessary to fulfil the identified lawful business purposes or as prescribed by law.

10.3. Guidelines and procedures shall be developed for the retention and disposal of personal information. These shall address minimum and maximum retention periods, and modes of storage.

10.4. Upon the expiration of identified lawful business purposes or withdrawal of consent, Leptos Group shall either securely erase or anonymize the data subjects' personal information. Data is anonymized to prevent unique identification of an individual.

11. Data Subject Rights and Requests

11.1. The organisation should ensure that it has established the following:

11.2. The organization has established mechanism for data subjects to raise requests related to their rights (access/rectification) electronically (especially where personal data are processed by electronic means).

11.3. Organization has established following related to right of access and rectification:
- 11.3.1. Documented process and mechanism for provisioning access to personal data and rectification.
- 11.3.2. Identified mandatory information to be provided to data subject
- 11.3.3. Guidelines for administrative fees can only be charged to data subject for subsequent PI access
- 11.3.4. Personal Data to be provided in electronic form unless requested otherwise

11.3.5. Track the received requests from data subjects and respond within 1 month with appropriate response

11.4. Assessments are performed regularly – and at least annually – of whether the rectification of personal data has been performed correctly and without undue delay.

11.5. Organization has established following related to right of deletion:

11.5.1. Policies and procedures to process/respond to PI deletion requests from data subjects within 1 month

11.5.2. Documented the Personal data deletion guidelines considering the grounds for deletion and the applicable exceptions

11.6. Organization has established guidelines for restrictions of data processing which address:

11.6.1. Documented grounds which are compared with criteria for restricting mentioned in the data subject request and a formal sign-off process to ensure that appropriate decisions are taken and implemented for a defined period of time

11.6.2. Process to inform data subject prior to lifting the restriction of processing of personal data

11.7. Organization has implemented mechanism to inform data subjects if it alters, restricts the processing of or removes personal data.

11.8. Organization has established guidelines to process data portability requests from data subjects. The guidelines are compliant with data portability considerations.

11.9. Organization has established means for data subject to object online.

12. Transfer Limitation

12.1. Leptos Group shall limit data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined

12.2. Leptos Group may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

13. Disclosure to Third Parties

13.1. Where reasonably possible, management shall ensure that third parties collecting, storing or processing personal information on behalf of Leptos Group have:

13.1.1. Signed agreements to protect personal information consistent with Leptos Group Data Privacy Policy and information security practices or implemented measures as prescribed by GDPR;
13.1.2. Signed non-disclosure agreements or confidentiality agreements which includes privacy clauses in the contract; and
13.1.3. Established procedures to meet the terms of their agreement with Leptos Group to protect personal information.

13.2. Personal information may be transferred outside European Union (EU) jurisdiction from where Leptos Group operates for storage or processing where any of the following apply:
13.2.1. The individual has given consent to the transfer of information
13.2.2. The transfer is necessary for the performance of a contract between the individual and Leptos Group, or the implementation of pre-contractual measures taken in response to the individual's request.
13.2.3. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between Leptos Group and a third party.
13.2.4. The transfer is necessary or legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
13.2.5. The transfer is required by law
13.2.6. The transfer is necessary in order to protect the vital interests of the individual.
13.2.7. The transfer is made under a data transfer agreement.
13.2.8. The transfer is otherwise legitimised by applicable law.

13.3. Remedial action shall be taken in response to misuse or unauthorized disclosure of personal information by a third party collecting, storing or processing personal information on behalf of Leptos Group

14. Security Practices for Privacy

14.1. Leptos Group information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by Leptos Group.
14.2. Leptos Group shall comply with all applicable aspects of Leptos Group Information Security Program or comply with the administrative, physical and technical safeguards implemented and maintained in accordance with the GDPR and relevant standards to protect Personal Data.
14.3. Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.
14.4. Management shall establish procedures that maintain the logical and physical security of personal information.
14.5. Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
14.6. Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices. (Refer: Appendix D – Data breach response guidelines)
14.7. Leptos Group must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows: (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

15. Quality of Personal Information

15.1. Leptos Group may perform additional validation procedures to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
15.2. Leptos Group shall ensure that personal information collected is relevant to the business purposes for which it is to be used.

16. Privacy Monitoring and Enforcement

16.1. Procedures shall be established for recording and responding to complaints/ grievances registered by data subjects.
16.2. Each complaint regarding privacy practices registered by data subjects shall be validated, responses documented and communicated to the individual.
16.3. Annual privacy compliance review shall be performed for identified business processes and their supporting applications.
16.4. A record shall be maintained of non-compliances identified in the annual privacy reviews. Corrective and disciplinary measures shall be initiated and tracked to closure, guided by Leptos Group management.
16.5. Procedures shall be established to monitor the effectiveness of controls for personal information and for ensuring corrective actions, as required.
16.6. Any conflicts or disagreements relating to the requirements under this policy or associated privacy practices shall be referred to the Data Privacy Officer for resolution.

17. Personal Identifiable Information (PII) of Leptos Group employee

Data protection laws govern the use of personally identifiable information. This term means any data relating to a living individual who can be identified using that data. Leptos Group may hold the following types of sensitive and non-sensitive PII:

- names, addresses, telephone numbers and other personal contact details;
- gender, date of birth, physical or mental health or condition;
- marital status, next of kin, racial or ethnic origin, sexual orientation, religious, philosophical, political or similar beliefs;
- national insurance or social insurance number, immigration status, trade union membership;
- personnel records including training, appraisal, performance and disciplinary information, and succession planning;
- bank details, salary, bonus, benefits and pension details and other financial information; and
- criminal offences committed (or allegedly committed) including any proceedings and sentencing in relation to any such criminal offence.

18. Staff data processing activities

Personal information about individuals may only be processed for a legitimate purpose. Leptos Group may undertake a number of activities with an individual employee's personal information including, but not limited to:

- salary, benefits and pensions administration;
- health and safety records and management;
- security vetting, criminal records checks and credit checks and clearances (where applicable and allowed by law);
- confirming information on résumés, CVs and covering letters, providing reference letters and performing reference checks;
- training and appraisal, including performance evaluation and disciplinary records;
- staff management and promotions;
- succession planning;
- equal opportunities monitoring;
- any potential change of control of a group company, or any potential transfer of employment relating to a business transfer or change of service provider;
- other disclosures required in the context of staff employment;
- promoting or marketing of Leptos Group, its products or services;
- provision of staff or business contact information to customers and agencies in the course of the provision of Leptos Group's services;
- CCTV monitoring for security reasons;
- compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches;
- establishing, exercising or defending Leptos Group's legal rights;
- disclosures to other companies in the Leptos Group group of companies, including companies in other countries to the extent permitted by law, including for the following purposes: as required in connection with the duties of the employee; legal compliance; audit; group level management; in connection with the fulfilment of customer and partner contracts;
- any other reasonable purposes in connection with an individual's employment or engagement by Leptos Group;
- providing and managing use of services provided by third parties, such as company provided mobile phones, company credit cards and company cars and billing for such services.

18.1. Leptos Group may also collect and process personal information about your next of kin, so they can be contacted in an emergency or in connection with use of a company car provided by Leptos Group. Their personal information will also be processed in accordance with the data protection laws and as described in the policy.

18.2. In order to fulfil the purposes set out above, Leptos Group may disclose personal information to contractors and suppliers that provide services to Leptos Group and who may assist in the processing activities set out above and also to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law or for administration/taxation purposes, to the extent local law allows and requires.

18.3. Leptos Group may disclose your personal information to third parties for the purposes of establishing and managing your employment relationship. For example, Leptos Group may disclose some of your personal information to:

- benefits providers (for example, pension and insurance providers);
- payroll and data processing suppliers and other service providers who assist us in establishing or managing your employment relationship with us;
- insurance claims and medical related service providers; and
- parties requesting an employment reference.

18.4. Leptos Group shall take appropriate measures to ensure that its contractors and suppliers also process personal information in a compliant way and such measures may include a data processing agreement.

18.5. Leptos Group may transfer personal information to other group companies, partners, suppliers, law enforcement agencies and to other organisations in all cases that are located outside of the country where you are based for the purposes of:

- HR administration (for example, staff recruitment);
- payroll processing for employees working outside the country where they are based;
- employee relocation;
- security clearances;
- visa applications;
- taxation and registrations for employees working outside the country where they are based;
- fulfilling Leptos Group's legal requirements;
- fulfilling customer contracts for the provision of Leptos Group's services;
- overseas legal proceedings;
- Outsourcing Leptos Group functions.

18.6. The laws of some jurisdictions may not be as protective as the laws in the country in which you are based. Leptos Group may transfer your personal information across provincial or national borders to fulfil any of the above purposes, including to service providers located in countries who may be subject to applicable disclosure laws in those jurisdictions, which may result in that information becoming accessible to law enforcement and national security authorities of those jurisdictions.

19. Record Keeping (Privacy Register)

19.1. Leptos Group shall keep full and accurate records of all data Processing activities.

19.2. Leptos Group must keep and maintain accurate corporate records reflecting Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

19.3. These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

20. Retention of records

20.1. Leptos Group has a statutory duty to keep certain records for a minimum period of time. In other cases Leptos Group shall not keep personal information for longer than is necessary or as may be required by applicable law.

21. Data Privacy Impact Assessments (DPIA)

21.1. The organisation should conduct Data Privacy Impact Assessment (DPIA) for its business activities for which the processing of personal data is "likely to result in a high risk to the rights and freedoms of natural persons". A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights

and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

21.2. The firm should assess all its business processes and define which of them are high-risk. For the purpose of the assessment it should use appropriate risk criteria to help on the factual identification of high-risk business processes. (ie. criteria as set in the Article 29 of GDPR PIA evaluation).

21.3. The organisation should choose a methodology for the implementation of its DPIAs. The DPIA should be compliant with the minimum features described in Annex 2 in Article 29 of GDPR on performing DPIA.

21.4. The company should continuously review and re-assess its business activities as certain changes could increase or decrease their risk.

22. Data Flow Management

22.1. For all high-risk business procedures as defined in the Privacy Impact Assessment.

22.2. Organisation should define guidelines for data mapping. Data mapping addresses below mentioned:

- Documenting the data processing activities.
- Type of personal data used for each processing activity along with personal data storage location.
- The organisation should identify and document data flows specific to how personal information is moving through the underlying systems and software within the organization (including third party operations).

23. Monitoring

23.1. Leptos Group's IT and communications systems are intended to promote effective communication and working practices within our organisation.

23.2. For business reasons, and in order to carry out legal obligations in our role as an employer, use of Leptos Group's systems on whatever platform including the telephone (mobile and fixed) and computer systems (including email and internet access), and any personal use of them, is monitored. If you access services by the use of passwords and login names on Leptos Group's IT and communication systems, this might mean that your personal access details are seen by Leptos Group.

23.3. Monitoring is only carried out if and to the extent permitted or as required by law and as necessary and justifiable for business purposes. The resulting log files may be used so that instances of attempted misuse and other security events can be detected, and that information is available to support any subsequent investigation. To the extent permitted by law and, where breaches of this and other Leptos Group policies or applicable law are found, action may be taken under the disciplinary procedure.

23.4. The employees are informed that the telephone system used by the Company allows identification of all dialled numbers and received calls.

23.5. Leptos Group reserves the right to retrieve the contents of messages, check searches which have been made on the internet, require the immediate return of devices supplied by Leptos Group and access data stored on such devices for the following purposes (this list is not exhaustive):

- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy (and employees acknowledge that the Company can use software to monitor the identity of senders and receivers of emails);
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of wrongful acts; or

- to comply with any legal obligation.

23.6. If evidence of misuse of Leptos Group's IT systems is found, Leptos Group may undertake a more detailed investigation in accordance with Leptos Group's disciplinary procedures, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary, such information may be handed to the police in connection with a criminal investigation. Investigations and disclosure of information to the relevant authorities shall be carried out only to the extent permitted by law.

24. CCTV

24.1. Some of Leptos Group's buildings and sites use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded. Use of CCTV and recording of CCTV data is only carried in accordance with Leptos Group approved guidelines.

24.2. Leptos Group shall take reasonable efforts to alert the individual that the area is under electronic surveillance.

25. Reporting Data Privacy Breach:

25.1. The GDPR requires Data Controllers to notify any Personal Data Breach to the Cyprus Data Protection regulatory authority and, in certain instances, the Data Subject.

25.2. Leptos Group shall put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where is legally required to do so.

25.3. Where there is a suspicion of a Personal Data Breach occurrence, the DPO, the information technology or security department should be notified immediately and should follow the Leptos Group SECURITY INCIDENT RESPONSE PLAN. All evidence relating to the potential Personal Data Breach should be preserved.

26. Exceptions and exclusions:

26.1. Controls related to monitoring of Leptos Group’s IT system and Infrastructure will not be applicable to Leptos Group’s operations in <this scenario or in this location>.

27. Glossary

Term	Definition
Anonymize	To process a collection of personal data or information such that a natural person cannot be identified on the basis of the output collection of data or information
Data subject	A living individual about whom personal information is processed by or on behalf of Leptos Group
Vulnerable data subject	A Data subject that may be over the age of 16 however do not have the competence to understand and consent for themselves
“Leptos Group”, “we”, “our”, “us”, “the Company”	LEPTOS GROUP SYSTEMS LIMITED / its Subsidiaries / its Group Companies / its affiliates, its directors, employees (excluding the User/affirming employee in this context), assigns and successors.

Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Personal Data or personal information	Any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person
Sensitive personal data or sensitive personal information	Definition of sensitive personal information as per various laws are stated below: <u>The Data Protection Act, United Kingdom</u> Sensitive personal data means personal data consisting of information as to: 1) the racial or ethnic origin of the data subject, 2) his political opinions, 3) his religious beliefs or other beliefs of a similar nature, 4) whether he is a member of a trade union, 5) his physical or mental health or condition, 6) his sexual life, 7) the commission or alleged commission by him of any offence, or 8) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. <u>The Federal Data Protection Act, Germany</u> 'Special categories of personal data' (Sensitive personal data) shall mean information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. <u>The Federal Data Protection Act, Switzerland</u> Sensitive personal data: data on: 1) religious, ideological, political or trade union-related views or activities, 2) health, the intimate sphere or the racial origin, 3) social security measures, 4) administrative or criminal proceedings and sanctions; - Data file: any set of personal data that is structured in such a way that the data is accessible by data subject; - Personality profile: a collection of data that permits an assessment of essential characteristics of the personality of a natural person;
Third party	All external parties – including without limitation contractors, interns, summer trainees, vendors, service providers and partners – who have access to Leptos Group information assets, information systems or who are pass personal information from them.

28. Appendix A: Privacy Principles

Leptos Group Data Privacy Policy aligns with Generally Accepted Privacy Principles. In view of the changing legislative and technological environment for data privacy, the Data Privacy Policy will undergo revisions. The guiding privacy principles articulated in this policy document are as follows:

- Management:
  Define, document, communicate, and assign accountability for Leptos Group Data Privacy policy and procedures
- Notice:
  Provide notice about Leptos Group Data Privacy policy and procedures and identify the purposes for which personal information is collected, used, retained, and disclosed
- Choice and Consent:
  Describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information
- Collection of personal information:
  Collect personal information only for the purposes identified in the notice
- Limiting Use, Disclosure and Retention:
  Limit the use, storage and retention of personal information is limited to the purposes identified in the data privacy notice and for which the individual has provided implicit or explicit consent. Retain personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately dispose of such information.
- Access for review and update:
  Provide data subjects with access to their personal information for review and update
- Disclosure to third parties:
  Disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual
- Security practices for privacy:
  Protect personal information against unauthorized access (both physical and logical)
- Quality of personal information:
  Maintain accurate, complete, and relevant personal information for the purposes identified in the notice
- Monitoring and enforcement:
  Monitor compliance with Leptos Group Data Privacy policy and procedures, and have procedures to address privacy related complaints and disputes