TECHNICAL MEASURES POLICY

KORPUS PRAVA HOLDING group of companies

KORPUS PRAVA LATVIA (SIA)

Korpus Prava
LAW & TAX

Original Issue Date:	25 May 2018
Approver(s):	Board of Directors
Owner(s):	Artem Paleev
Contact Person:	Ilya Parshikov
Classification:	TECHNICL MEASURES POLICY
Operational Applicability:	Clients, Employees
Geographic applicability:	Cyprus
Last Revision Date:	25 May 2018
Version:	1.0
Other Languages:	N/A

INTRODUCTION

This Technical Measures Policy is an integral part of the Privacy Policy of KORPUS PRAVA HOLDING group of companies and KORPUS PRAVA (LATVIA) SIA.

KORPUS PRAVA CORPORATE SERVICES LTD (KPCS LTD) is a registered Administrative Service Provider ("ASP") within the meaning of the Law Regulating Companies Providing Administrative Services and other Related Matters of 2012 (the "Law") and regulated by the Cyprus Securities and Exchange Commission ("CYSEC") with licence number 14/196. KPCS LTD by the nature of its activities is acting as the Controller and the Processor regarding to its clients and engages third parties as Processors from time to time. KPCS LTD also acts as the Processor for the third parties (banks, corporate administrators, etc.) from time to time. KPCS LTD acknowledges client's right to privacy as effected in the General Data Protection Regulation ((EU) 2016/679) ("GDPR") and the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018) which was issued for the purpose of effectively implementing certain provisions of the GDPR.

Other companies-members of KORPUS PRAVA HOLDING group may act as Controllers or Processors for KPCS LTD or each other from time to time in accordance with relevant agreements entered into by the companies of the group.

KORPUS PRAVA LATVIA (SIA) is not a company-member of the group, but it is connected to the group by business relationships and is the representative of the Controller KORPUS PRAVA CORPORATE SERVICES LTD in Latvia.

This Technical Measures Policy sets out all technical measures which KPCS LTD (the Company) performs to secure and protect personal data in accordance with GDPR and data protection legislation. Other companies of KORPUS PRAVA HOLDING GROUP and KORPUS PRAVA (LATVIA) SIA have to use this policy to organize and implement similar procedures in their premises and use electronic data base LOTUS in appropriate way.

NOTE: Company's website and its content are subject to pertinent copyright and intellectual property laws.

All personal data of clients and employees are contained in two types: hard copies and electronic copies. Hard copies are stored at the premises of Korpus Prava and electronic versions are stored in the electronic base LOTUS, which is installed on the computers of employees.

ACCESS TO PREMISES

KPCS LTD is registered and situated at Griva Digeni 84, office 102, 1st floor, 3101, Limassol, Cyprus. Premises are protected by the door which is equipped with the lock firm CISA and electronic contactless card system RFID. Premises of the company are opened only on business days. A business day always starts at 9 AM and ends at 6 PM. Employees have access to the premises only during the business day via using electronic card system, directors and IT specialist have access to the premises 24 hours a day 7 days per week via lock and electronic card system. Access to the premises out of business hours may only be granted to employees with the director's approval. Out of business hours premises are protected via Alarm System Delta 40B GSM which is always on in silent alarm mode. Video camera moulages are installed in the premises of the company, no personal data or other information about employees, clients or other visitors of the company is collected.

HARD COPIES

All personal data which are contained in hard copies must be stored by employees in such a way that data will not be visible to third parties. Hard copies are stored in special office cupboards. Archive files are stored in the Archive room. Access to the Archive room is granted only to employees. Employees have access to clients' personal data only in accordance with their job duties. Access to employees' personal data is granted only to Data Protection Officer, Director, Compliance Officer, Accountant and Office Manager. All employees give their prior consent to processing of their personal data in written form; employees' consents are kept in the respective employee's personal file.

ELECTRONIC COPIES

1. COMPUTER SYSTEM AND DESKTOP

Every employee has its individual personal computer.

Information computer system is built of the basis of HP Inc. servers and the following software: VwWare Inc., Microsoft Corporation, International Business Machines program, more specifically different versions of MS Windows, VMware ESXi and IBM Notes/Domino. Employees have access only to the data and information which are necessary for the performance of their job duties. Access control is based on passwords and personal certificates; AES-256 coding is used. Actual versions of antivirus program ESET Endpoint Antivirus for Windows is installed and used. Computers are connected using wired connections. Employees are allowed only to work with files containing personal data on the desktop. When the work with file containing personal data is finished the file must be saved in electronic database Lotus and deleted from the desktop and recycle bin.

2. IBM NOTES (LOTUS)

Every employee of the company has access to electronic data base IBM NOTES (LOTUS) which is used by all companies of KORPUS PRAVA HOLDING group and KORPUS PRAVA (LATVIA) SIA. Employees have access only to the data and information which are necessary for performing of their job duties.

IBM Notes is a client-server cross-platform application runtime environment that provides an interface to the IBM Notes and Domino software. IBM Notes can be used as an email client without an IBM Domino server, for example, as an IMAP client. IBM Notes and Domino provide email, calendars, discussions/forums, blogs, and an inbuilt personnel/user directory. In addition to these standard applications, an organization may use the IBM Domino Designer development environment and other tools to develop additional integrated applications such as request approval / workflow and document

management. Features include group calendars and schedules, SMTP/MIME-based email, NNTP-based news support, and automatic HTML conversion of all documents by the Domino HTTP task.

The Domino server includes security tools support S/MIME, SSL 3.0 with industry standard key sizes for HTTP and other Internet protocols, X.509 client certificates, and an integrated certificate authority. IBM Notes and Domino also use a code-signature framework that controls the security context, runtime, and rights of custom code developed and introduced into the environment. Notes use an execution control list (ECL) at the client level. The ECL allows or denies the execution of custom code based on the signature attached to it, preventing code from untrusted (and possibly malignant) sources from running. Notes and Domino allowed client ECLs to be managed centrally by server administrators through the implementation of policies. The code signatures listed in properly configured ECLs prevent code from being executed by external sources, to avoid virus propagation through Notes/Domino environments. Administrators can centrally control whether each mailbox user can add exceptions to, and thus override, the ECL.

Every database has an access control list (ACL) that specifies the level of access a user or a server can have to that database. A user's access level determines what tasks he or she can perform in the database. A server's access level determines what information the server can replicate. The names of access levels are the same for users and servers. Only a user with Manager access can create or modify the ACL. To set an ACL, the Manager selects the access level, user type, and access level privileges for each user or group in a database. Default entries in the ACL can be set when the Manager creates the database. The manager can also assign roles if the database designer determines this level of access refinement is needed by the application.

3. EMAIL

Employees may connect clients and transfer their personal data contained in electronic documents via email; the company uses email on the base of IBM Notes system described above.

Prior to sending an email to the client, the employee obtains client’s consent. As it described in the Privacy Policy consent for the usage of client’s name and email the client can be given through the website of the Company. The employee of the Company sends a letter to the client, containing the link to the website. If the client refuses to give his/her consent, the employee of the Company can’t contact the client any more. The right of withdrawal of consent is described in the Privacy Policy.

RECORD KEEPING

All hard copies and electronic documents containing personal data must be destroyed by employees not later than in 30 days after termination of clients’ relationship. All emails are destroyed automatically not later than in 30 days after termination of clients’ relationship. Hard copies and electronic documents containing personal data are allowed to be saved and stored for a longer period of time only for the purpose of compliance with legal requirements (including, without limitation, the provisions of AML laws, accounting regulations requirements), etc.

In the course of ensuring the safety and integrity of personal data, the Company frequently reviews its technical and organizational measures to take into account of the latest technological developments.