korpus prava

PRIVACY POLICY

KORPUS PRAVA HOLDING group of companies

Original Issue Date:	28 May 2018
Approver(s):	Board of Directors
Owner(s):	Artem Paleev
Contact Person:	Ilya Parshikov
Classification:	PRIVACY POLICY
Operational Applicability:	Clients, Employees
Geographic applicability:	Cyprus
Version:	3.0
Other Languages:	N/A

INTRODUCTION

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 of companies 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.

KPCS LTD has the right to outsource its data protection functions to third parties on the base of relevant agreements.

This Policy applies to all existing and potential clients as well as to any visitors of the Company's website and employees.

The Company is committed to protect the privacy of the personal data obtained from its clients, including information obtained during visits to the Company's website.

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

DEFINITIONS

Automated Decision-Making ("ADM"): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company Personnel: all employees, directors, members and generally any person in the employment of the Company.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subjects' wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

Controller: the person or organisation that determines when, why and how to process which personal data pertaining to data subjects.

Criminal convictions data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data subject: an identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment ("DPIA"): tools and assessments used to identify and reduce risks of a

data processing activity.

Data Protection Officer ("DPO"): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 28 member-states of the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation ("GDPR"): General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data specifically includes, but is not limited to: name, passport data, ID data, driving license data, residential address, contact details (phone number, fax, email), personal financial information (banking and tax information, information about property and assets, source and the amount of income), information about education, professional experience and business activities.

Personal data breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Privacy by design: implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Privacy Notice: informing of a data subject about the processing of personal data.

Privacy Policiy: general privacy statements applicable to the clients and the employees of the Company.

Processing: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Pseudonymisation: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related policies: the Company's policies, operating procedures or processes related to this Privacy Policy and designed to protect personal data, available here:

Special categories of personal data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Supervisory authority: Commissioner for Personal Data Protection.

SCOPE

The Company recognises that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that the Company takes seriously at all times. The Company is exposed to potential fines of up to EUR 20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

The Company is responsible for ensuring all Company Personnel comply with this Privacy Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance. The Company as an ASP performs the functions of the Controller and the Processor regarding GDPR. The Company performs its obligations on the grounds of prior consent received from the clients, employees or other data subjects and/or on the grounds of provisions of Article 6 of the GDPR related to lawfulness of the processing of personal data described below.

The Company as a Controller reserves the right from time to time engage the third-party Processor: (a) to provide services to the Controller's clients for and on behalf of the Controller; (b) to perform certain tasks within the framework of the Controller's provision of services and (or) its counterparties; and (c) to perform tasks or their parts in favour of the Controller. In this event the functions of the Processor may be performed by another company of the Group or a third party not related to the Group.

On the regular basis, the Company, in its capacity as an ASP, is acting as the Controller. However, in some cases, the Company may act as a Processor on behalf of the Controller – one of the companies of the Group or a third party not related to the Group. Examples of third parties not related to the Group: banks, partner corporate administrators, authorities, partner lawyers, etc. In both cases when the Company is acting as the Controller or the Processor the relevant agreement must be agreed. In either case, the Company has entered into the appropriate data processing agreements in order to ensure the integrity and security of the data subjects' personal data.

The Company as the Controller and the Processor must appoint a DPO who is responsible for overseeing this Privacy Policy and, as applicable, developing Related Policies. The DPO is acting in accordance with Article 37 of the GDPR and is tasked with the responsibility of monitoring compliance with this Privacy Policy is sufficient for GDPR purposes. The DPO is from time to time assisting and consulting the companies of the Group regarding GDPR and this Privacy Policy.

The post of the DPO is held by Mr Ilya Parshikov, whom you may contact by phone at +357 25 58 28 48 or via email at gdpr@korpusprava.com. Please contact the DPO with any questions about the operation of this Privacy Policy or the GDPR and other data protection legislation or if you have any concerns that this Privacy Policy is not being or has not been followed.

PERSONAL DATA PROTECTION PRINCIPLES

The Company adheres to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

a. Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

b. collected only for specified, explicit and legitimate purposes (purpose limitation);

c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation);

d. accurate and where necessary kept up to date (accuracy);

e. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (storage limitation);

f. processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

g. not transferred to another country without appropriate safeguards being in place (transfer limitation); and

h. made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data (data subject's rights and requests).

The Company is responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

LAWFULNESS, FAIRNESS, TRANSPERENCY

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Company may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that the Company processes personal data fairly and without adversely affecting the data subject.

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 the Company's legal compliance obligations;

d. to protect the data subject's vital interests;

e. to pursue the Company's 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 the Company processes personal data for legitimate interests need to be set out in this Privacy Policy and the consent sent to the client for approval and signing.

The GDPR requires the Controller to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Whenever the Company collects personal data directly from data subjects, including for human resources or employment purposes, the Company provides the data subject with all the information required by the GDPR including the identity of the Controller and DPO, how and why personal data would be used, processed, disclosed, protected and retained that personal data through a Privacy Notice which must be presented when the data subject first provides the personal data. A Privacy Notice must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them. A Privacy Notice may be provided to the data subject prior the consent (e.g. information message on the website) or be a part of the consent which may be signed or not (e.g. hard copy consent).

When personal data is collected indirectly (for example, from a third party or publicly available source), the Company must provide the data subject with all the information required by the GDPR as soon as possible after collecting or receiving the data. The Company must also check that the personal data was collected by the third party in accordance with the GDPR.

CONSENT

The Controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include a Consent. A data subject's consent to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. The Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If the consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. The data subject must be easily able to withdraw the Consent to processing at any time and withdrawal must be promptly honoured. The Consent may need to be refreshed if the Company intends to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented. When processing special category data or criminal convictions data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible.

As a general rule the Company obtains two type of Consents from the Clients. First Consent for the usage of his/her name and email the Client can give 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. Second Consent he/she gives for usage of personal data for provision of services and for receiving information. Second consent is usually given personally via signing a hard copy. The Client can sign only second Consent if first communication was personal during the meeting. The second consent is usually an additional document to the contract which is concluded with the client. In second Consent the Client usually declares that he/she gives his/her Consent to collection, storage, processing, cross-border processing and transfer of his personal data to third parties and third countries in case of provision of one or more of the following services:

- Company incorporation and administration;
- Legal and tax support;
- Accounting control and audit;
- Opening bank account;
- Consulting;
- Safekeeping services;
- Escrow services;
- Management and administration of investment entities;
- Services under Financial Account Tax Compliance Act (FATCA)/ Common Reporting Standard (CRS);
- Services under DAC 6 Directive;
- Outsourcing the data protection function.

Personal data would be collected only in case of the Client's request for one or more of the services mentioned above. The right to withdraw the Consent is indicated in both Consents and always declaimed by the employees of the Company during the meetings.

The Client may also give his/her consent to use his/her name and email to the Company to send him/her information related to the services mentioned above, marketing materials and information.

The Company needs to evidence Consent captured and keeps records of all Consents in accordance with this Privacy Policy so that the Company can demonstrate compliance with Consent requirements.

PURPOSE LIMITATION, DATA MINIMISATION, ACCURACY

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. The Company does not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Company has informed the data subject of the new purposes and they have Consented where necessary.

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. The Company may only process personal data when performing of job duties requires it. The Company cannot process personal data for any reason unrelated to job duties and does not collect excessive data. The Company ensures that when personal data is no longer needed for specified purposes, it is deleted or anonymised.

The Company ensures that personal data is held is accurate, complete, kept up to date and relevant to the purpose for which it was collected. The Company undertakes to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. The Company furthermore takes all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

SHARING PERSONAL DATA

Generally, the Company is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. Personal data may only be shared between employees, agents or representatives of the Group if the recipients have a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

The Company may only share the personal data it holds with third parties, such as but not limited to service providers, if:

a. they have a business need to know the information for the purposes of providing the contracted services;

b. sharing the personal data complies with the Privacy Notice provided to the data subject and, if required, the data subject's consent has been obtained;

c. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

d. the transfer complies with any applicable cross-border transfer restrictions; and

e. a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

In any event, the Company requires all third parties to respect the security of your personal data and to treat it in accordance with the law. The Company does not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. The Company transfers personal data originating in one country across borders when it transmits, sends, views or accesses that data in or to a different country.

The Company 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 the Company transfers the personal data ensures an adequate level of protection for the data subject's 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 justified pursuant to any one of the derogations stipulated in Article 49 of the GDPR the performance of a contract between the Company 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.

RECORD KEEPING AND STORAGE LIMITATION

The Company must keep and maintain accurate corporate records reflecting processing including records of data subjects' Consents and procedures for obtaining Consents. Clients' personal data, information and Consents are kept in electronic version in the database and in hard copies in Clients' files.

The Company must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which the Company originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements. The Company as a licensed ASP which is acting in Cyprus must comply with the Law and the Directive DI144-2-007-08 of 2012 Of the CYSEC for the Prevention of Money Laundering and Terrorist Financing ("the Directive"). In accordance with the Law and the Directive as a general rule the Company has to keep records (including identification documents) for a period of at least five (5) years, which is calculated after the termination of business relationships. The documents/data relevant to ongoing investigations are kept until the relevant authority (e.g. the Unit for Combating Money Laundering (the "MOKAS")) confirms that the investigation has been completed and the case has been closed.

The Company takes all reasonable steps to destroy or erase from its systems all personal data that it no longer requires. This includes requiring third parties to delete that data where applicable.

AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

a. a data subject has Explicitly Consented;

b. the processing is authorised by law; or

c. the processing is necessary for the performance of or entering into a contract.

Due to the scope of personal data processed and the nature of its business, the Company does not use Automated Processing and ADM.

PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

In accordance with GDPR the Company is required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

The Company must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that process personal data by taking into account the following:

a. the state of the art;

b. the cost of implementation;

c. the nature, scope, context and purposes of processing; and

d. the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

In relation to the nature of Company's business the Privacy by Design procedures are performed in the following way. From time to time individuals or company representatives can submit their enquiries through the website of the Company prior to becoming clients of the Company. While submitting they can voluntarily indicate their personal data, nicknames or other information. The enquiry can only be accessed by the person who has submitted it and the employee of the Company, while communication takes place online and the messages cannot be saved or stored. These measures are described in more detail in the Technical Measures Policy. At this stage the Company doesn't need any personal data. When an individual or a company representative requests any services and the Company needs to obtain personal data, the Company sends the Privacy Notice and proposes to the Client to sign the Consent as it is described in this Privacy Policy above.

In accordance with GDPR the Company must also conduct DPIAs in respect to high-risk Processing.

The Company should conduct a DPIA (and discuss findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

a. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

b. Automated Processing including profiling and ADM;

c. large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

d. large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

a. a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

b. an assessment of the necessity and proportionality of the Processing in relation to its purpose;

c. an assessment of the risk to individuals; and

d. the risk mitigation measures in place and demonstration of compliance.

SECURITY INTEGRITY AND CONFIDENTIALITY, PROTECTING PERSONAL DATA, REPORTING A PERSONAL DATA BREACH

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The Company has developed, implemented and maintains safeguards appropriate to our size, scope and business, our available resources,

the amount of personal data that the Company own or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). The Company regularly evaluates and tests the effectiveness of those safeguards to ensure security of processing of personal data. The Company takes particular caution in handling and protecting special categories of personal data and criminal convictions data from loss and unauthorised access, use or disclosure.

The Company must follow all procedures and technologies it puts in place to maintain the security of all personal data from the point of collection to the point of destruction. The Company may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested by the Company.

The Company maintains 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 business 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; and

c. Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

The Company complies with the Technical Measures Policy which is additional to this Privacy Policy and sets out all technical measures which the Company performs to secure and protect personal data in accordance with GDPR and data protection legislation.

In case of personal data breach, the Company as the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority unless the personal data breach is unlikely to result in risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach. The Company as the Controller documents any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

Any data breach recognised by employees must be reported to the DPO who resolves if to notify supervisory authority or not. The DPO draws an internal report which must contain information described above. The draft of Internal Data Breach Report is the APPENDIX 1 to this policy.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall communicate the personal data to the data subject without undue delay. The communication to the data subject shall be in clear and plain language the nature of the personal data breach and contain at least the information and measures taken by the Company. The communication to the data subject shall not be required if any of the following conditions are met:

a. the Company has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to assess it, such as encryption;

b. the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

DATA SUBJECT'S RIGHTS AND REQUESTS

In accordance with the GDPR data subjects have the following rights in relation to their personal data:

a. to withdraw Consent to processing at any time;
b. to receive certain information about the data Controller's processing activities;
c. to request access to their personal data that the Company holds;
d. to prevent the Company's use of their personal data for direct marketing purposes;
e. to ask the Company to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
f. to restrict processing in specific circumstances;
g. to challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
h. to request a copy of an agreement under which personal data is transferred outside of the EEA;
i. to object to decisions based solely on Automated Processing, including profiling (ADM);
j. to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
k. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
l. to make a complaint to the supervisory authority;
m. in limited circumstances, to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

The data subject may at any time withdraw his/her consent, request access to his/her personal data, request the restriction of processing or perform any other rights mentioned above via sending an email, mail or during personal meeting. The data subject may at any time upon request by email, mail or during the personal meeting receive any information regarding the usage of his/her personal data. The Company must verify the identity of an individual requesting data under any of the rights listed above. The Company must immediately forward any data subject request it receives to the DPO. The DPO must provide the requested information to the data subject free of charge via email or mail without undue delay (depending on the complexity of the data subject's request or in case that the data subject has made a number of requests, in which case, the Company will notify the data subject and keep him/her updated), and in any event within a month from the receipt of such request However, the Company may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive.

The Company wants to ensure that the data subject's personal information is accurate and up to date. If any of the information that the data subject has provided to the Company changes he/she may let the Company know the correct details by sending an email to gdpr@korpusprava.com.

The data subject may ask the Company, or the Company may ask the data subject, to correct information the data subject or the Company think is inaccurate, and the data subject may also ask the Company to remove information which is inaccurate.

The data subject may withdraw his/her consent allowing the Company to process and use his/her personal information at any time. If the data subject elects to withdraw his/her consent he/she is entitled to have the personal information the Company holds about the data subject deleted or erased without undue delay, following a relevant request to this effect. The data subject may also be entitled to require the Company to stop sharing this information and prevent any third parties from continuing to use this information. However, this will not affect the lawfulness of any processing carried out before the data subject withdraws his/her consent. If the data subject withdraws his/her consent, the Company may not be able to provide certain services to the data subject. The Company will advise the data subject if this is the case at the time he/she withdraws his/her consent.

The data subject may also exercise his/her right to have such information erased or deleted from the Company's system in so far as the information in question is no longer relevant for the purpose for which it was originally provided by the data subject for processing. The data subject's personal data will be erased or deleted except cases when the storage of data is required by law.

The data subject is also entitled to request an electronic copy of the personal data that he/she has provided and request that these be transmitted directly, where this is possible, to another entity without hindrance. The Company will provide to the data subject, or a third party he/she has chosen, his/her personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which the data subject initially provided consent for the Company to use or where the Company used the information to perform a contract with the data subject.

Furthermore, the data subject has a right to object, at any time, to the processing of the personal information that he/she has submitted provided such an objection can be justified on legitimate grounds.

COOKIES

Cookies are small text files placed on the data subject's computer to collect standard Internet log information and visitor behaviour information. The information is used to track visitor use of the website and to compile statistical reports on website activity. The Company's website provides information about cookies and the right not to accept them. Data subject can set his/her browser not to accept cookies and the above websites will tell how to remove cookies from the browser. The Company also notifies that in a few cases some of the Company's website features may not function if the cookies from the browser would be removed.

TRAINING AND AUDIT

Pursuant to the applicable data protection legislation, the Company is required to ensure that all Company personnel have undergone adequate training to enable them to comply with data privacy laws. The DPO of the Company has passed the necessary external training to perform his duties in accordance with the GDPR. The DPO of the company performs internal training for employees of the Company at least once a year.

The Company regularly reviews all the systems and processes under its control to ensure they comply with this Privacy Policy and checks that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

ACCOUNTABILITY

The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

a. appointing a suitably qualified DPO and an executive accountable for data privacy;

b. implementing Privacy by Design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of data subjects;

c. integrating data protection into internal documents including this Privacy Policy and Related Policies.

d. regularly training Company personnel on the GDPR, this Privacy Policy and Related Policies and data protection matters including, for example, data subject's rights, Consent, legal basis, DPIA and personal data breaches. The Company must maintain a record of training attendance by Company personnel; and

e. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

CHANGES TO PRIVACY POLICY

The Company reserves the right to make changes to this Policy from time to time and will notify its clients of such changes. This Policy with amendments will be uploaded on the Company's website without undue delay. Clients of the Company are responsible for reviewing the Policy after any such changes and such use shall constitute clients' agreement to the aforesaid changes.

ENQUIRIES

For any enquiries and information with regards to this Privacy Policy please email us at gdpr@korpusprava.com.

KORPUS PRAVA reviews this policy on an ongoing basis having regard to the relevant legislation and circulars provided by Office of the Commissioner for Personal Data Protection.

APPENDIX 1

INTERNAL DATA BREACH REPORT

Data subject name	Type of personal data	Type of breach, facts and effects	Action taken	Authority notification date	Data subject notification date

_____

Data Protection Officer

_____

Date