NORDIC SALES CREW OY – DATA PROTECTION POLICY

TABLE OF CONTENTS

DEFINITIONS

‘**Data subject’** means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**DPA**” means an agreement conducted in accordance with Article 28 of the GDPR between a controller and a processor that governs the processing of the personal data the processor processes on behalf of the controller.

‘**Compliance Measures’** are the organizational and technical measures with which the controller or the processor demonstrates that its processing activities comply with the Data Protection Laws.

‘**Consent’** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

‘**Controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"**Data Protection Laws**" means the Personal Data Act of Finland (523/1999), the GDPR and any other data protection laws in force and any legally valid instructions or orders given by the data protection authorities.

“**DPIA**” means the data protection impact assessment within the meaning of Article 35 of the GDPR.

“**DPO**” means a data protection officer within the meaning of Articles 37 to 39 of the GDPR.

'**GDPR'** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

'Personal data' means any information relating to a data subject.

'**Personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"**PICODF** " shall mean the person specified in Section 2 of Nordic Sales Crew Oy's Privacy Policy.

'**Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

1. INTRODUCTION

1.1 The purpose of this personal data protection policy is to establish the general framework for the protection of personal data we process (hereinafter "**Data Protection Policy"**). This Data Protection Policy describes the Compliance Measures of our company, which are the organizational and technical measures with which the controllers and the processors can comply and demonstrate that their processing activities comply with the Data Protection Laws. We use our Data Protection Policy as one of our internal tools to ensure that our personal data processing activities are lawful.

1.2 Our DPP is systematized according to:

(i) the lifecycle of personal data, which consists of five stages of data collection (Section 3), data storage (Section 4), data usage (Section 5), data forwarding (Section 6) and data deletion (Section 7); and

(ii) the common measures (Section 2) that are common to all stages.

This approach provides us a comprehensive method to ensure that our processing activities are lawful, as our DPP provides us guidance on how to lawfully process personal data in each specific stage of the processing, while having the necessary common measures in place to provide us general compliance with the Data Protection Laws.

1.3 We process personal data in two different roles, as the controller and as the processor.

We act as <u>the controller</u> when we process the personal data of the following categories of data subjects:	**We act as <u>the processor</u> when we process the personal data of the following category of data subjects:**
1.3.1 visitors of our website (hereinafter "**Visitors**"); 1.3.2 contact persons of our customers (hereinafter "**Customers**"); 1.3.3 contact persons of our potential customers (hereinafter "**Potential Customers**"); 1.3.4 our shareholders; 1.3.5 our employees; 1.3.6 our jobseekers; and 1.3.7 persons who contact us through email or other similar means (hereinafter "**persons who contact us**").	1.3.8 persons whose personal data we process on behalf of our customers due to us providing sales services to our customers (hereinafter the "**Customers of our Customers**").

Where our Compliance Measures differ as the controller from the Compliance Measures as the processor, we shall inform of the differences in the below mentioned way:

Our Compliance Measures as the controller are informed under the blue bar	**Our Compliance Measures as the processor are informed under the green bar**
- Example - Example	- Example - Example

Where our Compliance Measures are not marked with the abovementioned colored bars, our Compliance Measures are the same for all personal data we process.

1.4 Data processing activities against this DPP could result in sanctions and criminal penalties.

1.5 Our company is committed to reviewing our personal data protection strategies and objectives on an ongoing basis and to maintaining an effective personal data protection program. We are committed to high standards of compliance with the Data Protection Laws and require management and staff to adhere to these standards in preventing the unlawful processing of personal data. Adherence to this Data Protection Policy is absolutely fundamental for ensuring that all of our entities, regardless of geographic location, comply with applicable personal data protection legislation.

1.6 The Board of Directors of the company must accept this DPP in a meeting of the Board of Directors, after which they are in charge of the maintenance and the fulfillment of this DPP.

1.7 This DPP is based on continuous development, and the development measures are planned based on risk-based approach and e.g. audit findings. Thus, the DPP may be valid for a maximum period of one year following the decision of the Board of Directors, after which the Board of Directors must be review, possibly update and renew (the possibly updated version of) the DPP.

2. COMMON COMPLIANCE MEASURES

Compliance with Data Protection Laws and the accountability principle

2.1 Our compliance program with the Data Protection Laws is built around the accountability principle, and thus consists of three stages:

(I) having this DPP in written form;
(II) implementing this DPP into the actual practices of our company; and
(III) evaluating that this DPP is lawful and implemented into the actual practices of our company, by using audits in accordance with Sections 4.7 and 4.8.

By fulfilling all three stages described in this Section 2.1 we are able comply and demonstrate that we comply with the Data Protection Laws. Thus, by doing so we also comply with the accountability principle of the GDPR.

2.2 We shall ensure that our DPP is adequate, up to date and drafted with the help of data protection experts.

Data protection documentation

2.3 Our data protection documentation consists of:

Document name	**Purpose of the document**	**Publicity and availability in intranet**	**Reviews and actions**
2.3.1 DPP	By complying with this DPP, we can comply and demonstrate that we comply with Data Protection Laws.	Not public. Available to all our personnel in our intranet.	**Review**: The Board of Directors must review the document at least once a year. **Actions**: The Board of Directors are required to take necessary actions within one (1) week following the review.

			Additional actions: Please see Section 1.7 of this DPP.
2.3.2 DPAs (for more information please see Section 6)	These documents are data processing agreements that we conclude with every data processor that processes the personal data of our data subjects on our behalf and/or the data subjects of our customers on their behalf.	As a general rule, only the Board of Directors have access to the DPAs, as the DPAs may hold confidential information. However, our personnel in other positions may also be granted access to the DPAs if Board of Directors deems it necessary.	**Review**: The Board of Directors shall review the DPAs in accordance with each DPA. **Actions**: The Board of Directors shall take actions in accordance with the DPA
2.3.3 Training material	To educate our personnel in data protection	Not public. Available to all our personnel in our intranet.	N/A
2.3.4 Audit reports	A report of an internal or external audit of our data processing activities.	As a general rule, only the Board of Directors and PICODF have access to the reports, as the reports may hold sensitive information. However, our personnel in other positions may also be granted access to the reports if the Board of Directors deems it necessary.	**Review**: The Board of Directors shall review a report within one (1) week after receiving it. **Actions**: The Board of Directors is required to take necessary actions within one (1) week following the review.
2.3.5 Privacy Policy (for more information please see Section 2.5 and Annex 1)	(I) Record of processing activities as the controller (II) Privacy notice to data subjects	An updated version must always be kept available at our website: http://www.nordicsalescrew.com /tietosuojatiedote/ Available also to all our personnel in our intranet.	**Review**: PICODF shall review the document at least once a year. **Actions**: PICODF is required to take necessary actions within one (1) month following the review.
2.3.6 Record of processing activities as the processor	Record of processing activities as the processor for our customers.	Not public. Available to all our personnel in our intranet.	**Review**: PICODF shall also review the document at least once a year. **Actions**: PICODF is required to take necessary actions within one (1) month following the review. **Additional actions**: PICODF is required to update the record at once when it

			receives a new customer that uses its SaaS Services.

The position of a DPO in our company

2.4 According to the Article 37(1) some companies must assign a DPO to ensure that the company processes personal data in compliance with the Data Protection Laws. We are not required to have a DPO in our company, because:

- we are not a public body;
- our processing activities do not require regular and/or systematic monitoring of data subjects; and
- we do not process sensitive personal data on a large scale.

Privacy policy of our company and records of processing activities

Privacy Policy as the controller	**Records of processing activities as the processor**
2.5 Our privacy policy, which is found in http://www.nordicsalescrew.com/tietosuojatiedote/, contains Nordic Sales Crew Oy's records of processing activities as the controller, and it also acts as a communication from us to our data subjects through which we inform the data subjects of the ways Nordic Sales Crew Oy processes their personal data. We ensure that our privacy policy is always publicly, transparently and easily available at Nordic Sales Crew Oy's websites.	2.6 Our records of processing activities as the processor are found in our databases, and they are not publicly available. We shall provide our records of processing activities as the processor to authorities upon request and possibly to our customers, depending on the situation at hand.

DPAs

Concluding DPAs (controller's perspective)	**Concluding DPAs (processor's perspective)**
2.7 We shall ensure that we conduct DPAs with every processor that processes the personal data of the data subjects of Sections 1.3.1 – 1.3.7 on our behalf.	2.8 We shall ensure that anyone who uses our services, through which we process the personal data of the Customers of our Customers, agrees to an appropriate DPA before using our services.

Training and awareness program

2.9 We train our staff annually for the lawful processing of personal data by using the services of experts in personal data protection. We keep participant lists and course materials of the training sessions and store them safely. Our employees have free access to all our course materials.

Carrying out DPIA's

2.10 According to Article 35(1) of the GDPR, some controllers are required to carry out DPIAs, which are assessments aimed at verifying that the personal data processing activities comply with the requirements of the Data Protection Laws. Since we act as the processor for most of our data processing activities, and not as controllers, we are not obligated to perform DPIAs. However, we may perform DPIAs to better comply with the Data Protection Laws if we deem it appropriate or necessary.

2.11 If we decide to carry out DPIAs, they shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the company;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Laws taking into account the rights and legitimate interests of data subjects and other persons concerned.

Personal data breaches and notification of a data protection breach

Personal data breaches and notification of a personal data protection breach (controller's perspective)	**Personal data breaches and notification of a personal data protection breach (processor's perspective)**
2.12 In case of personal data breach that concerns the personal data of our data subjects, after becoming aware of the breach, we shall at once, and no later than 24 hours after becoming aware of the breach, arrange a meeting where the breach and the causes of the breach are assessed. In the meeting we assess if the breach is likely to result in a risk to the rights and freedoms of natural persons. A data breach is likely to result in a risk to the rights and freedoms of natural persons where:	2.15 In the case of a personal data breach concerns the personal of the Customers of our Customers, we shall follow the relevant DPAs that are found in our databases.

- the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage; - data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; - personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; - personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; - personal data of vulnerable natural persons, in particular of children, are processed; or - processing involves a large amount of personal data and affects a large number of data subjects. 2.13 If a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, we shall notify the data subjects without undue delay and the supervisory authority within 72 hours after having become aware of the breach. We use draft documents to notify data breaches: - Notifications made to the supervisory authority are conducted by using a draft	

document found in: https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta; and 2.14 Once we have contained the breach, we shall seek to fix it by using adequate means available. After the causes of the breach have been fixed and the breach has been communicated, the breach and the causes will be examined. The examination will set the guidelines for further actions and the actions try to guarantee that the breach would not happen again due to the same reasons.	

Data handling logs

2.16 As we mostly process personal data manually, we have deemed it not necessary to implement an information management software. PICODF shall evaluate the need for such a software on a yearly basis.

Requests and complaints from data subjects

2.17 The data subjects have the following rights:

Data subjects	Right to inspect	Right to rectify	Right to erasure	Right to restriction of processing	Right to data portability	Right to object	Automated individual decision-making, including profiling	Right to withdraw consent
Visitors	X		(XX)	(XX)		X		
Customers	X	X	XX	XX	X	X		
Potential Customers	X	X	XX	XX	X	X		
Affiliates	X	X	XX	XX	X	XX		
Shareholders	X	X	XX	XX				
Employees	X	X	XX	XX	X			
Jobseekers	X	X	XX	XX		X		XX
Persons who contact us through email or other similar means	X	X	XX	XX		X		

Customers of our Customers	DPA	DPA	DPA	DPA	DPA	DPA	DPA	DPA
X = data subjects can practically always use the right XX = data subjects can use the right under certain conditions (XX) = data subjects can use the right under certain conditions, but it is very unlikely that the conditions apply DPA = the rights are determined according to relevant DPA's								

- **Right to inspect**: The data subject has the right to know what, if any, data we have stored of her/him. While providing the requested information to the data subject, we must also inform the data subject of our regular sources of information, to what are the personal data used for and where is it regularly disclosed to.
- **Right to rectify and erasure**: The data subject has a right to request us to rectify the inaccurate and incomplete personal data concerning the data subject.

  The data subject can request us to erase the personal data concerning the data subject, if:
    - the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    - the data subject withdraws consent on which the processing is based on (concerns only the jobseekers and the persons who contact us);
    - the personal data has been unlawfully processed; or
    - the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which we are subject.

  The data subjects' rights to rectify and erase data does not concern the data which we must retain due to our legal obligations.

  If we do not accept the data subject's request to rectify or erase the personal data, we must give a decision of the matter to the data subject in a written form. The decision must include the reasons for which the request was not granted. The data subject may refer the matter to the relevant authorities (the Data Protection Ombudsman in Finland).

  We must inform the party to whom we have disclosed the personal data to or have received the personal data from of the rectification or erasure of personal data. However, there is no such obligation where the fulfilment of the obligation would be practically impossible or otherwise unreasonable.
- **Right to restriction of processing**: The data subject can request us to restrict the processing of the personal data concerning the data subject where one of the following applies:
    - the accuracy of the personal data is contested by the data subject for a period, enabling us to verify the accuracy of the personal data;
    - the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

- we no longer need the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.

If we have based the restriction of the processing of personal data on the abovementioned criteria, we shall give a notification for the data subject before removing the restriction.

- **Right to object**: Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning her/him for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- **Right to data portability**: The data subject shall have the right to receive the personal data concerning her/him, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent (concerns the jobseekers and the persons who contact us).
- **Automated individual decision-making, including profiling:** The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

  However, the data subject shall not have the aforementioned right if the decision is:
  - necessary for entering into, or performance of, a contract between the data subject and us;
  - is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
  - is based on the data subject's explicit consent.

- **Right to withdraw consent**: Where the legal basis for the processing of personal data is the consent of the data subject, the data subject shall have the right to withdraw her/his consent (concerns the jobseekers and the persons who contact us).

Requests and complaints from data subjects (controller's perspective)	**Requests and complaints from data subjects (processor's perspective)**
2.18 PICODF is in charge of the data files and the contacts from the data subjects described in Sections 1.3.1 – 1.3.7. 2.19 The rights of the data subjects of Sections 1.3.1 – 1.3.7 can be put into action only when the data subject has been satisfactorily identified.	2.20 If the Customers of our Customers contact us wishing to utilize their rights (see Section 2.17), we shall follow relevant DPAs in helping them to utilize their rights, because our customer is the controller of that personal data, whereas we are only the processor.

Certifications and codes of conduct

2.21 When valid certifications and codes of conduct are published by the relevant authorities and/or other such bodies, we shall revise our need for certifications and the compliance with the codes of conduct.

Audit plan

2.22 Data Protection Auditor	Nordic Law Oy
2.23 Audit fulfillment	(1) Audit planning - Our audit plan is based on Sections 2.22 – 2.24 of this DPP - Nordic Law Oy shall review our systems, operations, processes and people
	(2) Audit preparation - We contact and ask Nordic Law Oy for an audit schedule and an audit plan at least one (1) month before an audit ought to take place
	(3) Conducting audit - Yearly audit is held during May of each year - Other audits are held if Board of Directors deems them necessary
	(4) Report - Nordic Law Oy provides us an audit report with suggestions for possible corrective measures and, if necessary, a closing meeting within one (1) month after concluding an audit
	(5) Actions - Necessary actions based on audit reports must be taken within one (1) month after receiving an audit report
2.24 Record keeping	CEO is responsible for keeping records of all audits

3. DATA COLLECTION

Categories of data subjects

Categories of data subjects (controller's perspective)	**Categories of data subjects (processor's perspective)**

3.1 We collect personal data of the categories of data subjects described in Sections 1.3.1 – 1.3.7. We act as a controller for such data.	3.2 We receive personal data of the Customers of our Customers, when our customers willingly and on their own initiative decide to use our services. We act as a processor for such data.

Categories of personal data

Categories of personal data (controller's perspective)	**Categories of personal data (controller's perspective)**
3.3 The data files concerning Visitors may contain the following categories of personal data: - IP-addresses. 3.4 The data files concerning Customers and Potential Customers may contain the following categories of personal data: - contact information, such as full name, address, phone numbers, e-mail addresses and personal identification numbers; - nationality, age, gender, title or profession and language skills; - possible registration information, such as username, pseudonym, password and other unique identification; and - possible other information data subject discloses to us. 3.5 The data files concerning our shareholders, employees and jobseekers may contain the following categories of personal data: - contact information, such as full name, address, phone numbers, e-mail addresses and personal identification numbers; - videos and pictures; - nationality, age, gender, title or profession and mother tongue; - other information derived from the CVs, such as the work experience, educational background and other such skills;	3.7 The data files concerning the Customers of our Customers may contain the following categories of personal data: - contact information, such as full name, address, phone numbers, e-mail addresses and personal identification numbers; - nationality, age, gender, title or profession and language skills; - bank account data; and - all other possible Personal Data we process to sell our customer's product on the customer's behalf.

- bank account data; - location data; - possible registration information, such as username, pseudonym, password and other unique identification; - information relating to the implementation of communications and information relating to use of services, such as browsing and search information; and - possible other information gathered with the data subject's consent. 3.6 The data files concerning persons who contact us may contain the following categories of personal data: - contact information, such as full name, address, phone numbers, e-mail addresses and personal identification numbers; - information relating to the implementation of communications and information relating to use of services, such as browsing and search information; and - possible other information data subject discloses to us.	

Lawful purpose for data collection

Categories of data subjects	**Lawful purpose for data collection**	**Explanation**
3.8 Visitors	- Legitimate interest - Consent under the Finnish Act on Electronic Communications Services	We have a right to process personal data of Visitors based on the: - legitimate interests pursued by us, as it is necessary for us to process cookie data to improve our website so

		we can stay in business; and/or - under the Finnish Act on Electronic Communications Services, we are allowed to process cookie data due to implied consent.
3.9 Customers	- Contract - Our legitimate interests	We have a right to process personal data of the players of our games based on the: - performance of a contract between us through which Customer can use our service; and - legitimate interests pursued by us, as we need to market our services and evaluate the relationship to improve our services to keep us in business.
3.10 Potential Customers	- Our legitimate interests	We have a right to process personal data of Potential Customers based on the: - legitimate interests pursued by us, as we need to market our services to potential customers to keep us in business.
3.11 Our shareholders	- Our legitimate interests - Our legal obligations	We have a right to process personal data of shareholders based on the: - legitimate interests pursued by us, as it is necessary for us to process personal data due to our

		administrative tasks; and - legal obligation to which we are subject as a limited liability company.
3.12 Our employees	- Contract - Our legitimate interests - Our legal obligations	We have a right to process personal data of employees based on the: - performance of an employment contract; - legitimate interests pursued by us, as it is necessary for us to process personal data due to the employment relationship; and - legal obligation to which we are subject as the employer.
3.13 Our jobseekers	- Our legitimate interests	We have a right to process personal data of the jobseekers of based on the: - legitimate interests pursued by us, as it is necessary for us to process the personal data to evaluate the jobseekers and potential employment relationships; and / or
3.14 Persons who contact us	- Our legitimate interests	We have a right to process personal data of the persons who contact us through email or other similar means based on the: - legitimate interests pursued by us, as it is necessary for us to

		process personal data to handle the contacts made to us.
3.15 Customers of our Customers	- Contract	As a processor, we have a lawful initial purpose to collect the personal data of the Customers of our Customers based on: - the performance of a contract between us and our Customers.

Fair data collection

Fair data collection (controller's perspective)	**Fair data collection (processor's perspective)**
3.16 When we collect personal data of the data subjects of Section 1.3.1 – 1.3.7, we shall always, where applicable, provide the data subjects our privacy policy before any data is collected about them.	3.17 We ensure that we have formed adequate DPAs with our customers before we provide them with any of our sales services and collect any personal data on their behalf. 3.18 We do not provide the Customers of our Customers our privacy policy because we act as the processor for such data. It is our customers responsibility to inform those data subjects of the way their personal data is processed.

Purpose limitation and proportionality

Purpose limitation and proportionality (controller's perspective)	**Purpose limitation and proportionality (processor's perspective)**
3.19 Personal data of Visitors can be handled for the following purposes: - for improving our website; and - analysis and statistics. 3.20 Personal data of Customers and Potential Customers can be handled only for the following purposes:	3.24 Personal data of the Customers of our Customers can be handled only for the purposes that have been specifically defined in the relevant DPAs.

- management and development of the customer relationship; - customer service; - marketing; - to enable us to comply with our legal and regulatory obligations; and - analysis and statistics. 3.21 Personal data of our shareholders can be handled only for the following purposes: - to conduct business; and - to enable us to comply with our legal and regulatory obligations. 3.22 Personal data of our employees and jobseekers can be handled only for the following purposes: - management and development of the employee and jobseeker relationships; - management of employment contracts and other related matters; - to enable us to comply with our legal and regulatory obligations; and - analysis and statistics. 3.23 Personal data of persons who contact us can be handled for the following purposes: - customer service; - to enable us to comply with our legal and regulatory obligations; and - analysis and statistics.	

Regular sources of information

Regular sources of information (controller's perspective)	**Regular sources of information (processor's perspective)**
3.25 Information regarding the data subjects of Sections 1.3.1 – 1.3.7 are regularly gathered:	3.26 Information regarding the Customers of our Customers are regularly gathered from the data subjects themselves as we sell them the products of our customers.

- from data subjects themselves though our service, face-to-face or via phone, internet, e-mail or in other similar fashion; - with cookies and other similar tech; - by Nordic Sales Crew Oy's other affiliate companies; and - from the Population Register Center/Population Information System, Posti's address database, phone companies' databases and other similar private and public registries.	

4. DATA STORAGE

Data security

4.1 We ensure that we implement adequate technical and organizational measures to ensure adequate level of safety to the processing of personal data.

Access to personal data on an organizational level (controller's perspective)	**Access to personal data on an organizational level (processor's perspective)**
4.2 Only our authorized employees have access to the personal data: - only our employees in management position have authorization to handle the personal data of Visitors, Customers and Potential Customers; - only our employees in human resources position have authorization to handle the personal data of the data subjects of our shareholders, employees and jobseekers; and - only our employees who are in charge of managing contacts made to our company have authorization to handle the personal data of persons who contact us.	4.3 Only our employees in sales position have authorization to handle the personal data of the Customers of our Customers.

4.4 We have adequately protected all electronic machines through which we process personal data, by using up-to-date programs, appropriate technical security measures, as in firewalls, and so on.

4.5 We store all manual records safely and restrict access to them from the persons who are not authorized to process such data.

4.6 Where our employees do work out of office, we ensure that those employees process personal data only through protected means by providing those employees with protected working equipment or making sure that their home devices, through which they work, are adequately secured.

Auditing

4.7 This Data Protection Policy and our overall data processing activities will be internally reviewed and revised when necessary.

4.8 This Data Protection Policy and our overall data processing activities shall will be reviewed by external data protection experts annually and where necessary.

4.9 The Board of Directors are responsible for keeping records of all audits.

Mechanisms for periodic reviews

4.10 PICODF shall review the necessity of the personal data we have stored once a year. We retain accounts of the results of the reviews.

4.11 The Board of Directors must annually ensure that PICODF has complied with his/her obligations for periodic data retention reviews.

5. DATA USAGE

Purpose limitation

5.1 We shall use the personal data only for the purposes for which it was collected. See Section 3.8 – 3.15.

Marketing

We provide direct marketing in the following way as the controller:	
Category of data subjects	**The lawful purpose for direct marketing**
5.2 Customers	We provide marketing of our services because it is necessary for the purposes of our legitimate interests, as we have to keep us in business.

5.3 Potential Customers	We market our products because it is necessary for the purposes of our legitimate interests, as we have to market our products to keep us in business.

5.4 Where we provide direct marketing, we shall ensure that we provide a "soft opt-in" approach, which idea is that when we provide direct marketing to a party, we offer an opt-out option for the receiving party:

- in emails this means that we have to provide a link in each email that enables the receiving party to opt-out of our direct marketing emails in the future; and
- in phone calls this means that we have to delete the receiving party's contact information if he/she so wishes.

5.5 We do not use bought in lists of leads to whom we could provide direct marketing to.

6. DATA FORWARDING

Transfer restriction

Transferring personal data (controller's perspective)	**Transferring personal data (processor's perspective)**
6.1 We can transfer personal data of the data subjects of Sections 1.3.1 – 1.3.7 only if we have concluded adequate DPAs with the recipients who act as our processors.	6.2 We can transfer personal data of Customers of our Customers to the recipients that are specified in the relevant DPAs.

Deletion of data by processors and third parties

6.3 When our personal data is deleted from our databases, we shall ensure that the processors and third parties also delete such information.

Information transfer outside of EU or the European Economic Area

6.4 Personal data is not transferred to third countries.

7. DATA DELETION

Retention limits

Retaining personal data (controller's perspective)	Retaining personal data (processor's perspective)
7.1 We shall retain only the necessary data of the contact persons of our customers for a period of three (3) years following the end of customer relationships. 7.2 We shall retain only the necessary data of contact persons of our potential customers for a period of two (2) year following collection of the data, if the potential customers have not turned into our actual customers. 7.3 We shall retain only the necessary data of our current and former shareholders for indefinitely, as we are required to do under the applicable law. 7.4 We shall retain only the necessary data of our employees for a period of ten (10) years following the end of their employment in our company, because we have a legal obligation to provide our former employees with references during that period. 7.5 We shall not retain the data of the jobseekers, who were not employed by us, if the data subjects do not explicitly give us their consent to do so. Having received such a consent, we may retain only the necessary data of the data subjects for a period of six (6) months following explicit consent. 7.6 We shall retain only the necessary data of persons who contact us through email or other similar means for a period of one (1) year following the contact. 7.7 However, we may retain the data of all data subjects for longer than is described above, where we are required to do so by law, it is necessary due to legal proceedings and it is	7.8 When we retain the data of the Customers of our Customers, we shall comply with the relevant DPAs.

necessary for any similar reason. We shall be careful not to apply this Section in vain.	

7.9 We inspect the necessity of the personal data stored regularly and keep records of the inspections.

Deletion of data

7.10 We shall ensure that we erase all personal data, including copies and other similar data files, that we are not authorized to process.

7.11 We shall ensure that the data subjects can use their right of erasure in accordance with our privacy policy.

DATES AND SIGNATURES

[xx].[xx].2018

_____ _____

Mathias Dahlqvist Tong Cheng

_____ _____

Paavo Pörsti Juuso Saarinen

_____

Frans Westerlund