

## NOVA SERVICES ZRT. PRIVACY POLICY FOR JOB APPLICATIONS

### Introduction

- 1.1. **Nova Services Zrt.** as data controller (hereinafter referred to as the “**Company**” or the “**Controller**”) informs job applicants in this Privacy Policy (hereinafter referred to as the “**Policy**”) how it processes personal data concerning the applicants for the job vacancies it advertises.
- 1.2. When handling, recording, processing and transferring the personal data of the Data Subject, the Controller acts in compliance with 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, and repealing Regulation (EC) No 95/46/EC (“**GDPR**”), Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (the “**Information Act**”), and other statutory provisions and regulatory recommendations on data protection.
- 1.3. In order to comply with data security requirements, the Controller ensures the protection and security of the personal data of the data subject, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transferred, stored or otherwise processed.
- 1.4. The personal data are processed with the consent of the data subjects and pursuant to statutory authorisations, or to the extent necessary for the performance of a contract and in connection with the enforcement of the legitimate interests of the Controller. Through its internal organisational units, it takes all the data security, technical and organisational and administrative measures necessary to ensure an adequate level of security of personal data. To this end, the functions of operating and developing security, data protection and IT systems within the company are separate and independent.
- 1.5. We also state for what purposes and how we will use such data and how we ensure the retention and protection of personal data.

Please read the Privacy Policy carefully before submitting your application to us so that you understand how we process your personal data and your rights regarding data processing. If you require further information beyond what is set out in this Policy or if you have any comments or objections regarding the processing of your data, please contact **Nova Services Zrt** at the following contact details:

Registered office:	1095 Budapest, Soroksári út 30-34
Telephone:	+36-20-310-3441
E-mail:	<a href="mailto:info@novaservices.hu">info@novaservices.hu</a>

### 1. Definitions

**Controller:**

Company name:	<b>Nova Services Information Technology Services Private Limited Company</b>
Registered office:	1095 Budapest, Soroksári út 30-34
Company registration number:	01-10-141128
Website:	<a href="https://www.novaservices.hu/">https://www.novaservices.hu/</a>
Representative:	János Bacskai Board Member
Telephone:	+36-20-310-3441
E-mail:	<a href="mailto:info@novaservices.hu">info@novaservices.hu</a>
Data protection officer:	Zsigmond Fröhlich

### Definitions related to data processing:

For the purposes of this Policy, each of the definitions set out below has the following meaning:

*“personal data”* means any information relating to an identified or identifiable Data Subject; an identifiable Data Subject (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;

*“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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

*“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;

*“processor”* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

*“recipient”* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

*“third party”* means a natural or legal person, public authority, agency or body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

*“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;

*“sensitive data”* means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data and biometric data revealing the identity of natural persons, personal data concerning health and the sex life or sexual orientation of natural persons;

*“data concerning health”* means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

*“transfer”* means the making available of personal data to a specific recipient

*“personal data breach”*: a personal data breach means a breach of security relating to the processing of personal data that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Other terms defined in the Regulation are set out in Article 4 of the Regulation

## **The Data Subjects concerned**

The scope of the Policy applies to anyone who responds to a job advertisement of the Controller or who applies for a position not advertised by the Controller (hereinafter referred to as **“Applicant”** or **“Data Subject”**). By submitting their application to the Company, the Candidate accepts the terms of this Policy and consents to the processing of their data in accordance with this Policy. Without an advertised position, the Controller will notify the Candidate of the Policy immediately after the application and will request confirmation from the Candidate that they have read the Policy. The Controller has the right to unilaterally amend the Policy at any time.

Candidates are notified of this Policy by the Controller

- (a) where possible, before the data are provided, or
- (b) in the light of the specific circumstances in which the personal data are processed, within a reasonable period from the date on which the personal data were obtained, but not later than one month; or
- (c) if the personal data are used for the purpose of contacting the Candidate, at the time of first contact with the Candidate; or
- (d) if the data are likely to be disclosed to another recipient, at the latest when the personal data are disclosed for the first time.

## **2. Purposes, legal bases, scope and duration of processing, data security**

### **2.1. Purposes of the processing:**

- (I) recruitment;
- (II) communication;
- (III) enforcement of rights

**For purposes I and II, the legal basis for processing** is the Data Subject's voluntary consent pursuant to Article 6(1)(a) of the GDPR. If the Data Subject also provides sensitive

personal data in connection with their application, the legal basis for processing is the voluntary, explicit and informed consent of the Candidate, pursuant to Article 9(2)(a) GDPR. If the Candidate also provides personal data in connection with their application material relating to their reduced capacity to work, deterioration of health or impairment of health, the Controller also processes such data on the basis of the explicit consent pursuant to Article 9(2)(a) of the GDPR.

The data is processed by the Controller through its Website and other websites offering job advertisements for the purposes of registering applicants in the database, evaluating applications submitted, notifying applicants for advertised jobs after the selection process is completed and, with specific consent, for further storage in Nova Services Zrt.'s own database.

**Purpose of processing III:** Processing of the Candidate's personal data for legitimate interests pursuant to Article 6(1)(f) GDPR.

The purpose of the processing is to enable the Company to meet its obligation to provide evidence in the event of any legal action by the Candidate. In the event of rejection of the job application, the Company will keep the online and paper Candidate data for a further 3 years after the rejection for the purpose of possible redress to the Directorate General for Equal Treatment of the Office of the Fundamental Rights Commissioner. For this purpose of processing, the Company does not actively process the data, it only stores them.

Legal basis for the processing: the processing of the Candidate's personal data for the Company's legitimate interest pursuant to Article 6(1)(f) of the GDPR.

## **2.2. Scope of data processed and duration of data processing**

### **re I and II, Scope of data processed for recruitment/contact purposes**

The data processed by the Company from the Candidates are the following: all the data provided by the Candidate in the Data Submission Form or in their application/resume, in particular:

<b>Scope of data processed</b>	<b>Purpose of data processing</b>
Name of applicant	necessary for identification
place and date of birth	necessary for identification
mother's name	necessary for identification
photo	necessary for identification
e-mail address	necessary for contacting
address	necessary for contacting
title of position applied for	necessary for identifying the application
a list of previous work experience	necessary for the assessment of the application, for the selection of an employee with the appropriate competences

<b>Scope of data processed</b>	<b>Purpose of data processing</b>
qualifications	necessary for the assessment of the application, for the selection of an employee with the appropriate competences
foreign language skills	necessary for the assessment of the position, for the selection of the employee with the appropriate competences
sensitive data: e.g. data concerning health, medical data of a person with reduced working capacity	sensitive data are only processed if the processing is necessary to fill the position
other information included in the curriculum vitae sent	necessary for the assessment of the application, for the selection of an employee with the appropriate competences
the cover letter sent	necessary for the assessment of the application, for the selection of an employee with the appropriate competences
an indication of specific consent to the processing of data for 1 year after application if the Candidate is not hired	necessary for the legal basis for further processing in the event of non-selection
requested wage	necessary for the assessment of the application
trial work done during the selection process	necessary for the assessment of the application, for the selection of an employee with the appropriate competences

### **Scope, limits and duration of processing**

The Controller will process the personal data of Candidates only to the extent and for the duration necessary for the purposes set out above. Only personal data that is necessary for the purposes for which it is processed and is adequate to achieve those purposes may be processed.

The Controller will process the data of the Candidates for recruitment/contact purposes for the time necessary to achieve the purpose, i.e. until the application is assessed, until the advertised job is filled, until the employment contract is concluded, or for a further period of 1 year after the assessment of the application, only with the explicit consent of the Candidate, or until the Candidate's request for cancellation submitted in the meantime has been met, in order to enable the Company to assess the suitability of the Candidate's competences and to contact the Candidate if justified in the event of a vacancy for the same or a similar post at a later date. A request for erasure made by the Candidate in the meantime interrupts the processing, in which case the end of processing is the date when the erasure is completed. In the absence of a request for erasure by the Candidate, the Company will automatically erase the Candidate's personal data (except in the case of processing based on legitimate interest) at the end of the contact period (fulfilment of the purpose of processing). The data of any Candidate who has been hired will be further processed in accordance with the Company's Employee Privacy Policy.

### **re III, Scope of data processed for law enforcement purposes**

The scope of the data processed for this purpose is the same as the scope of the data processed during the recruitment process.

#### **Scope, limits and duration of processing**

Where the job application is rejected, the Company will keep Candidates' data processed for the purposes of rights enforcement for a further 3 years after the rejection for the purpose of possible repress to the Directorate General for Equal Treatment of the Office of the Fundamental Rights Commissioner. For this purpose of data processing, the Company does not actively process the data, it only stores them.

#### **4. Recipients of the processing**

Personal data of Candidates may be disclosed to the following persons within the Controller Company and the Companies belonging to the Group for the purposes and to the extent appropriate for those purposes:

The staff of the Human Resources Department for the following purposes:

- for recruitment purposes;
- preparation and storage of labour law documents and contracts.

The immediate superior of the position the Candidate is applying for, the middle manager of the relevant area and the representative of the Controller for the following purposes:

- for the purpose of recruiting their subordinates.

Persons who have access to personal data at the Controller are under a duty of confidentiality with regard to the personal data of Candidates, i.e. they must treat personal data and other information that they become aware of in the course of their duties or otherwise as confidential and not disclose it to third parties. This obligation continues without time limitation after the termination of the employment relationship.

Persons carrying out the processing are required to maintain the confidentiality of the personal data they process, to not use them for their own purposes, and to not disclose, transfer or make them available to anyone, except in the cases listed in the Policy.

#### **5. Source of the data:**

The Controller receives the data of the Candidates either directly from the Candidates or from a recruitment agency.

The Candidate may withdraw consent to processing at any time, but this does not affect the lawfulness of the processing carried out on the basis of consent prior to its withdrawal.

If the Candidate fails to provide personal data or provides incomplete data, depending on the type of incomplete data, the contact with the Candidate will fail or the Controller will not have sufficient data to assess the Candidate's suitability for the position, and thus the

Candidate's suitability for the position cannot be assessed and no employment contract can be concluded.

**6. The place of processing, the type of data processing technology used, data security:**

The Controller takes into account the requirement of data security in the design of its entire data protection process in accordance with the principle of *privacy-by-design*, i.e. data protection by default and by design. The Controller aims to minimise the processing of personal data to reduce the risks of data processing.

Persons who have access to personal data at the Controller are under a duty of confidentiality with regard to the personal data of Candidates, i.e. they must treat personal data and other information that they become aware of in the course of their duties or otherwise as confidential and not disclose it to third parties. This obligation continues without time limitation after the termination of the employment relationship. Persons carrying out the processing are required to maintain the confidentiality of the personal data they process, to not use them for their own purposes, and to not disclose, transfer or make them available to anyone, except in the cases listed in the Policy.

The Controller also takes the technical and organisational measures and complies with the procedural rules necessary to ensure data protection and data security.

The Candidate acknowledges that the Controller excludes any liability for any damage or loss resulting from any failure or malfunction of the IT connection. The Candidate acknowledges that any files they may attach will be subject to virus scanning and other data and information security screening by the Controller. The computer components of the system are located on the Controller's servers.

The Controller ensures the protection of the security of data processing by technical and organisational measures which provide a level of protection appropriate to the risks associated with the processing, by selecting the IT tools used and by operating them so as to ensure in respect of the data processed that:

- a) it is accessible to those authorised to access them (availability);
- b) authenticity and verification (authenticity of processing);
- c) that its unalterability can be verified (data integrity);
- d) it is accessible only to authorised persons and protected against unauthorised access (data confidentiality).

**Backup**

The Controller backs up its electronically stored data on a daily basis. The Controller ensures that the backups are stored on its own server. Legal basis for the processing for backups: legitimate interest of the Controller to comply with the requirements of the GDPR and to ensure the continuous and uninterrupted availability of data generated in



the course of its activities. The Controller handles large amounts of data, and has a material interest in the safe storage and recovery of that data in the event of a breach.

The purpose of the processing is to increase data security, to preserve and restore documents relating to the Controller's operations in the event of a data security problem, and to ensure the continuity of work processes.

Duration of backup storage: up to 5 years.

Personal data are stored in paper and electronic form on the Controller's servers at the Controller's headquarters.

## **8. Personal data breaches**

In the event of a personal data breach or data security incident, the Controller's employees must report the incident to the Data Protection Officer/Managing Director immediately after the incident is reported/detected.

If the personal data breach poses a high risk to the rights and freedoms of the Candidate, the Controller will inform the Candidate of the personal data breach without undue delay, including in particular:

- the name and contact details of the data protection officer
- the likely consequences
- the measures planned or taken to remedy the situation.

The Controller keeps a record of the personal data breaches, their known impact and the measures taken.

## **9. Processors**

To achieve the data processing purposes set out in Clause 2, the Controller may engage the services of third parties to perform certain of its tasks, which services may include the processing of Candidates' personal data. Such third parties (hereinafter referred to as "**Processors**") carry out the processing in accordance with the Controller's instructions and in compliance with the provisions of applicable law. Only the personal data necessary for the purposes of the processing will be transferred to each Processor for processing.

## **10. Data transfer**

The Controller may be entitled and obligated to transfer the personal data of Candidates to certain third parties in specific cases stipulated by law, in particular, but not limited to, a court, public authority, the police, prosecutor's office, local government or national security service. Candidates have the right to be informed of the transfer of their data to third parties, unless the provision of such information would jeopardise the purpose of the transfer.

The Controller keeps a record of data transfers, which includes:

- the date of transfer of personal data;



- 
- the legal basis for the transfer;
  - recipient of the transfer;
  - the scope of the personal data transferred.

The Controller represents that it will not transfer (or make available to a controller in a third country) the personal data of Candidates to a third country, i.e. a country outside the European Union.

The Controller will ensure that the legal conditions for processing (purpose, legal basis) are met during the transfer and that the transfer does not violate the rights of the Candidate.

## **11. Candidate's rights related to the processing**

*The Company draws the attention of the Data Subjects to the fact that in the event of a complaint or comment, it is advisable to contact the Company as Controller using one of the contact details indicated in this Policy.*

### **Rights of the Candidate**

#### **a) right of access**

The Candidate has the right to obtain from the Controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, the right to be informed of the personal data processed, the purposes of the processing, the categories of data, the recipients, the storage period, their rights and the source of the personal data.

The Company will provide the Candidate with a copy of the personal data processed. For additional copies requested by the Candidate, the Controller may charge a reasonable fee based on administrative costs.

#### **b) the right of rectification and erasure**

The Candidate has the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

#### **c) the right to erasure/‘right to be forgotten’**

The Candidate has the right to obtain from the Controller without undue delay the erasure of personal data concerning them. The Candidate may withdraw their consent to the processing within a given time limit, in which case the Controller has the right to process the data in accordance with the purpose of the processing until the end of such time limit. If the purpose of the processing ceases to exist or the Candidate has withdrawn their consent to the processing, the controller will no longer process the Candidate's data and will delete the personal data concerning the Candidate without further notice to the Candidate in accordance with its rules on scrapping data.

#### **d) restriction of the processing of the data;**

The Candidate has the right to obtain from the Controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the Candidate, for a period enabling the controller 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;
- the Controller no longer needs the personal data for the purposes of the processing, but they are required by the Candidate for the establishment, exercise or defence of legal claims; or the Candidate has objected to the processing; in which case the restriction applies pending the verification whether the legitimate grounds of the Controller override those of the Candidate.

Where processing is restricted on the basis of the above, such personal data shall, with the exception of storage, only be processed with the Candidate's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The Controller shall inform any recipient to whom or with which it has disclosed the personal data of the rectification, erasure, blocking or restriction of processing, unless this proves impossible or involves a disproportionate effort.

e) the right to data portability

The Candidate has the right to receive the personal data concerning them, which they have provided to the Controller, in a structured, commonly used and machine-readable format and has the right to transfer those data to a third party controller without hindrance from the Controller, if the processing is based on consent and the processing is automated. In exercising the right to data portability, the Candidate has the right to request, where technically feasible, the direct transfer of personal data between controllers. The exercise of this right is without prejudice to the right to erasure. That right does not apply where the processing is necessary for the performance of a task carried out in the exercise of a right of public interest. The exercise of the right shall not adversely affect the rights and freedoms of others.

f) right to object

The Candidate has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Candidate or for the establishment, exercise or defence of legal claims. The Candidate has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Unless the decision is:

- necessary for entering into, or performance of, a contract between the Candidate and the Controller;

- authorised by Union or Member State law to which the Controller is subject and which also lays down suitable measures to safeguard the Candidate's rights and freedoms and legitimate interests; or is based on the Candidate's explicit consent.

g.) Right to withdraw consent

Where the processing of personal data is based on the Data Subject's consent, the Data Subject has the right to withdraw consent at any time. Where consent is withdrawn, the processing is terminated by the erasure of personal data, provided that there is no other legal ground for the processing of their personal data. The withdrawal of consent has no consequences for the Data Subject. However, the withdrawal of consent does not affect the lawfulness of the processing previously consented to.

The Data Subject is entitled to exercise the above rights in relation to the legal grounds as follows:

	<u>Consent</u>	<u>Performance of a contract</u>	<u>Legal obligation</u>	<u>Legitimate interest</u>
<u>providing information</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<u>correction</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<u>restriction</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<u>erasure</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<u>objection</u>				<input checked="" type="checkbox"/>
<u>data portability</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<u>withdrawal of consent</u>	<input checked="" type="checkbox"/>			
<u>complaints</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<u>remedies</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## **12. Procedure in case of a request by the Candidate**

The Candidate may contact the Company representative identified at the beginning of this Policy at any of the contact details provided therein with any of the above requests or other questions or requests concerning their personal data.

The Controller shall process the request within 30 days of receipt of the written request. If necessary, taking into account the complexity of the request or the number of pending requests, the Company may extend the time limit for processing the request. The Candidate must be informed in advance of the fact and the reasons for the extension. If the Candidate's request is justified, the Controller will implement the requested measure within the procedural time limit and inform the Candidate in writing of the implementation. If the Controller rejects the Candidate's request, it will issue a written decision to that effect. In its decision, the Controller shall state the facts on which the decision is based, the grounds for its decision, with reference to the relevant legislation or case law, and inform the Candidate of the available legal remedies against its decision.

The Candidate is liable to pay the costs related to the exercise of their rights only if the Controller has informed the Candidate in writing within 8 days of receipt of the Candidate's request that the request is excessive and at the same time informed them of the administrative costs, but the Candidate has maintained their claim in writing despite these circumstances. The Candidate is deemed to have maintained the claim if, despite having been informed by the Controller, they do not withdraw their request within 5 working days or by the end of the administrative period. The Candidate who is liable for the costs shall pay such costs within 8 days of receipt of the payment notice issued by the Controller.

If the Candidate does not agree with the decision of the Controller or if the Controller fails to comply with the applicable procedural time limit, the Candidate may appeal to the supervisory authority or to a court.

### **Supervisory Authority**

If the Candidate considers that the processing of their personal data by the Controller violates the provisions of the data protection legislation in force, in particular the GDPR, they have the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information.

Contact details of the National Authority for Data Protection and Freedom of Information:

Website: <http://naih.hu/>

Address: 1055 Budapest, Falk Miksa utca 9-11, Mailing address: 1363 Budapest, Pf.: 9

Phone: +36-1-391-1400 Fax: +36-1-391-1410,

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

The Candidate also has the right to lodge a complaint with a supervisory authority established in another EU Member State, in particular in the Member State of their habitual residence, place of work or place of the alleged infringement.

### **Right to bring an action (Right of access to a court)**

Irrespective of their right to lodge a complaint, Candidates may take judicial action if their rights under the GDPR have been infringed in the processing of their personal data.

The Controller may be sued as a Hungarian data controller before a Hungarian court. For contact details of the courts in Hungary click on the following link: <http://birosag.hu/torvenyszekek>.

### **13. Miscellaneous**

The Controller reserves the right to unilaterally amend this Policy at any time in accordance with the law.

Budapest, 31 March 2023

**Nova Services Zrt.**

Controller