

## PRIVACY POLICY

### **- WEBSITE AND SOCIAL MEDIA PLATFORM USERS OF BONUS KFT. -**

---

#### **8.3. Processing personal data submitted as messages and documents through the carrier page of the Bonus Kft. website.**

1. Before data processing it is needed to inform the data subject
2. Upon request it is necessary to provide the Privacy Policy to the data subject
3. Contract execution
4. If the data subject after contract execution objects to the data processing, it may lead to the termination of the contract

### 8.3. Processing personal data submitted as messages and documents through the carrier page of the Bonus Kft. website.

In compliance with the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), we hereby inform you about the processing of personal data provided by you:

#### 1. DATA CONTROLLER:

<b>Name of data controller:</b>	BONUS Kft.
<b>Address of data controller:</b>	Ipartelepi út 2, H 7800 Siklós
<b>Contact details of data controller:</b>	e-mail      privacy@bonus-hungary.com telephone    +36 1 770 7005 website      https://www.bonus-hungary.com/
<b>Data collector officer (if available)</b>	-
<b>Contact details of data collector officer (if available)</b>	-

#### 2. DATA PROCESSED

##### Scope of data processing, purpose and legal basis of data processing

Personal data	Purpose of data processing	The legal basis for processing data
<b>Personal data provided:</b> name, e-mail address, phone number, position sought.  <b>Uploaded documents:</b> resume, cover letter.  <b>Any other personal data given as comment.</b>	Processing personal data of message senders through carrier page.	Legitimate interest - GDPR Article 6 paragraph 1 letter f)

## Data processing (storage) period:

Not relevant application files will be immediately deleted after assessment.

Relevant personal data are stored until withdrawal of consent, otherwise until maximum for a 1 year.

## Is data profiling done during data processing?

Answer	Options	A short, understandable description of profiling
Yes		
No	<input checked="" type="checkbox"/>	

## Is automated decision making done during data processing?

Answer	Options	A short, understandable description of automation
Yes		
No	<input checked="" type="checkbox"/>	

*If yes, the data subject has the right to request manual, human intervention.*

## Source of processed personal data:

Data given and documents uploaded by data subject.

## The data will be transmitted:

Category	Company's name, registered office address, business activity
<b>Data processors (performing technical tasks related to data processing)</b>	FastComet Inc. Suite 300 - #846, 350 Townsend Street, San Francisco, CA 94107, USA host provider
	Infocomplex Bt. Littke J. u. 21., H - 7632 Pécs, System administrator provider
	Microsoft Ireland Operations Ltd. One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521/Microsoft Corporation, 15010 NE 36th Street  Microsoft Campus, Building 92, Redmond, WA 98052 Mail system and cloud based storage provider, MS Office365
<b>Recipients</b>	Dr. Tamás, Marosvári, Király u. 23-25., H - 7621, Pécs Legal activity
<b>To third (non-EU) country</b>	FastComet Inc. Suite 300 - #846, 350 Townsend Street, San Francisco, CA 94107, USA host provider
	Microsoft Ireland Operations Ltd. One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521/Microsoft Corporation, 15010 NE 36th Street
	Microsoft Campus, Building 92, Redmond, WA 98052 Mail system and cloud based storage provider, MS Office365

## Joint data processing takes place:

Answer	Options	A short, understandable of joint data processing
Yes		
No	<input checked="" type="checkbox"/>	

Joint data controller's name	Registered office
Not relevant	

## Data access and security measures:

---

**Restriction of access** Not relevant

**Data security measures:** During data processing a corporate e-mail system is being used.  
The cloud based MS One Drive is authentication and password-protected. Data is being transferred to controllers on this platform.  
A daily backup is performed on the data set of the file server, the corporate e-mail system and the MS One Drive.  
Personal data is stored in a structured system on the software used by the company, the corporate governance system and the company's file server.  
Centralized password management and authorization take place.  
Uniform information security measures are applied at workstations.

---

## 3. THE RIGHTS OF THE DATA SUBJECT:

### The data subject rights under legal basis and their clarification.

Right to information - The data subject shall have the right to be informed about the means and the purposes of processing of personal data before it occurs.

Right to rectification - The data subject shall have right to have personal data concerning their rectified, if the personal data stored by the data controller incorrect is.

Right of access - The data subject shall have right to obtain their stored personal data from the controller.

Right to object - If the legal basis is based on legal interest or on public authority, the data subject shall have right to object processing their personal data, but it does not mean immediate erasure of their data.

Right to restriction of processing - If the data subject does not consider the controller authorized, they can request the suspension of data processing during the investigation.

Right to data portability - The data subject shall have right to request their personal data stored in digital tabular form.

Right to review automated decision making - the data subject shall have the right to request manual review of each data management process, where the controller applied such automated decision-making which has a legal effect on the data subject.

---

#### 4. FILLING A COMPLAINT

The data subject shall have the right to lodge a complaint with a supervisory authority.

**You can appeal to the National Authority for Data Protection and Freedom of Information.**

---

<b>Name</b>	National Authority for Data Protection and Freedom of Information (NAIH)
<b>Registered office</b>	Szilágyi Erzsébet fasor 22/c., H - 1125 Budapest
<b>Address</b>	1530 Budapest, Pf.: 5.
<b>E-mail</b>	ugyfelszolgalat@naih.hu
<b>Phone</b>	+36 (1) 391-1400
<b>Fax</b>	+36 (1) 391-1410
<b>website</b>	<a href="http://naih.hu">http://naih.hu</a>

---

#### 5. JUDICIAL REMEDY

Provisions for the judicial remedy are included in the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

Where the data subject objected to processing data, the data controller shall investigate the objection in the shortest possible time but within 15 days of the reception of the request, make a decision on its validity and inform the applicant in writing of its decision. If the data subject does not agree with the controller's decision, or if the controller fails to meet the deadline specified above, the data subject shall be entitled to turn to court within 30 days from the announcement of the decision or the last day of the deadline.

In the event of a violation of their rights and in the above cases the data subject may take legal action against the data collector. The court will deal with the matter out of turn. The data subject may bring action before a court having jurisdiction over their place of residence or stay by their choice. A party who does not have procedural legal capacity may also be a party to the lawsuit. The Data Protection Authority may intervene in the action for the court success of the data subject.

If the data controller causes damage to the data subject by unlawful data processing or by violating data security requirements, they are obliged to compensate it. If the data controller violates the data subject's right to privacy by unlawfully processing the data subject's data or by violating data security requirements, the data subject may claim restitution from the data controller. The controller shall be liable to the data subject for the damage caused by the controller and the controller is obliged to pay restitution to the data subject in case of violation of personality rights. A controller shall be exempt from liability of the damage cause and from the restitution if they prove that the damage or the violation of the data subject's rights to privacy was caused by an unavoidable cause outside the scope of data processing. No damages shall be paid, and no restitution shall be claimed, if the damage was caused by the injured party or the infringement because of violation of personal rights was caused by the data subject's wilful misconduct or gross negligence.