We ask you to thoroughly read the following Privacy Policy before you would use the Application!

DATA PRIVACY POLICY

on the data management in relation to the "EMPLATE Consumer App" mobile application service that is available for the visitors and consumers of West End City Center Shopping- and Entertaining Centre

INTRODUCTION:

Westend Ingatlanhasznosító és Üzemeltető Korlátolt Felelősségű Társaság
Registered office: 1062 Budapest, Váci út 1-3., company registration number: 01-09-684079
mobile: +36 30 2413160 e-mail: adat@westend.hu
data protection officer: Gránit-Pólus Management Zrt. (1062 Budapest, Váci út 3.)
e-mail: adat@granitpolus.com)
as Data Controller /hereinafter: „**Controller**"/

summarises in the following Privacy Policy the essential information in relation to the data processing of the natural persons personal data, which came to the attention of the Controller during the performance of its activity indicated in section 1. /hereinafter: **"Activity"**/.

Purpose of the Privacy Policy: **giving complete information to the** natural person that are identified or identifiable based on personal data /hereinafter: „**Data Subject**"/ **about the performed processing of the Controller** – in connection to the Activity detailed in section 1. of the current Privacy Policy -, especially, but not exclusively:

- on the scope of the processed data, the purpose, legal basis and period of the processing,
- on the third parties that are involved in the management and processing of the data, and
- on the rights of the Data Subjects and their possibilities on enforcement of rights.

Fundamental rules about data processing:

(i) Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information /hereinafter: „**Info Act**."/,

(ii) Regulation (EU) 2016/679 of the European Parliament 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 („**GDPR**")

Amendment of the Privacy Policy: the Controller reserves the right to unilaterally amend the contents of the Privacy Policy, especially in the case that changes of the legal regulations in relation to the data processing, or the instruction of the Hungarian National Authority for Data Protection and Freedom of Information – that are published in order to help the lawful practice of processing -, or the practical experience of the Controller about data protection requires such amendment.
In the case of the amendment of the Privacy Policy, the Controller takes care of the prior notification of the Data Subjects in time.

1. **The Activity performed by the Controller, to which the processing connects to, and the purpose of the processing in general:**

   Controller operates WestEnd City Center Shopping and Entertaining Centre /hereinafter: **"Shopping Cetnre"**/ at 1062 Budapest, Váci út 1-3., in which there are approximately 400 stores.

   Controller, as the operator of the above-mentioned facility, makes available the use of a special mobile application ("Emplate Consumer Application" / hereinafter: "**Application**"/) – which has been successfully used in several other European shopping centres, in order to provide the visitors of the Shopping Centre:

   - modern service,
   - quickly and directly supplying them with broad information about the stores and the commercial campaigns,
   - following and analysing their consumption needs and shopping habits, and
   - ensuring various reductions for the returning customers.

   First of all, the use of the Application makes finding the stores in the Shopping Centre easier, secondly, in the case the user of the Application signs up for an own customer "profile" by his/her choice, then he/she can obtain bonus points that can be redeemed while shopping, and he/she can get personal direct information about the offers – provided by the stores.

   The news and offers of the Shopping Centre and the stores are coordinated by the Controller, and it places them on the all-time actual platform of the Application.

   In the case that during the use of the Application, the Data Subject would look up a certain store, or he/she would obtain and/or redeem bonus points during its shopping or visit, then the facts and data of such action are registered by the Application, and the process of such data makes available the analysis of the Data Subject's visiting and/or shopping habits in the Shopping Centre, and based on this it makes available to send personal messages about the news, offers and discounts provided by the stores.

   It is necessary to give the personal data that are listed in section 5. of the Privacy Policy for the use of the Application, and it is exclusively the choice of the Data Subject – like the use of the Application as well – whether he/she provides certain data that are not necessary for the use of the Application.

2. **Processing operations:** in connection to the data specified in section 5.:

registering, systematising, storing, requesting, examining, connecting, restricting, deleting, and erasing the data.

3. **<u>Profiling</u>:** the Controller – in the case the Data Subject would sign up for a profile for the use of the Application and he/she would approve the process of his/her personal data for the purpose of profiling separately – makes analysis about the shopping habits, the preferred store of the Data Subjects, about the customer interests and satisfaction time to time by analysing the customer habits and shopping data that is generated during the use of the Application, in order to achieve the business purposes that are generally stated in section 1.

According to the regulations of the GDPR, the above-mentioned processing purposes constitute as "profiling", which means that during the automated processing of personal data, the Controller:

- can draw the conclusions about the personal scope of interests and personal preferences of the certain Data Subjects,
- and it can analyse the consumer habits of the Data Subjects by considering the above-mentioned characteristics and considering the movement of the Data Subjects inside the Shopping Centre, which analysis contributes to improve the services of the Shopping Centre and the supply of goods in the stores of the facility, in the long run.

4. **Legal basis of processing:** the consent of the Data Subject /point a) of section 1. of Article 6 of the GDPR/, which the Data Subjects gives by his/her first registration for the Application by downloading the Application and accepting the Data Privacy Policy /by clicking the "Accept" link/, and by separately accepting (or denying by the choice of the Data Subject) the data processing purposes of section 5.2., which expressed consent is the precondition of a successful registration, and of the Data Subject's use of the services provided by the Controller.

   The consent – by deleting the registration, in a way that is similar to the sign up – can be withdrawn any time. Withdrawing the registration does not affect the lawfulness of the processing prior to the withdrawal, which is based on the consent of the Data Subject.

   Right to object: the personal data that are processed according to the above is (partly) related to direct marketing purposes, and the Data Subject shall have the right to object any time to processing of personal data for such purpose according to the regulations of section 10.4. of the Privacy Policy.

   Right to negotiation: the Data Subject is entitled to request human intervention from the Controller, to express his/her point of view, and to submit an objection against the decision about processing the data.

<u>Priority information</u>:

In the case the Data Subjects would give his/her consent to the processing of his/her personal data by the Controller, in order to complete the processing purposes written in section 5.2.2 of the Privacy Policy (taking part in "loyalty programme" and data analysis based on the activity of the Data Subject /**"Profiling**/), then the processing is qualified as "profiling" as defined in the GDPR, for which the Controller draws the attention of the Data Subject.

5. The scope, source and purpose of the processed data:

<u>Registration:</u> the Data Subject can register in the Application in 2 ways:

(i) during the registration the Data Subject can decide that he/she signs up for an own profile ("account"), with which it ensures itself the possibility to obtain bonus points (to participate in loyalty program), to receive personal messages and discounts, and to redeem bonus points;

(ii) in the case the Data Subject down not sign up for a profile, then it will not be able to make us of the discounts of subsection (i), however, it will be able to us all other features in the application (accessing maps that show the location of the stores in the Shopping Centre, information in relation to the certain stores /opening hours, current sales, discounts/, other Shopping Centre related news and information /e.g. current events/).

The Data Subject may register **manually**, by giving his/her personal data requested during the registration, or via his/her **Facebook profile**, with the personal data in connection to the profile.

Is the Data Subject obliged to give personal data? **no**

The possible consequences of the lack of data providing:

the Application cannot be used fully without the personal data requested during the registration, which data are not listed in the following tables as "optional" /"not mandatory"/ data, but "required".

5.1.1. The following data are **required** when the Data Subject signs using **manual input**:

data:	source of data:	purpose of processing:
E-mail address	Data Subject provides it during the registration	Login authorization (one account pr. person) Account notifications (deletion notice, etc.)
Password	Data Subject provides it during the registration	Login authorization
Telephone number	Data Subject provides it during the registration	Login authorization /for two factor verification; to send and receive verification SMS/ (one account pr. person)
First name or nickname	Data Subject provides it during the registration	Profile information (in app and in emails) Support /to handle the performance of the user requests / *(providing real first name gives the possibility to send name's day messages and offers to the Data Subject.).*

The following data are **optional**, but not required when the Data Subject signs up using **manual input**:

data:	source of data:	purpose of processing:
Last name	Data Subject provides it during the registration	Support handling for the Data Subject
Gender	Data Subject provides it during the registration	Sending personalised marketing messages to the Data Subject (in relation to the gender of him/her)
Age	Data Subject provides it during the registration	Sending personalised marketing messages to the Data Subject (in relation to the age of him/her)
Facebook third party ID	Data Subject provides it during the registration	Sending personalised marketing messages to the Data Subject through Facebook

5.1.2. The following data are **required** when the Data Subject signs using their **Facebook profile** or the Application downloads the following data from the Facebook profile:

data:	source of data:	purpose of processing:
Email address	Data Subject provides it during the registration to Facebook	Login authorization (one account pr. person) Account notifications (deletion, notice, etc.)

Password	Data Subject provides it during the registration to Facebook	Login authorization
Telephone number	Data Subject provides it during the registration	Login authorization / for two factor verification; to send and receive verification SMS / (one account pr. person)
First name, or nickname	Data Subject provides it during the registration to Facebook	Profile information (in app and in emails) Support handling *(providing real first name gives the possibility to send name's day messages and offers to the Data Subject.).*
Last name	Data Subject provides it during the registration to Facebook	Support handling / to handle the performance of the user requests, to identify the Data Subjects more easily /
Facebook third party id	Data Subject provides it during the registration to Facebook	Sending personalised messages to the Data Subject on Facebook

(The Data Subject can sign up for a profile without using their Facebook profile.)
/a profile can be created in the Application without using Facebook, and in such case, Facebook does not receive the collected information in relation to the Data Subject/

In the case the Data Subject sings using their Facebook profile, then the Application may show advertisements in the news feed and on sponsored ad-places for the Data Subjects on Facebook as well, based on the data collected from the Application.

When logging into their profile created in the Application, the Application identifies the Data Subject by their e-mail address, password, mobile number and Facebook profile ID. The Facebook profile picture of the Data Subject is shown next to their name in the Application.
The Application analyses the data relating to the his/her device and to their use of application in order to show the most relevant marketing content in the Application for the Data Subject.

5.2. By downloading and using the "Emplate Consumer Application" the Data Subject may give his/her consent to the following processing purposes in separate steps (or they can refuse it as well):

5.2.1. receiving marketing messages and notifications from the Shopping Centre about the stores in the Shopping Centre (about their location, opening hours, services, discounts);

5.2.2. taking part in the "loyalty programme" provided by the Application, during which the Data Subject may obtain bonus points by using the Application, and by his/her activity (e.g. visits, movement in the Shopping Centre) and location data, which bonus points can be redeemed for actual shopping discounts in the stores of the Shopping Centre, and these activities the Controller analyses the shopping habits and preferences of the Data Subject for profiling purposes;

5.2.3. in the case the Data Subject signed up for a profile with their Facebook account, then the Shopping Centre is going to show advertisements on his/her Facebook feed

5.3. **Personal data generated by the use of the Application ("event tracking")**:

The Application uses "event tracking" in order to collect information about the use of the Emplate Consumer Application. The Application collects data with event tracking about the Data Subject who uses the Application regardless whether the Data Subject signs up for a profile or not.

5.3.1. *Data in relation to the Application collected and processed "events":*

The Application records so called “events” every time the Data Subjects does one of the following things:

- enters the Shopping Centre,
- passes by one of the stores of the Shopping Centre,
- or practices one of the activities listed in section 5.3.2. (“What the Data Subject did?”)

in the case the Data Subject uses the Application, the Application collects the following information in relation to the events:

Category	**Information**	**Description**	**Example**
Timestamp	Timestamp	When was the event created?	2019-09-01 13:37:10
Guest id	Guest id	The system generated id referring to the user	218919
Event type	Event type	The name of the event type collected	APP_START
Device information	Platform	The platform of the client	ANDROID / IOS
	App version	The current version of the app	2.2.0
	OS version	The version of the OS	5.0.1
	Device name	The device name	iPhone Xs Max
	Bluetooth enabled	Is bluetooth enabled?	true/false
	Location permission	Is location allowed?	true/false
	Location enabled	Is location services enabled on the device?	true/false
	Notifications allowed	Is the notifications allowed on the device?	true/false

The Data Subject receives points from the Application for the location data of the device used for running the Application, for visiting the stores and the Application notifies the stores about how many visits does a certain marketing campaign generate.
The Controller does not share the personal data of the Data Subjects with the stores of the Shopping Centre in any circumstances.
In the case the Data Subject contributes to receive notifications from the Application, then the Application is going to record the notifications as events.
The location data and the information in connection to the notification is added to the further information in relation to the use of the Application and the Controller uses these for marketing purposes.

5.3.2. *The Application collects the following event types with additional type-specific information:*

The Application collects the information in connection to the use of the application with event tracking. When the Data Subject does something in the application, then such action gets recorded as a describing event. When the Data Subjects does one of the following actions, data logging takes place (in the cases that require separate consent of the Data Subject, data logging can only take place if the logging of the certain activity of the Data Subject is in connection to the processing based on the consent of the Data Subject):

Category	**Event type**	**What the Data Subject did:**	**Information**
N/A	App start	Started the app	
	Screen view	Viewed a screen in the app	Screen name Duration (seconds)
	Beacon view	Was in the proximity of a beacon	Beacon id Duration (seconds)
	Bonus action	Obtained bonus points	Action type (eg. check-in) Value (points)

	Consents	Gave their consent	Type (eg. privacy)
	Push message	Received a push message	Message content
	SMS verification	Received an SMS with verification code	Phone number SMS code
Home	Clicked opening hours	Clicked the opening hours	
	Rating answer	Answered “do you like the app” pop up	Answer (yes/no/dismiss)
	Check-in button	Clicked the “Check-in”-button	Success/timed out
Campaigns	Campaign view	Saw a campaign in the campaign list	Campaign id Duration (seconds)
	Clicked shop name	Clicked the shop name in the campaign list	Shop id
	Campaign list settings	Filtered the campaign list	Filters
	Navigated campaign	Browsed from one campaign to another	Direction (forward/back)
	Coupon redemption	Redeemed a campaign coupon	Campaign id
Events	Event reminder	Added or removed an event reminder	Event id Added/removed
Shops	Clicked shop detail	Clicked an item in the shop detail screen	Shop id Detail (eg. phone, web)
	Subscription	Followed/unfollowed a shop	Shop id Followed/unfollowed
	Filtered shops	Filtered the shop list	Category ids
	Clicked search	Clicked the search button	
Profile	Clicked bluetooth help	Clicked the bluetooth help button	
	Clicked location help	Clicked the location help button	
	Dismissed Privacy Policy	Dismissed the privacy consent prompt	
Prize	Prize redemption	Redeemed a bonus prize	Prize id Cost (points)
	Cancel redemption	Canceled a redemption	Prize id
More	Clicked More item	Clicked an item in the More menu	Item name (eg. send mail)
Support	Support request	Send a request for support	Support message

The Application collected and analyses the events for the following purposes:

- Continuous optimization of the user interface to maximize usability,
- Identification of bugs and other issues,
- Personalized marketing,
- Support handling,
- Aggregated reporting for Controller and tenants.

In the case the Data Subject sends a support request (in relation to the use of the Application), then this is recorded as event with the information included in the request (in order to investigate and complete the request).

6. Place and duration of storing data:

Place:

DigitalOcean: Only EU (Frankfurt - Germany and Amsterdam - Netherlands)

Amazon Web Service: Only EU (Western Eurpe, not more exact)

Zendesk: EU and US, based on EU-US Privacy Shield, only for support data

GatewayAPI (Onlinecity.io): Only EU (not more exact), depends on the country you send SMS's to

Our processors store the Data Subject related information safely both in the EU and outside the EU.

Duration of storing the data:

the data are stored until the Data Subject withdraws their consent, but we store them for the following durations at the latest:

- data provided at the registration: until the withdrawal of consent;
- data provided for marketing messages: until the withdrawal of consent;
- data provided for the participation in loyalty programme: until the withdrawal of consent
- event tracking: until the withdrawal of consent, but for 10 years from the registration at the latest
- profile data: until the withdrawal of consent, but for 10 years from the registration at the latest.

We delete the personal data of the Data Subjects from our servers or anonymize them, if the Data Subject is inactive for 12 months, or he/she deletes his/her profile.

7. Does the Processor use the contribution of processor? yes

Processors:

7.1. **Emplate Central Europe ApS** (Registered office: C8200 Denmark, Aarhus, Helsingforsgade 27.) (Registration number: 40642552) /hereinafter: „Emplate"/

Emplate is the developer of the Application.

Task of the processor: Emplate provides the necessary technical background and IT services for the continuous operation of the Application.

Emplate provides a full service to the Controller for the data management purposes listed in section 5, including the continuous process of the data – listed in section 5 generated by using the Application, and the performance of the tasks that are necessary for the profiling.

In the case of malfunction, Emplate shall perform troubleshoot and recovery tasks that ensure the operation of the Application.

7.2. With whom does Emplate share the information?

Emplate uses the following sub-processors, with the consent and knowledge of the Controller, and the data given by the Data Subjects and for the use of the Application, and the data generated during the use of the Application together with the purpose of the data processing are shared with such sub-processors.

Handing over personal data – in the case of further sub-processors outside the European Union - takes place according to the provisions of the EU-US Privacy Shield. The EU-US Privacy Shield protects the fundamental rights of the EU persons whose personal data is forwarded to the United States of America for marketing purposes. This makes the free forwarding of the data available for the companies who received a certificate in the U.S.A. according to the provisions of the Privacy Shield.

(In the case the Data Subject would sign up for a profile with his/her Facebook profile, then the data collected from the Data Subject gets shared with Facebook as well.)

Name	Address	Data	Description of processing
Digital Ocean, Inc.	101 Ave of the Americas, 10th Floor New York 10013 USA	- All collected data	– Used for hosting the System
Amazon Web Services Inc.	410 Terry Avenue North Seattle, WA 98109-5210 USA	- All collected data	– store backups of the System – to send automatic emails from the system – store events from the system
Zendesk, Inc.	1019 Market Street San Francisco, CA 94103 USA	- Support tickets - Guest ID - E-mail addresses - First name - Last name - Device information	– Used to handle support requests from the System
Hubspot, Inc.	25 First Street, 2nd Floor Cambridge, MA 02141 USA	- Tenant e-mail addresses - Emplate Shop use information	– Used to handle e-mail sent to the tenants by using the Emplate Shop
ONLINECITY.IO ApS	Buchwaldsgade 50 5000 Odense C Denmark	- mobile numbers	– Used to send SMS from the System

8. Data privacy measures:

the Controller takes care of the proper data privacy by internal rules (determining regulations in relation to right of data privacy and secrecy, information security and access), by operating an IT system that meets the high technical standards of the age, organisational and educational measures.

The Controller selects the IT instruments used for the data processing and operates them in a way to ensure the followings at all times to the Data Subjects in relation to the managed data:

a) access (availability),
b) authenticity,
c) constancy of the data (integrity),
d) protection against unauthorised access (the confidentiality of the data).

During the data processing, the Controller ensures the followings:

- integrity of the IT system (taking into consideration the possible hazard points for data processing),
- comprehensiveness of the security of the IT system (the security covers every aspect of the of the IT system),
- continuity of the security of the IT system (the security takes place continuously in time),
- the proportionate nature to the possible risks.

The IT system of the Controller and its network is highly protected against IT breaches.

The Controller takes appropriate measures in order to protect the tights, freedom and legitimate interests of the Data Subjects, including ensuring the right to negotiation of the Data Subject referred to in section 4 of the Privacy Policy.

9. **Who can access the data?** the Controller ensures to protect the personal data of the data Subjects from the disclosure to unauthorised persons.
The Controller, as the operator of the Application has right of access to the data. Besides the Controller, only the processors named in section 7 can get to know the recorded data, exclusively for the purpose of performing their processing tasks (operating the software of the Application, ensuring the continuous operation of the server).
According authorisation defined in law, court, the Public Prosecutor's Office, investigating authority, authority dealing with administrative offences, administrative authority, National Authority for Data Protection and Freedom of Information, and other authorised authorities can ask the Service Provider about data processing, for handing over data and documents. According to the effective legislation, the Company may give out to courts, authorities only those data and only in an extent that are essential for the performance of the request.

10. THE RIGHTS OF THE DATA SUBJECTS, AND THE POSSIBLITY OF ENFOCING THEIR RIGHTS:

10.1. <u>THE DATA SUBJECT MAY REQUEST</u> by the Controller:

1. **information:** about the processing of his/her personal data;
2. **access:** to the concerning personal data - in which case the Controller gives information on whether it manages personal data concerning the Data Subject, and if so, what is its exact purpose, legal ground, scope of managed data, and the main regulations /stated in the current Information/ on data processing, and for the request of the Data Subject the Controller – according to the provisions and within the frameworks of the legal regulations – provides the copy of the managed personal data to the Data Subject;
3. **rectification of data:** rectification of inaccurate personal data concerning him or her, and to have incomplete personal data completed**;**
4. **erasure of data:** see in detail: section 11!
5. **restriction of processing the data**: for the request of the Data Subject, the Controller restricts the data processing, if one of the following criteria has been met:
   a) if the accuracy of the personal data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the personal data;
   b) if the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) if the Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) if the Data Subject has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject'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 Data Subject shall be informed by the Controller before the restriction of processing is lifted.

6. **in the case of personal data breach:** for the request of the Data Subject, the Controller gives information about the following aspects of the personal data breach:
   - circumstances,
   - effects and
   - measures taken in order to avert it.

7. **in the case of data forwarding**: for the request of the Data Subject, the Controller gives information about the legal foundation and the recipient of the data forwarding.

10.2. *RIGHT TO DATA PRTABILITY***:**

The following has to be ensured to the Data Subject: the exercise of its **right to data portability** according to the regulations of the GDPR, which states that the Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

10.3. *WITHDRAWING THE CONSENT***:** in the case of data processing, based on the consent of the Data Subject**, the data subject shall have the right to withdraw his or her consent at any time**.

10.4. *RIGHT TO OBJECT***:** the Data Subject shall have the right to object **at any time to processing of personal data** concerning him or her for the purposes of the legitimate interests pursued by the Controller or by a third party, including “profiling” based on section 3.
In the case of objection, the Company shall no longer process the personal data unless the Company demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

10.5. *PROCEDURE***:** the Company shall notify the Data Subject about the implemented measures according to the request of Articles 15 – 22 of the GDPR within 1 month from the receipt of the request of the Data Subject, which deadline can be extended with 2 month if necessary /taking into consideration the complexity of the request and the amount of the requests, according to Article 12 (3) of the GDPR/. The Company is obliged to notify the Data Subject about the extension of the deadline within one month, and the Company must indicate the reason of the extension as well.

11. ERASUE OF THE DATA: **the Company is obliged to erase every personal data** without undue delay, **if:**

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- the data subject objects to the processing, and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing,
- the personal data have been unlawfully processed,
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject,
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

The erasure of the data can not be requested, if the processing is necessary:

- for exercising the right of freedom of expression and information,
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- for reasons of public interest in the area of public health, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
- for the establishment, exercise or defence of legal claims.

12. <u>LEGAL REMEDIES</u>:

12.1. PROPOSING COMPLAINT**:** we suggest that before initiating authority or court procedure, the Data Subject should exercise the option of request, complaint, objection (and consultation about all of these) that can be presented to the Controller.

The phone number, e-mail address and postal address of the Controller available for this purpose /according to the provisions in the Introduction of the current Policy /:

E-mail: **adat@westend.hu**

Mobile: **06 30 2413160** (the contact detail of the all-time director in charge for Westend)

Post: Westend Ingatlanhasznosító és Üzemeltető Korlátolt Felelősségű Társaság
1062 Budapest, Váci út 1-3. sz.

12.2. INITIATING AUTHORITY PROCEDURE**:**

The Data Subject may initiate an authority procedure on data protection in the case it believes that the Company has breached its obligations on processing the personal data of the Data Subject. Competent authority:

National Authority for Data Protection and Freedom of Information

address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.,
phone: +36 (1) 391-1400,
e-mail address: ugyfelszolgalat@naih.hu,
website: http://naih.hu

12.3. INITIATING COURT PROCEDURE**:**

in the case that the Data Subject would not agree with the decision of the Controller on the request or objection of the Data Subject, or the Controller would fail to give answer within deadline, then the Data Subject my turn to court within 30 days – from the communication of the decision, or the last day of the deadline.
The lawsuit can be addressed in front of the law court competent for the place of residence or place of stay of the Data Subject – according to its choice – as well.

In the case you would have any question, suggestion in relation to the current Privacy Policy, we ask you to indicate that to us on the phone number or e-mail address given in section 12.1. or in writing send a letter to the postal address of the Controller.