GENERAL DATA PROTECTION POLICY

Effective as of 25.05.2018

Latest update: 12.10.2020

I. Controller (Company)

Name of the Company:	Immo-Land Kft.	Saját Raktár Kft.	Conflex Kft.	MESTERPRINT-INGATLAN Kft.	Snooker 2000 Kft.
Registered office and postal address:	1119 Budapest, Hadak útja 7-9.	1119 Budapest, Hadak útja 7-9.	1119 Budapest, Hadak útja 7-9.	1039 Budapest, Pünkösdfürdő utca 52-54.	1117 Budapest, Budafoki út 111-113.
Registering authority:					
Company Registration Number:	01-09-68272	01-09-912864	01-09-164447	01-09-170377	01-09-687960
Tax Registration No.	11909824-2-43	14634965-2-43	10738713-2-43	24293143-2-41	12472512-2-43

E-mail address:	info@selfstore.hu
Website:	www.selfstore.hu
Phone number of the customer service:	+3630 533 1313
E-mail address of the customer service:	**Headquarters** info@selfstore.hu
Place of complaint handling, contact information of customer service offices:	**Self Store Csepel** 1211 Budapest, Alumíniumhengerde u. 15-19. csepel@selfstore.hu +3670 372 7032 **Self Store Budafok** 1222 Budapest, Nagytétényi út 48. budafok@selfstore.hu +3670 372 7033 **Self Store Zugló** 1142 Budapest, Erzsébet királyné útja 106. zuglo@selfstore.hu +3670 372 7034 **Self Store KÖKI** 1191 Budapest, Vak Bottyán utca 32. koki@selfstore.hu +3620 334 8886 **Self Store Debrecen** 4028 Debrecen, Kassai út 131/A debrecen@selfstore.hu +3620 244 7756 **Self Store Óbuda** 1039 Budapest, Pünkösdfürdő utca 52-54.

	obuda@selfstore.hu +3670 372 7035 **Self Store Ferencváros** 1097 Budapest, Földváry utca 4. ferencvaros@selfstore.hu +3670 372 7036 **Self Store Váci** 1044 Budapest, Váci út 83. vaci@selfstore.hu +3670 372 7037 **Self Store Józsefvaros** 1089 Budapest, Vajda Péter utca 10/b jozsefvaros@selfstore.hu +3670 372 7038 **Self Store Újbuda** 1117 Budapest, Budafoki út 111-113. ujbuda@selfstore.hu +36 20 777 0130
Name of the hosting provider:	Servergarden Kft.
Address of the hosting provider:	1106 Budapest, Fehér út 10, White Office Irodaház, II./208

Data protection regulations applied by the Company

- Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR);
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter referred to as "Privacy Act");
- Section 169 of Act C of 2000 on Accounting (on retaining documents)
- Government Decree No. 297/2001. (XII. 27.) on Money Exchange Services

DEFINITIONS

1. "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); 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.
2. "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;

3. “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;
4. “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
5. “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;
6. “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;
7. “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (“purpose limitation”);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).
g) The controller shall be responsible for, and be able to demonstrate compliance with, the above (“accountability”).

Details of processors employed by the Company:

1. Operator of our e-mail system: Servergarden Kft. (1106 Budapest, Fehér út 10, White Office Irodaház, II./208);
2. Hosting service provider: Servergarden Kft. (1106 Budapest, Fehér út 10, White Office Irodaház, II./208).
3. Providing software management and data processing services: Piros Attila e.v. (4029 Debrecen, Karácsony György utca 5, 2. emelet 13. ajtó), Mnp-Szoftverház Kft. (1113 Budapest, Badacsonyi utca 21. 1. em. 3.)

Cookie policy

We use cookies on our website. Cookies are files that store information in your web browser, for which your consent is necessary.

Cookies are used in compliance with the provisions of Act C of 2003 on Electronic Communications, Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services and the requirements of the European Union.

Websites which operate in the member states of the European Union shall obtain the users' consent in order to use cookies and to store such cookies on the users' computer or other device.

1. Policy regarding the use of cookies

This policy regards the cookies used on www.selfstore.hu.

2. What are cookies?

Cookies are small files which contain letters and numbers. Cookies are tools used for exchanging information between the web server and the user's browser. Such data files cannot be run, they do not contain spyware or viruses and they cannot access the content of the users' hard drive.

3. How do we use cookies?

Through the information provided by cookies, internet browsers can be recognised easier, thereby users will receive relevant and customised content. Cookies make browsing more comfortable, including online data protection needs and relevant advertisements. With the help of cookies, website operators may also prepare anonymous statistics of the behaviour of website visitors. Thereby web designers are enabled to personalise the appearance and the content of the website even more.

4. What cookie types do we use?

Websites use two types of cookies:

- Session cookies, which will be stored on your device as long as you are on the website.
- Persistent cookies, which will be stored on your device for a longer period of time, depending on the settings of your browser, or until you delete them from your device.
- Third party cookies are cookies set in your browser by a third party (e.g. Google Analytics). These will be set in your browser if the website you visited uses services provided by the third party.

<u>Essential session cookies (session-id):</u>

These cookies are essential in order to navigate on the website and necessary for the operation of the website's functions. Without approving such cookies, the website and certain parts thereof may not appear or errors may occur.

<u>Analytical or performance cookies:</u>

These cookies help us to distinguish the visitors of the website and to collect data regarding the visitors' behaviour on the website. These cookies enable the website, for instance, to

remember log-ins in cases you have requested it. These cookies do not collect information that are suitable for identifying you, they store data collectively and anonymously. (e.g. Google Analytics)

Functional cookies:

The purpose of these cookies is to improve user experience. For example, they detect and remember the device you used for opening the website or the information you previously provided and requested to be stored: such as auto-login, selected language, changes to the font size or type, or to other customisable elements of the website. These cookies do not track your activities carried out at other websites. However, information collected by such cookies may include personal identification data that you have provided.

Targeting and advertising cookies:

These cookies enable websites to provide you with (marketing) information that suit your interests the most. For this, your explicit consent is necessary. These cookies collect detailed information about your browsing behaviour.

5. Do cookies store personal data?

Most cookies do not store personal data and users cannot be identified through them. Stored data are necessary for a more comfortable browsing experience and such data are stored in a way that no unauthorised person may access them.

6. Why are cookies important on the Internet?

Cookies are used for making browsing more convenient for users, as they choose advertisements and content for users in accordance with their browsing history. Disabling or restricting cookies may render some websites inoperable. Disabled or restricted cookies, however, shall not mean that users will not see adverts, it only means that the adverts and contents that pop up will not be “customised”, meaning they are not tailored to the needs and interests of the user. A few examples of using cookies:

- Presenting contents, services and products that are tailored to the user’s needs.
- Offers collected in accordance with the user’s interests.
- Remembering log-ins in cases you have requested it (stay logged in).
- Remembering parental control filters regarding web contents (family mode, safe search).
- Restricting the frequency of adverts; i.e. restricting the number of times an advert may appear for users on the given website.
- Placing adverts that are relevant for the user.

- Geotargeting

7. Safety and data security factors.

Cookies are not viruses or spyware. Since they are simple text files, they cannot be run, therefore, they cannot be deemed to be programmes. However, sometimes information is hidden (maliciously) for other purposes so they may operate as spyware. Therefore, virus scanners and antivirus programs may erase cookies constantly.

Since the Internet is a device used for browsing and web servers constantly communicate with each other, meaning they send data back and forth, if a hacker interrupts that process, they may extract information stored by cookies. One reason for that may be if Internet settings (WiFi) are not encrypted properly. By exploiting such vulnerability, they may extract information from cookies.

8. Management and erasure of cookies

Cookies may be erased or disabled in the browser you use. Browsers enable cookies by default. This option may be disabled or existing cookies may be erased in the settings of the browser. In addition, you may set whether the browser shall send a notification when sending a cookie to the device. However, it is important to mention that disabling or restricting such files will spoil the browsing experience or errors may arise in connection with the functions of the website.

- Settings usually can be found under the menu item “Options” or “Settings” of the browser. All browsers are different, therefore please use the menu item “Help” of your browser in order to find the appropriate settings.

- In order to disable Google Analytics cookies, you may install the so called “Google Analytics plugin”, which prevents the website from sending information about you to Google Analytics. For further information with regard to the above please visit the following links:

Google Analytics & Privacy or Google Principles and Standards

9. Further useful links

If you wish to learn more about cookies and their use, visit:

All About Cookies

Facebook cookies

Complaint handling

The purpose of data processing is to investigate complaints lodged by the clients of the Company and to respond to such complaints.

The legal basis for data processing is the voluntary consent of the client pursuant to Point a) Paragraph (1) Section 5 of the Privacy Act.

CCTV system

In commercial units operated by the company, the Company uses a camera system that is able to record images. The purpose of using the electronic surveillance system is to protect the assets stored in the commercial unit, as well as, to control the cash counting process in the customer service offices, and, in connection with that, to protect the assets of the Employer. The control of the performance of the specified activities is justified and necessary considering the amount of the assets managed in the customer service offices.

The field of view of the cameras operating in the commercial units operated by the Company records, on one hand, the entrance, the safe deposit box, the customer service desk, the clients, and, on the other hand, the customer area, the corridors of the building, the area in front of the elevators and the passageways.

The recordings may be accessible by those who are authorised to do so as a result of their activities, in order to be able to perform their tasks. The recordings may be viewed upon the request of courts, authorities or persons proving their right and legitimate interests to do so, unless it disproportionally violates other persons' rights, or if it is assumed that the purpose of using the surveillance system is infringed. Besides persons involved in the recordings, only those persons are entitled to view the recordings, who are entitled to view such recordings anyway in accordance with the above.

The legal basis for data processing is the voluntary consent of the client pursuant to Point a) Paragraph (1) Section 5 of the Privacy Act.

Processed data: images of the employees and clients.

In case of commercial units, the recorded images will be destroyed or erased if they are not used within at least 50 days following their record (Section 11 of Government Decree No. 297/2001. (XII. 27.). In this regard, the usage of recorded images or other personal data in any judicial, official, labour law or other procedure as evidence that is deemed to be usage.

Access control system

The Company uses access control system in the customer service buildings. The purpose of using access control system is to ensure that only those will enter the building, who work on that site as employees, or who rent storage units at the given site as the lessees of the Company. The keycards of the keycard entry system having unique identifiers open the magnetic lock of the given storage unit.

Data recorded by the access control system may only be processed by the security office, being the controller. The data may be accessible by the CEO and those employees or agents of the Company who have to do so as a result of their activities, in order to be able to perform their tasks.

The legal basis for data processing is Point a) Paragraph (1) Section 5 of the Privacy Act, to which the employee gives its consent by accepting the card.

The following data are processed in case of employees: name, time or arrival, time of leaving, name of the entrance.

The following data are processed in case of lessees: name, number of the storage unit, time or arrival, time of leaving, name of the entrance, direction.

The name and address data of the employees recorded by the access control system will be destroyed upon the termination of their entry rights, while the employees' data generated during the operation of the entry system will be destroyed upon the termination of their entry rights, but no later than 6 months after that data is generated.

The name and storage unit number of lessees recorded by the access control system will be destroyed upon the termination of their entry rights, while lessees' data generated during the operation of the entry system will be destroyed upon the termination of their entry rights, but no later than 6 months after that data is generated.

Information of processors employed by the Company: Immo-Land Kft (1119 Budapest, Hadak útja 7-9).