**Privacy Policy**

**1. Introduction**

1.1. Hereby we are to inform you about the privacy policy of Happy Business Services Ltd. (henceforth: HBS or Company).

1.2. Please, read this text carefully, since it contains vital information about the way how your personal data is being controlled.

1.3. The scope of this Privacy Policy is the data controlling of natural persons only. The data of Legal Persons or any other organizations that do not count as Legal Persons are not considered to be personal.

1.4. Regarding this Privacy Policy, the following legal acts are applied:

* The General Data Protection Regulation (EU) decree 2016/679 (also known as GDPR), whose text can be found here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1605602506800>
* The Hungarian Act CXII. of 2011 (Information Act; Infótörvény).

**2. Concepts and Definitions**

2.1. **The Data of the Data Controller**

Name: Happy Business Services Ltd.

Address: HU-1137, 18. Szent István körút, Budapest, Hungary

E-mail: info@hbs.hu

Company registration number: 01-10-046757

VAT Number: 22923820-2-41

2.2. Person Concerned: any person who is or can be identified by their data which are being controlled.

2.3. Natural Person: any living person subject of personal rights, such as the protection of their personal data. In this Privacy Policy, any person who visits the webpage and/or gives their personal data thereon counts as Natural Person.

2.4. Personal Data: any information which refers to a person, especially but not limited to their name, address (postal or email), telephone number, identification number(s) given by any authorities or companies; any data referring to the person’s physical, physiological, mental, economical, cultural or social identity and any conclusion regarding the person drawn from any of their data.

2.5. Data Controlling: any automatized or manually performed process applied to data regardless of the method of processing. The term includes collecting, recording, systematization, storing, altering, applying, query from public or private databases, transferring, publishing, harmonizing, attaching/connecting, deleting, destroying and the prevention of the further use of the data.

2.6. Data Processing: any technical or technological operation used for data controlling, regardless of the method and tools applied, or the place where the operation happens.

2.7. Data Processor: any natural or legal person, or an organization without a legal personality who is assigned by the Data Controller to the task of processing data. Data processing may happen based on a contract between the data processor and HBS.

2.8 Data Deleting: aka. Erasure, making data unrecognizable in a way which guarantees that the particular data cannot be recovered in the future.

2.9. Consent:an unambiguous express from the side of a Natural Person which has been performed voluntarily, clearly and definitely based on an adequate form of informing, in which he/she agrees that their Personal Data can be controlled by the Data Controller. The scope of a consent may be all personal data, or certain processes of data controlling.

2.10. Profiling: an automatized form of data processing of personal data whose aim is to interpret, evaluate or predict certain personal parameters of a natural person (e.g. preferences, interests).

2.11. Objection aka. Protest: a notice given by a person so that they express an objection to the controlling of their personal data, or they express a request of ceasing of Data Controlling, or deleting their data.

2.12. Data Transferring: making data available for a certain third party.

2.13. Data Breach aka. Breach: an incident which leads to security issues, which means the loss, alteration or destruction of data (accidentally or illicit), and/or the illicit publishing or accessing to data.

2.14. Webpage: <https://covid-19.hbs.hu>, including any of its sub-pages.

**3. General Information**

3.1. The legal base of the data controlling performed by HBS is the consent of the person concerned. The person concerned may withdraw their consent anytime. However, the legality of any data controlling prior to the withdrawal remains unaffected. Data confirming the fact of the consent is stored by HBS as long as the consent needs to be proven or any interest of HBS makes it necessary.

3.2. The person concerned is responsible for the authenticity and accuracy of the data given by them. HBS is not to confirm the authenticity of any data given by the person concerned. HBS shall not be responsible for the consequences of any false or incorrect data given by the person concerned, nor for any damages to the person concerned or any third party caused by these data.

3.3. Unless any law orders it otherwise, HBS shall use the obtained personal data for the purposes, time period and extent defined in this Privacy Policy.

3.4. All data are stored at the following place: Netlify Inc. (325 3rd St, Suite 296, San Francisco, CA 94107, USA)

**4. Personal Data Controlling**

4.1. The Company shall not use any personal data for different purposes to those of defined in this Privacy Policy. Unless any law orders it otherwise or this Privalcy Policy gives different information, the personal data given by the person concerned shall be controlled as long as the person concerned uses the services of the webpage. Deletion shall take place in the shortest possible time after the person concerned has expressed its claim for deletion. Unless any law prohibits it, in case of illicit or misleading data controlling, any criminal act performed by the person concerned, or incoming attack against the system (server), the Company reserves the right to delete the personal data of any person concerned if their registration (to the webpage) ceases to exist. However, in case of any suspicion of a felony or liability of common law the Company reserves the right to store any personal data during the period of the legal procedure. If there is no law or any contradicting statement of this Privacy Policy applied, the Company shall control the personal data given by the person concerned until the person concerned expresses their will for cease controlling their personal data (or until the person concerned unregisters).

4.2. The Company shall control any obtained personal data according to the corresponding law and this Privacy Policy. No data shall be transferred to third parties with the exceptions of those stated in this Privacy Policy. In any case the Company is to use any data for any other purposes, the person concerned shall be informed about this fact; shall express their consent thereunto or have the opportunity to express their objection.

4.3. All data obtained by the Company shall be protected with appropriate measurements, especially against unauthorized access, alteration, transferring, publishing, deleting, destroying, unintentional destruction or damage, and unavailability due to any changes to the technological background of data controlling.

4.4. The system applied by the Company may collect data on the activities of the person concerned in a way that no data collected during this process can be connected to any personal data given by the person concerned, or to any data generated by other webpages and/or services.

4.5. Any personal data may be transferred to any third parties that secede from HBS or merges with HBS. (This is called the legal succession of data controlling.) In case of these events data of the person concerned is being transferred to the necessary extent. No further consent from the person concerned need be obtained, but HBS shall inform the person concerned priorly about the transfer. In case of objection, no data shall be transferred.

4.6. The Controller shall have the right and be obliged to transfer personal data available to and stored by the Controller in a lawful manner to the competent authorities if required to do so by law or by final decisions of authorities. The Controller cannot be hold responsible for such data transfer or for resulting consequences.

**5. Cookies and Similar Technologies**

Our Cookie Policy is available on the following page:

**6. The Cases of Data Controlling**

6.1 Registration, Logging in and Filling in Forms.

To visit and use the webpage of the Company no registration is needed. However, the Company reserves the rights to provide content or services in the same webpage which can be visited and/or used only after the visitor have registered, in the future. In this case the following section shall be applied.

Purpose: enable the service provided by webpage, displaying personalized content and advertisements, compiling databases of statistics, improving the informatic system, protecting the rights of the person concerned. Any data given by the person concerned may be used by the Company for creating user groups so that targeted content and/or advertisements may be displayed for these groups.

Further purposes are: recording the data of the person concerned, give access to certain content, maintaining contact to make the use of the service, or to make the use of the service easier. The form to be filled out at logging in is for identifying the person concerned, enabling the alteration and/or deletion of their data, and simplifying the procedure of ordering.

Data are being controlled: name, telephone number, e-mail address. If the person concerned orders any product after a request has been sent, the data controller records the shipping and invoicing data, as well, namely: company name, tax number (VAT number), delivery address. In case the customer of the product is a legal person, their shipping and invoicing data are not considered personal.

Duration: until the consent has been withdrawn. If the person concerned deletes their registration, their personal data connected to their registered/logged in status shall be deleted without undue delay.

Legal basis: GDPR act, 6. article, (1) paragraph, a) point, in accordance with Ektv. tv. 13/A. § (4) paragraph.

6.2. Data Controlling of Orders

Scope: any person using the webpage of the Company and asks for quotation on any product.

Purpose: the personal data given are used only for giving an offer, without these data the Company cannot process (efficiently) the quotation.

Data being controlled: name, address, telephone number, e-mail address, name, quantity, price of the product(s) to be purchased, payment method, in case of a private person invoicing and shipping method, the IP address and time of the current visit of the webpage.

Duration: the data of the person concerned are controlled until the fulfillment of the made contract. In case of a legal dispute, the Company shall store the data until a final decision has been reached unless it is obligated by law that the Company shall transfer the personal data to certain authorities (e.g. tax department), and the Company shall store the data until it has been completed. An example for mandatory data controlling is storing the issued invoices for a duration determined by the accounting law. In case of a waiver, due to the legitimate interest for defense against the customer’s claim any personal data connected to the order from the expression of the waiver to the time of prescription shall be stored. In case the ordered product is warranty and/or guarantee covered, the Company stores any data from the order to the end of the warranty or guarantee period (whichever is longer) to fulfill the needs of the person concerned regarding their warranty and/or guarantee claims.

Legal basis: GDPR act 6. article, (1) paragraph, c) point; accounting law (Számv. tv.) 169. §, (2) paragraph, Hungarian act of taxation 2017. CL. 78. §, considering the Ektv. act 13/A § (1) and (2) paragraphs.

6.3. Data Controlling of Delivery

In case a contract has been made between the person concerned and HBS, the Company transfers the personal data described below to the logistics company so that they can ship the products have been ordered to the person concerned.

Scope: any private person the Company delivers the products ordered to the specified address of fulfillment for.

Data being controlled: name, address, e-mail address and telephone number of the recipient, package number, value of package, invoicing and shipping method, amount of c.o.d. fee, invoicing name and address, any other information given willingly to the Company in connection with commorancy at the address, any comment attached to the order and data included therein.

Purpose: the fulfillment of orders, documenting the purchase and the payment, fulfillment of accounting obligations.

Duration: 8 years, according to accounting law (Ektv.) 169. § (2) paragraph

Legal basis: GDPR 6. article, (1) paragraph, b) point, considering Ektv. act 13/A § (1) and (2) paragraphs

Third parties data is being transferred to: warehouse, any company involved in delivery

Legal basis of data transferring: GDPR 6. article, (1) paragraph, f) point – data transfer is necessary for pursuing legitimate interest of the Company and the logistics service provider; without that the fulfillment and confirmation of a contract would not be possible.

On logistics service providers (LSPs)

In case postal service is taken for delivering the ordered products to the fulfillment address, the personal data of the person concerned may be controlled (as a data controller) by the postal service provider, in accordance with the regulations of the postal act (Postatv.), 54. §. In case of a logistics service provider is taken for the delivery, the personal data shall be stored by the LSPs of the Company until the products have been delivered – unless it is obligatory according to the law for the LSPs to store the data further to transfer them to competent authorities (e.g. tax department).

Regarding the services provided by a postal or courier service, their Terms of Services and/or Privacy Policies shall be considered normative. These are accepted by the person concerned by accepting this Privacy Policy.

The commissioned service providers of the Company as follows:

Warehouse, cargo handling, printing the bill and/or invoice of delivery

GSP Global Solutions Provider (59–61. Lőrinci út, 2220 Vecsés, Hungary)

Parcel delivery

GLS General Logistics Systems (GLS, 2. Európa u., 2351, Alsónémedi, Hungary)

6.4. Data Controlling in Connection with Newsletters.

If the person concerned has subscribed to the newsletter of the webpage, any personal data given during this process is used only for enabling the sending of the newsletter, and only in case of a consent given for that by the person concerned. The newsletter contains commercial and direct marketing elements, as well.

Scope: name, e-mail address, consent to approaches with a purpose of direct marketing and its appointment, data obtained from previous purchases, the delivery method used, analytical data of sending and delivering messages (e.g. sending or opening an email, clicking on links and its date and time, reason for not being able to send a message).

Purpose: sending newsletters via e-mail for those who expressed their interest in it (the newsletters contain commercials, too), displaying marketing messages, spreading information on the products and services of the Company (including up-to-date information and discounts), approaches of direct marketing, maintaining contact. The Company controls only those data that have been given by the person concerned.

Duration: any personal data given for enabling the sending of newsletters to the person concerned are stored by the Company only until the person concerned unsubscribes the newsletter. In case of unsubscription the Company shall not approach the person concerned with any newsletters or offers. The person concerned can unsubscribe the newsletter – thus, withdraw their consent – any time and cost-free. In case of unsubscription any personal data given by the person concerned for receiving newsletters are being deleted without undue delay.

There are several methods of unsubscribing the newsletter: 1) clicking on the “unsubscribe” link in any e-mail that contains the newsletter, 2) sending an email with the corresponding content to the address displayed on the webpage or 3) contacting the Company via telephone.

Legal basis: GDPR 6. article, (1) paragraph, a) point, corresponding Ektv. tv. 13/A § (4) paragraph, and Grt. 6. § (1) paragraph, a) point.

The Company may involve third parties for the newsletter service from time to time. These parties are to be considered as data processors. The commissioned data processor as follows:

Name of data processor: Muuw Pictures Ltd.

Address: fszt. 2., 13. Csikó sétány, 1023 Budapest, Hungary.

The nature of data processing: the optimization and handling of advertisements and newsletters.

**7. Data Processors, Data Transferring**

The Company may appoint third party data processors so that the proper operation of the webpage can be maintained, the orders can be fulfilled and other activities in connection with the services the webpage (including marketing) can be performed.

To control the legality and inform all the people concerned the Company keeps a data transfer record which contains all the appointments when any personal data controlled by the Company are transferred, the legal basis of transferring, the persons concerned whose data are transferred, the scope of data transferring, just as well as any other data that are considered mandatory, according to the data controlling law.

The commissioned data processors are as follows:

Name of data processor: Muuw Pictures Ltd.

Address: fszt 2., 13. Csikó sétány, 1203 Budapest, Hungary

The nature of data processing: the optimization and handling of advertisements and newsletters

Name of data processor: GSP Global Solutions Provider

Address: 59–61. Lőrinci út, 2220 Vecsés, Hungary

The nature of data processing: warehouse, cargo handling, printing the bill and/or invoice of delivery

Name of data processor: GLS General Logistics Systems

Address: GLS, 2. Európa u., 2351, Alsónémedi, Hungary

The nature of data processing: parcel delivery

Name of data processor: Google LLC

Address: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

The nature of data processing: producing statistical data with the help of analytical cookies

Name of data processor: Facebook Ireland Ltd.

Address: 4 Grand Canal Square Grand Canal Harbour Dublin 2, Ireland

The nature of data processing: producing statistical data with the help of analytical cookies and “tracking pixels”

Name of data processor: Netlify Inc.

Address: 2325 3rd St #215, San Francisco, CA, USA

Nature of data processing: cloud hosting, form handling

**8. Data Safety and Protection**

8.1. HBS ensures the safety and protection of the controlled data in accordance with the corresponding regulation.

8.2. HBS applies all the technical and organizational measurements and defines all the necessary procedural regulation to protect the safety of the controlled data – so that all data will be protected from unauthorized access, alteration, transferring, publishing, deleting, destroying, unintentional damaging or destroying, and becoming unavailable due to any changes affecting the applied technical background.

8.3. HBS takes into consideration the general state of development of the available technologies to determine and apply the measurements of data protection. In case more data controlling methods are available, HBS chooses the one of higher level of data protection unless it would mean disproportional effort to the Company. These requirements shall be enforced to any other data processor, too.

8.4. HBS is obliged to enforce any third parties data may be transferred or given to to comply the measurements detailed above. Given that the data transfer of HBS has been legal, HBS shall take no responsibility for any damage caused by these third parties.

8.5. All employees HBS and people who are working for HBS on the basis of any legal relationship are obligated to comply all the measurements of data controlling, safety and protection described in this Privacy Policy.

8.6. HBS stores all personal data given by persons concerned in databases protected by passwords to protect the secrecy and integrity of these data. HBS protects the personal data with proper infrastructural elements (e.g. firewalls, content filters, anti-malware softwares).

8.7. HBS makes a log out of all data accesses to record when and which file of which account of person concerned is being accessed. Every computer data of persons concerned are being controlled on are constantly protected by an anti-malware system approved by the HBS. This ensures that no unauthorized person can access to any personal data.

8.8 Automatized data processing of personal data are protected by the data controller and processor with the measurements as follows:

a) prevention of unauthorized data entry

b) prevention of unauthorized use of automatized data processing systems via data transmission devices

c) controllability and traceability of data transmission devices to trace what servers are or can be the data transmitted to

d) controllability and traceability of what personal data, when and by whom are being recorded in the data processing system

e) the possibility of recoverability of the installed systems in case of a malfunction

f) a report is being generated when an error occurs during the automatized data processing.

8.9 Invoicing

Any personal data recorded by the Company during an order of a person concerned are being processed in the Novitax business data processing system.

Persons concerned: any private person who makes a purchase

Scope: name, e-mail address, invoicing name and address, order identification number, name, price and quantity of the ordered product(s)

Purpose: fulfilling the invoicing obligation to fulfill the contract made with the person concerned

Legal basis: Ektv. 13/A § (1)–(2) paragraph, GDPR 6. article (1) paragraph, c) point

Duration: 8 years, according to Számv. tv. 169 § (2) paragraph.

**9. The Rights of the Person Concerned**

9.1. The right to be informed forehand

The person concerned has the right to be informed about all the facts related to data controlling and processing, in a clear and legible form, prior to the start of data controlling.

9.2. Information needs to be provided

The person concerned has the right to receive feedback whether the controlling of their personal data has been under process. If yes, they have the right to access their personal data.

I. Information to provide in case of personal data obtained from the person concerned

If the personal data are being obtained from the person concerned, the data controller shall give the following information at the time of obtaining the data as follows:

a) name and availability (telephone number, e-mail address) of the data controller or their representative;

b) name and availability (telephone number, e-mail address) of the data protection officer;

c) purpose and legal basis of personal data controlling;

d) in case of data controlling based on pursuing legitimate interest the interests of the data controller and/or third party;

e) the recipients of personal data (if there are any) and the categories of recipients (if there are any);

f) the fact itself if any data is transferred to third countries or international organizations.

Moreover, at the time of obtaining personal data, the person concerned receives the following supplementary information so that the Company ensures the fairness and transparency of data controlling:

a) the duration of personal data storing; if it is not possible or not applicable the considerations applied for defining the duration;

b) the right of the person concerned to request access for, correct, delete or restrict the controlling of their personal data from the data controller, just as well as the right of data portability;

c) the right to withdraw a consent at any time in case the data controlling on the legal basis of a consent, which does not affect the legality of data controlling prior to the withdrawal;

d) the right to make a complaint at the supervisory authority;

e) if the basis of providing personal data is law, obligations or prerequisites of making a contract, whether the person concerned is obligated to give personal data, and the possible consequences if personal data is not given;

f) if there is automated decision-making – including profile-making –, legible information the logical background applied, on the significance and the possible consequences of this sort of data controlling in these cases.

I. Information to provide in case of personal data obtained from other sources

If the personal data are being obtained not from the person concerned, the data controller shall give the following information at the time of obtaining the data as follows:

a) name and availability (telephone number, e-mail address) of the data controller or their representative;

b) name and availability (telephone number, e-mail address) of the data protection officer;

c) purpose and legal basis of personal data controlling;

d) the categories of personal data;

e) the recipients of personal data (if there are any) and the categories of recipients (if there are any);

f) the fact itself if any data is transferred to third countries or international organizations.

Moreover, at the time of obtaining personal data, the person concerned receives the following supplementary information so that the Company ensures the fairness and transparency of data controlling:

a) the duration of personal data storing; if it is not possible or not applicable the considerations applied for defining the duration;

b) in case of data controlling based on pursuing legitimate interest the interests of the data controller and/or third party;

c) the right of the person concerned to request access for, correct, delete or restrict the controlling of their personal data from the data controller, just as well as the right of data portability;

d) the right to withdraw a consent at any time in case the data controlling on the legal basis of a consent, which does not affect the legality of data controlling prior to the withdrawal;

e) the right to make a complaint at the supervisory authority;

f) the source of the obtained personal data, including the fact whether they are obtained from a public access source;

g) if there is automated decision-making – including profile-making –, legible information the logical background applied, on the significance and the possible consequences of this sort of data controlling at least in these cases.

III. The information given according to I. and II. shall happen as follows:

a) in a reasonable period of time after the personal data have been obtained considering the exact circumstances of data controlling, but in 1 month at longest;

b) in case personal data are being used for maintaining the contact with the person concern, at the time of the first contact made at latest; or

c) if personal data are expected to be transferred to other recipients as well, at the time of the first transferring made at latest.

If the data controller is to perform further data controlling due to any other purpose than obtaining the personal data, the person concerned shall be informed about this purpose alongside with all relevant supplementary information.

These described above need not be applied if and to the extent

a) the person concerned is already aware of the information in question;

b) the person concerned published the personal data in question at a public place (including websites) where anyone got access to them, and the personal data were available at the time of data collection performed by the Company;

c) providing the information in question has proven to be impossible, mean disproportional effort (especially archiving of public interest, scientific, statistic or historical research purposes), or complying the obligation compromises the data controlling or makes it impossible. In these cases, the data controller shall apply appropriate measurements to protect the rights, freedom and legitimate interest of the person concerned (including making the information publicly accessible);

d) obtaining or publishing the data in question is compulsory according to the applied local or European Union law, which includes appropriate measurements to protect the legitimate interest of the person concerned; or

e) according to the local or European Union jurisdiction that prescribes the obligations of confidentiality of certain profession(s) (including the case when the legal basis of obligations of confidentiality is law) the personal data in question have to remain confidential.

3.9 The right to access

The person concerned has the right to receive a feedback about the process how their data are being controlled. If so, they have the right to access the information as follows:

a) the purposes of data controlling;

b) the categories of personal data;

c) categories of recipient(s) whom personal data are or will be transferred, included especially third country recipients and international organizations;

d) the duration of personal data storing; if it is not possible or not applicable the considerations applied for defining the duration;

e) the right of the person concerned to request the correction, deletion or restriction of data controlling, and to object personal data controlling;

f) the right to make a complaint at any supervisory authority;

g) in case the data have not been obtained from the person concerned, every information available on their source(s);

h) if there is automated decision-making – including profile-making –, legible information the logical background applied, on the significance and the possible consequences of this sort of data controlling at least in these cases.

In case any personal data is being transferred to third countries or international organizations, the person concerned has the right to be informed on guarantees of data transfer.

The data controller shall share the copy of any personal data controlled with the person concerned. For any further copies requested by the person concerned, the data controller may charge the person concerned due to administrative costs, to a reasonable extent. If the person concerned has submitted their request in an electronic form, the information shall be provided in a wide-spread (file) format unless the person concerned requests for a different format. The right to request for a copy cannot affect disadvantageously other people’s rights and freedom.

9.4. The right to erasure and to be forgotten

The person concerned has the right to request for the erasure (deletion) of their personal data which shall happen without undue delay. The data controller is obligated to delete the personal data of the person concerned without undue delay in any of the following cases:

a) the collected or processed before are not used in the future for their original purpose;

b) the person concerned has withdrawn their concern and there is no other legal basis of data controlling;

c) the person concerned has objected against data controlling and there is no other legal basis of data controlling;

d) it has been proved that the data controlling has been illicit;

e) to comply any European Union or local law applied for the data controller the personal data has to be deleted;

f) the personal data collection has happened to provide services in connection with the information society.

If any data that are subject of deletion were published priorly, the data controller shall delete them. The data controller shall inform any other data controllers involved that the person concern requested the deletion of the copy of their personal data, and/or links giving access to these data. At applying the reasonably expected steps (including technical procedures) the available technologies and the costs of the procedure shall be considered, too.

The 2 points above shall not be applied if the data controlling is necessary

a) for applying the rights of being informed and freedom of deliverance;

b) for complying any European Union or local law applied for the data controller, or performing a task of public interest or applying public power license delegated to the data controller;

c) due to public interest of public healthcare

d) for archiving due to public interest, scientific or historical research, statistical data controlling if the rights described above likely compromise the data controlling or make it impossible; or

e) for proposing, applying or protecting legal interests.

9.5. The right to restrict

The person concerned has the right to restrict the data controlling in case of any of the following:

a) the person concerned disputes the accuracy of their personal data – in this case restriction applies for the duration of revising and/or correcting the accuracy of the data;

b) the data controlling is illicit and the person concerned objects against deletion and requests for the restriction of data use;

c) the data controller does not need the personal data for controlling any more, but the person concerned requests for them to submit, enforce or defend a legal claim;

d) the person concerned has objected against the data controlling, in which case the restriction persists until it has been decided whether the legitimate reasons of the Company have priority over the legitimate reasons of the person concerned;

If the data controlling falls into any category of restriction described above, the personal data affected can only be used with the consent of the person concerned, for submitting, enforcing or defending legal claims, in the defense of the rights of another natural or legal person, or for the common interest of importance of the European Union or any member state, with the exception of storing.

The data controller shall priorly inform the person concerned whose request is the basis of the data controlling restriction if the restriction has been released.

9.6. Right to data portability

The person concerned has the right to receive their personal data that they gave to the data controller or concern them in an organized, wide-spread, electronic format. Moreover, the person concerned has the right to transfer these data to another data controller without any hindrance from the data controller they received the personal data from in case:

a) the basis of data controlling is a consent or a contract; and

b) the data controlling happens in an automated form.

During the right to data portability is being exercised according to the point above, the person concerned has the right to request for the direct transfer between the data controllers assuming it is technically manageable.

Exercising this right cannot hinder the rights or freedom of other persons.

9.7. Right to object

The person concerned has the right to object against controlling their own personal data (including profile-making based on the provisions detailed as follows) due to reasons of their own situation; should data controlling take place due to the needs of public interest, applying public power license delegated to the data controller, or enforcing legitimate interest of any third party, at any time.

In this case the data controller shall proceed no further data controlling unless the data controller proves that the basis of controlling are compelling legitimate reasons that have priority over the interests or freedom of the person concerned, or are in connection with submitting, enforcing or defending legal claims.

If the personal data are controlled for direct solicitation, the person concerned has the right to object against controlling their data for this purpose at any time. This includes profile-making, as well, assuming this activity is in connection with direct solicitation.

If the person concerned objects against data controlling in the purpose of direct solicitation, no personal data shall be controlled henceforward for this purpose.

The person concerned shall be informed expressly about their right for objection. This piece of information shall be displayed in an unambiguous form, separated from all other information.

If personal data controlling takes place due to scientific, historical research or statistical reasons, the person concerned has the rights to protest due to their own reason against data controlling unless it is necessary for proceeding tasks of public interest.

**10. Automatic Decision-Making and Profiling**

The person concerned has the rights to exclude their personal data from the scope of decisions originated exclusively from automated data controlling (which includes profile-making) if the decision has a legal effect on them, or affects them with a similar significance. This shall not be applied, if the decision

a) is necessary for making or complying a contract between the person concerned and the data controller;

b) is enabled by any European Union or local law applied for the data controller that also states measurements for protecting the rights, freedom or legitimate interest of the person concerned;

c) is based on the expressed consent of the person concerned.

The data controller is obligated to take appropriate measurements to protect the rights, freedom or legitimate interest of the person concerned, minimally including the right to request for human intervention, express their standing-point, and submit an objection against the decision.

**11. Data Breach**

In case of any breach that likely means high risk regarding the natural persons’ rights or freedom, the Data Controller informs the person concerned without undue delay.

Informing the person concerned shall happen in an unambiguous and articulate form, containing as follows:

a) the nature of the breach

b) the probable consequences of the breach

c) the actions planned or performed to handle the breach, including the actions which are to lessen the possible negative consequences

d) provides the contact of the data protection officer, or if he/she is not available at that time, of a person who is able to give ample amount of information about the situation.

The Data Controller need not inform the persons who are involved in case of any of the following:

a) the data controller performed appropriate technical or organizational actions of defense; these actions have been performed for the benefit of the person concerned who is affected by the breach – especially measurements which have made the data affected by the breach incomprehensible for the unauthorized (eg. by using encryption on the data);

b) the data controller performed actions after the breach to ensure that the rights and freedom of the person concerned are most likely not in risk of danger anymore;

c) informing the persons concerned would require measurements of disproportional effort. In this case the persons concerned shall be informed with the help of published information or in any other form of similar efficiency.

In case the data controller has not informed the person concerned about the breach yet, the supervising authority may order to inform the person concerned if according the estimation of the authority the risk of the breach is likely high.

**12. The Right to Legal Remedy**

If the person concerned suspects that the law of data protection has been broken, they have the right to register a complaint, especially at the member state of their regular residence, workplace, or at the state where the suspected infringement has happened.

The supervisory authority the complaint has been submitted to is obligated to inform the person concerned on the result of their complaint, just as well as on the fact that he/she has the right to request legal remedy.

12.1. The right to request an effective judicial legal remedy against the supervisory authority

Every person concerned has the right to request an effective legal remedy to challenge a legally enforcing decision of the supervisory authority that affects them. If the supervisory authority does not handle the complaint or fails to inform the person concerned within 3 months about the result of the submitted complaint, the person concerned has the right to request for a legal remedy.

Any changes or amendments of the Privacy Policy shall be published on the Webpage. Regarding the controlling of personal data, the Privacy Policy in force shall be applied, regardless of the fact that at the time when the person concerned registered or provided personal data in any other way there might have been an earlier Privacy Policy in force.

**Contact**

In case of questions, notes or requests regarding this Privacy Policy, registering a complaint or exercise rights, please, contact us using any of the following accessibilities:

Name: HBS Hungary Ltd.

E-mail: [info@hbs.hu](mailto:info@hbs.hu)

Telephone: 36-1-452-1700

The data protection officer of HBS

Name: Kéri András

E-mail: [andras.keri@hbs.hu](mailto:andras.keri@hbs.hu)

Telephone: 36-30-2512-097

**In force**

This Privacy Policy has been in force since 30th Sept. 2020