Please read this leaflet carefully before using FeverFriend™ (LázBarát™) services.

PRIVACY NOTIFICATION FOR THE FeverFriend™ APPLICATION AND ABOUT USING THE WEBSITE

The goal of the FeverFriend™ Project is to change the negative social attitudes associated with fever, and disseminating, implementing and putting good practices into practice. Within this framework, the Company pays particular attention to legal, fair, transparent and safe handling of personal information provided by users of the application or the website.
The terms and conditions set forth in this prospectus are intended to determine the frames of data handling of the Company and inform all those involved in the data processing, about the details of handling the personal datas given by them or other intermediaries - in particular parents or legal representatives. It also aims to provide short, concise and clear information about what purpose, legal basis, conditions and warranties and how long we handle and store the defined personal information before giving it, and also informs about the rights of the concerned, the obligation of the controller, the data processor used by the controller, and about the organization the data subject may appeal to for legal remedy when exercising his rights.

1. NAME OF DATA CONTROLLER:

Name: Civil Support Nonprofit Ltd.
Postal address: 46 Kossuth Lajos utca, Pilisszentkereszt, 2098 Hungary
Headquarters: 3 Csévi út, Piliscsaba, 2081 Hungary
Websites: www.lazbarat.hu, www.joalaz.hu, www.alaz.hu, www.feverfriend.eu
Email: infolazbarat@gmail.com
Phone numbers: +3620 4729459 and +3626 346005
Represented by Dr. Henrik Szőke Ph.D. (the "Data Controller")
Data Protection Officer:
Name: dr. Gergely Hajnal
Email: gergely.hajnal@gmail.com
Phone number: +3630 495 16 09

2. DEFINITIONS RELATING TO DATA MANAGEMENT

The definitions that occur during the processing of personal data are defined by the GDPR. For the sake of transparency and clarity, the Data Controller ascertain the most important concepts in this section, taken from GDPR.
"Personal data": means any relevant information applying to an identified or identifiable natural person ("data subject"); a natural person is identifiable if he/she is possible to identify directly or indirectly, specially by some identification such as name, number, location data, online identity or one or more physical, physiological, genetic, intellectual, economic or social factors relating to his/her identity.
"Special data": personal data relating to racial or ethnic origin, political opinion, religion or belief or suggesting worldview or trade union membership; and genetic and biometric data for the unique identification of natural persons, health information, and relevant personal information on the sexual life or sexual orientation of natural persons; The processing of this data is, as a rule, prohibited.
"Data management": means any automated or not automated operation or combination of operation of personal data or data files such as collection, recording, systematization, proportioning, storing, transforming or altering, querying,, introspection, use, communication through dissemination or otherwise making available, coordination or linking, restriction, deletion or destruction;

"Restriction of data management": means the marking of stored personal data for the purpose of future restriction;
"Controller": shall mean the natural or legal person, public authority, agency or any other body which defines its purposes and means of processing personal data itself or together with others; if the purposes and means of data management are EU or Member State law, specific to the controller or the specific aspects of the appointment of the controller may be defined by Union or national law;
"Data processor": shall mean any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
"Recipient": shall mean any natural or legal person, public authority, agency or any other body to whom the personal information is disclosed, whether or not it is a third party. Public authorities which, in the framework of an individual investigation, may access to personal data in accordance with the law of either the EU or the Member State, shall not be treated as such recipients; the treatment of such data by these authorities shall be in accordance with applicable data protection rules in accordance with the purposes of data management;
"Third party": shall mean any natural or legal person, public authority, agency or any other body that is not the data subject itself, the data controller, the data processor or with persons under the direct control of the controller or the processor authorized to process personal data;
"Consent of the data subject": means a voluntary, specific and appropriate proclamation evidently made by the data subject, by which he/she indicates consent for the management of the personal data by statement or an unambiguous act that expresses confirmation;
"Privacy incident": means a security breach that has occured because of transmitting, storing or otherwise handling personal data that caused unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access;
"Provider": organization or legal entity providing service or services for registered users with a user profile;
"Supervisory authority": means an independent authority established by a Member State under Article 51 of the GDPR;
"Patient": For the purposes of this Privacy Statement, the term "Patient" means the person whose personal data specified by the application is registered provided by the user in order to obtain information regarding the feverish condition of the above person, and advice on possible treatment options.

3. APPLICABLE LAW

- 2016/679 regulation of the European Parliament and the Council (EU) about the protection in point of handling personal data of natural persons, the free flow of such data; and the repealing of Regulation (EC) No 95/46 ("GDPR");
- Act CXII of 2011 on Information Self-Determination and Freedom of Information;
- Act V. of 2013 on the Civil Code;
- Act XLVII of 1997 (hereinafter referred to as Eüak.) about the handling and protection of health care and related personal data
- Act CLIV of 1997 on Health; (hereinafter referred to as: Eutv.)

4. OTHER IMPORTANT INFORMATION CONCERNING DATA MANAGEMENT

The FeverFriend™ application can be downloaded freely and for free as a mobile application to mobile devices, and the FeverFriend™ also runs a separate website where more information is available about how the application works.

The application does not qualify as a medical device. The application categorizes a condition based on the data given by its user and based on evidence available in literature for which it will diagnosticate a duty or duties to be done. However, this does not replace the specific medical, specialist medical history, opinion and the set up diagnosis.

Before starting the application, ask your GP, pediatrician or attending physician for advice. If the medical opinion and the treatment recommendation given by the application does not match, the medical opinion prevails, the suggestion made by the application is for information purposes only, and FeverFriend™ is not responsible for any damages resulting from its interpretation. Using or respecting the recommendation given by the application can happen solely by the responsibility of the user of the application.

5. PURPOSE OF DATA PROCESSING, SCOPE OF PERSONAL DATA PROCESSED, AND LEGAL BASIS AND DURATION OF DATA PROCESSING

5.1. User registration via website or application

Data Controller Activity: Carrying out operations about creating a profile with users (registering), contacting. Registration allows the usage of the application, entering data, direct communication between the Service Provider and the user.

Purpose of Data Management: Contacting stakeholders, enabling the use of the application. Announcement of changes to the website and information about the application.

Legal basis for data management: The expressed, appropriate, voluntary contribution of the previously informed data subject under Article 6 (1) (a) of the GDPR.

Stakeholders: People completing registration.

Personal Information Managed:
- name (first and last name)
- e-mail address

The Controller will not and mustn't provide the personal data you provide for purposes other than those stated above.

Data Management Duration: Data Controller for the data specified above is concerned until your registration is revoked, terminated.
Data Controller sends regular reminders to registrants to affirm their consent to the website and application.
The Controller does not forward the above stated personal information to a third country or international organization.

Rights of the data subject: the data subject may
(a) request information on the processing of personal data concerning him or her,
and access to this personal information,
(b) apply for their correction,
(c) request their cancellation,
d) request a restriction on the processing of personal data,
(e) raise objection to the processing of personal data,

(f) exercise the right to data portability,
(g) exercise his/her right of appeal.

The data subject may hand in a complaint to the National Data Protection and Freedom of Information Authority ("NAIH") as defined at the end of this leaflet or appeal to the venue.

Consequences of failure of providing data: In case of failure of registration, the data subject cannot use the service provided by the application.

5.2. Cookies on the FeverFriend™ website

A cookie is an alphanumeric information packet with a variable content sent by a web server and is stored on the user's computer for a predetermined period of validity.
A website can use the cookie to make the user experience even more effective.
According to the law, cookies may be stored without the consent of the data subject on the legitimate interest of the Data Controller if, on the device of the data subject, this is strictly necessary for the sake of the operation of the website.
For the use of all other types of cookies - that is, cookies that are not a website necessary for its proper functioning, -ie for marketing or statistical purposes - the consent of the data subject is required.
FeverFriend™ manages the following cookies on its website:

Name of cookie	Wich data are reached?	purpose of cookie
has_js	Javascript licence	is required to run javascript, technical cookie, which indicates Javascript licensed
cookie-agreed-hu	The user has accepted the request for consent use of cookies	indicates cookie acceptance
SESS...	Unique worksession identification	session cookie user login, after taht Drupal session ID cookie

Legal basis for data management: Legal basis for data processing in case of the above cookies (according to the Article 6 (1) (f) GDPR) is in the data controller's legitimate interest that during loading and running of the website the website should not collapse but function smoothly for the user, and that the user of the website receives appropriate information about cookies based on consent, and he/she may exercise the right laid down in Article 6 (1) (a). The above cookies are helping the appropriate session, the smooth functioning of the homepage. Cookies at the end of the session, or when closing the browser are automatically deleted from the affected computer.

Name of cookie	Wich data are reached?	Purpose of cookie
_gat	Most commonly used cookies by Google Analytics with the help of which Google Analytics as service, can provide information for the owner of the website and can prepare statistics about the circulation of the website - e.g.,	The _gat cookie, according to Google, serves to control the frequency of the request - it's limiting data collection from busy websites. The website occurs in each page request.

_ga A	periodically how many users visit the site, what pages are viewed and how long for. All three cookies are connected toGoogle Universal Analytics.	_ga cookie is for differentiating each user (more specifically for each browser). As a value it contains a randomly generated number (ex: GA1.2.255322818.1517541613). It can be used to produce long-term statistics about user visits to your site. The website occurs in each page request.
_gid		A _gid cookie stores unique value to every page you visit, it contains a generated number (ex: GA1.2.255322818.1517541613). It may be used like using a _ga cookie. The website occurs in each page request.

Legal basis for data management: In the case of the above cookies, the visitor of the website indorses his/her voluntary decided contribution according to the Article GDPR. 6. (1) (a), based on relevant information. The visitor can denote if disabling or enabling the above cookies. With Google Analytics cookies, Data collector collects information about your use of the website, eg. which page the visitor viewed, where he/she clicked, the number of pages you were looking for, how long each view was, what error messages he/she encountered.

Name of cookie	Wich data are reached?	Purpose of cookie
__atuvc __atvus: AddThis	These personal cookies were created and are read by AddThis community shared page to ensure it so that the user can see an updated counter if you share a page and will return to it, yet before the sharing counter cache is upgraded.	These cookies are about the AddThis widget operation. This widget is often embedded in websites, helpingcontent sharing on social media AddThis platforms. AddThis cookies also provide statistical information about the number of times a user shared one content and how you use the built-in AddThis feature on the site. The personal identification is possible only if you are personally registered with AddThis service and consented. www.addthis.com/privacy/opt-out

Legal basis for data management: In the case of the above cookies, the visitor of the website indorses his/her voluntary decided contribution according to the Article GDPR. 6. (1) (a), based on relevant information.

The visitor can choose to turn off or enable the above cookies. Data Controller added these cookies to the cookies it uses for a functional, experience enhancing purpose to make content sharing simpler.

Duration of storage of personal data: The duration of storage of cookies differs from cookie to cookie - see the chart.

The identity of the potential data controllers entitled to access the data, and the recipients of the personal data: The data can only be known by the data controller and the web site operator.

Consequences of failure to provide data: If certain cookies are not allowed by the affected, a less personalized experience will appear on the website, but functionally it will not interfere with the operation.

5.3. Use of services provided by an application; the foundation of the profile of the patient in fever (hereafter referred to as a patient) given by the user

Data Controller Activity: The application gives advice about treatment options and methods for the fever-patient according to the data obtained from the series of questions and the relevant literature. This is based on the definition of the certain data of the patient.

Purpose of Data Management: According to the Eüak. Article 4 (3) (promoting health) the data of the patient given by the registered user, serves that the application can provide more personalized advice on how to treat your fever.

In addition to the patient data provided, accurate responses driven by the application are required in order to ensure that the personalized counseling should truly reflect on the patient's condition. The personal information specified here is not sufficient for the counseling.

The Data Controller draws attention to the fact that in the case of a person under 16 years of age, only the person exercising parental authority over the child is the one who can give the datas. If the Registered Person has reached the age of 16, she/he can only record her/his own datas beyond the above case. The contracting authority expressly declares this to the registered user!

Legal basis for data management: The voluntary decided contribution of the affected or the person exercising parental responsibility over the affected child under the age of 16, according to the Article GDPR. 6. (1) (a), based on relevant information.

Stakeholders:
a) registered persons over the age of 16
b) stakeholders whose details were provided by the registered person (children under 16 years of age)

Personal Information Managed:
- patient name (alias may be entered)
- gender of the patient;
- patient's date of birth;
- patient weight;
- patient height;
- acute illness affecting the heat center;

- chronic diseases;
- number of siblings.

Duration of Data Management: Data Manager is handling the above information to achieve the goal defined in Eüak. Article 4 (2) (d),ie. to achieve the research, with providing the appropriate warranties (pseudonym and data encryption), in accordance with the Article 89 (1) GDPR and the purpose of data management for the duration of the research objective or until the consent of the person concerned or the person exercising parental authority is revoked.

The Controller does not forward the above mentioned certain personal information to a third country or an international organization.

Rights of the data subject: the data subject may
(a) request information on the processing of personal data concerning him or her, and the access to this personal information,
(b) apply for their correction,
(c) request their cancellation,
d) request a restriction on the processing of personal data,
(e) object to the processing of personal data,
(f) exercise his/her right to data portability,
(g) exercise his/her right of appeal.

The data subject may lodge a complaint with the National Data Protection and Freedom of Information Authority ("NAIH"), as defined at the end of this leaflet, or can go to court to the Competent Authority.

Consequences of failure to provide data: The affected person can't reach the user interface to use the service provided by the application, if the data of the patient defined in the patient's profile is not complete or missing.

5.4. Use of services provided by an application; personal data given by the user to the questions regarding the condition of the feverish, ill person

Data Controller Activity: The application gives advice about treatment options and methods for the fever-patient according to the data obtained from the series of questions and the relevant literature.

Purpose of Data Management: The data about the patient provided by the registered user according to the Eüak. Article 4 (3) (promoting health) serves that the application can provide more specific, more personalized advice on how to treat the fever condition.

In addition to the patient data provided, accurate responses driven by the application are required in order to ensure that the personalized counseling should truly reflect on the patient's condition. The personal information specified here is not sufficient for the counseling.

The Data Controller draws attention to the fact that in the case of a person under 16 years of age, only the person exercising parental authority over the child is the one who can give the datas. If the Registered Person has reached the age of 16, she/he can only record her/his own datas beyond the above case. The contracting authority expressly declares this to the registered user!

Legal basis for data management: The voluntary decided contribution of the affected or the person exercising parental responsibility over the affected child under the age of 16, according to the Article GDPR. 6. (1) (a), based on relevant information.

Stakeholders:
a) registered persons over the age of 16
b) stakeholders whose details were provided by the registered person (children under 16 years of age)

Personal Information Managed:
Data on the patient's current, fever-related condition:
- Hydration data: recent urine time, skin elasticity and turgor,
  tear ducts, tongue, fluid intake, possible diarrhea, vomiting and their types,
- Skin condition, colour, quality, skin rash
- Respiratory conditions, shortness of breath, wheezing, breathing rate
- Heart-rate
- degree of fever, method of measurement, location of fever measurement,
- other data relating to general well-being and consciousness.

Duration of Data Management: Data Manager is handling the above information to achieve the goal defined in Eüak. Article 4 (2) (d), ie. to achieve the research, with providing the appropriate warranties (pseudonym and data encryption), in accordance with the Article 89 (1) GDPR and the purpose of data management for the duration of the research objective or until the consent of the person concerned or the person exercising parental authority is revoked.

The Controller does not forward the above mentioned certain personal information to a third country or an international organization. The controller reserves the right to forward the anonymized data deprived of personal information.

Rights of the data subject: the data subject may
(a) request information on the processing of personal data concerning him or her, and the access to this personal information,
(b) apply for their correction,
(c) request their cancellation,
d) request a restriction on the processing of personal data,
(e) object to the processing of personal data;
(f) exercise his/her right to data portability.
(g) exercise his/her right of appeal.

The data subject may lodge a complaint with the National Data Protection and Freedom of Information Authority ("NAIH"), as defined at the end of this leaflet, or can go to court to the Competent Authority.

Consequences of failure to provide data: The affected person can’t make full and complete use of the service provided by the application, if the data of the patient’s condition defined by the application is not complete or missing. The application will not produce a valid result if the data is not fully entered.

Data Processors:

Names	Headquarters	Data processing task
Csaba Eczl	B1 / B 2/2. Jószerencsét Ltp. 2084, Pilisszentiván Hungary	website operation (control, technical update, security system development, other improvements, repair tasks)
Google Ireland Limited	Gordon House, Barrow Street, Dublin, D04 E5W5, Dublin	Google Analytics cookies
Adamis Lukács	7 Acél u., 2000 Szentendre Hungary	application and web page programming
Ádám Ridovics	3-13. Százados út, 1087, Budapest Hungary	application and web page programming
Henrik Szőke	46 Kossuth Lajos utca, 2098, Pilisszentkereszt Hunagry	project manager, science processing of data
23VNet Ltd	18 Victor Hugo u., 1132, Budapest Hungary	hosting provider

The Controller does not forward the above certain personal information to a third country or an international organization. The controller reserves the right to forward the anonymized data deprived of personal information.

6. ENFORCEABLE RIGHTS OF STAKEHOLDERS REGARDING DATA MANAGEMENT

The Data Controller shall ensure that the rights of data subjects are enforced as follows:
The controller shall give the data subject the opportunity to submit his/her application associated with the exercise of his/her rights through the contact details in this prospectus in any of the following ways: (i) by mail, (ii) by email, (iii) by phone.

Controller fulfils the data subject's request without undue delay, but in any case within 30 days from arrival, and informs the data subject briefly, transparently,in an accessible, clear and comprehensible manner. The Data Controller shall also decide on the refusal of the application within this period and inform the data subject of the refusal of the application, the reasons therefor, and the relevant legal appeal.

The data controller shall, as a rule, comply with the data subject's request by e-mail, unless the data subject requests otherwise.
Telephone information may only be provided at the request of the data subject if he/she has verified his identity. Controller does not use the postal address or telephone number of the affected for any other purpose.

The Data Controller shall not charge a fee or reimbursement for the fulfillment of the requests of the data subjects detailed below. However, if a new, unjustified, excessive request from the data subject is received for the same set of data within one year of the previous request made, the Data Controller reserves the right to set out a reasonable repayment of expenses in portion of the workload, for the fulfillment of the request or to refuse to act on the application, with due justification.

6.1. Right to information and access

The data controller shall, at the request of the data subject, provide brief, transparent, comprehensible, clear information in an easily accessible manner about the following:

- whether your personal data is being processed by the Data Controller;
- the name and contact details of the Data Controller;
- the data processing, the names of the data processors defined in the paragraphs above, and
- contact information;
- the personal data of the concerned managed by the Data Controller and the source of those;
- the purpose of the processing of personal data and the legal basis for the processing;
- the duration of the data management;
- the recipients or categories of recipients who has been or will be apprised of the personal data, including in particular recipients of a third country, and international organizations;
- the rights of the data subject;
- the circumstances, effects and resolution of a possible privacy incident and the arrangements made for prevention.

6.2. Right to rectification

The controller shall, at the request of the data subject, rectify any inaccurate personal data concerning the data subject.

The controller shall inform any recipient, who was reported the personal data, about the rectification, unless it proves impossible or requires a disproportionate effort. At the request of the data subject, the Data Controller shall inform the data subject of these recipients.

6.3. Right to delete ("forget")

At the request of the data subject, the Data Controller shall delete the personal data relating to the data subject in case of the following reasons:

- Personal data are no longer needed for the purpose for which they were collected or the data subject was treated in an other way;
- the data subject protests against the data management;
- personal data have been unlawfully processed by the Data Controller;
- personal data must be deleted in order to fulfill its legal obligation as prescribed by EU or Hungarian law applicable to the Data Controller.

The controller shall inform any recipient, who was reported the personal data, about the rectification, unless it proves impossible or requires a disproportionate effort. At the request of the data subject, the Data Controller shall inform the data subject of these recipients.

6.4. Right to Restrict Data Management

At the request of the data subject, the Data Controller shall restrict data processing if any of the following is met:

- the data subject disputes the accuracy of the personal data, in which case the restriction is for the period, which allows the Data Controller to verify the accuracy of the personal data;
- the data processing is unlawful, but the data subject opposes the deletion of the data and instead he/she requests restrictions on its use;

- the Data Controller no longer needs personal data for data management purposes, but the affected requires them to submit, validate or defend legal claims.

The controller shall inform any recipient, who was reported the personal data, about the rectification, unless it proves impossible or requires a disproportionate effort. At the request of the data subject, the Data Controller shall inform the data subject of these recipients

6.5. Right to portability

The data controller shall, at the request of the data subject, make personal information relating to the data subject available to the data subject.Data Controller further undertakes that these personal data may be transmitted by the data subject to another data controller without this being put back by the Data Controller.

6.6. Right legal appeal

If the data subject considers that the Data Controller has violated his/her right to protection of personal data in the course of its processing, you may seek redress under the applicable law at the competent authority, that is you can make a complaint to NAIH (address:22/c. Erzsébet Szilágyi fasor, 1125 Budapest; postal address:Pf. 5., 1530 Budapest; Website: www.naih.hu; e-mail address: ugyfelszolgalat@naih.hu; phone number: + 36-1 / 391-1400) or contact the competent court.

The Data Controller undertakes to cooperate with the court concerned or NAIH during these proceedings and he/she releases the data regarding the processing of data to the court concerned or NAIH.

The Data Controller also undertakes to compensate for damage caused by a breach of data security requirements or if the personal data of the data subject has been processed unlawfully. The affected may claim damages in the event of a violation of his/her privacy. Data manager is exempt from liability if the damage was caused by an unavoidable cause outside the scope of the data management, and further if the damage or injuria caused by violation of privacy was caused intentionally or comes from his seriously careless behavior.

7. DATA SECURITY MEASURES

The Data Controller shall ensure the security of the data. Data manager has done the technical and organizational measures and established the rules of procedure to ensure that the data recorded, stored or managed are protected or prevented, and prevents their destruction, unauthorized use, or unauthorized alteration. He also calls third parties to whom the data subject has been transferred that they are obliged to comply with the requirement of data security.

The Data Controller shall ensure that the data being processed shouldn’t be accessed, published, transmitted, modified, or deleted by any unauthorized persons.

The Data Controller will do its utmost to ensure that the data is not damaged or destroyed. The above commitment is also ordered to the employees and partners of the Data Controller, taking part in data management, so also including data processors acting on behalf of the Data Controller.

8. MANAGING PRIVACY INCIDENTS

If the Data Controller perceives any accidental or unlawful destruction, loss, alteration, unauthorized transmission, or disclosure of the personal data transmitted, stored or otherwise processed by the Data Controller, or incident that results in unauthorized access, (hereinafter referred to as "privacy incident"), he/she is required to comply with GDPR 33-34., report the incident to NAIH and inform the data subject or data subjects about the privacy incident, if it is likely to be high risks to the rights and freedoms of natural persons.
The person being aware of any privacy incidents referring to the Personal Data transmitted, stored, or otherwise processed by the Data Controller as described above, can report it to the Data Controller at the contact details below:
By phone: +36204729459
Via email to: infolazbarat@gmail.com

In addition to indicating the subject of the privacy incident, the notifying person must specify:
- name of the notifier,
- contact details of the notifier: telephone number and/or e-mail address,
- (in the case of an employee) his organizational unit,
- whether the incident affects the IT system.

The Controller shall examine the application within 1 business day, or if the incident is considered serious, without delay and, if necessary, he requests further data from the notifier. Within 72 hours of the incident being reported, the Data Controller shall provide the data service to NAIH.

The data service shall include the following:
- the nature of the data protection incident, including the categories and approximate number of data subjects, as well as the categories and approximate number of data affected by the incident;
- the name and contact details of the contact person providing further information;
- the probable consequences of the privacy incident;
- measures taken or planned by the Data Controller to remedy the data protection incident, including, where applicable, any measures to mitigate the consequences of any adverse effects arising from the privacy incident.

In case the privacy incident requires further investigation, the Data Controller shall take the necessary steps during the investigation to estimate the actual and potential effects of the privacy incident, with the involvement of appropriate professionals. A report will be drawn up by the experts consulted. The report must include a proposal about the necessary security measures to averse the privacy incident.

It is up to the Data Controller to take action.

If the Data Controller believes that the privacy incident is likely to be at high risks to the rights and freedoms of natural persons, the controller must inform the data subject without unjustified delay of the privacy incident.

The data controller shall clearly and unambiguously state the nature of the data protection incident highlighting the following:
- the name and contact details of the contact person for further information;
- the likely consequences of a privacy incident;

- measures taken or planned by the Data Controller to remedy the data protection incident, including, where applicable, any measures to mitigate the consequences of any adverse effects arising from the privacy incident.

The controller shall not inform the data subjects if:
- he/she has taken appropriate technical and organizational security measures and these measures have been applied to the data affected by the privacy incident, in particular measures - such as the use of encryption - which render the data unintelligible for unauthorized persons;
- took further measures following the data protection incident to ensure that the high risk to the rights and freedoms of the data subject is unlikely to materialize;
-the communication would require a disproportionate effort as the number of stakeholders involved is so high, that the Data Controller could only inform them by undue expenditure in the up-mentioned way. In this case, the Data Controller shall disclose the appropriate information.

9. RECORD OF PRIVACY INCIDENTS

The Data Controller keeps a record of the privacy incident.

The following shall be recorded in the register:
- the scope of the personal data concerned,
- the scope and number of those involved in a data protection incident,
- the date of the privacy incident,
- circumstances and effects of the data protection incident,
- the measures taken to address the data protection incident,
- other data as defined by the law governing data processing.

The Controller must retain the data in the records about the data protection incident for 5 years, in case of incidents involving personal data , and 20 years, in case of incidents involving special data.

10. RIGHT OF LEGAL APPEAL

The Data Manager can be reached in connection with any questions or comments relating to data management on any of the accessibilities given in this information.
There is also a right of appeal or complaint to the National Data Protection and Freedom of Information Authority:

Name: National Data Protection and Freedom of Information Authority
Headquarters: 12 / C., Szilágyi Erzsébet fasor 1125, Budapest
Mailing address: Pf. 5.,1530 Budapest
Phone: + 36-1-391-1400
Fax: + 36-1-391-1410
Website: www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

The Data Subject can bring a suit against the Data Controller In the event of a violation of his rights. The court is acting out of line in the case. The Data Controller must prove that the Data Management suits the requirements of the law. The lawsuit can be instituted at the Court of Justice of the residence or place of residence - regarding the choice of the plaintiff.

The Data Controller undertakes to cooperate with the court concerned or NAIH during these proceedings and to release the data regarding data management to the court concerned or NAIH.

The Data Controller also undertakes to compensate for damage caused by processing the personal data of the data subject unlawfully or by a breach of data security requirements. The person concerned, in the event of a violation of his/her privacy, may claim damages. Data manager is exempt from liability if the damage was caused by an unavoidable cause outside the scope of the data management and if the damage or violation of privacy comes from intentional or seriously careless behaviour of the affected.

The Data Controller reserves the right to change this information at any time.

February 11, 2020