DATA MANAGEMENT AND DATA SECURITY POLICY

JDC Hungary Foundation

1st April, 2019

Contents

I. INTRODUCTION

JDC Hungary Foundation as data controller (hereinafter: **Foundation** or **Data Controller**) hereby informs its users, supported persons, recruiters and the visitors of its website and community site (hereinafter jointly: **data subjects** or **users**), that it respects the rights of the data subjects to their personal data, therefore during its data management it acts in line with this data management and data security policy (hereinafter: **Policy**). The relevant version of the Policy is available in electronic form and on paper in the Foundation's office. Based on the above, the Data Controller acknowledges the provisions of the Policy to be binding on itself and during its operation it acts pursuant thereto.

This Policy regulates the data management activity performed in connection with the services provided by the Foundation to the data subjects.

On the http://www.mozaikhub.hu, https://szarvas.camp/, http://www.jdchungary.hu/website, Data Controller also publishes a Data Protection Information Bulletin, which is formally separate from the present Policy, which shall be considered as an annex of this Policy, and which provides information about the data management in connection with the use of the website.

The result of the Data Protection Impact Assessment performed on the basis of section 35 (3) b.) of the GDPR shall serve as a basis of this Policy.

II. DEFINITIONS

Data Controller uses the following definitions in this Policy and in the annexes thereof:

- '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;

- 'management' 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;

- 'restriction of management' means the marking of stored personal data with the aim of limiting their management in the future;

- 'profiling' means any form of automated management of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

- ‘pseudonymisation’ means the management of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

- ‘data 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 management of personal data; where the purposes and means of such management 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;

- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- ‘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 management of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the management;

- ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

- ‘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 management of personal data relating to him or her;

- ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise managed;

- ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- ‘biometric data’ means personal data resulting from specific technical management relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

- ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

- ‘Colleague’ means a natural person beng in mandate, labor or other legal relationship with the Data Controller, who contributes to the performance of Data Controller’s services;

- ‘medical treatment’ any activity, which aims the direct examination, cure and care of the data subject and furthermore the management the examination data of the data subject, for the purpose of the preservation of health, furthermore the preventing, early detection, determination, curing of diseases and the maintenance or remedy of the deterioration arisen as a result of the disease;

- 'medical secret' means the health and personal data which the controller has become aware of in the course of medical treatment, as well as any other data relating to completed medical treatment or data, which the controller has become aware of in connection with the medical treatment;

- ‘Info Act’ means Act CXII of 2011 on the information self-determination and freedom of information;

- ‘GDPR’ means Regulation of the European Parliament and of the Council (EU) 2016/679;

- ‘Health Data Act.’ means Act XLVII of 1997 on the Management and Protection of Health and Personal Data Related to Them;

III. PERSON OF DATA CONTROLLER

1. For the purposes of this Data Protection and Data Security Policy, Data Controller shall be:

1. **Name: JDC Magyarország Alapítvány (JDC Hungary Foundation)**
   Registered seat: 1053 Budapest, Ferenciek tere 7-8. II. lph. I. em. 5.
   Registration No.: 01-01-0012517
   Tax No.: 18942408-2-41
   Email: info@jdchungary.hu

2. **Data Protection Officer:**

   Appointed data protection officer under section 37 (1.) c. of GDPR (management of data concerning health):

   Registered seat: Itamar Albek
   Office address: 220 E 42nd St., New York City, New York, Amerikai Egyesült Államok
   Phone number: 212-687-6200
   E-mail: ItamarA@jdc.org

   Tasks of the data protection officer:
   Provides information and advice to the Data Controller or Data Processor, and employees performing data management on their obligations, examining the compliance with the Regulation and other EU or national data protection provisions, as well as with the Data Controller or Data Processor's personal data protection rules, including assignment of responsibilities, awareness-raising and training of those involved in data-management operations and related audits are also kept up to date with the supervisory authority in contact with the authority responsible and, where appropriate, in any other matter.

2. Data protection organization of the Data Controller

1. The Data Controller is committed to data protection, and therefore, in accordance with the legal and operational changes, it will amend this Policy.
2. The data protection, data management, data security and information security related management of the Data Controller shall be performed by the operative director of the Data Controller performing the operative management of the Data Controller, who requests the Data Protection Officer's opinion on data management, data security and information security matters.
3. Deletion, rectification, blocking or destruction of data may only be performed by the competent Colleague if he / she has ascertained that the terms and conditions set out in the law, the Regulations or other acts are fulfilled.
4. In relation to the data management and data protection, every Colleague shall
   a) get aware of and keep the rules,
   b) attend training,
   c) provide information to the data subjects,
   d) forwarding without delay in written form (including also e-mails) all queries and/or asserting of rights arriving from outside of the Data Controller, to the data protection officer or to the general director of the Foundation,
   e) report immediately upon the occurrence of an incident to the data protection officer or to the general director of the Foundation in the event of a data protection or data security incident, and to contribute to the prevention, compensation, and detailed investigation of the incident.

3. General tasks related to the enforcement of the data subject's rights

The Data Controller's general procedure related to the exercising and enforceing of the data subjects' rights is as follows:

1. The Data Controller shall, without unreasonable delay, but within a maximum of 30 days from the receipt of the request (15 days in the case of a objection), inform the data subject of the steps taken in relation to the application or of any factual or legal reason for not complying with the request; about the rights of the data subject and the legal remedies open to the data subject: the possibility of recourse to the court and the National Authority for Data Protection and Freedom of Information.
2. If the reason for the rejection of the application does not exist, the Data Controller shall notify in writing all the data recipients of the data to whom the data was previously transferred for the purpose of data management, and, if necessary, the exercise of the right contained in the request.

4. Educating the Data Controller's data protection organization

1. Provision of data management and data protection training for Colleagues on an annual basis is the responsibility of the Data Controller. The training shall be documented.
2. The data protection related training of the new Colleagues shall be performed by the management of the Data Controller, it shall document the training. The management of the Data Controller may entrust the data protection officer with the tasks related to education.

IV. THE PURPOSE OF THE POLICY

The primary purpose of this Policy is to define and adhere to the basic principles and provisions for the management of data of natural persons in contact with the Data Controller in order to protect the data of natural persons in accordance with the relevant statutory and official resolutions.

The Data Controller will take the necessary measures to comply with the data protection provisions of the legislation in force, and in particular, but not exclusively with Act CXII of 2011 on the information self-determination and freedom of information, Regulation of the European Parliament and of the Council (EU) 2016/679, Act XLVII of 1997 on the management and protection of health and personal data related to them, Act XLVII of 2008 on the prohibition of unfair commercial practices against consumers, Act CXXXIII of 2005 on the rules of personal and property protection and private investigative activities, Act XLVIII of 2008 on the essential conditions and certain limitations of economic advertising activities.

V. SCOPE OF THE POLICY

This Policy shall be effective from 25th May, 2018 until further notice or revocation.

The personal scope of the Policy extends to the Data Controller as well as to persons whose data are contained in data management under the scope of these Policy, as well as to persons whose rights or legitimate interests are affected by data management.

The material scope of this Policy covers the data management and data of the Data Controller, including any electronic and / or paper-based data management.

VI. THE RIGHTS AND REMEDY OPTIONS OF THE DATA SUBJECT

The rights and remedies available to the data subject under the GDPR Regulation are defined below and communicated to those concerned.

Right of information, also known as the "right of access" of the data subject

At the request of the data subject, the Data Controller shall provide information on:

a) the data and categories of personal data which it manages,
b) the purpose of the management,
c) the legal basis for the management,
d) the duration of the management,
e) the duration of the storage of the data or, where this is not possible, the criteria for determining that period,
f) if the data were not collected from the data subject, any available information on their source,
g) the data of the processor, if a data processor has been used,
h) the circumstances, effects and measures taken to counteract the data protection incident, furthermore
i) in the case of transmission of the personal data of the data subject, the legal basis, the purpose and the addressee of the transfer.

The information is free of charge if the person requesting the information has not submitted a request for information to the Data Controller for the same data year. In other cases, a cost reimbursement can be established. Repayment of costs already paid must be refunded if the data have been illegally treated or the request for information has led to a correction.

The data subject may request from the controller access, rectification, erasure or restriction of management of personal data relating to him or her and may object to the management of such personal data and the right to portability of his or her data.

Exercising the rights of the data subject

The Data Controller - by simultaneously suspending data management - shall examine the objection as soon as possible after the submission of the request, but within a maximum of 15 days, and shall inform the applicant in writing of its outcome. If the applicant's objection is well founded, the Data Controller terminates the data management, including further data collection and data transfer, and locks the data, and notifies the persons to whom the personal data affected by the protest has previously been forwarded of any protest or action taken on it, and who are obliged to take action to enforce the right of objection.

If the data subject disagrees with the Data Controller's decision or the Data Controller fails to comply with the time limit referred to, he / she is entitled to apply to the court within 30 days of its notification.

The data subject may lodge a complaint with the following contact details:

National Authority for Data Protection and Freedom of Information
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Telephone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
www: http://www.naih.hu e-mail: ugyfelszolgalat@naih.hu

In case the Data Controller has used a Data Processor, the Data Controller shall be liable to the data subject for any damage caused by the Data Processor and the Data Controller shall also pay to the data subject the penalty for violation of moral rights by the Data Processor. The Data Controller shall be exempt from liability for damage caused and for payment of penalty if it proves that the damage or the violation of privacy of the data subject has been caused by an unavoidable cause beyond the scope of data management

There is no need to compensate for the damage and no claim for penalty in so far as the damage caused to the victim or the violation of the right to the personality arose from the willful or gross negligence of the data subject.

VII. PRINCIPLES AND PURPOSE OF DATA MANAGEMENT

The Data Controller complies with the data management principles of Article 5 of the GDPR.

The purpose of data controlling is to collect, store and process the data of the data subject for the sake of contacting with the data subject in order to fulfill the service contracts concluded with the data subject, to participate in the programs of cultural education, entertainment, to fulfill the legal obligations of the Data Controller, the prevention, investigation and exploration of abuses

For the purposes of data management, only the number of health and personal identification data that is essential for the purpose of data management can be managed.

The Data Controller specifies the specific legal basis (s) and purpose (s) of the data management when defining each data management activity. The provision of data concerning health and other specific data is required to provide medical assistance.

VIII. LEGITIMATE PURPOSE OF DATA CONTROLLING

Since the provision of personal data and data concerning health is required for the organization of grants and events, the data subject gives his / her prior and voluntary consent for the management of his / her personal data for the purpose of supporting, educational, and cultural activities of the Foundation, and for transferring them to a designated data processor.

Voluntary consent, as an agreement, should also be understood as the behavior by which the data subject using the website accepts that all the regulations related to the use of the website, including this Policy, are automatically extended to him or her, or the conduct in which - after notification - the data subject enters and is present in the area monitored by the camera system operated by the Data Controller.

The Data Controller hereby informs the data subjects that the data subject is entitled to withdraw his / her consent at any time. Withdrawal of consent does not affect the legality of the consent-based data management prior to revocation.

The Data Controller informs data subjects that the consequence of non-provision of data is that the Data Controller is unable to provide support, or that the data subject is not provided with any advice / service, educational, cultural or dissemination services, either verbally or in writing, or he /she is not informed about the events by the Data Controller.

IX. RETENTION PERIOD OF DATA MANAGEMENT

Duration of data management for support services:
According to the tables detailed in Section X.

Duration of data management concerning labor data management:
In case the data subject as applicant applies for the database of job applicants and he / she consents to the further management of his / her data after the filling of the given position being aware of the purpose and deadline, the Data Controller manages the data for 2 years after the collection thereof.

The data management rules concerning the employees are set out in the Data protection information sheet for employees, which is attached to this Policy.

X. CERTAIN ACTIVITIES RELATED TO DATA MANAGEMENT AND THE SCOPE OF MANAGED DATA

General terms

Data collection: During the data collection the time of the data collection and the person collecting the data shall be recorded in the documentation. All records and entries shall be authenticated with signature or paraph and if necessary, with date, in case of electronic data management, the clear identification of the registrant shall be secured.

Modification of data: If, for some reason or mistake, the data entered has to be modified, this can only be done so that the original data can be established. The change must also be marked with a paraph, and in the case of electronic data management, the clear identification of the registrant and the logging of the entry must be ensured by the system.

Deletion of data: Data may only be deleted on the basis of this Policy. In the course of deletion, the data protection rules shall be adhered, especially regarding unauthorized access. During deletion, manually handled data must be physically destroyed and, in the case of electronically stored data, irreversibly changed.

Data management concerning supports

Scope of data subjects: All natural persons and non-natural legal entities who provides consent to the Data Controller or agrees with the Data Controller – alongside providing his / her / its personal data – in connection with the supporting services provided by the Data Controller.

The activity and process involved in data management are:

a) The Data Controller informs the data subject about the conditions of the service, support, etc. according to the laws.
b) The data subject, at his / her own discretion, voluntarily and without influence decides on the use of the Data Controller's service / services. If he / she intends to use it, he / she will provide a consent statement and / or agreement with the Data Controller by providing the above data.
c) The data subject acknowledges that the data and information provided on his / her health data sheet are necessary for the performance of the services and, where applicable, the choice of medical care, and declares that the data provided are complete.
d) The consent statement and / or agreement, along with the personal data, data concerning health and in case of legal entities the data concerning financial status which are connecting to and essential for the provision of the service shall be stored by Data Controller in a specially dedicated electronic registry system (in excel format) and / or on paper. The Data Controller maintains a separate inventory for the data management activities under Article 30 of the GDPR
e) Data Controller in order to comply with the requirements of the data security, pays special attention to data concerning health and other special personal data.

Scope and purpose of the data concerned by the date management:

1. **Szarvas Camp**

The Szarvas International Jewish Youth Camp started its journey in 1990 with the aim of creating a community that nurtures and enhances individual and community development based on entertainment education, in a secure, supportive and diverse environment, with qualified leaders and excellent professionalism. The purpose of the camp is to ensure that the Jewry it represents are inclusive and open to everyone. Help campers to experience their own Jewish identity, providing them with the opportunity to find a community. With age-specific occupations, they want children to make friends, play sports, relax and enjoy a Jewish community experience during 12-day tours. In the Szarvas Camp, besides the permanent programs, young people can participate in study groups falling in their sphere of interest. The trainings are held by trained youth leaders and are run by professional specialists.

The Foundation stores and manages the data provided by the data subject for the sole purpose of finalizing the registration as a worker or volunteer at the Szarvas Camp, for establishing, documenting and recording the legal relationship.

The Foundation does and may not use the data provided for purposes other than those specified above. The release of data to third parties or authorities, unless otherwise provided by law, is possible with the prior explicit consent of the data subject. The management of the mandatory information provided during registration starts with registration and it is canceled upon request.

The provided personal data may be deleted at any time after the deletion request has been sent. Upon receipt of the request, the Personal Data will be deleted from the system by the Foundation within 5 (five) business days.

The above provisions do not affect the fulfillment of statutory retention obligations, as well as the management of Data on the basis of additional contributions made during registration on the website or otherwise.

In order to apply for the Szarvas Camp, those concerned must complete a registration form which must include the following information:
a) personal data (family and forename (s), place and date of birth, mother's birth name, nationality, address, passport information);
(b) data relating to education;
(c) work data;
d) financial data.

The data are primarily available to the Foundation and the Foundation's internal staff and to partner companies contributing to the operation of the Szarvas Camp, but they are not disclosed to third parties.

Internet accesses relating to Szarvas Camp:

- https://szarvas.camp/
- https://www.instagram.com/szarvascamp/
- https://twitter.com/szarvascamp
- https://www.facebook.com/Szarvas-Intl-Jewish-Youth-Camp-111136492237001/

purpose of the data management	GDPR Article 6 Section (1) points a. and b. (contribution of the data subject, performance of the contract)
categories of the data subjects	Jewish related candidates from 7 to 18 years of age, subject to the provisions of Article 8
range of the personal data	Name, date and place of birth, mother's name, address, phone number, e-mail, ID number, health condition, religious affiliation, data of legal representative
data transfer to 3. persons	Yes, listed in annex No. 1.
data transfer to abroad	Yes
period of data preservation	during the participation in the program
security measures	in an electronic way on servers located at Szarvas Camp

2. **Mission program**

The purpose of the mission program is to ensure that the supporters of the Foundation may get to know the operation of the Foundation and the persons they support.

purpose of the data management	GDPR Article 6 Section (1) points a. and b. (contribution of the data subject, performance of the contract)
categories of the data subjects	persons receiving supports
range of the personal data	Name / birth name / place of birth / date of birth / mother's name / permanent address / place of residence / phone number / e-mail address
data transfer to 3. persons	No
data transfer to abroad	No
period of data preservation	2 years
security measures	locked in office cabinet

3. **Mozaik HUB**

Mozaik Hub aims to provide professional and financial support to Jewish community NGOs that contribute to the advancement of Jewish life, the Jewish community and Jewish values. With its activity, Mozaik Hub wants to contribute to the development of a community-based, nonprofit ecosystem with more professional, stable capacity and impact.

Internet accesses relating to Mozaik Hub:

https://www.facebook.com/mozaikhub
https://www.youtube.com/channel/UCWarUAYokOYV6Xs-jpcUUNw
https://www.instagram.com/mozaik_hub/
https://twitter.com/MozaikHub
https://www.linkedin.com/groups/8468710/

Conclusion of grant agreements:

purpose of the data management	GDPR Article 6 Section (1) points a. and b. (contribution of the data subject, performance of the contract)
categories of the data subjects	supported persons
range of the personal data	In case of civil organizations: Name/registered seat /Registration No. / Representative(s) Gazdasági társaság esetén: Name / Company registry No./ registered seat / Tax No. / Representative(s) In case of self-employed contractor: Name / Registration No. / Tax No. / Registered seat In case of individuals: Name / address / Place and date of birth / Mother's name / Tax ID No. / ID Card No.
data transfer to 3. persons	No
data transfer to abroad	Yes
period of data preservation	5 years
security measures	password protected online server

MANAGEMENT OF SUPPORTERS' DATA IN GENERAL

purpose of the data management	GDPR Article 6 Section (1) points a. (contribution of the data subject)
categories of the data subjects	supporters
range of the personal data	name /address / / e-mail / /bank account No.
data transfer to 3. persons	yes
data transfer to abroad	yes
period of data preservation	8 years
security measures	locked in office cabinet, file with password

Management of data of those applying for jobs

Data Controller allows data subjects to apply for a job application it advertises in the way or method in the job application (eg on an electronic or paper basis).
Data Subjects: Any natural person applying for a job application announced by the Data Controller.
Sphere and purpose of data management:

Name	Identifying
Place and date of birth	Identifying
Applied position	Identifying the application
Experiences – former work place and the time spent there	Necessary for the evaluation of the position's occupancy

Education	Necessary for the evaluation of the position's occupancy
Foreign language knowledge	Necessary for the evaluation of the position's occupancy
CV, cover letter	Necessary for the evaluation of the position's occupancy

The purpose of the data management is the application for the job and contacting.
Duration of data management: until the target is reached; or based on the consent of the data subject, until the end of 2 years after the application; or until the deletion request of the data subject.

Registry of the employee's data

The Data Controller is obliged to collect data and transfer data to the national tax and customs authorities and to the social insurance authority on the basis of the legislation in force in the case of establishment of establishing a social security relationship, so employment relationship, simplified employment or agency relationship.
Establishment of a legal relationship is based on voluntary consent, but the provision of data is mandatory under the relevant legislation.

Data subjects: Any natural person who establishes an employment relationship or other legal relationship with the Data Controller for which the Data Controller has a reporting obligation.

The scope of the data managed is the scope of the data specified in the legislation, and the purpose of data management is to fulfill the obligations under the legislation.

The Data Controller records the data for 5 years from the end of the calendar year of the exit of the Employee provided that the scrapping of labor, wage and social security records is prohibited.

The Data Controller provides the employees with a separate data management information sheet about the management of the employees' data, which is attached to this Policy.

Management of children's data: If the data management is necessary in order to preserve or protect the health of a minor child, to hand over the data and to make the statements relating thereto, the legal representative is entitled.

Under Article 8 (1) of the GDPR, the management of personal data relating to information society services provided directly to children is lawful if the child is 16 years of age. In the case of a child under the age of 16, the management of the personal data of children is only lawful if and to the extent that the consent has been given or authorized by the child's parent.

Website Visits and Cookies
According to the Data Management Information available on the Website.

XI. DATA PROCESSING, DATA TRANSMISSION, DISCLOSURE REGISTRY

The data of the Data Processors is listed in Annex No. 2.

In case the Data Controller uses data processor, the following rules must be followed and enforced:

The Data Controller is responsible for the legality of the instructions to the data processor regarding data processing operations. Where processing is to be carried out on behalf of the Data Controller, the Data Controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. The processor shall not engage another processor without prior specific or general written authorisation of the Data Controller. In the case of general written authorisation, the processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Transmission of data is carried out with the consent of the data subject, without prejudice to the interests of the data subject, in full compliance with an adequate IT system, while respecting the purpose, legal basis and principles of data management. The Data Controller shall not forward the personal data of the data subject without his consent, and shall not make it available to a third party, unless required by law.

Data Controller shall fulfill its obligation to keep disclosure records in the scope of transmitting data in a way that it registers the information concerning the data transmission into an excel file serving also as data registry.

XII. DATA SECURTIY

Personal data can only be managed according to the purpose of the given data management. Data Controller ensures data security. For the sake of this it shall take the necessary technical and organizational measures with regard to data files stored by means of IT tools. The Data Controller ensures that the data security rules provided for in the relevant legislation are enforced.

It also ensures the security of the data, takes the technical and organizational measures, and establishes the procedural rules set out in this Policy that are necessary to enforce the applicable laws, data and confidentiality rules.

This means that only employees with access and access codes can access their computer systems (excel files), and the data operations performed in the system can be tracked. Permissions are full for all accessers.

The security level of the data stored on the server is high.
With regard to the saving and storing of the mailing system, Google and Microsoft has permission.

Paper-based data management is done by the Data Controller so that paper-based documents are stored in a lockable cabinet and in case of archiving they are stored in traceable paper boxes in a lockable warehouse.

In particular, the Data Controller, within the scope of its IT security tasks, shall:

a) take measures to protect against unauthorized access, including protection of software and hardware devices, and physical protection (access protection, network protection);
b) take measures to ensure the recovery of data files, including regular backups and separate, secure handling of copies (mirroring, backup);
c) ensure the protection of data files against viruses (virus protection);
d) ensure the physical protection of data files and devices carrying them, including protection against fire damage, water damage, lightning strikes, other elementary damage, and recoverability of damage resulting from such events (archiving, fire protection);
e) ensure that the data managed is accessible to authorized persons (availability);
f) ensure the authenticity and authentication of the data managed (authenticity of data management);
g) ensure that the data integrity can be verified (data integrity);
h) ensure that the data is protected against unauthorized access (data confidentiality).

In the course of the management of the data – especially during the storage, correction, deletion thereof -, the requesting of information by the data subject and the data subject's objection, the Data Controller shall provide the required level of protection.

During the data management the Data Controller shall preserve
a) the confidentiality: it protects information so that it can only be accessed by someone who has the right to do so;
b) the integrity: it protects the accuracy and completeness of the information and management method;
c) Availability: it ensures that when an authorized user needs it, he can actually access the information he needs and have the relevant tools at his disposal.

Data protection breach:

Data Controller registers possible data protection breaches, indicating the connecting facts, effects, and actions to remedy the data protection breach.

The incidental data protection breach:
- shall be reported by the Data Controller without delay within 72 hours of it becomes aware thereof to the National Authority for Data Protection and Freedom of Information, except the data protection breach is unlikely to pose a risk to the rights and freedoms of the natural persons.
- If the data protection breach is likely to pose high risk to the rights and freedoms of the natural persons, the Data Controller shall, without unreasonable delay, inform the data subject of the data protection breach.
- the Data Controller shall keep records of the data protection breaches.

The NAIH Privacy Incident Notification System is available on the following path: https://dbn-online.naih.hu/public/login, or it might be submitted via the forms available on the Authority's website.

In the report on the data protection breach:
- nature of the data protection incident, including, if possible, the categories and approximate number of data subjects involved and the categories and approximate number of data affected by the incident shall be described;

- the name and contact details of the DPO or other contact person providing further information shall be included;
- the likely consequences of the data protection breach shall be explained;
- the measures taken or planned by the controller to remedy the data protection incident, including, where appropriate, measures to mitigate any adverse consequences arising from the data protection incident shall be described.

If the Data Controller can prove, in accordance with the principle of accountability, that the data protection breach is unlikely to pose a risk to the rights and freedoms of natural persons, the notification may be omitted. (For example, a letter sent to the wrong address by the data controller will be returned without being opened, ie unauthorized person could not access it.)

The data subject should not be informed of the data protection breach if

- the Data Controller has implemented appropriate technical and organizational measures and has applied these measures to the data affected by the data protection breach (in particular, measures such as the use of encryption that make the access to personal data by non-authorized persons inexplicable);
- the Data Controller, following the data protection incident, has taken further measures that ensure that the high risk posing to the data subject's rights and freedoms is unlikely to be realized;
- the information would require disproportionate effort. (In such cases, the data subjects shall be informed by means of publicly available information or a similar measure shall be taken to ensure that the data subjects are informed equally efficiently. For example, by way of publishing a press release)

The data protection breach record sheet and the notification sheet are attached to the Policy.

Budapest, 1st April, 2019