

**Privacy Statement of
The Trusteeship of Matthias Church**

REGARDING ITS WEBSITE'S AND MOBILE APPLICATION'S DATA PROCESSING OPERATIONS
RELATED TO THE DATA SUBJECT

The present Privacy Statement (hereinafter referred to as: 'Privacy Statement or Statement') contains all information about the data processing operations of **The Trusteeship of Matthias Church** (hereinafter referred to as: '**Service Provider/data controller**') regarding its website's and mobile application's data processing operations related to the data subjects, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as: **General Data Protection Regulation/GDPR**) and with the Hungarian Act CXII of 2011 on the Right to Informational Self-Determination and on Freedom of Information (hereinafter referred to as '**Privacy Act**') and other relevant legislation on ensuring the protection of personal data.

To maintain the security of your personal data, we will take the necessary and appropriate measures to ensure that while using:

a) on the one hand **our website www.matyas-templom.hu for online information and purchase**, and

b) on the other hand our mobile application "**Mátyás-templom Budapest**" our users, visitors and other data subjects shall be provided with information on the processing of their personal data in a consistent, transparent, comprehensible and easily accessible way and **to facilitate the exercise of your rights as a data subject**.

In the present Privacy Statement we describe the online and on-site data processing operations related only to the usage of our website and our mobile application, as well as we inform you about data processing regarding the Service Provider's presence in social media and the information provided for the data subjects purchasing online tickets on security camera usage at the place of service.

The use or copying of the whole text or the contents of the present Privacy Statement by any third party without the consent of the lawyer who drafted the Statement is prohibited. Service Provider may change the text of the present Statement in accordance with its data management practices.

This Privacy Statement is an annex to the Privacy Regulation (hereinafter referred to as 'Regulation') available at the seat of Service Provider.

Please read the contents of this statement carefully and feel confident to contact us with your questions.

CHAPTER I

DESCRIPTION OF DATA CONTROLLER AND DATA PROCESSORS

Data Controller

The publisher of the present Privacy Statement as the data controller/Service Provider:

The Trusteeship of Matthias Church

Registered seat: 14 Országház Str. Budapest 1014

Tax Number: 18334588-2-41

Represented by: László Süllei

Email address: gondnoksag@matyas-templom.hu

Phone nr.: +36-1 489-0716

Website: www.matyas-templom.hu

Data Processors

The Trusteeship of Matthias Church as Service Provider is considered to be the data controller when managing the personal data of the ones concerned as data subjects. We also use data processors to maintain our website and mobile application, the online and on-site ticket purchase possibilities and to provide our services and perform our activities. Data processors are bound by the obligation of confidentiality with regard to the data obtained. Data processor treats personal data in accordance with the agreement between them and Service Provider to the extent of performing their duties.

Please be advised that, with respect to the data provided through our website and our mobile application, only the following data processor partners listed may see and manage any data provided by the data subject.

Based on the applicable regulations, in order to entrust a data processor, Service Provider does not need to ask for the prior consent of the **person concerned (data subject)**, but you need to be **informed about the process**. Accordingly, **we inform the ones concerned about the contact details of the data processors**, who may handle the given data strictly for the purpose specified by us for the safety of our users and visitors and for faster and more convenient administration during our services.

1. Web hosting partner

We contract with an external partner for web hosting services, who may only have the ability to access and see – but not to further process – the personal data of the natural persons concerned as follows:

Name of the data processor: Xineon-IT Műszaki Szolgáltató Kft.

Registered seat: 3/9. 37. Népfürdő Str. Budapest, 1138

Company Registry number: 01-09-939944

TAX number: 22708342-2-41

Represented by: Szabolcs Kárpáti

Phone number: +36 1 608 0980

Email address: info@xineon-it.hu

Website: www.xineon-it.hu

For more information on our data processor's privacy policy: <https://www.xineon-it.hu/adatkezelesi-tajekoztato/>

Purpose of data processing: proper operation of the website, providing the user and visitor the opportunity to contact us.

Legal basis for the data processing: consent of the data subject.

Time of data processing: until termination of the contract between the data controller and the processor or until the data subject's withdrawal of consent, with regard to the fact that the personal data provided while making contact may only be viewed by the hosting provider, but that data is not stored on the server, it is received directly into the Service Provider's closed system.

Scope of the data processed: data given during online purchases.

2. The data processing partner promoting online payment services on the website and on the mobile application

Name of the data processor: PayPal (Europe) S.à.r.l et Cie, S.C.A.

Registered seat: 22-24 Boulevard Royal L-2449, Luxembourg

Contact: <https://www.paypal.com/lu/smarthelp/home>

Email address: dpo@paypal.com

Website: www.paypal.com

For more information on our data processor's privacy policy:

<https://www.paypal.com/hu/webapps/mpp/ua/privacy-full#14>

Purpose of data processing: to ensure the operation of the online ticket purchase service and in-app ticket purchase, and secure purchase of the desired product via secure electronic payment.

Legal basis for the data processing: consent of the data subject, fulfillment of legal obligations.

Time of data processing: The data processor manages the data for the purpose of providing the service, so until such time, the data processor manages the data entrusted to them until the end of the contract period between them and Service Provider. It differs from this only if it is necessary for other

purposes to further process the data, such as: Fulfillment of legal obligation: Billing, accounting; Customer Complaint Management; Prevention of money laundering and terrorist financing. In these cases, you can find out the exact time of data processing from our data processing partner's privacy policy, or by contacting them at the given contact or email address.

Scope of the data processed: Data they receive from a data controller as a Service Provider in order to complete your payment and give you the information related to it: Purchase data (purchase amount, detailed cart content). Information (name, e-mail) required for making a wire transfer payment. Data generated by credit card and wire payment transactions: Transaction data (payment transaction identifiers, date, content).

3. The data processing partner providing billing services

Name of the data processor: Billingo – Octonull Kft.

Registered seat: 6. floor I. 74. József krt. Budapest, 1085

Postal address: 5. Jókai Str. Balatonfüred 8230

Company Registry number: 01-09-1981177

TAX number: 25073364-2-42

Represented by: Albert Sárospataki

DPO: Anita Bartal

Phone number: 06 70 904 8287

Email address: hello@billingo.hu

Website: www.billingo.hu

For more information on our data processor's privacy policy: <https://www.billingo.hu/adatkezelesi-tajekoztato>

Purpose of data processing: Billingo is provided with the data required for the invoice to be issued to the data subject, which is stored by the data processor in an online system and issues an invoice on behalf of the data controller with the parameters specified by the data controller.

Legal basis for the data processing: with the use of the service, the data subject gives his or her consent to process the transmitted data to the extent and for the time necessary for the performance of the service.

Time of data processing: until termination of the contract between the data controller and the data processor or until the withdrawal of the consent of the data subject.

Scope of the data processed: the name, address, billing data of the data subject and items of the bill.

4. The data processing partner operating the security camera system

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and the Act CXXXIII of 2005 (Property Protection Act) an electronic surveillance system is in place in the private area.

Name of the data processor: Hegedűs Zoltán e.v.

Registered seat: 5 Guruló köz, Budapest 1112

Registry number: 55163925

TAX number: 56510588-143

Purpose of data processing: safety of life and property, as well as detection of violations of law, crimes, identifying the perpetrator, prevention of violations and their proof.

Legal basis for the data processing: data processing based on a legitimate interest of the controller (Point f) Paragraph 1 Article 6 of GDPR GDPR)

Time of data processing: authorized by the law, the image and sound recording may be stored for up to 3 business days from the date of recording, and thereafter shall be immediately destroyed, unless it is required to be further used (eg. as proof or forwarded to authorities).

Scope of the data processed: an image of a person entering and staying in the area monitored by the electronic surveillance system capable of recording images within the area of competence of the camera, the inference from movement and behavior.

Place and safety of data storage: It is stored on a server at the seat of Matthias Church, the security of which is governed by the internal regulations in force at any given time.

5. The data processing partner operating the newsletter service

Name of the data processor: ActiveCampaign, LLC.

Registered seat: 1 North Dearborn Street, 5th floor Chicago, IL 60602

Email address: info@activecampaign.com

Website: <https://www.activecampaign.com>

For more information on our data processor's privacy policy:
<https://www.activecampaign.com/legal/privacy-policy>

Purpose of data processing: briefings, offers and information provided to the data subject.

Legal basis for the data processing: consent of the data subject. The Service Provider provides the data of the data subjects who have consented to the Service Provider to send newsletters to them during the registration, customer search or purchase.

Time of data processing: until the termination of the contract between the controller and the processor or until the withdrawal of the consent of the data subject.

Scope of the data processed: email address of the data subject.

CHAPTER II

DEFINITIONS

For the purposes of the present Privacy Statement, in accordance with Article 4 of the GDPR Regulation:

1. *'personal data'* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. *'processing'* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. *'restriction of processing'* means the marking of stored personal data with the aim of limiting their processing in the future;

4. *'profiling'* means any form of automated processing 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;

5. *'pseudonymisation'* means the processing 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;

6. *'controller'* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

7. *'processor'* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

8. *'recipient'* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

9. *'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 authorised to process personal data;

10. *'consent of the data subject'* means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

11. *'personal data breach'* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

12. *'consent'* means a voluntary and explicit expression of the wish of a data subject, based on appropriate information, and giving his or her unambiguous consent to the processing of personal data

concerning him or her, either wholly or in part;

13. *'protest'*: a statement by the data subject that he or she objects to the processing of his personal data and requests the termination of the data processing or the deletion of the data processed.

14. *'data processing'* means performing technical tasks related to the data processing operations, irrespective of the method or device used to perform the operations and wherever they are carried out, provided that the technical task is performed on the data.

15. *'transfer of data'* means forwarding the data to a specific third party.

16. *'disclosure'*: making available the data to the public.

17. *'deletion of data'* means the process of rendering data unrecognizable in such a way that it is no longer possible to recover it.

18. *'sets of personal data'* means the total amount of data processed in a register.

CHAPTER III

PRINCIPLES

We handle the processing of personal data of those concerned, in accordance with Article 5 of the GDPR Regulation, taking into account the following principles:

1. Principle of legality, fairness and transparency: we process personal data in a lawful, fair and transparent manner in relation to the data subject;

2. Principle of purpose limitation: personal data is collected for a specific, explicit and legitimate purpose and is not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Principle of data minimisation: personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; Regarding this principle, we do not ask for personal data, that is not necessary for proceeding our services.

4. Principle of accuracy: personal data must be accurate and, where necessary, kept up to date; We make every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. If you as a data subject consider, that one or more personal data of yours was given or was indicated by us inaccurately, we would kindly like to ask you to let us know through an e-mail sent to gondnoksag@matyas-templom.hu, so that we can correct it.

5. Principle of storage limitation: personal data shall be kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the GDPR Regulation subject to implementation of the appropriate technical and organisational measures required by the GDPR Regulation in order to safeguard the rights and freedoms of the data subject. To this end, we take into account that personal data provided by the data subject will be stored only for the time necessary, depending on the time of provision of the service, on legal requirements and on the data subject's consent, meaning that different time periods may be required for each of our data management activities.

6. Principle of integrity and confidentiality: we process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7. Principle of accountability: As a liable data controller, Service Provider is responsible for acting upon principles listed in 1-6. and is prepared to demonstrate compliance.

CHAPTER IV

LAWFUL TREATMENT OF THE DATA SUBJECT'S PERSONAL DATA

1. [Data process operation with the consent of the data subject]

(1) On our website, when purchasing tickets and using our mobile application, registration and in-app purchases the personal data described in Chapter V of the present Statement will be processed based on the consent of the data subject. In case of data processing based on consent, the consent of the data subject to the processing of personal data shall be requested by us prior to the start of data processing. If data processing serves multiple purposes at the same time, the consent must be given for all data processing purposes. These objectives are set out in Chapter V of the present Statement. By accessing the present Privacy Statement if you use the website or the mobile application, you consent to the use of this Privacy Statement by ticking the appropriate box.

(2) We would like to inform you about our obligation, that where the consent of the data subject is given by means of a written declaration covering other matters as well, the request for consent shall be clearly distinguished from those other matters in a clear and easily accessible form, in a simple language, and shall not contain unfair terms. Any part of the statement containing the consent of the data subject that does not meet the requirements of the law is not binding.

(3) We would also like to inform you, that in order for the data subject's consent to be based on the information given by us, the data subject must at least be aware of the identity of the controller (Service Provider) and the purpose of the processing of personal data. Giving consent is not considered to be voluntary if the person concerned does not have a real or free choice and is unable to deny or withdraw consent without it causing any damage to him or her. The data of the Service Provider can be found in Chapter I of the present Statement, while the purpose of data process is stated in Chapter V.

(4) Data process is considered to be lawful if it is required in the context of a contract or at an intention to conclude a contract. Service Provider shall not set up a condition for entering into a contract by requesting personal data that is not necessary for the performance of the contract. If we enter into a service contract with you, we may need to request additional personal data in order to prepare the contract, which will be the subject of separate communication. If the contract is not concluded, the data provided through that separate communication will be deleted from our system.

(5) The possibility of withdrawing consent shall be made available to the data subject in an understandable, easily accessible form, in a clear and simple manner and shall not contain unfair terms. **Please be advised that if you wish to withdraw your consent, you may do so by sending an email** to gondnoksag@matyas-templom.hu. In case of withdrawal, we will immediately delete the data and inform the data subject in a reply email. If the fulfillment of our legal obligation or contractual obligation (eg. provision of a service, invoice, fulfillment of accounting obligation) requires further processing of certain data, we will inform you in a reply email.

(6) If personal data has been given with the consent of the data subject, we may process the given data without further specific consent and after the withdrawal of the consent of the data subject for the fulfillment of our legal obligation unless otherwise provided by law.

(7) The consent should be voluntary, meaning it is free from all external influences and can possibly serve as a legal basis if there is a real choice for You, as the data subject and there is no risk of deception, intimidation, coercion or other significant negative consequences in the event of denial of consent. In the absence of a voluntary decision, we would not have the appropriate legal basis for data processing. Without question, we always base your consent on your voluntary decision regarding our consent-based data processing activities, providing you with an uninfluenced choice.

(8) Given that there is a possibility that a minor under the age of 16 may inquire, purchase a ticket through the website, or use our mobile app, we consider it important to note the following: one specific matter of the legal basis for consent is Article 8 of the GDPR Regulation, which requires the consent of the parent for the lawfulness of data processing involving minors under 16 years of age. In the case of a child under the age of 16, the processing of children's personal data is only lawful if and to the extent that the consent has been given or authorized by the parent exercising parental authority over the child. Parental guardians are kindly requested to inform us immediately if they become aware that they have not given their consent or authorization to the processing of personal data of a child under the age of 16, being under parental supervision. By informing us, we can take the necessary steps to delete the personal data provided.

2. [Our obligation on providing information]

We keep the present Privacy Statement available to those concerned in an easily accessible way on our website and at our seat. The Statement informs the data subject in a publicly accessible manner, before and during the processing of the data, of all facts related to the management of their data, including the purpose and legal basis of the data process, the person entitled to data processing, the duration of the data process, about the fact if the personal data of the data subject is processed according to the data subject's consent (Section 5 Article 6 of the Privacy Act) and regarding who is entitled to know the data. **Our provision of information also covers the rights and remedies of the data subject concerned, that you may find in Chapter IX., X. and XI. of the present Statement.**

3. [Data process operation based on the fulfillment of a legal obligation]

Data process operation based on the fulfillment of a legal obligation is independent from the consent of the data subject. Before starting the data process we must inform the data subject, that the process of data is based on a legal obligation. In such case we inform the data subject in a clear and detailed way before the beginning of the data process operation about all facts related to the process of his or her data, especially the purpose and legal basis of the data process, the person entitled to data processing, the duration of the data process, about the fact that the personal data is processed according to a legal obligation and regarding who is entitled to know the data. The information provided by us also covers the rights and remedies of the data subject concerned. In case of mandatory data process, the information may also be given by disclosing a reference to the provisions of the legal obligation that contains the necessary information covered by this paragraph.

4. [Data process operation based on a legitimate interest]

Personal data may be processed if the data processing is necessary for the purpose of enforcing the legitimate interest of the Service Provider, exceptionally a third party, unless the right to the protection of the personal data of the data subject and the respect of his or her privacy represents a higher value than that legitimate interest. Such legitimate interest may make the data processing lawful, regardless of the consent of the data subject if the legitimate interest only restricts the right and privacy of the data subject to the extent necessary and proportionate. In the case of such interest-based data process, the principle of graduality and, if possible, the presence of the data subject shall be ensured. As data controller, we must conduct a written legitimate interest test for the lawfulness of data processing based on our legitimate interest and inform those concerned in an easily accessible way. Currently, as a Service Provider, our only legitimate interest-based data management is the operation of our security camera system, for which Service Provider retains the legitimate interest test performed at Service Provider's headquarters. In the event of further interest-based data processing, we will supplement the present Statement with this information.

CHAPTER V

DATA PROCESS OPERATIONS ON OUR WEBSITE AND SOCIAL MEDIA PLATFORMS

1. Contacting us

(1) A natural person initiating contact by email or telephone request may voluntarily provide the Service Provider with the following information when contacting the Service Provider. Service Provider stores it only with the express request and consent of the data subject:

1. name (surname, first name);
2. telephone number;
3. email address;
4. any other personal data provided by the data subject voluntarily as a content of his or her message.

(2) **The purpose of processing the personal data:** providing information about our services, establishing contact between the natural person and us as Service Provider. Providing personalized client service and offer if required.

(3) **The legal basis for data process** is the consent of the data subject. In the case of telephone or e-mail communications, you may give your consent to the management of your personal information when communicating with Service Provider. If you wish to withdraw your consent, you can do so by sending us an email with your request to gondnoksag@matyas-templom.hu. If there is no obligation to further process the data due to our legal obligation or our contractual data management activities under Section (5), we will promptly delete the data and will inform you in a reply email.

(4) **The recipient of the personal data** described in Section (2) is solely Service Provider. When a person contacts the Service Provider, the data transmitted is not visible to the data processor or other third party and the data is not stored in the storage space. The data is sent directly to gondnoksag@matyas-templom.hu email account managed exclusively by the Service Provider. In the case of communication by telephone or direct personal inquiry, if data are required, the Service Provider shall enter them into its own closed system.

(5) **The duration of personal data storage** shall last until 3 years after contacting us, but the latest until the consent of the data subject is withdrawn (until a request on deleting the data is submitted by the data subject). If the data subject concludes a contract with the Service Provider after the hereby described way of contacting us, then further data management is governed by our contractual data management terms.

2. Information on the cookie policy of our website

(1) Cookies collecting statistical data: These cookies only collect statistical data, so they do not process personal data. During their operation, they observe how you use the website, which topics you look at, what you click on, how you scroll the website, which pages you visit. However, the information is only collected anonymously. For example, you can find out how many visitors we have on the website per month. Additionally, these statistics help us adjust our site to user needs. Google Analytics helps us in gathering such data. You can find more information on Google Analytics' data process activities here:

<https://support.google.com/analytics/answer/6004245?hl=en>

3. Personal information provided during registration in the mobile application

(1) With the consent of the data subject, we will manage the email address of the registered users of the mobile application for the purpose of registering and managing the user account for the provision of the service.

(2) **Purpose of the processing of personal data:** To facilitate and secure the purchase of tickets. Ensuring full use of the features of the mobile application and also providing a convenient, fast – QR code based – entering to the Matthias Church Visitor Center, and to enhance the visitor experience.

(3) **The legal basis of the processing of the data** shall be the consent of the data subject. The data subject may indicate his or her consent to the processing of his or her personal data by ticking the appropriate box. The present Statement is accessible via a link posted there when downloading the mobile application. This application requires you to read and accept the present Statement. If you wish to withdraw your consent and thus wish to cancel your registration, you can do so by sending an email to gondnoksag@matyas-templom.hu and you also need to delete your account in the mobile application. In order to delete the data, we will immediately contact our mobile-application developing partner and delete the data, and will inform the data subject in a reply email. If due to the fulfillment of our legal obligation or contractual obligation (eg fulfillment of an order (purchase of tickets), issuing of an invoice) further processing of certain data is necessary, we will inform you in a reply email.

(4) **The personal data referred to in paragraph (1) shall be addressed** to the Service Provider and the data processing partner operating the mobile application. According to this, when the person concerned registers on our mobile application, the data transmitted to us will be seen by this data processing partner in addition to us.

(5) **The period of storage of personal data** shall be valid until the registration, but not later than the mandatory retention period prescribed by law or the withdrawal of the consent of the data subject (request for deletion). Please note that if you made an online purchase through our mobile application, the period of data storage for the purpose of providing the service will be as set out in section 4 below.

4. Personal information provided when purchasing tickets online (website) and in the mobile application or when purchasing products in our webshop

(1) **Purpose of data management:** based on the consent of the data subject and the conclusion of a contract, in case to conclude, perform, terminate a contract, to grant discount, to purchase tickets, to issue invoice we process the following personal data required for the online service from our registered and non-registered users who contracted us for the purpose of ticket purchase (**scope of data processed:**)

1. surname and forename,
2. email address,
3. billing address,
4. payment data,
5. upon shipping, the data subject's shipping address.

(2) Such data processing shall also be considered lawful where it is necessary to take steps at the request of the data subject prior to the conclusion of the contract. **The personal data will be addressed to the Service Provider, our employees and our data processing partners for online shopping, billing and ticket delivery.** With the exception of the payment data contained in paragraph (3), the period of storage of personal data shall be the period specified in the prevailing applicable law, in the absence thereof, and accordingly 5 years after the termination of the contract and thereafter shall be deleted.

(3) **Payment data processing:** For the purpose of concluding, executing, terminating, providing a contract, granting discount, and issuing an invoice for the purpose of performing a contract, we will process the payment data necessary (payment method, cardholder name, credit card details) of the individual. Such data processing shall be considered lawful even if such processing is necessary to take action at the request of the data subject prior to the conclusion of the contract.

The scope of the data processed: payment method, cardholder name (card name), card number, expiration date.

Legal basis for data management: based on the legal title of the contract. The information may also be provided in the contract. The provision of the data is a condition for the provision of the contracted service.

Recipient of the data: The recipient of the personal data is the data processing partner of the Service Provider that makes and facilitates online shopping, billing and shipping procedures. The data subject may pay the fee for the service by credit card or bank transfer. The recipient of the payment data being the data processor contracted with the Service Provider for the execution of payment services. The Service Provider does not see payment data, we only receive a code that is linked to the payment through the data processor but is not traceable to the natural person. The payment processor shall have the necessary security and IT measures and systems in place to ensure the secure handling of payment data. If required in the event of a temporary disruption or other failure of the payment service system, - if online payment can be secured - the Service Provider shall keep the payment data encrypted.

Duration of data storage: Credit card data will be encrypted and disclosed only for the purpose of the transaction and only by authorized persons. Once the service has been completed, the data will no longer be disclosed or accessed. Data will be deleted after 8 years.

5. Information on the interactive feature installed in the mobile application

(1) Please be advised that our mobile application provides an active, logged in visitor - user - during a visit to the Matthias Church Visitor Center special entertainment features (hereinafter referred to as "Features") when entering the area of a specific attraction, landmark. Our mobile app thus provides those features on the user's mobile device immediately upon entering that location by detecting the mobile device's location through sensors. Please be advised that this function of the mobile application works in an anonymous way, the person concerned cannot be traced back to the visitor, so the location of the person concerned is not followed and our system does not store any data or conclusions about it. Please also be advised that the device through which the physical data is tracked for this feature to work is encrypted. The feature works automatically as it activates the content upon entering the located area, so no additional action by the user (e.g. reading a QR code on your device) is required. For further information regarding the function of this feature and its non-personal nature, please feel free to contact us by sending an email to gondnoksag@matyas-templom.hu.

(2) Please be advised that this feature of the mobile application allows us to retrieve statistics on the visibility of individual attractions and landmarks, which statistics are not based on personal data or on the location of the visitors concerned or any other personal data. It is provided solely by the technical design

of each area.

6. Data process operation on our social media platforms

- (1) We would like to inform You, that we maintain the '**Mátyás-templom/ Matthias Church/ Budavári Nagyboldogasszony Főplébánia**' Facebook and the '**matthiaschurchofficial - Matthias Church**' Instagram and account (hereinafter collectively referred to as: social media platforms).
- (2) Complaints submitted to Service Provider through our social media platforms are not considered to be formally submitted.
- (3) Personal data published by visitors on the social media platforms of ours are not processed by us.
- (4) Visitors are subject to the Privacy and Service Terms of the social media platforms.
- (5) In case of an unlawful or offensive content posted on our social media platforms, we may exclude the person from the site without notice and may delete his or her comment.
- (6) We are not responsible for any unlawful data content or comments published by our social media platform users. We are not responsible for any problems that may result from malfunctioning of the social media platforms, causing a breach in personal data protection.
- (7) Service provider shall be entitled to publish images or videos on the social media platforms of the data subject solely with the given consent of the data subject, excluding the category of mass recordings.
- (8) The provisions in this section also apply to any of our future social media platforms of ours.

7. Information on safety camera surveillance system

(1) In the area of Service Provider, at venues opened for our visitors we use electronic monitoring systems for the protection of human life, bodily integrity, personal freedom, business secrecy and property protection, which allows the recording of images. Through this, the conduct of the person concerned that the camera records is also considered as personal data. By entering the area, the cameras may record your behavior as well.

(2) The legal basis for data processing is the legitimate interests of Service Provider and the consent of the data subject.

(3) We are obliged to place a warning sign, information on the location of the electronic monitoring system in a clearly visible place, in order to inform third parties wishing to appear in the area. Such a sign or information should be provided for each camera. This information includes the fact that electronic monitoring system is being used, the purpose of recording and storing the data and its duration, the person applying the system, the storage location of the record containing the personal data and about the rights of the persons concerned.

(4) Recording the persons entering the observed area may be made and handled with their consent. The consent may also be given by an implied consent, in particular if the natural person entering the observed area enters the area despite the indication of the use of an electronic surveillance system at its entrance.

(5) Recordings may be kept for up to 3 (three) business days, if not used, then shall be deleted. It is considered to be a use if the recorded image and other personal data are to be used as evidence in court or other official procedures.

(6) Anyone whose right or legitimate interest affects the recording of the data may, within 3 (three) business days from the date of recording, request the data controller not to destroy or delete the data.

(7) It is not possible to use a camera surveillance system in an area where observation may violate human dignity, especially in toilets. The camera's position should not be directed specifically at the surveillance of the data subject. The fact that the camera's overall angle of view includes the area in which the person concerned carries out its activities does not constitute an explicit observation of the data subject if it is proportionate and justified to the data subject [eg. reception desk/ specific attraction or landmark, where the recording is not specifically, exclusively and unambiguously aimed at monitoring the person concerned, but with the area observed from the security point of view these places are also in the picture at a proportional and a reasonable extent].

(8) If no one can legally stay at the area of the Service Provider and the visitor center – especially outside the operating hours – then the entire area of the workplace can be observed.

(9) In addition to those authorized by the law, the staff of the surveillance system, our manager and deputy manager, the employee supervisor of the area monitored are authorized to view the data recorded by the camera system for the purpose of detecting violations and monitoring the operation of the system.

(10) **We would sincerely like to ask you to please do not enter the area of our visitor center and please be aware of this fact prior purchasing you ticket, if you are not willing to give consent to record your image as set above**, as we are not responsible for your failed visit for this reason as a Service Provider.

CHAPTER VI

INFORMATION ON THE RIGHTS AND OBLIGATIONS BETWEEN THE DATA CONTROLLER AND THE DATA PROCESSOR

(1) Data processors listed in the registry of data processing activities shall comply with the technical and organizational measures, including data security, to ensure compliance with the requirements of the GDPR Regulation, in particular in terms of expertise, reliability and resources.

(2) Data processors shall be bound by the obligation of confidentiality with regard to data made available to them by the Service Provider.

(3) In the course of its activities, the data processor shall ensure that persons authorized to have access

to the personal data concerned, unless they are already under the obligation of confidentiality by an appropriate legal obligation, undertake to observe confidentiality with regard to the personal data which they become aware of.

(4) The data processor must have appropriate hardware and software tools and must implement technical and organizational measures suitable for ensuring the lawfulness of data processing and the protection of the rights of data subjects.

(5) The Service Provider as a data controller shall enter into a written contract with the data processor for the data processing activity, which shall include the data processing rights and obligations.

(6) The Service Provider, as a data controller, has the right to monitor the data processor's performance of the contract referred to in paragraph (5).

CHAPTER VII

DATA SECURITY MEASURES

1. [Data security measures]

(1) For the purposes of personal data security, we are obliged to take all technical and organizational measures and establish the procedural rules necessary to ensure data protection regarding any of our data management activities.

(2) We protect the data by appropriate measures against accidental or unlawful destruction, loss, alteration, injury, unauthorized disclosure or unauthorized access to it.

(3) We classify and manage personal data as confidential.

(4) With regard to the data arriving through our website, electronic data processing and record keeping is carried out by means of a computerized information system that meets the requirements of data security.

(5) If the data of the natural persons concerned are handled by a paper-based document suitable for our data processing operations, they must be managed and kept at the premises of our seat and office, in accordance with the provisions of the Regulations and the present Privacy Statement (legal basis, scope of processed data, retention period).

(6) We ensure the control of incoming and outgoing electronic communications for the protection of personal data.

(7) Only we have access to documents that are in progress and undergoing data processing, and those are kept securely closed.

(8) We ensure appropriate physical protection of the data and the means and documents carrying them.

CHAPTER VIII

MANAGEMENT OF PERSONAL DATA BREACH

1. [Concept of personal data breach]

(1) A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (Article 4 of GDPR Regulation 12)

(2) The most common reported breaches may include: loss of laptop or mobile phone, unsafe storage of personal data; unsafe transfer of data, unauthorized copying, forwarding of clients, guest, customer, partner lists, attacks against the server, breaking the website.

2. [Managing and remedy of personal data breach]

(1) Prevention, management of personal data breach, compliance with applicable legal requirements is our responsibility as Service Provider.

(2) If our IT data processor partner notices a breach in the course of performing their duties, they shall observe the personal data breach and notify us immediately. Access and access attempts must be registered in the IT systems and analyzed continuously.

(3) Personal data breaches can be reported at our central e-mail address (gondnoksag@matyas-templom.hu), telephone number, so visitors, clients, contractors, partners and others considered can report the underlying signs or events and security weaknesses.

(4) In the event of a personal data breach being reported, we will immediately examine the notification, identify the breach and decide whether it is a real breach or a false call. The following should be examined and established:

- a) the date and place of the event (breach);
- b) description, circumstances and effects of the event (breach),
- c) the range and number of data compromised during the breach;
- d) the scope of persons affected by the compromised data;
- e) the description of the measures taken to prevent the breach;
- f) the description of the measures taken to prevent, remedy and reduce the damage.

(5) In the event of a personal data breach, the affected systems, persons, data must be delimited and separated, and the evidence supporting the incident must be collected and preserved. It is then possible to start repairing the damage and restoring the lawful operation.

3. [Register of personal data breach]

1. A record of personal data breach shall be kept, including:

- a) the scope of the personal data concerned;

- b) the scope and number of data subjects affected by the personal data breach;
- c) the date of the personal data breach;
- d) the circumstances and effects of the personal data breach;
- e) the steps taken to remedy the personal data breach;
- f) other data specified in the law regarding the relevant data processing operation.

(2) We retain data relating to personal data breach in the register for 5 years.

4. [Reporting personal data breach to the authority]

Data breaches that are likely to endanger the rights and freedoms of natural persons shall be reported by us to the competent supervisory authority, the National Data Protection and Freedom of Information Authority (NAIH) pursuant to Article 33 (1) of the GDPR. The GDPR requires the controller to notify the NAIH of the incident without undue delay and, if possible, no later than 72 hours after becoming aware of the breach. Our notification shall be made electronically or on paper through the NAIH Data Breach Reporting System. (<https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html>)

CHAPTER IX

RIGHTS, LEGAL REMEDIES OF THE RELATED PERSON

Below, we inform the data subject about the rights and remedies available to the natural person concerned with regard to the protection of personal data. **The submission and processing of the request of the data subject are governed by the provisions of Chapter XI.**

1. [The right to preliminary information and the right of access by the data subject]

The data subject is entitled to be informed of facts and information related to data process operations prior to the commencement of these operations. Please contact gondnoksag@matyas-templom.hu for information. If requested, we will provide you with the requested information without undue delay, but no more than one month, stating whether your personal data are being processed and, if so, you have the right to know what personal data are being processed, on what legal basis, for what purpose, for what period of time; and to whom, when, under what law and which personal data of yours we provide access to; to whom we transmit your personal data; the source of our access to your data; whether we use automated decision-making and, if so, its logic, and in the case of pursuing profiling, we also inform you.

You may request a copy of your personal data, which will be provided for the first time free of charge, after which you may be charged a reasonable fee based on administrative costs. Please note that in order to meet our data security requirements, we have the right to verify your identity when requesting and making copies.

The data subject has the right to receive feedback from the data controller on whether personal data are being processed and, if such processing is in progress, the data subject shall have access to personal data and related information as defined in the GDPR Regulation. (Article 15 of GDPR Regulation).

2. [The right to rectification]

Upon request, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. If the data subject credibly verifies the accuracy of the corrected data, we will comply with the request within a maximum of one month and will inform the

data subject accordingly.

3. [The right to erasure ('the right to be forgotten')]

Upon request, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay if one of the grounds set out in the GDPR Regulation applies. (Article 17 of GDPR Regulation) Where the data processed are necessary for law enforcement purposes or, for example, for settlement with a public authority, the data processing may be carried out on the basis of a legal obligation or a legitimate interest. Upon deletion, the data controller shall also notify the data processors involved of the deletion obligation.

The data controller shall delete the personal data relating to the data subject without undue delay if any of the following grounds applies:

- a) personal data are no longer required for the purpose for which they were collected or otherwise processed;
- b) the storage period set by the controller has expired;
- c) the data subject has withdrawn his or her consent as the basis for the processing and there is no other legal basis for the processing;
- d) the data subject objects to the processing and there is no legitimate reason for the processing;
- e) the personal data have been unlawfully processed;
- f) personal data must be deleted in order to comply with a legal obligation under Union or national law applicable to the data controller;
- g) personal data have been collected in connection with the provision of information society services.

4. [Right to restriction of processing]

Upon request, the data subject shall have the right to obtain from the controller – through our contact information described in point 1. – the restriction of processing if the following conditions specified in the GDPR Regulation are met:

- a. contest the accuracy of your personal information (limited to the time of our review);
- b. the processing is unlawful and the data subject opposes the erasure of the data and instead requests that their use be restricted;
- c. the data controller no longer needs personal data for the purpose of processing, but the data subject requires them to assert or defend a legal claim; or
- d. the data subject has objected to the data processing (we restricted to the time during which the legitimate interest of the data controller is established).

5. [Notification obligation regarding rectification or erasure of personal data or restriction of processing]

We shall communicate and inform upon any rectification or erasure of personal data or restriction of processing carried out all recipient to whom or with whom the personal data have been disclosed, unless this proves impossible or requires a disproportionate effort. At the request of the data subject, the we shall inform the data subject about those recipients. (Article 19 of GDPR Regulation)

6. [The right to data portability]

By applying the conditions set out in the GDPR Regulation, data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. (Article 20 of GDPR Regulation)

7. [The right to object]

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1) (data processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; the legitimate interests of the controller or by a third party, with exceptions) (Article 21 of GDPR Regulation) In the event of an objection, the data controller may not further process the personal data except for a legitimate reason which prevails over the interests of the data subject or is necessary for the establishment, exercise or defense of legal claims.

8. [Automated individual decision-making, including profiling]

We do not use or perform profiling, automated decision making or automated mechanisms. We do not allow our data processors to make automated decision making or profiling, except with the express written consent of the data subject. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (Article 22 of GDPR Regulation)

9. [Restrictions]

Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22. (Article 23 of GDPR Regulation) In the event of a restriction, personal data may only be stored. Further data processing may only be conducted with the data subject's consent, for the purposes of legal proceedings or the public interest.

10. [Informing the data subject of a personal data breach]

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we shall communicate the personal data breach to the data subject without undue delay. (Article 34 of GDPR Regulation)

CHAPTER X

The Data Subject's Right of Appeal

1. [Right to lodge a complaint with the supervisory authority]

The data subject has the right to lodge a complaint to the supervisory authority if the data subject considers that the processing of personal data concerning him or her violates the GDPR Regulation. (Article 77 of GDPR Regulation)

2. [Right to an effective judicial remedy against the supervisory authority]

Each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of the supervisory authority concerning them, or if the supervisory authority does not handle the complaint or does not inform the person concerned of the progress or the outcome of the complaint within three months. (Article 78 of GDPR Regulation)

3. [Right to an effective judicial remedy against the controller or the processor]

Each data subject shall have the right to an effective judicial remedy if he or she considers that his or her rights under the GDPR Regulation have been infringed as a result of the processing of his or her personal

data in non-compliance with the GDPR Regulation. (Article 79 of GDPR Regulation) If you believe that your personal data has been processed in violation of applicable data protection requirements, you may lodge a complaint with the supervisory authority – see section Chapter X Point 2 for contact details. You also have the right to initiate court procedure, that shall proceed out of turn. In this second case, you are free to choose whether to file your claim with the competent regional court of your place of residence (domicile) or place of temporary residence (temporary address) or of the Service Provider's seat. You can search for the regional court of your place of residence at <https://birosag.hu/birosag-kereso>. According to the Service Provider's seat, the Budapest-Capital Regional Court has jurisdiction.

CHAPTER XI

SUBMISSION OF THE DATA SUBJECT'S APPLICATION OF REQUEST AND THE MEASURES TAKEN BY US AS DATA CONTROLLER

1. [Measures based on the request of the data subject]

(1) In the cases covered by the present Privacy Statement, the data subject may primarily submit his or her request by email to gondnoksag@matyas-templom.hu. As data controller we shall inform the data subject of the measures taken on his or her request for the exercise of his or her rights without undue delay, but no later than one month after application of the request. If for any reason we are unaware of the submission of the request, we are obliged to act promptly and without any delay along with informing the data subject.

(2) Where necessary, taking into account the complexity of the application and the number of applications, this deadline may be extended by a further two months. We shall inform the data subject of the extension of the deadline by indicating the reasons for the delay within one month of receiving the application of request.

(3) If the data subject submitted the application by electronic means, the information shall, as far as possible, be provided by electronic means, unless otherwise requested by the data subject.

(4) If we do not take any measures following the request by the data subject, we must inform the data subject without any delay, but at the latest within one month from receiving the application of the request, of the reasons for the non-execution of the measure and also about the data subject's right to lodge a complaint with the supervisory authority and his or her right to appeal at court.

(5) We provide the information set out in Articles 13 and 14 of the GDPR Regulation and the information on the rights of the data subject (Articles 15 to 22 and 34 of the GDPR Regulation) free of charge. If the data subject's application of request is unfounded without any doubt or is highly exaggerated, in particular because of its repetitive nature, we may charge fee calculated based on the administrative costs of providing for the requested information or refuse to take measures. It is us who bear the burden of proving that the application of request is unfounded highly exaggerated.

(6) If we have reasonable doubts as to the identity of the natural person submitting the request, we may request further information necessary to confirm the identity of the person concerned.

2. Contact details of the supervisory authority:

Hungarian National Authority for Data Protection and Freedom of Information

<http://naih.hu>

Address: 9-11. Falk Miksa Street Budapest, 1055

Postal address: 1363 Budapest, Pf .: 9.

Email: ugyfelszolgalat@naih.hu

Phone number: +36 (1) 391-1400