Privacy Policy

1. Identification of controller

We inform you that the website https://embrighter.com/ is run by

BRODEX Hímző és Hímzőgép Programkészítő Kereskedelmi és Szolgáltató Betéti Társaság
(BRODEX Embroidery and Embroidery Machine Design Digitizing Commercial and Service Limited Partnership)

Short name: BRODEX Bt. (BRODEX LP)
Registration number: 08-06-008294 - Registry Court of Győr (Győri Törvényszék Cégbírósága)
Tax number: 20339762-2-08
Headquarters: 129 Dózsa György Quay, Győr 9026, Hungary (Magyarország, 9026 Győr, Dózsa György rakpart 129.)
Place of business: 129 Dózsa György Quay, Győr 9026, Hungary (Magyarország, 9026 Győr, Dózsa György rakpart 129.)
Telephone: +36 30 4966 933
E-mail address: info@embrighter.com

(Controller hereafter).

2. Legal requirements concerning processing, scope of present policy

2.1. Service of website identified by address above (website hereafter), run by Controller identified above (Controller hereafter), is supplies services from Hungary. In accordance with this, Hungarian and European law applies to service, Users during they are using services (including processing). Controller uses information about Users primarily based on these regulations:

- 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 (General Data Protection Regulation), (GDPR hereafter)
(AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet),

- Regulation CVIII of 2001 on Electronic commercial services and services related to some aspects of information society
(az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.))

- and Regulation XLVIII of 2008 on Basic conditions and some limits of economic advertising activities (és a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (Grt.)).

2.2. Present policy applies to processing done during the usage of the website, drawing on services offered there, as well as fulfilling orders on the website.

2.3. Based on present policy, Users are: natural persons browsing website and drawing on services of website, and natural persons ordering products from Controller.

3. Legal bases of processing

3.1. Legal basis of processing done by Controller lies upon GDPR Article 6, Paragraph (1), Point a) about consent of User to processing, and Article 6, Paragraph 1, Point b) of GDPR, which states that processing is necessary for fulfillment of contracts in which User is one of the parties.

3.2. In case of processing based on given consent, User previously agrees to processing by marking an indicator box above processing agreement placed at relevant places. User can read about processing anytime under “Privacy Policy” appearing at every page of the website, or by clicking on “Privacy Policy” link in processing agreement mentioned in this point, through which Controller provides User in advance with obvious and detailed information. By marking the indicator box above processing agreement, User declares that they have read Privacy Policy and consents to handling their data in accordance with present policy knowing its content.

3.3. In certain cases, Controller is required to do some processing actions, or its rightful interest might be the legal basis to process data. User can read about these in more detailed below, in chapters about each case of processing.

4. Processing related to operation of information technology service

4.1. Controller uses ‘cookies’ to run the website and to collect technical data about the visitors of the website.

4.2. Controller represent a specific reference for visitors of the website: ‘Information about the use of cookies’

5. Processing related to receiving and answering messages

5.1. Concerned parties in processing: Users who have sent messages to Controller by sending an e-mail to Controller using the e-mail address(es) appeared on the webpage.

5.2. Legal basis for processing: User’s consent according to GDPR Article 6, Paragraph

(1), Point a).

User is entitled to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

5.3. Determining the scope of data handled:

The following data of User who sent an e-mail
- name
- e-mail address
- the subject of the message
- other possible data that was given in a message sent by User

Controller handles information concerning received messages from User only content wise, and does not require User to give personal data within. When such non-required information is provided though, they are not stored and Controller deletes them immediately from the information technology system.

5.4. Purpose of processing: to ensure exchange of messages between Controller and User.
Services involved:
- receiving e-mail messages (by using e-mail address(es) on the website),replying to messages sent to Controller the above mentioned ways within 2 working days.

5.5. Duration of processing: until answering a request or accomplishing a claim. Afterwards, Controller deletes data that is handled for these purposes. If there are more exchanges of messages, data are erased after the claim has been accomplished.
If contracting occurs during the process of exchange messages, and content of messages is important with regard to the contract, legal basis and period of processing happens based on Point 8.

5.6. Method of data storage: on separate data managing lists in the information technology system of Controller until the end of information exchange.

6. Processing related to sending newsletters

6.1. Concerned parties in processing are: Users who sign up for newsletters at website by providing personal data through filling up the related form on the website.

6.2. Legal basis of processing: User’s consent based on GDPR Article 6, Paragraph (1), Point a) and User’s consent based on law regulating economic advertising activities § 6, Paragraph (1) and (2). User gives voluntary consent by reading this Privacy Policy and filling up the form about receiving newsletters, clicking on the consenting agreement box there. Either way, User consents to handle their personal data described in Privacy Policy, and to receive newsletters.

Newsletters provide useful information to users, as well as aims **direct sales purposes**.

User can sign up for this service regardless of drawing on other services, and it is voluntary. It is based on User's decision after being informed. In case User does not take the newsletter service, they do not encounter any drawbacks when using website or any other services, it is not a criterion to use any other services at website.

6.3. Scope of data:
- e-mail address.

6.4. Goal of processing: sending newsletters to User by Controller in e-mails about Controller's services, information about the latest products/services and actualities, offers and advertisements.

6.5. Duration of processing: Controller handles information until User's cancellation of consent (User unsubscribes), or until deleting data based on User's request.

6.6. Method of data storage: on separate data managing lists in Controller's information technology system.

7. Processing related to registration

7.1. Scope of parties concerned: Users registering at website.

7.2. Legal basis of processing: based on GDPR Article 6, Paragraph (1), Point a), User's consent. User can give User's voluntary consent by clicking on the icon which has the shape of a schematic human-figure then click on button "Register" or during ordering by clicking on button "Create an account". After these User needs to fill up the data sheet that appears and put a tick into the square in front of data management statement, finally click on button "CREATE".

User is entitled to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

7.3. Scope of handled data: Data asked and answered in the registration form mentioned above.

Scope of data:
- surname,
- first name,
- e-mail address,
- password.

Passwords are stored with encryption codes by Controller's system as a result of which Controller cannot learn User's password.

7.4. Scope of handled data: registration on the web page and as part of it to ensure specific access to contents available there.

Related services to this:

- to create a personal account, to ensure access to it for User
- to make further on-line orders easier, it stores data that is necessary to fulfill the order and to make it possible for Users to modify these data on their own
- to store the details of previous orders and to make available to reach these stored orders in User's account

7.5. Duration of processing: As for registered Users, duration of processing lasts until Users request for data deletion. Processing may finish when User deletes their registration or when Controller deletes User's registration. User may delete their registration anytime, or can ask Controller to do so. Such incoming requests are handled and accomplished immediately, but within no more than 10 working days after the request arrives.

7.6. Method of storing data: on separate processing list within Controller's information technology system.

8. Processing related to orders

8.1. Scope of parties concerned: Users put in an order at website.

8.2. Legal basis of processing: based on GDPR Article 6, Paragraph (1), Point b), according to which processing is necessary to accomplishing contracts where User is one of the parties.

8.3. Scope of data handled: Processing involves personal data and contacts.

Users who are making an order:
- billing name
- billing address
- telephone number
- e-mail address
- indication of the ordered embroidery design(s)
- price of ordered embroidery design(s)
- payment method
- time of order
- time of payment.

In case of online payment, data of bank card used for payment is not revealed to Controller, as User provides payment service provider directly with such data.

8.4. Goal of processing: to make and fulfil contracts realized through orders.

8.5. Duration of processing: in order to fulfil orders, Controller handles information mentioned above until it is prescribed by the Act on Accounting (Számviteli Törvény) about keeping certificates. According to the Act on Accounting (Számviteli Törvény), this period is at least 8 years after making out an invoice, after passing this deadline, Controller deletes data within one year.

Other data possibly processed during ordering – e.g. important messages between User and Controller about orders – are processed by Controller for 5 years after contracting – general term of limitation concerning civil demands. Among those are data on the invoice (name, address, data in connection with the ordered program and with the way its price was paid), and also in some cases further data of the order and of the acknowledgement as part of the contractual documentations.

8.6. Method of data storage: On separate processing list within the Controller's information technology system, and on accounting documents that correspond to related laws about keeping bills for certain periods of time.

9. Data management concerning refunds

9.1. In case of money refund when User paid by credit card or by any other online payment ways through paying services User can get back the paid amount of money through the given means of payment or paying service that was originally used. In case User paid by bank transfer or asks refund this way then Controller pays back the amount of money by bank transfer.

9.2. Scope of parties concerned: User who placed the order and affected by money refund.

9.3. Legal basis of processing: according to GDPR Article 6 paragraph 1, point (c) in compliance with legal obligation of the Controller.

9.4. Scope of data handled:
- order ID,
- the sum to be refunded,
- legal title of refund,
- User's name,
- bank account number in case User paid by bank transfer or wants the money back by bank transfer.

9.5. Goal of processing: in case it is on a warranty, a right of withdrawal or a guarantee proceeding, the goal is to fulfil their duty in accordance with A'ct V of 2013 on the Civil Code (Polgári Törvénykönyvről szóló 2013. évi V. törvény)', 'Government Decree 45/2014 (II 26) Article 23, Paragraph 1 on Detailed Rules of Contracts between Customers and Business (a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló 45/2014. (II. 26.) Korm. rendelet)' or 'Government Decree 151/2003. (IX.22.) Article 5, Paragraph 5,6,7 on compulsary warranty on certain consumer durables' (az egyes tartós fogyasztási cikkekre vonatkozó kötelező jótállásról szóló 151/2003. (IX. 22.) Korm. rendelet 5. § (5), (6), illetve (7) bekezdés)' depending on the legal title.

9.6. Duration of processing: in order to refund, Controller handles information mentioned above until it is prescribed by the Act on Accounting (Számviteli Törvény) about keeping certificates. According to the Act on Accounting (Számviteli Törvény), this period is at least 8 years after making out an invoice, after passing this deadline, Controller deletes

data within one year. The circle of handled data is mainly data which is included in the sales notname, address, data relating to product concerned with refund, the sum to be refunded).

Other data - that are not subject to the accounting documents - possibly processed during ordering (e.g. important messages between User and Controller about orders) is processed by Controller for 5 years after contracting – general term of limitation concerning civil demands. The interruption of the limitation period shall prolong the processing period until the new date of limitation.

9.7. Method of data storage: on a list of data-processing kept separately on Controller's IT system and also data that is necessary for maintaining proper accounting is kept on accounting documents in order to fulfil its obligation of retention of supporting documents provided by Accounting Act.

10. Forwarding data

10.1. Scope of concerned: Users choosing online payment during purchasing on the website, regardless of using other services.

10.2. Addressee of data forwarding:

Stripe Payments Europe Ltd.

Registration number: 513174
Tax number: IE 3206488LH
Headquarters: C/O A&L Goodbody, IFSC, North Wall Quay, Dublin 1., Ireland
Postal address: C/O A&L Goodbody, IFSC, North Wall Quay, Dublin 1., Ireland
E-mail: dpo@stripe.com
Website: https://stripe.com/

Company as service provider of the online purchase service that can be used on Controller's website.

10.3. Legal basis of data forwarding: User's legitimate interest based on GDPR Article 6, Paragraph (1), Point a).

Recipient is obliged to run a fraud prevention and scout system in connection with offering payment services and has the right to handle personal data that is necessary for these. Recipient has developed its system regarding to legal obligations, for its operation data forwarding by Controller is necessary. Accordingly to this it is Recipient's legitimate interest to run a fraud prevention and scout system to meet its legal obligations. Recipient falls under the following provisions:

- Act CCXXXVII of 2013 165. § (5) Paragraph on Credit Institutions and Financial Enterprises (a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 165. § (5) bekezdése),

- Act CCXXXV of 2013 92/A. § (3) Paragraph Point f) on some payment services (az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 92/A. § (3) bekezdés f) pontja),
- Act LXXXV of 2009 14. § (1) Paragraph Point v) on providing payment services (a pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény 14. § (1) bekezdés v) pontja).

Fraud prevention and providing proper operation of online services are both Controller's and Recipient's legitimate interest. Both organisations' main source of revenue connects to proper operation of payment services. Nevertheless these are User's interests as well, in particular to avoid abuse of bank card data.

Data forwarding allows preventing and detecting frauds and troubleshooting of possible stumbling block that might appears during the process of payment.

Forwarded data comes from User's data handled during booking/ordering and these data are forwarded through electronic channels which ensure encrypted data traffic solely for Recipient and only after payment is done and which are not used for any other purposes by Recipient. Therefore, data forwarding puts no significant risk on User, it has no other visible effect on them.

Forwarding data is necessary for reaching goals described here and is suitable for making payment services safer.

In view of the above and taking the built in guarantee operations into account, forwarding does not mean unreasonable degree encroachment into Users' personal lives, therefore data forwarding is a necessary and proportional data processing operation.

A separate documentation is made about the consideration of interests whose details can be required by User from Controller.

10.4. Scope of data forwarding:

- data that is necessary for the order transaction,
- surname,
- first name,
- telephone number,
- e-mail address,
- address,
- Unique identifier of the transaction.

Bank card data given during payment is directly provided for payment service provider, so Controller does not gain access to them.

10.5. Purpose of forwarding data: Operating and managing online payment service appropriately, confirmation of transactions, operating fraud-monitoring to protect users' interests. This is a system to reveal frauds related to online payment, supporting the control of bank transactions – and providing help through customer support service.

10.6. To learn more about Stripe's data management and further circumstances of data

management - among others plea of law, purpose, scope of handled data, duration of data management - please visit https://stripe.com/en-hu/privacy/.

10.7. Controller does not forward information to third parties for business or marketing purposes.

10.8. Controller forwards information only to official bodies in accordance with legal requirements beyond the above mentioned cases.

11. Using data processing

Controller draws on the following businesses to process data.

11.1. Storage space service provider

11.1.1. Parties involved in data processing: Users visiting website, regardless of using services.

11.1.2. Controller uses

Shopify International Limited

Tax number: IE 3347697H
Premises: 2nd Floor 1-2 Victoria Buildings, Haddington Road, Dublin 4, D04 XN32, Ireland
Postal address: 2nd Floor 1-2 Victoria Buildings, Haddington Road, Dublin 4, D04 XN32, Ireland
E-mail: abuse@shopify.com
Website: https://www.shopify.com/

as website storage place provider (Data Processor hereafter).

11.1.3. Defining the scope of data involved in data processing: this relates to all information mentioned in present policy.

11.1.4. Goal of data processing: To ensure functioning of website in an information technological way for Users who are involved.

11.1.5. Period of data processing: It correlates with processing periods indicated in this policy for processing with various objectives.

11.1.6. Nature of data processing: Processing data exclusively means to provide storage space necessary for the operation of website in an information technological way.

11.2. Website developer

11.2.1. Parties involved in data processing: Users visiting website, regardless of using

any of its services.

11.2.2. Controller makes use of the following company as data manager

Doppio Creative Reklámügynökség Korlátolt Felelősségű Társaság
(Doppio Creative Ltd.)

Registration number: 01-09-340655
Tax number: 26712505-2-43
Headquarters: 1st floor number 5, 7/a Alkotás Street, Budapest 1123 Hungary (Magyarország, 1123 Budapest, Alkotás utca 7/a 1. em. 5.)
Place of establishment: 1st floor number 5, 7/a Alkotás Street, Budapest 1123 Hungary (Magyarország, 1123 Budapest, Alkotás utca 7/a 1. em. 5.)
Telephone: +36 30 529 1204
E-mail: hello@doppio.hu
Website: https://doppio.hu/

Company as the developer of the website (Controller hereafter)

11.2.3. Defining the scope of data involved in data management: this relates to all information mentioned in present policy.

11.2.4. Purpose of data management: To ensure the function of the website in an information technological way through data management that is expressed through necessary informational technology operations.

11.2.5. Period of data management: It is the same period as it has already been defined as data management periods at the separate sets of data for different data management purposes in present Policy.

11.2.6. Processing data exclusively means technical operations that are necessary for the operation of website in an information technological way

11.2.7. As for data management concerning implementation of Data processor's marketing campaigns, detailed information is given in document "Privacy Policy in connection with cookies".

11.3. Data management related to giving invoices

11.3.1. Parties involved in data management: Users making an order on the website, regardless of using other services of the website.

11.3.2. Controller makes use of the following company as data manager

Billingo Technologies Zártkörűen Működő Részvénytársaság
(Billingo Technologies Private Limited Company)

Short name: Billingo Technologies Zrt. (Billingo Technologies cPlc.)
Registration number: 01-10-140802

Tax number: 27926309-2-41
Place of establishment: 1st floor, 6 Árbóc Street, Budapest 1133, Hungary (Magyarország, 1133 Budapest, Árbóc utca 6. I. emelet)
Postal address: 1st floor, 6 Árbóc Street, Budapest 1133, Hungary (Magyarország, 1133 Budapest, Árbóc utca 6. I. emelet)
Telephone: +36 1 500 9491
E-mail: hello@billingo.hu
Website: https://www.billingo.hu/

that has developed and operates the invoicing software that is used by Controller (Data manager hereafter)

11.3.3. Defining the scope of data involved in data management: data processing affects the name and address of those who order and also the name of the ordered item(s) and/or service(s), time of purchasing, the price and invoices about any other fees.

11.3.4. Purpose of data management: to ensure the operation of the softver on an information technological way that is necessary for giving invoices data management that is expressed through informational technology operations that is necessary for operating the software safely.

11.3.5. Period of data management: the obligation of keeping invoices comes from the Act of Accounting and it says invoices have to be kept for 8 years from the time of invoicing.

11.3.6. Nature of data management: Data management exclusively covers only technical operations to manage software about making invoices on an information technological way.

11.4. Data management related to accounting services.

11.4.1. Parties involved in data management: Users making an order.

11.4.2. Controller makes use of the following company as data manager

BARÁTH SZÁMVITELI Korlátolt Felelősségű Társaság
(BARÁTH SZÁMVITELI Limited Liability Company)

Short name: BARÁTH SZÁMVITELI Kft. (BARÁTH SZÁMVITELI Ltd.)
Registration number: 08-09-015649
Tax number: 14127012-1-08
Place of establishment: 1st floor/19, 8 Körkemence Street, Győr 9023, Hungary (Magyarország, 9023 Győr, Körkemence utca 8. 1. em. 19.)
Postal address: 1st floor/19, 8 Körkemence Street, Győr 9023, Hungary (Magyarország, 9023 Győr, Körkemence utca 8. 1. em. 19.)
Telephone: +36 96 410 974

As the accountant of Controller’s economic performances (Data manager hereafter)

11.4.3. Defining the scope of data involved in data management: data management affects the name and address of the person who orders, and also the name of the ordered item(s), time of purchasing, the price and other fees that might be contained in the invoice.

11.4.4. Purpose of data management: To meet accounting obligations required by the applicable legislation in connection with Controller's economic activities by using the services of above named Data manager.

11.4.5. Duration of data management: up to the time arising out of Accounting Law which gives the period invoices are obliged to keep - the year that follows the 8th year period after the date of issued of the invoice.

11.4.6. Nature of data management: Data management solely means work carried out to meet accounting obligations and control, which is done by Controller through paper form medium or digital data kept in software.

11.5. Data management serves no other purposes.

11.6. Controller makes use no other Data managers apart from those described above.

12. User's rights concerning data management

12.1. **Right to access**: Controller gives information for User's request about data being handled by itself and by Data Processor, their sources, goals of data processing, its legal basis, period, name and address of Data Processor, its activities related to data processing, consequences and effects of a possible data protection incident and actions done in order to avoid such cases, furthermore, in case of forwarding concerned person's personal data, about the legal basis and addressee of data forwarding. Controller provides information without any unreasonable delay, within maximum one month after the arrival of the request.
Within the framework of the right to access, Controller provides User with a copy of personal data involved in processing, within maximum one month after the arrival of the request. For further demands from User, Controller calculates a reasonable fee based on administrative costs (see Chapter 13).

12.2. **Right to portability of data**: User has the right to get personal data about themselves in an articulate, widely used format, readable on devices, furthermore, has the right to forward these pieces of information to another Controller without the obstruction of Controller that has User's data according to User's consent, if:
a) processing is based on User's consent or contract; and
b) processing is automatized.

Practising the right to portability of data, User has the right – if it is technically practicable – to ask Controllers to forward information between each other directly.

12.3. **Right to correction**: User has the right to ask for correction of their data, which

Controller fulfills without any unreasonable delay, within maximum one month after the arrival of the request. Considering the goal of processing, User has the right to ask for completing their missing personal data – for example through an additional declaration.

12.4. **Right to limitation of processing**: Controller marks personal data in order to limit processing. User may ask for such limitation if one of the following cases occur:
a) User disputes accuracy of personal data, in this case limitation exceeds for the period that enables Controller to check the accuracy of personal data;
b) processing is illegal, and User objects against deleting their data and asks for limitation of use;
c) Controller does not need personal data for processing, however, concerned party lays claim to them in order to propose, realize or protect legal demands; or
d) User has objected to legal processing done by Controller; in such cases limitation exceeds over a period in which it becomes clear whether Controller's legal interests dominate over concerned party's legal interests.

12.5. **Right to cancellation**: Controller deletes information if:
a) personal data is no longer needed for reasons they were recorded, or were handled differently;
b) User withdraws their consent to processing, and there are no other legal bases for it;
c) User objects to processing and there are no prior rightful reasons for processing, or User objects to processing with direct sales objectives;
d) personal data was handled illegally;
e) personal data must be deleted to fulfil legal obligations claimed by European Union or member state laws;
f) User requests deletion or objects to processing, and data was recorded to offer services related to information technological society directly to children.

Controller informs User and all Controllers that are provided with information about the correction, limitation and deletion. Notification might be neglected if it seems to be impossible, or requires unreasonable efforts. Controller informs User on demand about these addressees.

12.6. **Right to objection**: User has the right to object to their data being managed rightfully by Controller at any time because of personal reasons. In such cases, Controller cannot handle personal information any longer, except when Controller proves that there are obligatory rightful reasons for processing, having priority over concerned person's interests, rights and freedoms, or reasons that are related to proposal, enforcement or defence of legal demands.

13. Fulfilling of User's requests

13.1. Controller offers notification and taking actions for free, as described in Point 12. If User's request is obviously unfounded, or – especially for its repeated nature – exaggerated, Controller

a) might charge a reasonable price, or

b) might deny taking actions based on request,
considering data requested, or administrative costs of measures to be taken to fulfil request.

13.2. Controller informs User without any unreasonable delay, but maximum one month after receiving the request about actions that has been taken, including issuing copies of data. If necessary, considering the complexity of request and numbers of requests this deadline can be made longer with additional two months. Controller informs User about elongation of deadline together with indicating reasons of delay within one month after receiving the request. If concerned User sends their request electronically, Controller provides information electronically, except when concerned User asks for it in a different way.

13.3. If Controller does not take any steps as reaction to User's request, without delay but within maximum of one month after receiving the request, Controller informs User about reasons why there have been no actions taken, and about the possibility of filing a complaint at Authority mentioned in Point 15 and can have the right to legal remedy described there as well.

13.4. User can hand in their request to Controller in any way that identifies them. Identifying Users who hand in a request is necessary because Controller can deal with only those requests that are entitled. If Controller has justified doubts about the identity of natural person handing in a request it can ask for other pieces of information to assure the identity of concerned User.

13.5. User can send their requests to Controller to the address **129 Dózsa György Quay, Győr 9026, Hungary (Magyarország, 9026 Győr, Dózsa György rakpart 129.)** or to the e-mail address **info@embrighter.com** Controller considers requests sent in e-mail genuine only if it was sent from an e-mail address registered at Controller's database. However, using another e-mail address does not mean in observance of such requests. Time of receiving e-mails is the first day after the e-mail was sent.

14. Data protection, data safety

14.1. Controller assures the safety of data and through technical and organizational actions, as well as internal rules of procedure ensures that laws and other data and secret protection rules are kept. Controller protects data especially against illegal access, change, forwarding, making public, deletion or effacement of data, moreover, it protects against accidental effacement and damage, as well as inaccessibility of data as a result of change in applied technology.

14.2. Data related to measuring number of visitors of the website and habits describing use of website are handled in Controller's information technological system in a way that prevents Controller to link data to anyone, right from the beginning.

14.3. Processing takes place to reach articulated and legal goals described in present policy to a necessary and proportional degree, based on relevant laws and

recommendations, keeping appropriate safety measures.

14.4. In order to achieve these, Controller uses “https” protocol to reach the website, through which web communication can be encrypted and individually identifiable. Controller stores information in encrypted data stocks on separate lists insulated from each other based on processing goals to which certain Controller employees – performing tasks indicated in present policy – have access to, who have to protect data and it is their responsibility to handle this policy and relevant laws in an appropriate manner.

14.5. Passwords are stored with encryption codes by Controller’s system as a result of which Controller cannot learn User’s password.

15. Prosecution of rights

Concerned parties may practice their prosecution of rights based on Civil Code Act V of 2013 (Polgári Törvénykönyvről szóló 2013. évi V. törvény) and GDPR at a courthouse, and can turn to the National Authority for Data Protection and Freedom of Information:

Nemzeti Adatvédelmi és Információszabadság Hatóság
(National Authority for Data Protection and Freedom of Information)

Address: 9-11. Falk Miksa Street, Budapest 1055, Hungary (Magyarország, 1055 Budapest, Falk Miksa utca 9-11.)
Postal address: P.O. Box 9 Budapest 1363, Hungary (Magyarország 1363 Budapest, pf.: 9.)
Telephone: +36 1 391 1400
Fax: +36 1 391 1410
E-mail: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu/

In case choosing a process involving a courthouse, the lawsuit – based on concerned User’s choice – can be initiated at the courthouse in concerned person’s residence or place of stay, as courthouses are competent in confiscation of such a lawsuit.

Download/print the document: HERE

2023.06.25.

BRODEX Bt.