

Privacy Policy

Purpose of the policy, name of the data controller

This document provides information on the processing of your personal data and your rights in relation to it in accordance with the European Union Regulation (Regulation 2016/679 of the European Parliament and of the Council, hereinafter referred to as GDPR) and the Hungarian legislation (Act CXII of 2011 on the right to informational self-determination and freedom of information, hereinafter referred to as the Info Act).

Name of the data controller, contact details

Name of the data controller:

DJ Store Professional Kft. (hereinafter referred to as the Company or Data Controller)

Mailing address of the data controller:

1116 Budapest, Nádorfejérvári út 31. fsz.2.

Data controller's e-mail address: [djstore \[at\] djstore \[dot\] hu](mailto:djstore@djstore.hu)

Data controller's telephone number: 0614664756

Data controller registration number: NAIH58233/2012

Our company's data management principles are in line with the applicable data protection legislation, in particular the following:

Act CXII of 2011 – on the right to informational self-determination and freedom of information (Infotv.);

Act V of 2013 – on the Civil Code (Ptk.);

Act CLV of 1997 – on consumer protection (Fgytv.);

Act C of 2000 – on accounting (Számv. tv.);

Act CVIII of 2001 – on certain issues of electronic commerce services and services related to the information society (Eker. tv.);

Act C of 2003 – on electronic communications (Eht.);

Act CXXXIII of 2005 – on the rules of personal and property protection and private investigation activities (SzVMt.);

Act CLXIV of 2005 – on trade (Kertv.);

Act XLVIII of 2008 – on the basic conditions and certain limitations of economic advertising activities (Grt.);

Act II of 2012 – on violations, violation procedure and violation registration system (Sztv.);

Act CLIX of 2012 – on postal services (Postatv.);

Act XC of 2017 – on criminal procedure (Be.);

19/2014 (IV. 29.) NGM Decree – on the procedural rules for handling warranty and guarantee claims regarding things sold under a contract between a consumer and a business (Szav. r.)

Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR Regulation)

Concepts and interpretations related to personal data

personal data: data that can be linked to the data subject - in particular the name, identification mark of the data subject and one or more physical, physiological, mental, economic, cultural or social identity - and the conclusion that can be drawn from the data concerning the data subject;

special data: a) personal data concerning racial origin, nationality, political opinion or party affiliation, religious or other worldview, membership of an interest-representative organization, sexual life, b) personal data concerning health, pathological addiction, and criminal personal data;

data management: any operation or set of operations performed on data, regardless of the method used, such as collection, recording, recording, organization, storage, alteration, use, consultation, transmission, disclosure, alignment or combination, blocking, erasure and destruction, as well as preventing further use of data, taking photographs, sound or image recordings and recording physical characteristics suitable for identifying a person (e.g. fingerprints or palm prints, DNA samples, iris images);

data processing: the performance of technical tasks related to data processing operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data;

data transfer: making data available to a specific third party;

disclosure: making data available to anyone;

data controller: the natural or legal person or an organisation without legal personality who, alone or jointly with others, determines the purposes of the processing of data, makes and implements decisions relating to the processing of data (including the means used), or has them implemented by the data processor;

data processor: the natural or legal person or an organisation without legal personality who processes data on the basis of a contract - including a contract concluded on the basis of a legal provision;

data erasure: making data unrecognizable in such a way that their recovery is not possible.

Principles of data management

Only personal data that is essential for the purpose of data processing and suitable for achieving the purpose may be processed. Personal data may only be processed to the extent and for the period necessary to achieve the purpose.

Personal data shall retain this quality during data processing as long as the relationship with the data subject can be restored. The relationship with the data subject can be restored if the data controller has the technical conditions necessary for restoration.

During data processing, the accuracy, completeness and – if necessary with regard to the purpose of data processing – up-to-dateness of the data must be ensured, and the data subject must only be identified for the period necessary for the purpose of data processing.

Personal data may be processed if:

- the data subject consents to it or

- it is ordered by law or – based on the authorization of law, within the scope specified therein – by a local government decree for a purpose based on public interest (hereinafter: mandatory data processing).

Personal data may also be processed if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party or parties receiving the data, unless these interests are overridden by the interests of the data subject in relation to fundamental rights and freedoms (Directive 95/47/EC of the European Parliament and of the Council. Article 7(f)).

Personal data may be processed – in the absence of legal requirements – only with the consent of the visitor. The nature of the data provision – whether voluntary or mandatory – must be explained before the data is collected. In the case of mandatory data provision, the law governing the data processing must be indicated. During data processing, the data may only be used for the specified purpose.

In addition to the purpose of data processing, clear information must be published about who will manage and process the data.

The data controller shall plan and implement data processing operations in such a way as to ensure the protection of the privacy of data subjects when applying this Act and other rules relating to data processing.

The data controller, or within its scope of activity the data processor, shall ensure the security of data and shall take the technical and organisational measures and establish the procedural rules necessary for the enforcement of this Act and other data and confidentiality protection rules.

Data shall be protected by appropriate measures, in particular against unauthorised access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, and against inaccessibility resulting from changes in the technology used.

In order to protect data files managed electronically in various registers, it shall be ensured by appropriate technical solutions that the data stored in the registers cannot be directly linked and assigned to the data subject, except where permitted by law.

During the automated processing of personal data, the data controller and the data processor shall take additional measures to ensure

- a) the prevention of unauthorized data entry;
- b) the prevention of the use of automatic data processing systems by unauthorized persons using data transmission equipment;
- c) the verification and establishment of which bodies the personal data have been or may be transmitted using data transmission equipment;
- d) the verification and establishment of which personal data have been entered into the automatic data processing systems, when and by whom;
- e) the recovery of installed systems in the event of a malfunction and
- f) the preparation of a report on errors occurring during automated processing.

When defining and applying measures to ensure data security, the data controller and the data processor must take into account the current state of the art. Among several possible data processing solutions, the one that ensures a higher level of protection of personal data must be chosen, unless this would entail a disproportionate burden for the data controller.

The visitor may request information at any time during data processing, or check the content of his/her data, and may request their correction, modification, alteration or deletion at any time upon request.

The visitor may modify or withdraw his/her consent to data processing at any time.

Data processing is usually carried out automatically. Once the purpose of data processing has been fulfilled, the data must be deleted in accordance with legal requirements.

Data may only be transmitted and different data processing operations may only be linked if the visitor has consented to it or if the law permits it, and if the conditions for data processing are met for each personal data item.

Before implementing data processing, the service provider must publish understandable and clear information on the method and purpose of data collection, taking into account legal requirements, and - in the case of voluntary data provision - on the indication of its voluntary nature.

Legal background, legal basis, purpose of data processing on the website, personal data processed

4.1. Legal basis for data processing

The Data Controller processes and protects data in compliance with the following applicable laws.

- Act CXII of 2011 on the right to informational self-determination and freedom of information (hereinafter: the Info Act)
- 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
- Act CVIII of 2001 on certain issues of electronic commerce services and services related to the information society (hereinafter: the Electronic Commerce Act).
- Act XLVIII of 2008 on the basic conditions and certain limitations of commercial advertising activities (hereinafter: the Commercial Advertising Act).

4.2. General information about cookies

4.2.1. The visitor to the website must be informed on the website about the use of cookies and their consent must be requested.

4.2.2. A cookie is a piece of data that the visited website sends to the visitor's browser (in the form of a variable name-value pair) so that it can store it and later be loaded by the same website. A cookie can be valid until the browser is closed, or for an unlimited period of time. Later, the browser sends this data to the server with every HTTP(S) request. This modifies the data on the user's computer.

4.2.3. The essence of a cookie is that, due to the nature of website services, it is necessary to identify a user (e.g. that they have entered the site) and to be able to handle it accordingly in the future. The danger lies in the fact that the user is not always aware of this and it may be possible for the website operator or other service provider whose content is integrated into the site (e.g. Facebook, Google Analytics) to track the user, thereby creating a profile about him/her, in which case the content of the cookie can be considered personal data.

4.3. Types of cookies:

Technically essential session cookies: without which the site simply would not function functionally, these are necessary to identify the user, e.g. to manage whether he/she has logged in, what he/she has put in the basket, etc. This is typically the storage of a session-id, the other data is stored on the server, which is therefore more secure. There is a security aspect, if the session cookie value is not generated correctly, there is a risk of session-hijacking attacks, therefore it is absolutely necessary that these values are

generated correctly. Other terminology calls all cookies that are deleted when you exit the browser a session cookie (a session is a browser session from launch to exit).

Usage cookies: this is the name you usually give to cookies that remember the user's choices, for example, how the user wants to see the page. These types of cookies essentially mean the settings data stored in the cookie.

Performance cookies: although they have little to do with "performance", this is usually the name given to cookies that collect information about the user's behavior within the website they visit, the time spent, and clicks. These are typically third-party applications (e.g. Google Analytics, AdWords, or Yandex.ru cookies). They are suitable for creating visitor profiles.

You can find out more about Google Analytics cookies here:

<https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage>

You can find out more about Google AdWords cookies here:

<https://support.google.com/adwords/answer/2407785?hl=hu>

Accepting or allowing the use of cookies is not mandatory. You can reset your browser settings to refuse all cookies or to indicate when a cookie is being sent. Most browsers automatically accept cookies by default, but these can usually be changed to prevent automatic acceptance and offer you the choice each time.

4.4. You can find information about cookie settings for the most popular browsers at the links below.

Google Chrome: <https://support.google.com/accounts/answer/61416?hl=hu>

Firefox: <https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn>

Microsoft Internet Explorer: <http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-11>

Microsoft Edge: <http://windows.microsoft.com/hu-hu/windows-10/edge-privacy-faq>

Brave: <https://support.brave.com/hc/en-us/articles/360048833872-How-Do-I-Clear-Cookies-And-Site-Data-In-Brave>

Safari: <https://support.apple.com/hu-hu/HT201265>

However, we would like to draw your attention to the fact that certain website functions or services may not function properly without cookies.

4.5. Information on the cookies used on the Company's website and the data generated during the visit

4.5.1. Data processed during the visit: Our Company's website may record and process the following data about the visitor and the device used for browsing when using the website:

the IP address used by the visitor,

the type of browser,

the characteristics of the operating system of the device used for browsing (set language),

time of visit,

the (sub)page, function or service visited.

clicks.

We retain this data for a maximum of 90 days and may use it primarily to investigate security incidents.

4.5.2. Cookies used on the website

Technically necessary session cookies

The purpose of data processing: to ensure the proper functioning of the website. These cookies are necessary for visitors to browse the website, to use its functions smoothly and fully, and to use the services available through the website, including, among other things, in particular, to record the actions performed by the visitor on the given pages or to identify the logged-in user during a visit. The duration of the data processing of these cookies applies only to the visitor's current visit, and this type of cookie is automatically deleted from the visitor's computer at the end of the session or when the browser is closed.

The legal basis for this data processing is Section 13/A. (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Elkertv.), according to which the service provider may process personal data that are technically indispensable for the provision of the service for the purpose of providing the service. All other conditions being equal, the service provider must select and in all cases operate the means used in the provision of information society services in such a way that personal data are processed only if this is absolutely necessary for the provision of the service and for the fulfilment of other purposes specified in this Act, but even in this case only to the extent and for the period necessary.

Cookies facilitating use:

These remember the user's choices, for example in what form the user would like to see the site. These types of cookies essentially mean the setting data stored in the cookie.

The legal basis for data processing is the visitor's consent.

The purpose of data processing: Increasing the efficiency of the service, enhancing the user experience, making the use of the website more convenient.

This data is rather on the user's machine, the website only accesses and recognizes the visitor through it.

Performance cookies:

They collect information about the user's behavior within the visited website, the time spent, and clicks. These are typically third-party applications (e.g. Google Analytics, AdWords).

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

Purpose of data processing: website analysis, sending advertising offers.

Links

The pages of djstore.hu contain numerous references and jump points to pages maintained by other service providers, where djstore.hu has no influence on the practices related to the processing of personal data. We draw the attention of our visitors that if they click on such jump points, they will be transferred to the pages of other service providers. In such cases, if they feel the need, they should read the statement of the service providers of the pages regarding the protection of personal data.

4.5.3. Data processing related to the camera system operating in our store

Our store is monitored by a camera system that provides online data transmission and recording. The cameras serve preventive purposes on the one hand, and on the other hand, they help to clarify illegal activities. The camera system is operated by our company.

The task of the camera system is to continuously ensure the protection and security of the store. The cameras monitor the store entrance, the sales area and the sales counter 24 hours a day, thus enabling continuous monitoring of events. Strict rules apply to the storage and handling of recordings, and the only person who can view the recordings is the managing director of our company.

By default, we store the recordings recorded by the cameras for 20 days. If we detect illegal behavior in the monitored area, we may contact the police and hand over the relevant recordings to the competent authorities. In such cases, the recordings will not be deleted after 20 days; they will be retained for evidentiary purposes until the case is finally concluded.

4.6. Data processing related to ordering and invoicing

Legal background and legal basis for data processing.

The background to data processing is the provisions of Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.) and Act C of 2000 on accounting (Sztv.). The legal basis for data processing is the Infotv. In accordance with your consent in accordance with Section 5 (1) a) and – in the event of withdrawal of your consent – to fulfil the legal obligation of the Data Controller under Section 6 (5) a) of the Information Act.

Purpose of data processing: Issuing invoices in accordance with the law and fulfilling the obligation to retain accounting documents. Pursuant to Section 169 (1)-(2) of the Information Act, business companies must retain accounting documents directly and indirectly supporting the accounting settlement.

Scope of data processed: Name, telephone number, address and e-mail address are required for ordering, and name and address are required for issuing the invoice.

Duration of data processing: Invoices issued must be kept for 8 years from the date of issue of the invoice, pursuant to Section 169 (2) of the Information Act. We inform you that if you withdraw your consent to the issuance of the invoice, the Data Controller is entitled to retain your personal data obtained during the issuance of the invoice for 8 years based on Section 6 (5) a) of the Information Act.

4.7. Data processing related to the delivery of goods

Legal background and legal basis for data processing: The background for data processing is the provisions of Act CXII of 2011 on the right to informational self-determination and freedom of information (Information Act). The legal basis for data processing is your consent in accordance with Section 5 (1) a) of the Information Act.

Purpose of data processing: In the case of the delivery of goods, the purpose of data processing is to deliver the ordered goods to you in cooperation with our contractual partner, adapting them to your needs.

Scope of data processed: For data processing, it is necessary to provide your name, delivery address and telephone number.

Duration of data processing: The Data Controller processes the data until the delivery of the ordered goods.

4.8. Data processing related to sending newsletters

Legal background and legal basis for data processing: The background for data processing is Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.) and Act XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activities (Grt.). The legal basis for data processing is your consent in accordance with Section 5 (1) a) of the Infotv. and Section 6 (1)-(2) of the Grt.

Purpose of data processing: The purpose of data processing is to inform you about the latest and best offers and promotions. We would like to inform you that in the newsletter we place advertisements not only of the Data Controller, but also of other companies, but we do not transfer or forward your personal data to them.

Scope of processed data: For data processing, it is necessary to provide your name and e-mail address.

Duration of data processing: Withdrawal of your consent.

4.9. Data processing related to sending and displaying personalized advertisements

Legal background and legal basis of data processing: The background of data processing is Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.) and Act XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activity (Grt.). The legal basis for data processing is your consent in accordance with Section 5 (1) a) of the Infotv. and Section 6 (1)-(2) of the Grt.

Purpose of data processing: The purpose of data processing is to provide you with personalized offers that best suit your needs and preferences.

Scope of data processed: During data processing, the Data Controller uses cookies to record which products you have previously visited.

Duration of data processing: Withdrawal of consent.

The independent measurement and auditing of our website traffic and other web analytics data is also performed by an external service provider. The codes of the following service providers have been embedded in the code of the djstore.hu page in order to track users and display personalized recommendations:

Google Analytics - <https://policies.google.com/privacy>

Google Floodlight - <https://policies.google.com/privacy>

Facebook Pixel - <https://www.facebook.com/policy.php>

Árkereső Trusted Shop Widget - <https://www.arukereso.hu/static/adatvedelem.html>

4.10. Data processing associated with contact

Legal background and legal basis of data processing: The background of data processing is the provisions of Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.). The legal basis for data processing is your consent in accordance with Section 5 (1) a) of the Infotv.

Purpose of data processing: To be able to answer your question.

Scope of data processed: When contacting you, you must provide your name and contact information (e-mail address or telephone number).

Duration of data processing: We store messages sent during contact for a maximum of one month, but you have the option to request the deletion of personal data provided during contact at any time.

4.11. Data processing associated with the enforcement of a warranty claim

Name of data processing: The Data Controller provides a 1-year warranty for the individual products it sells. For this period, the Data Controller stores the data necessary for the enforcement of the warranty claim, and may use and transmit the data to the extent necessary for the enforcement of the claim.

Legal background and legal basis for data processing: The background for data processing is Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.) and Act V of 2013 on the Civil Code (Ptk.). The legal basis for data processing is your consent in accordance with Section 5 (1) a) of the Infotv.

Purpose of data processing: Enforcement of the warranty claim.

Scope of data processed: During data processing, the Data Controller processes your name, address, characteristics of the purchased product and date of purchase.

Duration of data processing: The data is processed by the Data Controller for 1 year [warranty period].

4.12. Data processing related to registration

Legal background and legal basis of data processing: The background of data processing is the provisions of Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.). The legal basis for data processing is your consent in accordance with Section 5 (1) a) of the Infotv.

Purpose of data processing: The purpose of data processing is to identify the user and maintain contact during the use of the service.

Scope of data processed: When registering, it is necessary to provide name, e-mail address, password, and whether or not to request the newsletter service.

Duration of data processing: We store the data provided during registration for five years, but you have the option to request the deletion of the personal data provided at any time.

4.13. Further data processing

If the Data Controller intends to carry out further data processing, it will provide prior information on the essential circumstances of the data processing (legal background and legal basis for data processing, purpose of data processing, scope of data processed, duration of data processing).

We inform you that the Data Controller must comply with written requests for data from authorities based on statutory authorization. The Data Controller keeps a record of data transfers in accordance with Section 15 (2)-(3) of the Information Act (to which authority, what personal data, on what legal basis, when the Data Controller transferred it), the content of which the Data Controller will provide information on upon request, unless the provision of such information is prohibited by law.

4.14. Other provisions

The user is obliged to provide true and complete information during registration regarding the questions on the registration form, and to update the registration data accordingly in the event of any changes.

In the event of untruth, incompleteness or inaccuracy of the data provided by the user, DJ Store Professional Kft. has the right to partially or completely suspend or terminate the user's access.

DJ Store Professional Kft. reserves the right to immediately terminate the user's right to use and access the Website at any time, at its sole discretion, if the user violates the terms of the Privacy Policy or the provisions of any applicable laws.

On the use of a data processor and their activities related to data processing

Data processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller; (Article 4(8) of the Regulation)

The use of a data processor does not require the prior consent of the data subject, but it is necessary to inform him/her. Accordingly, we provide the following information:

5.1. Accounting-related data processing

Name of the data processor: E.G.M. Adó-Kontír Ltd.

Correspondence address of the data processor: 1116 Budapest, Talpas u. 3.

E-mail address of the data processor: info [at] adokontir [dot] hu

Telephone number of the data processor: +361-209-3675

The Data Processor contributes to the accounting of accounting documents based on a written contract concluded with the Data Controller. In doing so, the Data Processor processes the name and address of the data subject to the extent necessary for accounting records, for a period in accordance with Section 169 (2) of the Hungarian Data Protection Act, and then deletes it immediately.

5.2. Data processing activities related to the delivery of goods

Name of the data processor: GLS General Logistics Systems Hungary Ltd.

Mailing address of the data processor: 2351 Alsónémedi, GLS Európa u. 2.

E-mail address of the data processor: info [at] gls-hungary [dot] hu

Telephone number of the data processor: +36 29 88 66 70

The Data Processor participates in the delivery of the ordered goods based on a written contract concluded with the Data Controller. In this process, the Data Processor may process the customer's name, address, e-mail address and telephone number until the delivery of the ordered goods, after which it will be deleted immediately.

Name of the data processor: FOXPOST Zrt.

Mailing address of the data processor: 3300 Eger, Maklári út 119.

Email address of the data processor: info@foxpost.hu

Phone number of the data processor: +36 1 999 0369

The Data Processor participates in the delivery of the ordered goods based on a written contract concluded with the Data Controller. In this process, the Data Processor may process the customer's name, address, e-mail address and telephone number until the delivery of the ordered goods, after which it will be deleted immediately.

Name of the data processor: Magyar Posta Zrt.

The data processor's mailing address is: Budapest, Dunavirág utca 2-6.

The data processor's email address is: idopontegyeztetes@posta.hu

The data processor's phone number is: +36 1 767 8200

The Data Processor assists in the delivery of the ordered goods based on a written contract concluded with the Data Controller. In doing so, the Data Processor may process the customer's name, address, email address and phone number until the delivery of the ordered goods, after which it will delete them immediately.

5.3. Data processing activities related to sending newsletters

Name of the company operating the newsletter sending system: UNAS Online Ltd.

Registered address of the company operating the newsletter sending system: 9400 Sopron, Kőszegi út 14.

Phone number of the company operating the newsletter sending system: +36 99 200 200

E-mail address of the company operating the newsletter sending system: unas [at] unas [dot] hu

The Data Processor participates in sending newsletters based on a contract concluded with the Data Controller. In the process, the Data Processor processes the name and e-mail address of the data subject to the extent necessary for sending the newsletter, and deletes it immediately upon the data subject's request.

5.4. Data processing for the purpose of storing personal data

Name of the data processor: UNAS Online Ltd.

The data processor's registered office address is: 9400 Sopron, Kőszegi út 14.

The data processor's telephone number is: +36 99 200 200

The data processor's contact details are: unas [at] unas [dot] hu

The Data Processor stores personal data on servers based on a written contract with the Data Controller. It is not authorized to view personal data.

5.5. Data processing for the purpose of storing personal data

Name of the data processor: Online Comparison Shopping Ltd.

Mailing address of the data processor: 1074 Budapest, Rákóczi út 70-72.

The data processor's e-mail address is: info [at] arukereso [dot] hu

In order for the Trusted Shop program of www.arukereso.hu (Online Comparison Shopping Kft. 1074 Budapest, Rákóczi út 70-72., Tax ID: 24868291-2-42, Company Registration Number: 01-09-186759), the customer's e-mail address and the name of the product purchased are forwarded to arukereso.hu after purchases made here. The purpose of the data transfer is to request and display customer feedback, and to store the customer's e-mail address for the purpose of customer satisfaction surveys related to the Trusted Shop Program. The personal data transmitted in this way is processed by Online Comparison Shopping Kft. in accordance with the Data Protection and Data Management Policy of www.arukereso.hu.

5.6. Data processing for the storage of personal data

Name of the data processor: Cofidis Hungary Branch

Mailing address of the data processor: 1133 Budapest, Váci út 96-98.

Email address of the data processor: infohu [at] cofidis [dot] hu

When applying for a Cofidis Product Loan, the user expressly agrees that the following data – necessary for concluding the contract – will be transferred to Cofidis Hungary Branch for the purpose of submitting a loan application: full name, date of birth (year/month/day), mother's name, telephone number, email address, order identifier, order value, name of ordered products, parameters of the chosen loan structure. The user expressly accepts that after the transfer of data, the provisions of the business regulations and data processing information of the Cofidis Hungarian Branch shall govern the handling of the transferred data (including its retention and deletion).

Data security measures

The Data Controller declares that it has taken appropriate security measures to protect personal data against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, and against inaccessibility resulting from changes in the technology used.

Persons under the age of 16 are not allowed to shop in our webshop! Persons under the age of 16 may only use our webshop if they have obtained the consent of their legal representative (parent or guardian)!

Your rights during data processing - Rights of the data subject

Within the period of data processing, you have the right to:

Transparent information, communication and facilitation of the exercise of the data subject's rights

Right to prior information - if personal data are collected from the data subject

Information of the data subject and information to be provided to him/her if the personal data were not obtained by the data controller from him/her

Right of access of the data subject

Right to rectification
Right to erasure ("right to be forgotten")
Right to restriction of data processing
Notification obligation related to rectification or erasure of personal data or restriction of data processing
Right to data portability
Right to object
Automated decision-making in individual cases, including profiling
Restrictions
Informing the data subject about the data protection incident
Right to lodge a complaint with the supervisory authority (right to a judicial remedy)
Right to an effective judicial remedy against the supervisory authority
Effective judicial remedy against the controller or processor right to a remedy

1. Transparent information, communication and facilitation of the exercise of the data subject's rights

1.1. The controller shall provide the data subject with all information and any communication relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language, in particular for any information addressed to children. The information shall be provided in writing or by any other means, including, where appropriate, by electronic means. At the request of the data subject, oral information may also be provided, provided that the identity of the data subject has been otherwise verified.

1.2. The controller shall facilitate the exercise of the data subject's rights.

1.3. The controller shall inform the data subject without undue delay, and in any event not later than one month from the date of receipt of the request, of the measures taken in response to the request to exercise his or her rights. This period may be extended by a further two months under the conditions laid down in the Regulation, of which the data subject shall be informed.

1.4. If the controller does not take action on the data subject's request, it shall inform the data subject without delay, but no later than one month from the date of receipt of the request, of the reasons for not taking action and of the right to lodge a complaint with a supervisory authority and to seek a judicial remedy.

1.5. The controller shall provide the information and information on the data subject's rights and the action free of charge, however, in the cases specified in the Regulation, a fee may be charged.

The detailed rules are set out in Article 12 of the Regulation.

2. Right to prior information – if personal data are collected from the data subject

2.1. The data subject shall have the right to be informed of the facts and information relating to the data processing before the data processing is started. In this context, the data subject must be informed of:

- a) the identity and contact details of the controller and its representative,
- b) the contact details of the data protection officer (if any),
- c) the purpose of the intended processing of personal data and the legal basis for the processing,
- d) in the case of processing based on legitimate interest, the legitimate interests of the controller or a third party,
- e) the recipients of the personal data - to whom the personal data are disclosed - and the categories of recipients, if any;
- e) where applicable, the fact that the controller intends to transfer the personal data to a third country or to an international organisation.

2.2. In order to ensure fair and transparent data processing, the controller shall inform the data subject of the following additional information:

- a) the period for which the personal data will be stored or, where that is not possible, the criteria for determining that period;
- b) the data subject's right to request from the data controller access to, rectification, erasure or restriction of processing of personal data concerning him or her, and to object to the processing of such personal data, as well as the data subject's right to data portability;
- c) in the case of processing based on the data subject's consent, the right to withdraw consent at any time, without affecting the lawfulness of the processing carried out on the basis of consent before its withdrawal;
- d) the right to lodge a complaint with a supervisory authority;
- e) whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for entering into a contract, and whether the data subject is obliged to provide the personal data, as well as the possible consequences of not providing the data;
- f) the fact of automated decision-making, including profiling, and at least in such cases, the logic involved, and intelligible information on the significance of such processing and the foreseeable consequences for the data subject.

2.3. Where the controller intends to process personal data for purposes other than those for which they were collected, the data subject shall be informed of that purpose and of any relevant additional information prior to the further processing.

The detailed rules on the right to prior information are set out in Article 13 of the Regulation.

3. Information to be provided to the data subject and information to be provided to the data subject where the personal data were not obtained by the controller

3.1. If the controller has not obtained the personal data from the data subject, the data subject shall be informed by the controller of the facts and information referred to in point 2 above, as well as of the categories of personal data concerned, the source of the personal data and, where applicable, whether the data originate from publicly available sources, no later than one month after the personal data were obtained; if the personal data are used for the purpose of communicating with the data subject, at least upon first communication with the data subject; or if the data are expected to be communicated to other recipients, no later than upon first communication of the personal data.

3.2. The additional rules referred to in point 2 above (Right to prior information) shall apply.

The detailed rules for this information are set out in Article 14 of the Regulation.

4. Right of access of the data subject

4.1. The data subject shall have the right to obtain from the controller information as to whether or not personal data concerning him or her are being processed and, where such processing is taking place, access to the personal data and related information. (Article 15 of the Regulation).

4.2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards in place for the transfer in accordance with Article 46 of the Regulation.

4.3. The controller shall provide the data subject with a copy of the personal data which are the subject of the processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on the administrative costs.

The detailed rules on the data subject's right of access are set out in Article 15 of the Regulation.

5. Right to rectification

5.1. The data subject shall have the right to obtain from the controller, at his request, the rectification of inaccurate personal data concerning him or her without undue delay.

5.2. Taking into account the purpose of the processing, the data subject shall have the right to obtain the completion of incomplete personal data, including by means of a supplementary statement.

These rules are set out in Article 16 of the Regulation.

6. Right to erasure ('right to be forgotten')

6.1. 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 be obliged to erase personal data concerning him or her without undue delay if

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws his or her consent on which the processing is based and there is no other legal basis for the processing;
- c) the data subject objects to the processing of his or her data and there are no overriding legitimate grounds for the processing,
- d) the personal data have been processed unlawfully;
- e) the personal data must be erased for compliance with a legal obligation to which the controller is subject under Union or Member State law;
- f) the personal data were collected in connection with the provision of information society services directly to a child.

6.2. The right to erasure may not be exercised if the processing is necessary

- a) for the exercise of the right to freedom of expression and information;
- b) for compliance with an obligation under Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) for reasons of public interest in the field of public health;
- d) for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes, where the right to erasure would likely render impossible or seriously jeopardise such processing; or
- e) for the establishment, exercise or defence of legal claims.

The detailed rules on the right to erasure are set out in Article 17 of the Regulation.

7. Right to restriction of processing

7.1. In the event of restriction of processing, such personal data may be processed, with the exception of storage, only with the consent of the data subject, or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for important public interests of the Union or of a Member State.

7.2. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- a) the data subject contests the accuracy of the personal data, in which case the restriction shall apply for a period enabling the controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the data and requests the restriction of their use instead;
- c) the controller no longer needs the personal data for the purposes of the processing, but the data subject requires them for the establishment, exercise or defence of legal claims; or
- d) the data subject has objected to the processing; in this case, the restriction shall apply for the period until it is established whether the legitimate grounds of the controller override those of the data subject.

7.3. The data subject shall be informed in advance of the lifting of the restriction of processing.

The relevant rules are set out in Article 18 of the Regulation.

8. Notification obligation in relation to the rectification or erasure of personal data or the restriction of processing

The controller shall inform all recipients to whom or with whom the personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves a disproportionate effort. Upon request, the data subject shall be informed of these recipients by the controller.

These rules are set out in Article 19 of the Regulation.

9 Right to data portability

9.1. Under the conditions set out in the Regulation, the 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 shall have the right to transmit those data to another controller without hindrance from the controller to whom the personal data have been provided, where

- a) the processing is based on consent or a contract; and
- b) the processing is carried out by automated means.

9.2. The data subject may also request the direct transmission of personal data between controllers.

9.3. The exercise of the right to data portability shall be without prejudice to Article 17 of the Regulation (Right to erasure ("right to be forgotten")). The right to data portability shall not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This right shall not adversely affect the rights and freedoms of others.

The detailed rules are set out in Article 20 of the Regulation.

10. Right to object

10.1. The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him or her based on public interest, the performance of a task carried out in a public interest (Article 6(1)(e)) or legitimate interest (Article 6(f)), including profiling based on those provisions. In this case, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

10.2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such purposes, including profiling where such processing is related to direct marketing. If the data subject objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed for such purposes.

10.3. These rights shall be expressly brought to the attention of the data subject at the latest when the data subject is first contacted and the information shall be displayed clearly and separately from any other information.

10.4. The data subject may also exercise the right to object by automated means based on technical specifications.

10.5. Where personal data are processed for scientific and historical research purposes or for statistical purposes, the data subject shall have the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The relevant rules are set out in the Regulation's article.

11. Automated decision-making in individual cases, including profiling

11.1. 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.

11.2. This right shall not apply where the decision:

- a) is necessary for entering into, or the performance of, a contract between the data subject and the controller;
- b) is permitted by Union or Member State law applicable to the controller and which also lays down suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject; or
- c) is based on the data subject's explicit consent.

11.3. In the cases referred to in points a) and c) above, the controller shall implement suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject, including at least the right of the data subject to obtain human intervention on the part of the controller, to express his or her point of view and to object to the decision.

Further rules are set out in Article 22 of the Regulation.

12. Restrictions

Union or Member State law applicable to the controller or processor may restrict the scope of the rights and obligations (Articles 12-22, Article 34, Article 5 of the Regulation) by means of legislative measures, provided that the restriction respects the essence of the fundamental rights and freedoms.

The conditions for this restriction are set out in Article 23 of the Regulation.

13. Informing the data subject about the data breach

13.1. Where the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall inform the data subject about the data breach without undue delay. The notification shall describe the nature of the data breach in a clear and intelligible manner and shall include at least the following:

- a) the name and contact details of the data protection officer or other contact person who can provide further information;
- c) the likely consequences of the data breach;
- d) the measures taken or planned by the controller to remedy the data breach, including, where appropriate, measures to mitigate any adverse consequences resulting from the data breach.

13.2. The data subject does not need to be informed if any of the following conditions are met:

- a) the controller has implemented appropriate technical and organisational protection measures and these measures have been applied to the data affected by the personal data breach, in particular measures such as encryption that make the data unintelligible to persons not authorised to access the personal data;
- b) the controller has taken further measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is unlikely to materialise;
- c) providing information would involve a disproportionate effort. In such cases, the data subjects shall be informed by means of publicly available information or a similar measure ensuring that the data subjects are informed in an equally effective manner.

Further rules are set out in Article 34 of the Regulation.

14. Right to lodge a complaint with a supervisory authority (right to a judicial remedy)

The data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data concerning him or her infringes the Regulation. The supervisory authority to which the complaint has been lodged shall inform the customer of the progress of the procedure relating to the complaint and its outcome, including the fact that the customer has the right to seek a judicial remedy.

These rules are set out in Article 77 of the Regulation.

15. Right to an effective judicial remedy against the supervisory authority

15.1. Without prejudice to other administrative or non-judicial remedies, every natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him or her.

15.2. Without prejudice to other administrative or non-judicial remedies, every data subject shall have the right to an effective judicial remedy where the competent supervisory authority does not deal with a complaint or does not inform the data subject of the progress or outcome of the complaint lodged within three months.

15.3. Proceedings against a supervisory authority shall be brought before the courts of the Member State in which the supervisory authority is established.

15.4. Where proceedings are brought against a decision of a supervisory authority on which the Board has previously issued an opinion or taken a decision under the consistency mechanism, the supervisory authority shall be obliged to send that opinion or decision to the court.

These rules are set out in Article 78 of the Regulation.

16. Right to an effective judicial remedy against the controller or processor

16.1. Without prejudice to any administrative or non-judicial remedies available to you, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of personal data concerning him or her not being in accordance with this Regulation.

16.2. Proceedings against the controller or processor shall be brought before the courts of the Member State in which the controller or processor is established. Such proceedings may also be brought before the courts of the Member State in which the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its official authority.

These rules are set out in Article 79 of the Regulation.

Legal remedies

If you believe that the Data Controller has violated any legal provision relating to data processing or has not fulfilled any of your requests, you may initiate an investigation procedure with the **National Authority for Data Protection and Freedom of Information Authority** in order to terminate the allegedly unlawful data processing

You can file a complaint with the **Hungarian National Authority for Data Protection and Freedom of Information Authority**:

Name: **Hungarian National Authority for Data Protection and Freedom of Information Authority**

Registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Mailing address: 1530 Budapest, P.O. Box: 5.

Telephone: 0613911400

Fax: 0613911410

E-mail: ugyfelszolgalat@naih.hu

Web site: <http://www.naih.hu>

Modification of data processing information

The Data Controller reserves the right to amend this data management information. By using the website after the amendment comes into force, you accept the amended data management information.