

Privacy Information

Privacy Information

Effective: from Sept. 08. 2021. until withdrawal

(hereinafter: "Information") written by

NeoCons Plus Korlátolt Felelősségű Társaság

Company registration number:	03 09 135405
Registered office:	6120 Kiskunmajsa, Csontos Károly u. 99.
Tax number:	23532452-2-03
Statistical code:	23532452-4621-113-01
Electronic contact details:	www.neoconsplus.hu
E-mail:	info@neoconsplus.hu
Phone:	+36 30 862-5691
Legal representatives:	Zsolt Bódi Managing Director independently, Evelin Buri Managing Director independently

hereinafter: "**Service Provider or Data Controller**" as the operator of the <https://www.neoconsplus.hu> website and subpages (hereinafter: "Website") in order to give the users and visitors of the Website (hereinafter: "Data Subject" or "Data Subjects") adequate, detailed information about the scope of data processed by the Service Provider, as well as the manner, objective and legal basis of data management as well as the enforcement of the constitutional principles of data protection, the enforcement of the requirements of data security, as well as the prevention of unauthorized access to the data of the data subjects and of modifications to and unauthorized disclosure or use of the data.

In terms of the above, the Service Provider declares that this Privacy Information has been written on the basis of and in compliance with the valid and effective privacy policy (hereinafter: "Policy"), and accordingly, the Service Provider processes personal data in connection with the operation of the Website only on the basis of the content of this Information.

Relevant data protection legislation:

The material scope of the Information covers all processes implemented by the Service Provider during the operation of the Website when personal data are processed as defined in Subsection 2 of Section 3 of Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: Privacy Act).

In addition to the above, laws that are of particular importance in terms of this Information:

- Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (hereinafter "GDPR")
- The Constitution of Hungary
- Act V of 2013 on the Civil Code
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Privacy Act)
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services (especially Sections 13/A.-13/B.)
- Act C of 2003 on electronic infocommunication

Definition:

Data Subject: any natural person defined, identified or identifiable directly or indirectly on the basis of personal data;

Consent: any freely given, informed and specific indication of the Data Subject's will, by which the Data Subject gives unambiguous consent to the processing of personal data relating to him or her;

Personal data: Any data that can be associated with the Data Subject - especially the name or identification number of the data subject, as well as one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of the data subject, and conclusion about the data subject deductible from the data concerned;

Data Controller: the natural or legal person, as well as organization without legal entity which, alone or jointly with others, determines the purpose of the processing of data; makes and executes the decisions regarding data management (including the means used), or has them executed by the processor;

Data management: irrespective of the method used, any operation or all of the operations on the data, such as the collection, capturing, recording, organization, storing, modification, use, retrieval, transmission, disclosure, alignment or combination, restriction, erasure and destruction of the data, and the prevention of the further use of data, capturing photographic, sound and image records and recording physical properties (e.g. finger- or palm print, DNA sample, iris image) suitable for identifying a person;

Privacy Information

Data transmission: making the data available to specific third person data processors, especially the data processors specified (if any) by Service Provider,

Data processing: completion of data management operations and technical tasks, regardless of the method and means used to perform the operations and the place of application.

Disclosure: making the data available for anyone

Data erasure: making the data unrecognizable in such a way that its restoration is no longer possible;

Machine processing: it includes the following actions if they are implemented in whole or in part by automated tools: data storage, logical or arithmetic operations on the data, modifying or storing data, deleting, retrieving and distributing the data.

Cookie: A cookie is a small text file that is stored on the hard drive of the computer or mobile device and is activated upon subsequent visits. Websites use cookies to record information about visits (visited pages, time spent on our pages, browsing data, exits etc.) as well as personal settings, but these are data that cannot be associated with the Data Subject. This tool supports the establishment of the user-friendly website in order to enhance the online experience of the Data Subjects. Most of the web browsers automatically accept cookies, but Data Subjects can delete or disable them. Since all browsers are different, Data Subjects can set their cookie preferences with the toolbar of the browser individually. If the Data Subject does not wish to enable any cookies from the visited websites, he or she can modify the web browser settings to get notifications about the cookies sent, or can simply disable all cookies, or only cookies sent by specific websites. Data Subjects can always delete cookies stored on their computer, notebook or mobile phone as well. More information about settings can be found in the Help section of the browser. If the Data Subject decides to disable cookies, he or she has to abandon some functions of the websites (e.g. the website does not remember that the Data Subject has remained logged in). There are two types of cookies: session cookies and persistent cookies.

Session cookies: they are stored on the computer, notebook or mobile only temporarily, until the Data Subject leaves the given website; these cookies help the system remember information while the Data Subject visits one page from another, so the Data Subject does not have to enter or fill in the specific information repeatedly.

Persistent cookies: They are stored on the computer, notebook or mobile even after the Data Subject has left the website. These cookies help the website recognize the Data Subject as a returning visitor – but it does not identify the Data Subject personally. Persistent cookies are stored on the computer or mobile of the Data Subject as files for a maximum of six (6) months.

Flash cookies Adobe Flash Player, which is used for running certain types of animated banners and various videos (youtube, vimeo), can store information on your computer, notebook or mobile. Accepting flash cookies cannot be set through the web browser. If the Data Subject does not want to enable Flash cookies, this shall be set on the Adobe website: www.adobe.com/privacy/cookies.html. If the Data Subject disables Flash cookies, it is possible that he or she may not use certain functions of the Website, e.g. videos in the articles may be displayed incorrectly.

System: All technical solutions operating the Website and services of the Data Controller available through the web (hereinafter: System).

In terms of other terms in this Information, interpretative definitions in Section 3 of the Privacy Act shall be understood.

Voluntary consent

The data subject visiting, using the website consents, by submitting the data, to the use and management of these data by the Service Provider for the purposes and during the period specified in this Information.

Service Provider manages the personal data of the natural person Data Subjects specified in the Policy and in this Information based on their voluntary, informed and specific consent pursuant to Subsection (1) of Section 5 of the Privacy Act, also into account the network security aspects, pursuant to Subsection (1) of Section 5 of the Privacy Act.

For the reason that personal data always get under the data management of Service Provider with the voluntary, informed and specific consent of the Data Subject, as regards the personal data of Data Subjects when the Data Subject is not identical with the person providing the relevant personal data, the Data Subject is responsible for the authenticity and manageability of the personal data, except if any bad faith of the Service Provider excluded this responsibility.

Purposes of data management

Service Provider declares to manage personal data only for exercising its rights or fulfilling its obligations. Service Provider shall not use the managed personal data for private purposes and the data management is always in compliance with the principle of purpose limitation – if the purpose of data management has ceased to exist or the management of data is otherwise unlawful, the data shall be erased.

The purpose of this Information is to ensure that the Service Provider informs the Data Subject in all cases about the purpose of data management as well as the legal basis for data management and all important information about data management.

Privacy Information

Service Provider may manage the data during the visit to and use of the Website for the following purposes.

- Ensuring the availability, view and use of the Website;
- Storing personal settings;
The system of the Service Provider identifies the Data Subject during the visit to and use of the Website with the help of normal cookies as an individual user to remember language preferences and login status.
- Anonymous statistical log;
During each visit, the Website's analytical software stores anonymous, normal cookies to find out how many people have visited the website and what contents and information Data Subjects are interested in. Service Provider stores all analytical information without name and uses them for technical as well as marketing purposes. For example, this way one can know how many visitors each subpage has on a monthly basis. Among the former, the name of the Data Subjects cannot be learnt and no profiling is carried out.
- Identifying anonymous and logged in visitors;
Websites use a cookie to determine if you are an anonymous or logged in visitor. If you are logged in, the website display a slightly different content compared to anonymous visitors. If this cookie is not present, or you disable it, the website understands it as if you were an anonymous visitor and the "login" function is not displayed. However, if the cookie is enabled, the website remembers that you have "logged in".
- The aims of using automatically recorded data are the assessment of the visitor data of the Website, the understanding of the needs of Data Subjects, statistics creation, the technical development of the IT system serving the Website, the protection of user rights;
The Service Provider measures the visitor data of the Website using the Google Analytics service. During the use of this service, non-personal data that are not suitable for identifying the Data Subject are transferred. Google's Privacy Policy can be found here: www.google.hu/policies/privacy
- Keeping contact with the Data Subjects and facilitating the flow of information;
On the Website, the Data Subject has the opportunity to contact with the Service Provider directly, when relevant contact data can be submitted by filling in a dedicated form. However, the Data Subject can submit the data upon accepting the data management regulation of the Service Provider also in terms of the information to be submitted; this can be done by checking a checkbox, otherwise the message cannot be sent.
Regarding the latter, the legal basis for data management is the consent of the data subject [Point a) of Subsection (1) of Section 5 as well as Subsection (6) of Section 6 of the Privacy Act), pursuant to which "in other cases opened at the data subject's request, as regards the personal data he has supplied, the data subject's consent shall be deemed to have been granted".

The legal basis for data management

Service Provider manages the personal data specified in the Policy and this Information pursuant to **Subsection (1) of Section 5 as well as Subsection (5) of Section 6 of the Privacy Act**, based on the voluntary consent of natural person Data Subject, and taking into account network security aspects, for the performance of its legal obligations pursuant to **Subsection (1) of Section 6 to the Privacy Act**, and in addition to the consent of the Data Subjects, pursuant to **Subsection (3) of Section 13/A of Act CVIII of 2001** on certain issues of electronic commerce and information society services as well as relevant laws.

That is, the Service Provider processes the data lawfully pursuant to the following points of Subsection (1) of Article 6 of Chapter II of the GDPR Regulation: a) *"the data subject has given consent to the processing of his or her personal data for one or more specific purposes"*; c) *"processing is necessary for compliance with a legal obligation to which the controller is subject"*; and f) *„processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

Scope of data managed by the Service Provider

The identification number, date, time, username and/or name, e-mail address, the IP address of the computer of the Data Subject or the unique network identification (Media Access Control, i.e. MAC address) of the smart device of the Data Subject, review, textual review, any additional personal data provided during direct contact.

If the Data Subject gives consent, the Service Provider may publish the following data: date, time, username and/or name, review and the review text.

Beyond the above, the Website may be accessed by anyone without revealing his or her identity and providing his or her personal data and can obtain information on the Website and its linked pages freely and without limitations. Non-personal

Privacy Information

information, statistical data are collected automatically by the Service Provider in a manner that is not suitable for identifying the Data Subjects, if required, in an anonymized or encrypted form regarding the visit to the Website. No information that is suitable for identification can be obtained from these data regarding the Data Subjects even indirectly, therefore data management in this respect does not fall under the Privacy Act.

The manner of data recording

The Service Provider receives and obtains the data of the Data Subjects pursuant to the Policy and this Information, based on their voluntary consent in each case. The Data Subject shall be responsible for the authenticity of the personal data submitted in all cases. Service Provider does not check the personal data submitted.

Viewing, visiting as well as using the Website by the Data Subject shall be understood – until the Data Subject makes a statement to the contrary – as the consent of the Data Subject for the management of the data of the Data Subject specified in this Information in accordance with the Policy and the Information.

Principles of data management

Personal data may only be obtained and processed in a fair and lawful manner.

Personal data may only be stored for specified and lawful purposes and may not be used otherwise.

The scope of the data managed shall be proportionate to the purpose of their storage and shall be in compliance with and may not extend beyond this purpose.

Appropriate security measures shall be taken to protect the personal data stored in automated data files against accidental or unlawful destruction or accidental loss as well as unlawful access, modification or dissemination.

Data transmission

Service Provider is entitled and obliged to transmit the available and lawfully stored personal data which shall be transmitted by law or binding regulatory obligation to the competent authorities. Service Provider shall not be responsible for the transmission of such data and the resulting consequences.

The Data Controller shall not transmit the personal data of the Data Subjects to a foreign third country - international organization (outside the European Union, to a non-EEA state), unless explicitly approved by the Data Subject and under the conditions set out in the written declaration by the Parties, by ensuring the guarantees as of the provisions of the GDPR. The former obligation does not cover the cases specified in Article 45 of the GDPR, based on which if the data transmission is targeted to a state and/or international organization about which a valid "decision on adequacy" issued by the Committee is in effect, no additional permission is required for such a data transmission. Upon the execution of this document, a decision on adequacy has been approved for the following third countries: Andorra, Argentina, Faroe Islands, Guernsey, Israel, Jersey, Canada, Isle of Man, Switzerland, Uruguay, USA (Privacy Shield), New Zealand – *for Japan and South Korea, the adequacy procedure is ongoing* –.

The security of data management

In accordance with the obligation as of Section 7 of the Privacy Act, Service Provider shall do its utmost to ensure the safety of the data of the Data Subject and takes the required technical and organizational measures and establishes procedural rules that are necessary for the enforcement of the Privacy Act as well as other data and secret protection rules.

Service Provider primarily manages data in the framework of machine processing – Website and server systems, the management of any data requiring human involvement may only take place in exceptional and justified cases.

The system serving the Website is physically located in the office under the ISZT INTERNET SERVICE PROVIDERS Network Coordination Center Nonprofit Limited Liability Company (1132 Budapest, Victor Hugo utca 18-22) on the server computer, this is where the data are physically managed and the data of the Data Subjects are stored.

The so-called cloud applications are also part of the system serving the Website. The Service Provider chooses its cloud service partners with the utmost care and takes all generally reasonable actions to conclude a contract in view of the data security interests of Data Subjects, to ensure that the data management principles of such partners are transparent and regularly checks data security. The data of the Data Subjects are stored in the cloud. Data Subject hereby explicitly consents to the data transmission required for using the cloud applications by acknowledging this Information.

Privacy Information

Service Provider protects the data especially against unauthorized access, modification, transmission, disclosure, erasure or destruction as well as accidental destruction and damage. The data recorded automatically, technically during the operation of the system(s) of the Service Provider shall be stored in the system after their generation for a period necessary for ensuring the operation of the System. Service Provider ensures that these automatically recorded data may not be associated with other personal data – with the exception of cases required by law. If the Data Subject has terminated his or consent to or objects to the management of his or her personal data, the Data Subject will not be identifiable based on the technical data – not including investigating authorities and their experts.

Links: It is possible that on the Website of the Service Provider there are references or links to pages maintained by other service providers, financial enterprises (including buttons for login and sharing opportunities, logos), where Service Provider has no influence on the practice of personal data management and where no data is shared/transmitted by Service Provider. Service Provider calls the attention of the Data Subjects that by clicking such links, they may be redirected to the pages of other service provider or financial enterprises. In such cases, Service Providers recommend that Data Subjects shall read the privacy rules on the use of such pages.

In such cases, employees performing data management at the organizational units of the Service Provider shall keep the personal data learnt as business secrets. For this purpose, our employees managing and having access to personal data have made a confidentiality statement. At the same time, employees of the Service Provider are also obliged separately and shall ensure during that work that unauthorized persons may not view the personal data. The storage and placement of personal data has been established so that unauthorized persons may not access, learn, change or destruct the personal data.

The prevailing managing director of the Service Provider determines the organization of data protection, the tasks and competencies relevant to data protection and related activities, specifies the person performing the control of the data management taking into account the specifics of Service Provider.

Based on Article 35 of the GDPR Regulation, the data management by the Service Provider in connection with the operation of the Website does not pose a high risk to the rights and freedoms of natural persons in view of the nature, scope, circumstances and purposes of data management, therefore it is not necessary to perform a data protection impact assessment.

Duration of data management

One hundred eighty (180) days after the Website was viewed;
Upon direct contact, until the case is settled (the purpose is achieved);
For session cookies, until the Data Subject leaves the Website.

In addition:

- As a general rule, until the purpose of data management is realized.
- Regarding rights and obligations related to a legal relationship, until their termination.
- Lastly, until the authorization by the Data Subject has been withdrawn and/or until the termination of the circumstance requiring data management or the failure of the purpose to be achieved with data management.
- Otherwise the Data Controller shall delete the managed data upon the request of the Data Subject, except for the data that shall be managed owing to a settlement dispute between the parties or other legal dispute – *until it is closed* – and/or due to a legislative requirement. Regarding a latter, the following shall be understood especially, but not exclusively:
 - Pursuant to Subsection (3) of Section 78, the data concerned shall be stored for 5 years
 - Pursuant to Subsection (1)-(2) of Section 169 of the Accounting Act, the data concerned shall be stored for 8 years
 - For a longer period of time, as provided by law.
- The Data Controller reserves the right to manage the relevant data to the extent necessary beyond the above deadlines until the deadline available for enforcing any justified claims based on the rights and obligations arising from the activity that gives cause for data management.

Source of data management

The managed data are directly recorded from the Data Subject.

In compliance with the obligation specified in Subsection (3) of Article 14 of Chapter III of the GDPR, if the personal data have not been obtained from the Data Subject – *especially if they have been provided by a registered user regarding the Data Subject*

Privacy Information

entitled to use the Service –, Data Controller shall notify the Data Subject without delay, but within one month at the latest through the contact details known – *if known, possibly via e-mail* – of the following:

- the identity and contact details of the Data Controller and the representative of the Data Controller – if any;
- the contact details of the data protection officer, if any;
- the purpose of the planned management of personal data and the legal basis for data management;
- categories of the personal data involved;
- recipients of the personal data and the categories of recipients, if any;
- where appropriate, the fact that the Data Controller wishes to transmit the personal data for a third country recipient or an international organization as well as the existence of the adequacy declaration of the Committee, or the absence thereof, or upon data transmission specified in Article 46, Article 47 or the second paragraph of Subsection (1) of Article 49 of the GDPR, the specification of appropriate and suitable guarantees as well as a reference to the methods for obtaining the copies thereof or to their availability.
- the duration of storing personal data, or if it is not possible, the relevant factors in determining this duration;
- if the data management is based on point f) of Subsection (1) of Article 6 of the GDPR, the legitimate interests of the data controller or third party;
- the right of the data subject to request access to as well as correction, erasure or restriction of the management of his or her personal data from the data controller, to object to the management of these personal data as well as the right of the data subject to data portability;
- upon data management based on point a) of Subsection (1) of Article 6 of the GDPR or point a) of Subsection (2) of Article 9 of the GDPR, the right to withdraw consent at any time without prejudice to the lawfulness of data management based on the consent prior to the withdrawal;
- the right to submit a complaint to a supervisory authority;
- the source of personal data, and if applicable, information on whether the data derive from publicly available sources;
- the fact of automated decision making mentioned in Subsections (1) and (4) of Article 22 of the GDPR as well as information available about the logic applied in such cases and the relevance and expected consequences of such data management on the data subject.

Possibility of the modification of the Information and the Policy

Service Provider reserves the right to unilaterally modify the Policy and this Information in the future. The new regulations are published on the Website.

Provision of information, right to object, data erasure, restriction of data management

The Data Subject may request information about the management of his or her personal data and may request the correction as well as erasure – except for data management required by law – of his or her personal data based on this Information and the Policy of the Service Provider, especially via the contact details specified on the Website.

Upon the request of the Data Subject submitted in e-mail, Service Provider informs the Data Subject about his or her personal data management, the purpose, legal basis and duration of the data management, the name, address (registered office) and data management-relevant activities of the data processor as well as the persons who receive or who have received the data and the purpose thereof. Service Provider shall provide the information in the shortest possible time after the request has been received, but within fifteen (15) days at the latest in writing, in a clear manner, free of charge – the Service Provider may charge a fee only in the case specified in Subsection (5) of Section 15 of the Privacy Act.

The information also covers the information specified in Subsection (1) of Section 15 of the Privacy Act, if the information provision to the data subject may not be refused by law.

Service Provider shall correct any personal data that are not true. The personal data shall be erased by the Service Provider if its management is against the law, if it is requested by the Data Subject – in this case, within a maximum of five (5) days –, if the data is incomplete or incorrect – and this cannot be corrected lawfully –, provided that erasure is not excluded by law, if the purpose of data management has ceased to exist, if the legally specified deadline for data management has expired, or if ordered by court or the Hungarian National Authority for Data Protection and Freedom of Information.

Service Provider shall notify the Data Subject and everyone to whom the data has been transmitted for the purpose of data management of the correction as well as erasure. The notification can be omitted if it does not violate the legitimate interest of the data subject with regard to the purpose of data management.

If the Data Subject uses personal data in an unlawful or misleading manner, or the Data Subject commits a criminal offence,

Privacy Information

Service Provider reserves the right to keep the relevant data upon such use as a proof to be used in a possible litigation or non-litigation procedure until the end of the procedure. The latter can also be applied if the Data Subject has requested the erasure of personal data in order to prevent or at least hinder the enforceability of the legitimate claim of the Service Provider.

The Data Subject may object to the management of his or her personal data pursuant to Subsection (2) of Section 21 of the Privacy Act, especially

- if the management or transmission of the personal data is exclusively required for the performance of a legal obligation of the Service Provider or the enforcement of the legitimate interest of the Service Provider, the data receiver or third person, except for mandatory data management;
- if the use or transfer of the personal data is carried out for the purpose of direct marketing purposes, polling or scientific research; and
- in other cases specified by law.

The Service Provider shall investigate the objection within the shortest possible time, but within fifteen (15) days at the latest, shall make a decision regarding the foundations thereof and informs the requestor about the decision in writing. The Service Provider shall suspend data management for the duration of investigation, for a maximum of five (5) days. If the objection is justified, the head of the organizational unit managing the data shall act in accordance with Subsection (3) of Section 21 of the Privacy Act.

If the Service Provider finds that the objection of the Data Subject is justified, it shall discontinue data processing – including any further data recording and data transmission–, shall lock the data, and shall notify everyone to whom the personal data involved in the objection have been transmitted of the objection and the measures taken, who shall take action in order to enforce the right to objection. If the Data Subject does not agree with the decision of the Data Controller, and if the Service Provider fails to meet the deadline, the Data Subject may apply to court within thirty (30) days from the information provision about the decision or the last day of the deadline.

The Service Provider shall reimburse any damage caused to others by the unlawful management of the data of the Data Subject or by the breach of the technical data protection requirements. The Service Provider shall be exempt from liability if it proves that the damage was caused by an unavoidable cause outside the scope of data management. The damage shall not be reimbursed if it was due to the intentional or negligent conduct of the injured party.

Information provision to the data subjects may be disregarded / rejected or restricted based on the provisions specified in Subsection (2) of Section 16 of the Privacy Act – for the reasons specified in Subsection (1) of Section 9 or Section 19 of the Privacy Act, with detailed justification –, if

- the Data Subject is already in possession of the information;
- the provision of the information concerned proves impossible or would require disproportionate effort, especially regarding data management for public interest archiving purposes, scientific or historical research purposes or statistical purposes taking into account the conditions and guarantees specified in Subsection (1) of Article 89 of the GDPR Regulation, or if the information provision obligation would make it impossible or seriously jeopardize the achievement of the purposes of such data management. In such cases, the Data Controller shall take appropriate measures – including the public disclosure of information – to protect the rights, freedoms and legitimate interests of the Data Subject;
- the acquisition or disclosure of data is expressly required by an EU or member state law applicable to the Data Controller on the appropriate measures for the protection of the legitimate interests of the data subject; or
- the personal data shall remain confidential based on a professional confidentiality obligation required by an EU or member state law, including statutory confidentiality obligation.

Otherwise, the Data Subject is entitled to get access to his or her personal data and the following information:

- The copy of personal data (fee for additional copies)
- The purposes of data management
- The categories of the data
- Data regarding automated decision making and profiling

Privacy Information

- Source-related information upon data receipt
- The recipients with whom the data have been or will be shared
- Information about data transmission to a third country, guarantees
- The duration and related aspects of storage
- Rights of the data subject
- Right to appeal to the authority

Manner of exercising the right to access: If the Data Subject submitted the request electronically, the information shall be provided in a widely used electronic format, unless requested by the Data Subject otherwise.

The right to request a copy may not adversely affect the rights and freedoms of others.

If the data controller has disclosed the data and shall erase it by taking reasonable measures taking into account the available technology and the costs of implementation in order to inform other data controllers regarding the erasure of the links, copies or duplicates concerned.

The Data Subject may not use the right of erasure and the right to be forgotten if the data management is required: for the freedom of expression, the performance of a legal obligation or the exercise of public authority, for public interest in the field of public health, public interest archiving, scientific and historical research purposes or the enforcement of legal claims

Service Provider shall restrict data management upon the request of the Data Subject if:

- the Data Subject disputes the accuracy of personal data
- the data management is against the law and the Data Subject objects to the deletion of data
- if the Service Provider no longer needs the personal data, but the Data Subject requires them for the submission, enforcement or protection of legal claims
- if the Data Subject has objected to data management and the Service Provider is still investigating the case.

Obligation to notify

Service Provider shall inform each recipient with whom the data have been shared about the correction, erasure or restriction. Except if this is impossible or requires disproportionate effort.

Data portability

The Data Subject is entitled to receive the data that he or she has made available to the Service Provider:

- in a structured, widely used, machine-readable format,
- is entitled to transfer them to another data controller,
- is entitled to request the direct transfer of data to another data controller –
- if it is technically feasible,

except for data management in public interest or for the purpose of exercising a public authority.

Possibilities of the enforcement of rights

Upon the breach of the rights of Data Subjects, they may enforce their rights against the Service Provider before the court of arbitration pursuant to the prevailing and effective general terms and conditions of the Service Provider, or – based on the provisions of the privacy Act and relevant legislation – may apply to the Hungarian National Authority for Data Protection and Freedom of Information (mailing address: 1534 Budapest, Pf.: 834; address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.). The court shall give priority to the case. I hereby accept and put this Information into force on this date.

Date: Kiskunmajsa, Sept. 08. 2021.

NeoCons Plus Korlátolt Felelősségű Társaság

NeoCons Plus Kft.
6120 Kiskunmajsa Csontos Károly u. 99.
120/1148/01310119-00100001
adószám: 23532452-2-03
Cg.: 03-09-135405

Zsolt Bódi
Managing Director