

Privacy Policy

The rights of the natural persons concerned
about the rules governing the management of their personal data
Regulation of the European Parliament and of the Council of 2016/679
as booked

The provisions of the GDPR will apply to issues not regulated here.

The full text of the Regulation is available here in your language:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

CHAPTER I

I. Scope of the Prospectus

1. The purpose of this Prospectus is to record Dr. Jenő Oláh as an individual lawyer (HU, 4028 Debrecen, Kassai út 129. II / 219, Debrecen Lawyer's lawyer's number: 547 / VIII, registration number: 0592, tax number: 50241532-2-29 Debrecen Lawyer's Chambers Code: 36066443 – here in after referred to as "Data Controller" and "Lawyer") and the Privacy Policy of the Attorney, which is recognized by the lawyer as a data controller.

2. This Prospectus contains the Principles for the Management of Personal Data provided by the Users on the Attorney's Website at www.drolahjeno-ugyved.hu.

3. In preparing the provisions of this Prospectus, the Attorney has taken particular account of the provisions of the European Parliament and Council Regulation 2016/679 ("General Data Protection Regulation" or "GDPR Regulation" or: Regulation), 2011 Law on Information Self-determination and Freedom of Information. CXII. ("Infotv."), Act V of 2013 on the Civil

Code ("Act"), and Act XLVIII of 2008 on the Fundamental Terms and Limitations of Commercial Advertising Activity. ("Grtv.").

II. Definitions: As defined in Article 4 of the GDPR Regulation.

(Full text of the GDPR Decree can be downloaded from the starting page of the website.)

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

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

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

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

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

(6) **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

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

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

(9) **‘recipient’** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 EN Official Journal of the European Union L 119/33 framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

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

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

(12) **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

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

(14) **‘biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

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

CHAPTER II

Name of the controller

Name: Dr. Oláh Jenő

Form of operation: other organization - individual attorney

Address: 4028 Debrecen, Kassai út 129. II / 219. .

Chambers of Commerce: Debreceni Bar Association

Chamber ID: CASS: 36066443

Tax number: 50241532-2-29

CHAPTER III

Name of processors

Provider IT Service Provider (Website, Hosting):

Gáspár György e.v.: 3508 Miskolc, Almáskert út 25. (EV51175474 asz: 68069137-1-25)

Credit card payment provider:

OTP Mobile Service Ltd., 1093 Budapest, Közraktár u. 30-32. Tax number: 24386106-2-43 e-mail: ugyfelszolgalat@simple.hu)

The accounting service provider:

INTERWORLD-2003 Trading & Service Deposit Company
4100 Berettyóújfalu, Kálvin tér 8. 1st em.
Company Registration Number: 09 06 012759
Tax number: 21841170-1-09

Postal service provider:

Hungarian Post Private Limited Company
Headquarters: 1138 Budapest, Dunavirág street 2-6.
Company Registration Number: Cg. 01-10-042463

Electronic Signature Service Provider in Business Registration Procedures:

Microsec Zrt.
1031 Budapest, Záhony street 7. D. ép
Tax number 23584497-2-41

Electronic delivery service provider using the "E-PER" -called system of the Ministry of Justice:

NISZ National Infocommunications Service Provider Private Limited Company
1081 Budapest, Csokonai u. 3.
Business Registration Number: 01 10 041633

CHAPTER IV

Ensuring the lawfulness of data management

1. Data management based on the consent of the person concerned

(1) In that case if the data subject has given consent to the processing of his or her personal data for one or more specific purposes when he or she appears at the lawyer's office - the consent of the person concerned to the processing of his or her personal information should be provided regard on the rules of referral laws and lawyer ethics.

(2) A consent shall also be given to the designation of a relevant box by the concerned recipient (customer, potential client, inquirer, etc.) when attending the Lawyer's website, when making use of information society services, and any other statement or action that

clearly indicates the consent of the person concerned in the context of his intended personal data management. Silence, the foreground square or non-action is therefore not a consent.

3. Contribution shall cover all data management activities for the same purpose or purposes. If data management serves multiple purposes at a time, the consent must be given for all data management purposes.

4. If the consent of the party concerned is provided in the context of a written statement that applies to other matters, such as the conclusion of a contract of sale or service, the request for consent must be presented in a clearly distinct manner from these other cases, in a clear and easily accessible form, with simple language. Any part of such a declaration containing the consent of the person concerned that violates the Decree shall not have binding force.

(5) A lawyer may not conclude a contract for the performance of a contract for the processing of personal data that is not required for performance of the contract unless otherwise provided by law.

(6) The withdrawal of consent should be allowed in the same simple way as the granting of the consent.

(7) If the personal data has been collected with the consent of the data subject, the data controller may handle the data recorded without the need for a different legal provision for the fulfillment of the legal obligation that he or she may have, without further special consent and withdrawal of the consent of the person concerned.

2. Data management based on the fulfillment of a legal obligation

(1) In the case of data processing based on a legal obligation, the provisions of the applicable law shall govern the scope of the manageable data, the purpose of data management, the length of the data storage, and the addressees.

(2) The data management based on the fulfillment of a legal obligation is independent of the consent of the party concerned, as data management is defined by law. In this case, the data controller must be informed prior to the processing of the data that the data is compulsory and that the data subject must be clearly and thoroughly informed about all the facts related to his or her data management, including the data and legal basis of data management, data handling and data processing, the duration of the data handling, if the personal data of the person concerned is handled by the data controller on the basis of the legal obligation that he or she is responsible for, and on who can know the data. The information should also include the rights and remedies available to the data subject in question. In the case of mandatory data handling, information may also be disclosed by making public the reference to the legal provisions containing the foregoing information.

3. Facilitating the exercise of data subject rights

The data controller must ensure that the rights of the data subject are exercised throughout the data management of the lawyer.

CHAPTER V

Visitor data management on the lawyer's website - information on the use of cookies

1. The web site visitor must be informed of the application of the cookies on the website and, with the exception of technically indispensable sessions (cookies), must be requested.

2. General information about cookies

2.1. Cookie is a data that the visited website sends to the visitor's browser (variable name value) to store it and later the same website can fill its contents. Cookies can be valid, valid until the browser closes, but for an unlimited period of time. Later on, all HTTP (S) requests will also send this information to the server. This changes the data on the user's machine.

2.2. The essence of the cookie is that by the very nature of the web site services you need to designate a user (eg entering the page) and can handle it accordingly. The risk lies in the fact that this user is not always aware of and may be able to follow the user from the web site operator or other service provider whose content is built into the site (such as Facebook, Google Analytics), resulting in a profile and in this case the contents of the cookie can be considered as personal information.

2.3. Types of Cookies:

2.3.1. Technically indispensable session (s): without which the page simply would not work functionally, they would be used to identify the user, it needs to be handled if you have entered what you did in the basket, etc. This typically stores a session-id; other data is stored on the server, making it safer. There is a security aspect when the session cookie value is not well generated, there is a risk of session hijacking, so it is imperative that these values are generated properly. Other terminology is called a session cookie for each cookie that is deleted at the time of exit from the browser (a session is a browser usage from start to exit).

2.3.2. Cooking Cookies: So you name cookies that comment on the user's choices, such as how you want the user to see the page. These types of cookies are essentially the setting data stored in the cookie.

2.3.3. Cooking Cookies: Although they do not have much to do with 'performance', they usually call cookies that gather information about the user's behavior, time spent, and clicks on the site they visit. These are typically third-party apps (such as Google Analytics, AdWords, or Yandex.ru cookies). They are suitable for profiling from the visitor.

Learn more about Google Analytics cookies here:

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

To learn more about Google AdWords cookies:

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

2.4. Accepting or enabling cookies is optional. You can reset your browser settings to reject all cookies or to indicate when a cookie is just being sent. Most browsers accept cookies automatically as default, but they can usually be changed to prevent automatic acceptance and offer options every time.

See the links below for the most popular browser cookie settings

- Google Chrome: <https://support.google.com/accounts/answer/61416?hl=en>
- Firefox: <https://support.mozilla.org/en/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn>
- Microsoft Internet Explorer 11: <http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies#ie=ie-11>
- Microsoft Internet Explorer 10: <http://windows.microsoft.com/en-US/internet-explorer/delete-manage-cookies#ie=ie-10-win-7>
- Microsoft Internet Explorer 9: <http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies#ie=ie-9>
- Microsoft Internet Explorer 8: <http://windows.microsoft.com/en-US/internet-explorer/delete-manage-cookies#ie=ie-8>
- Microsoft Edge: <http://windows.microsoft.com/en-us/windows-10/edge-privacy-faq>
- Safari: <https://support.apple.com/en-US/HT201265>

However, we also note that certain site features or services may not function properly without cookies.

3. Information about the cookies used on the website of the attorney's law and about the data generated during the visit.

3.1. The data system managed during the visit: The electronic system of our website may use the web site to record and manage the following information about the visitor and the device he / she browses:

- the IP address used by the visitor,
- browser type,
- features of the operating system of the device used for browsing (configured language)
- visit date,
- the visited (sub) page, feature or service.
- click.

These data are kept for up to 90 days and can be used primarily to test security incidents.

3.2. Cookies on the website

3.2.1. Technically indispensable sessions are sessions

The purpose of data management is to ensure the proper functioning of the website. These cookies are needed to allow visitors to browse the web site, seamlessly and fully utilize its features, services available through the website, including - in particular - a comment by a visitor on a particular site or the identity of a logged in user during a visit . The duration of this cookie's data management is limited to the visitor's current visit, this type of cookies will automatically be deleted from your computer when the session is completed or when the browser is closed.

The legal basis for this data management is the 2001 CVIII., On certain electronic commerce services and information society services. Law 13 / A. (3), according to which the service provider may treat the personal data necessary for the provision of the service for the purpose of providing the service technically indispensable for the provision of the service. If the other conditions are identical, the service provider must choose and always operate the tools used to provide the information society service in such a way that personal data is processed only if it is strictly necessary for the provision of the service and for the fulfillment of other purposes set out in this Act required, but in this case also to the extent and time required.

3.2.1. Cooking Cookies:

They note the user's choices, for example, in what form the user wants to see the page. These types of cookies are essentially the setting data stored in the cookie.

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

The purpose of the data management is to increase the efficiency of the service, increase user experience and make the use of the site more convenient.

This data is rather on the user's computer, the web site only accesses and recognizes the visitor (s).

3.2.2. Cooking Cookies:

Collect information about the user's behavior, time spent, and clicks on the site you visit.

These are typically third party applications (eg Google Analytics, AdWords).

Legal Basis for Data Management: Contribution of the Contributor.

The aim of the data management is to analyze the website and send the promotional offers.

CHAPTER VI Information on the rights of the person concerned

I. The rights of the person concerned briefly summarized:

1. To promote transparent communication, communication and the exercise of the relevant case law
2. Right to prior information - where personal data are collected from the data subject
3. Information to the person concerned and information to be made available if personal data are not obtained from the data controller
4. Right of access to the subject
5. Right to rectification
6. The right to cancel ("the right to be forgiven")
7. Right to Restrict Data Management
8. The obligation to notify you of correcting or deleting personal data or limiting your data handling
9. Right to data storage
10. Right to Protest
11. Automated decision-making in individual cases, including profiling
12. Restrictions
13. Informing the person concerned about the privacy incident
14. Right to complain to a supervisory authority (right to an administrative remedy)
15. Right to an effective remedy against a supervisory authority
16. Right to an effective remedy against data controller or data processor

II. Rights of the data subject in detail:

1. To promote transparent communication, communication and the exercise of the relevant case law

1.1. The data controller shall provide the data subject with all information and information on the management of personal data in a concise, transparent, comprehensible and easily accessible form, in a clear and unambiguous manner, in particular for any information addressed to children. The information shall be provided in writing or otherwise, including, where appropriate, the electronic path. Oral information may be provided at the request of the person concerned, provided that the identity of the person concerned has been verified otherwise.

1.2. The data controller must facilitate the exercise of the rights of the data subject.

1.3. The data controller shall inform the data subject of undue delay, but in any event within one month of the receipt of the request, of the measures taken on his or her application for the exercise of his rights. This time limit may be extended by two additional months under the terms of the Regulation. to which the person concerned should be informed.

1.4. If the data controller fails to take measures in response to his request, he shall inform the data subject without delay and within one month of the receipt of the request for reasons of non-action and whether he or she may file a complaint with a supervisory authority and exercise his right of judicial redress.

1.5. The data controller provides information and action about the information and rights of the user free of charge, but fees may be charged in the cases described in the Regulation.

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

2. Right to prior information - where personal data are collected from the data subject

2.1. The person concerned has the right to be informed about the facts and information related to data management prior to commencing the processing of data. In this context, the person concerned should be informed:

- (a) the identity and contact details of the data controller and his representative,
- b) contact details of the Data Protection Officer (if any),
- (c) the purpose of the planned treatment of personal data and the legal basis for data processing,
- d) in the case of data handling based on the validation of a legitimate interest, on the legitimate interests of the data controller or third party,
- (e) the addressees of personal data with whom personal data are communicated, and the categories of recipients, if any;
- (e) where applicable, the fact that the data controller wishes to transmit personal data to a third country or an international organization.

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

- (a) the duration of the storage of personal data or, where this is not possible, the criteria for determining that period;

- (b) the right of the data subject to request the data controller to access, correct, delete or restrict the personal data relating to the data subject, and object to the handling of such personal data and the right to the data concerned to be covered;
- (c) in the case of data handling based on the consent of the party concerned, the right to withdraw the consent at any time without prejudice to the lawfulness of the data processing carried out on the basis of the consent prior to the withdrawal;
- (d) the right to lodge a complaint addressed to the supervisory authority;
- e) whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for the conclusion of a contract and whether the data subject is obliged to provide personal data and the possible consequences of the lack of data provision;
- f) the fact of automated decision making, including profiling, something at least in these cases of the logic employed and the understandable information about how this data management is and what its consequences are likely to be.

2.3. If the data controller wishes to perform further data processing for personal purposes other than the purpose of their collection, he / she must inform the person concerned of this different purpose and any relevant additional information prior to further processing. The detailed rules for the right of prior information are contained in Article 13 of the Regulation.

3. Information to the person concerned and the information to be made available if personal data are not obtained from the data controller.

3.1. If the data controller has not obtained the personal data from the data subject, the data controller shall be kept by the data controller within no more than one month after the personal data has been obtained; where personal data are used for contact with the data subject, at least when contacting the person concerned; or if it is expected to communicate with other addressees, it must notify the facts and information referred to in paragraph 2 above, the categories of personal data concerned, the source of personal data and, where applicable, the fact that the data publicly available sources.

3.2. Further rules are set out in Section 2 (Right to Advance Advice). Detailed rules for this information are contained in Article 14 of the Regulation.

4. Right of access to the subject

4.1. The person concerned has the right to be informed by the data controller about whether his personal data is being processed and, if such data is being processed, he has the right to personal information and to the 2-3. You will receive access to related information in this section. (Article 15 of the Regulation).

4.2. Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed about the corresponding guarantees provided for in Article 46 of the Regulation.

4.3. The data controller shall provide the data subject with a copy of the personal data subject to data handling. For additional copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. Detailed rules for the right of access to the subject are set out in Article 15 of the Order.

5. Right to make corrections

5.1. The data subject shall have the right to rectify any inaccurate personal data that he or she is entitled upon request by the Data Controller without undue delay.

5.2. Taking into account the purpose of data management, the person concerned has the right to request the addition of incomplete personal data, including by means of an additional declaration. These rules are contained in Article 16 of the Regulation.

6. The right to cancel ("the right to be forgotten")

6.1. The data subject shall have the right to delete personal data concerning him without undue delay, and the data controller shall be required to delete the personal data of the data subject without undue delay if: a) personal data are no longer needed for the purpose for which they are collected or otherwise treated; (b) the party concerned withdraws the consent of the data controller and does not have any other legal basis for data processing; (c) the data subject is objecting to data handling and has no prior legitimate reason for data handling; (d) the personal data has been unlawfully handled; (e) the provision of information society services offered directly to a child for the collection of personal data.

6.2. (B) the fulfilment of an obligation under the law of the Union or of a Member State applicable to the data controller or to carry out a task carried out in the exercise of public authority exercised in the public interest or in the exercise of a public authority delegated to the data controller (c) public interest in the field of public health; (d) for public interest archiving, for scientific and historical research purposes or for statistical purposes, provided that the right of revocation is likely to render impossible or seriously jeopardize this data management; (e) to submit, enforce or protect legal claims. Detailed rules on the right to cancel are set out in Article 17 of the Regulation.

7. Right to Restrict Data Management

7.1. In the case of limitation of data processing, such personal data may only be disclosed with the consent of the person concerned or the submission, validation or protection of legal claims or the protection of the rights of a natural or legal person in the interest of the Union or of an important public interest of a Member State.

7.2. The data subject is entitled to request that the Data Controller restricts the processing of data if one of the following conditions is met: a) the person concerned disputes the accuracy of the personal data; in this case the restriction concerns the period of time that the Data Controller can check the accuracy of the personal data (b) Data handling is illegal and the data subject is opposed to the deletion of the data and instead asks for their use restriction; (c) the Data Manager no longer needs personal data for data processing but the data subject requires them to submit, enforce or protect legal claims; or (d) the person concerned objected to data handling; in this case, the restriction applies to the duration of determining whether the data controller's legitimate reasons prevail over the legitimate grounds of the party concerned. The person concerned must be informed in advance of the discontinuation of the restriction of the data. The relevant rules are contained in Article 18 of the Regulation.

8. The obligation to notify about the correction or deletion of personal data or the limitation of data management

The data controller informs all recipients of all corrections, deletions or restrictions on data management with whom or with which personal information has been communicated, unless this proves impossible or requires disproportionate effort. At the request of the data subject, the data controller shall inform the addressees thereof. These rules are set out in Article 19 of the Regulation.

9. Right to Data Access

9.1. Subject to the conditions set out in this Decree, the data subject shall have the right to receive the personal information provided to him by a data controller in a fragmented, widely used machine-readable format and shall be entitled to transmit this data to another data controller without obstructing the the data controller that provided the personal data, if: (a) the processing of data is either a contribution or a contract; and (b) data management is carried out automated.

9.2. The person concerned may also request the direct transfer of personal data between data controllers.

9.3. The exercise of the right to data storage shall not be in breach of Article 17 of the Regulation (Right of Cancellation). The right to subsistence is not applicable in the event that the task of data processing is in the public interest or exercised in the exercise of its public authority powers conferred on the data controller

10. The right to protest

10.1 The person concerned has the right to object at any time to his / her personal data in the public interest for reasons of his or her own (Article 6 (1) (e)) or legitimate interest (Article 6 (f)), including profiling based on those provisions. In this case, the data controller may not process the personal data unless the data controller proves that the data processing is justified by compelling reasons of lawfulness that prevail over the interests, rights and freedoms of the data subject, or for the purpose of submitting, enforcing or protecting legal claims.

10.2. If your personal data is handled for direct business, the person is entitled to object at any time to the handling of personal data relating to that purpose, including profiling, if it is related to direct business acquisition. If the person objects to the handling of personal data for direct business purposes, the personal data can no longer be treated for this purpose.

10.3. These rights should be explicitly mentioned in the notice of first contact with the person at the latest at the latest, and the related information must be clearly identified and disclosed separately from any other information.

10.4. The right to protest can also be exercised by automated means based on technical specifications.

10.5. If the personal data are handled for scientific and historical research purposes or for statistical purposes, the data subject is entitled to object to the processing of personal data

relating to his / her own personal situation, unless it is necessary for the performance of a task for public interest purposes. The relevant rules are contained in the Article of the Regulation.

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

11.1. The data subject shall be entitled to exclude from the scope of any decision based solely on automated data management, including profiling, which would have a bearing on him or would have a significant effect on him.

11.2. This entitlement shall not apply if the decision is:

- (a) necessary for the conclusion or performance of the contract between the data subject and the data controller;
- (b) be made available to the data controller by means of Union or Member State law which also lays down appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; or
- c) is based on the express consent of the concerned party.

11.3. In the cases referred to in points (a) and (c), the data controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, including at least the right of the data subject to request human intervention, The rules are set out in Article 22 of the Regulation.

12. Restrictions

The EU or Member States' law applicable to a data controller or data processor may restrict the scope of rights and obligations (Articles 12 to 22, Article 34 and Article 5) by means of legislative measures if the restriction respects the essential content of fundamental rights and freedoms. The conditions for this restriction are laid down in Article 23 of the Regulation.

13. Informing the concerned about the privacy incident

13.1. If the privacy incident is likely to pose a high risk to the rights and freedoms of natural persons, the data controller must inform the data subject of the data protection incident without undue delay. This information must clearly and unambiguously describe the nature of the privacy incident and include at least the following: (a) the name and contact details of the Data Protection Officer or other contact person providing information, (c) the likely consequences of the data protection incident, d) measures taken or planned by the data controller to remedy a data protection incident, including measures to mitigate any adverse consequences resulting from the data protection incident, where applicable.

13.2. The data subject shall not be informed if any of the following conditions are met: (a) the data controller has implemented appropriate technical and organizational protection measures and applies those measures to data covered by the data protection incident, in particular measures such as the use of encryption - making the data unenforceable for unauthorized persons who have access to personal data; (b) after the data protection incident, the data controller has taken further measures to ensure that the high risk of the rights and freedoms of the person concerned is no longer likely to be realized (c) the provision of information would require a disproportionate effort. In such cases, the data subject shall be informed by means of publicly disclosed information or similar measures shall be taken to ensure that such information is equally effective. Further rules are set out in Article 34 of the Regulation.

14. Right to complain to the supervisory authority (right to appeal)

The person concerned has the right to complain to a supervisory authority, in particular in the Member State of habitual residence, place of work or suspected infringement if, in his / her opinion, the handling of personal data relating to it is in violation of the Regulation. The supervisory authority to which the complaint has been filed shall inform the client of the procedural developments in the complaint and of the outcome thereof, including the fact that the client is entitled to seek judicial redress. These rules are contained in Article 77 of the Regulation.

15. Right to an effective remedy against a supervisory authority

15.1. Without prejudice to other administrative or non-judicial remedies, all natural and legal persons are entitled to effective judicial remedies against the legally binding decision of the supervisory authority.

15.2. Without prejudice to other administrative or non-judicial remedies, all persons shall be entitled to an effective remedy if the competent supervisory authority does not address the complaint or within three months shall not inform the person concerned of the procedural developments or results of the complaint lodged.

15.3. The proceedings against the supervisory authority shall be instituted before the courts of the Member State in which the supervisory authority is situated.

15.4. If a decision is taken against the decision of the supervisory authority for which the Board has previously issued an opinion or has taken a decision under the unity mechanism, the supervisory authority shall send that opinion or decision to the court. This rule is contained in Article 78 of the Regulation.

16. Right to an effective remedy against data controller or data processor

16.1. Without prejudice to any available administrative or non-judicial remedies, including the right to complain to a supervisory authority, all concerned shall be entitled to an effective judicial remedy if it considers that their rights under this Regulation have been infringed as a result of the non-compliance of their personal data with this Regulation.

16.2. The data controller or processor shall be initiated before the court of the Member State in which the data controller or the processor is established. Such proceedings may also be instituted before the courts of the Member State in which the person concerned is habitually resident, unless the data controller or the data processor is a public authority of a Member State acting within the scope of his public authority.

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

Jenő Dr. Oláh is attorney at law