

## The controller information to the client of personal data subject to processing

pursuant to Article 13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as „GDPR”) and Section 19 et seq. of Act No. 18/2018 on personal data protection and amendments and supplements to certain laws, as amended by subsequent regulations (hereinafter referred to as the „Act”)

(hereinafter referred to as the „Information”)

---

The **DECENT Group a.s.** company, organization ID no.: 50 955 900, registered office: Rajska 15, 811 08 Bratislava, Slovak Republic, registered in the Commercial Register kept by the Bratislava I District Court, section Sa, entry no. 6614/B (hereinafter referred to as „Company” or „Controller”), (terms stated in this Information are defined in the General Business Terms and Conditions of the Controller published on the Controller’s Website, which regulate the rights and obligations of the Client and the Controller when using the Digital Proof Application),

informs its Clients about the protection of personal data pursuant to the Article 13 of the GDPR and Section 19 of the Act are as follows:

1. For the purposes of this Information, **the Client** shall mean a natural person registered within the Digital Proof Application with whom the Controller has a specific legal relationship related to the use of the Digital Proof Application based on a contractual relationship or the Controller’s legitimate interest.
2. For the purposes of this Information, **Clients** may include also Authors of documents (*natural persons who have created Files*) or persons authorized by companies (so called *Agencies*) who have stored File Hash on behalf of Authors within the Blockchain Database.
3. **The Digital Proof Application** is a software application used via the Controller’s website, which has been developed and used in order to obtain timestamps for objective confirmation of authorship in respect of individual stored Files. The Digital Proof Application allows a registered Client to save the Hash of any File in an invariable and transparent Blockchain Database in compliance with General Business Terms and Conditions and obtain a Certificate based on which the Client may declare, as the Author, that he/she had the File at the date of saving including File Content .
4. **Pursuant to the GDPR and the Act, the Controller acts toward the Client as the controller**, i.e. the person who specifies, alone or jointly with other persons, the purpose of and means for processing of Personal Data and processes Personal Data on their own behalf.
5. **The Controller process the following Personal Data of the Client:**

List of personal Data subject to processing	Purposes of personal data processing (Article 5(1) of the GDPR and Section 7 of the Act)	Legal basis for personal data processing (Article 6(1) of the GDPR and Section 13(1) of the Act)	Legal/contractual requirement/requirement conditioning conclusion of an agreement/obligation of the Data Subject to provide personal data/possible consequences of a failure to provide personal data (Article 6(1) of the GDPR and Section 13(1) of the Act)
---	---	---	--

<p><b>a. Registration data of the Client stored within the Digital Proof Application, in particular:</b></p> <p>i. <u>Compulsory data</u>: name, surname, date of birth, city, post code, and country of residence, e-mail address.</p> <p>ii. <u>Optional data</u>: middle name, place of birth, address, country, employer identification, profession, telephone number.</p>	<p>Registration and use of the Digital Proof Application services.</p>	<p>The personal data processing is necessary to perform the agreement to which the Client is a party or to implement a measure before entering into an agreement based on the Client's request (<i>Article 6(1)(b) of the GDPR and Section 13(1)(b) of the Act</i>).</p>	<p>The Controller's contractual requirement.</p> <p>A failure to provide personal data will result in the impossibility to identify the Client and thus the impossibility to conclude an agreement establishing the cooperation between the Client and the Controller.</p>
<p><b>b. Invoicing data, in particular:</b> Name, surname, city, post code, and country, telephone number</p>	<p>Entering into an agreement with the Client who orders the Digital Proof Application services subject to charges.</p>	<p>The personal data processing is necessary to perform the agreement to which the Client is a party or to implement a measure before entering into an agreement based on the Client's request (<i>Article 6(1)(b) of the GDPR and Section 13(1)(b) of the Act</i>) in connection with the obligation to process personal data under special legal regulations (<i>Article 6(1)(c) of the GDPR and Section 13(1)(c) of the Act</i>), accounting and tax regulations in particular.</p>	<p>The Controller's contractual requirement.</p> <p>A failure to provide personal data will result in the impossibility to identify the Client and thus the impossibility to conclude an agreement establishing the cooperation between the Client and the Controller.</p>
<p><b>c. Name, surname, and e-mail address for purposes of newsletter mailing</b></p>	<p>Nationwide mailing of commercial offers concerning products and services related to the Digital Proof Application.</p>	<p>The Controller's legitimate interest (<i>Article 6(1)(f) of the GDPR and Section 13(1)(f) of the Act</i>).</p>	<p>The Controller's legal entitlement.</p> <p>The Data Subject may unsubscribe from newsletters at any time.</p>

6. **Identification and contact data of the Controller** (*Article 13(1)(a) of the GDPR and Section 19(1)(a) of the Act*) are:

- a. Business name: **DECENT Group a.s.**
- b. Registered office: **Rajská 15, 811 08 Bratislava, Slovak Republic**
- c. Organization ID no.: **50 955 900**
- d. Registration: **Commercial Register kept by the District Court of Bratislava I, Section Sa, entry no. 6614/B**
- e. Contact data: **hello@digitalproof.io**

7. **Legitimate interests of the Controller or third-party legitimate interests where Personal Data is processed under Article 6(1)(f) of the GDPR and Section 13(1)(f) of the Act** (*Article 13(1)(d) of the GDPR and Section 19(1)(d) of the Act*):

Personal data (*processed for the purposes of newsletter mailing*) is processed based on the Controller's legitimate interest to contact Clients repeatedly to offer or update the Digital Proof Application services.

8. **Identification of the recipient or recipient category if any** (*Article 13(1)(e) of the GDPR and Section 19(1)(e) of the Act*):
  - a. An external co-worker of the Controller.
9. **Information about whether the Controller intends to transfer Personal Data to a third country or an international organization and identification of that third country or international organization** (*Article 13(1)(f) of the GDPR and Section 19(1)(f) of the Act*):

The Controller does not intend to carry out such transfers.
10. **The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period** (*Article 13(2)(a) of the GDPR and Section 19(2)(a) of the Act*):
  - a. the Personal Data under clause 3(a) of this Information: throughout the period of registration within the Digital Proof Application and 5 years after the end of the registration,
  - b. the Personal Data under clause 3(b) of this Information: throughout the term of the contractual relationship and then for the period set out in special legal regulations (*accounting regulations in particular*),
  - c. the Personal Data under clause 3(c) of this Information: throughout the period of registration within the Digital Proof Application and two years after the end of the registration.
11. The Controller does not erase the personal data of Clients collected for the purposes of provision of the Application services (*i.e. obtaining of a timestamp*) and stored within the Blockchain Database due to the fact that such data is necessary for **enforcement of legal claims of authors** under Article 17(3)(e) of the GDPR in conjunction with the provision of Section 23(4)(d) of Act no. 18/2018.
12. The Controller hereby informs Clients that upon use of the Digital Proof Application services and storage of a File Hash within the Blockchain Database, a Certificate is generated for the Client with all registration data provided by the Client.
13. Upon verification of the Verification File via the Verification Page, third persons (*i.e. the persons provided with a file or the Verification File*) will be provided with a Certificate containing the Author's personal data to the following extent:
  - a. name and surname,
  - b. year of birth,
  - c. address to the extent: city and country,
  - d. contact data to the extent: telephone number and e-mail address,
  - e. name of the company (*the company with which the Author is employed, for which the Author carries out business activities based on a contract, or which is owned by the Author*).
14. **The existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the Client or to object to processing as well as the right to data portability** (*Article 13(2)(b) of the GDPR and Section 19(2)(b) of the Act*):

The Client has the following rights in relation to the Controller:

- a. Right of access by the Client

The Client shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint to initiate proceedings pursuant to section 100 of the Act or the right to lodge a complaint with a supervisory authority pursuant to the Article 77 of the GDPR;

- Where the personal data are not collected from the data subject, any available information as to their source;
- The existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) GDPR and pursuant to Section 28 (1) and (4) of the Act and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Controller will provide a copy of the personal data that is being processed. Any additional copies requested by the Client may be charged by the Controller for an appropriate fee corresponding to the administrative costs. Where an application is submitted by electronic means, the information shall be provided in the commonly used electronic form, unless a different mean is requested.

Information must be provided immediately, not later than within 1 month. The Controller has the right to prolong the processing time of the application for another 2 months if the request is complex or frequent. However, the notification must be made within one month of the reason for the extension of the processing period.

In the case of an unjustified or too frequent request, the Controller has the right to charge a reasonable charge or to reject the application. It must explain the reason for the refusal and the right to refer the complaint to the supervisory authority.

b. Right to rectification

The Client shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the Client shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Information must be provided immediately, not later than within 1 month. The Controller has the right to prolong the processing time of the application for another 2 months if the request is complex or frequent. However, the notification must be made within one month of the reason for the extension of the processing period.

In the case of an unjustified or too frequent request, the Controller has the right to charge a reasonable charge or to reject the application. It must explain the reason for the refusal and the right to refer the complaint to the supervisory authority.

c. Right to erasure ('right to be forgotten') or right to restriction of processing

The Client shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- The Client are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- The Client withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- The Client objects to the processing and there are no overriding legitimate grounds for the processing, or the Client objects to the processing;
- The personal data have been unlawfully processed;
- The personal data have to be erased for compliance with a legal obligation under the GDPR, the Act, a special regulation or an international treaty binding on the Slovak Republic;
- The personal data have been collected in relation to the offer of information society services.

Previous two sentences shall not apply to the extent that processing is necessary:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation which requires processing by the GDPR, the Act, a special regulation or an international treaty binding on the Slovak Republic or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- For the establishment, exercise or defence of legal claims.

The Client shall have the right to obtain from the Controller restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the Client, for a period enabling the Controller to verify the accuracy of the personal data;
- The processing is unlawful and the Client opposes the erasure of the personal data and requests the restriction of their use instead;
- The Controller no longer needs the personal data for the purposes of the processing, but they are required by the Client for the establishment, exercise or defence of legal claims;
- The Client has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the Client.

Where processing has been restricted, such Client shall, with the exception of storage, only be processed with the Client's consent 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 reasons of important public interest.

d. Right to object

Where personal data are processed for direct marketing purposes, the Client shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the Client objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

e. Right to data portability

The Client shall have the right to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided, where:

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

The Controller has a data portability period of time of 1 month; it can be extended by 2 months if the portability is complicated. They must provide information about this and explain why the extension has occurred. In the event that the Controller does not take the steps required for data portability, they must inform the Client about the reasons and on their right to file a complaint with the supervisory authority.

15. **Right to withdraw consent to processing of personal data at any time** (*Article 13(2)(c) of the GDPR and Section 19(2)(c) of the Act*)

The Client shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

16. **The right to file an application under Section 100 of the Act or the right to lodge a complaint with a supervisory authority pursuant to the Article 77 of the GDPR** (*Article 13(2)(d) of the GDPR and Section 19(2)(d) of the Act*)

Without prejudice to any other administrative or judicial remedies, the Client shall have the right to lodge a complaint with the supervisory authority, in particular in the Member State of his usual residence, place of work or the alleged breach, if he considers that the processing of personal data it is contrary to the GDPR.

The Client has the right to file a petition for personal data protection with the Personal Data Protection Office. The purpose of the procedure is to determine whether the rights of natural persons have been violated in the processing of their personal data or a violation of the GDPR, the Actor a specific privacy policy has been breached and, if it is found to be inappropriate, to impose remedies or a fine for violation of the GDPR, Act or a special regulation for the protection of the Client.

The petition must include:

- a. Name, surname, correspondence address and signature of the petitioner,
- b. Identification of the subject against which the proposal is directed, including the name, surname, permanent address or name, registered office and identification number, if assigned,
- c. The subject of the proposal, indicating the rights to be violated in the processing of personal data,
- d. Evidence to support the claims made in the proposal,

- e. A copy of the document or other evidence of the exercise of the right under the law or a special regulation, if such a right is invoked by the Client, or a statement of reasons worthy of special consideration for the non-application of the right in question, if the application was filed by the Client.

A petition's template will be published at the Personal Data Protection Office's website (<https://dataprotection.gov.sk/uouu/en>).

17. **The existence of automated decision-making, including profiling** (*Article 13(2)(f) of the GDPR and Section 19(2)(f) of the Act*):

The Controller does not use automated decision-making or profiling.

In Bratislava, on 30th of August 2019

**DECENT Group a.s.**

Matej Michalko, Chairman of the Board