Consumer Agreement

PLEASE, READ THESE SERVICE AGREEMENTS, INCLUDING TERMS OF SERVICES, SERVICE ORDER FORM, INVOICE, SERVICE LEVEL AGREEMENT, AND THE DATA PROCESSING AGREEMENT THAT IS PART OF THIS SERVICE AGREEMENT, VERY CAREFULLY. BY DOWNLOADING, ACCESSING, OR USING THE "iDenfy" MATERIALS, CUSTOMER AGREES TO BE BOUND BY THIS GENERAL AGREEMENT AND ALL TERMS INCORPORATED BY REFERENCE. IF CUSTOMER DOES NOT AGREE TO ALL OF THE BELOW TERMS, OR IF YOU ARE NOT ENTITLED TO REPRESENT THE CUSTOMER, DO NOT USE THE "iDenfy" MATERIALS AND/OR SERVICES.

iDenfy (hereinafter referred to as the "Service Provider/iDenfy") and the client (details of the client shall be provided in the Service Order Form. The client, hereinafter referred to as the "Client/Service Recipient/Customer"), hereinafter collectively referred to as the Parties and individually as the Party, have entered into this agreement, hereinafter the Terms, Service Order Form, Invoice, Service Level Agreement, and the Data Processing Agreement shall be referred to as **the Agreement/Contract:**

Terms of services

The Terms of Services ("**Terms**") apply to your access to, and use of, the websites, mobile applications, software development kits, and other products and Services that have linked to these Terms offered by "iDenfy". These Terms do not alter in any way the terms or conditions of any other agreement you may have with "iDenfy" for products, services, or otherwise. If you are using the Services on behalf of any entity, you represent and warrant that you are authorised to accept these Terms on such entity's behalf and that such entity agrees to be responsible to us if you violate these Terms.

"iDenfy" reserves the right to change or modify these Terms at any time and in our sole discretion. If "iDenfy" makes changes to these Terms, we will provide notice of such changes, such as by providing notice through the Services or by updating the "Last Updated" date at the top of these Terms. Your continued use of the Services will confirm your acceptance of the revised Terms. We encourage you to frequently review the Terms to ensure that you understand the terms and conditions that apply to your use of the Services. If you do not agree to any amended Terms, you must stop using the Services.

Definitions

In this Agreement, including its preamble, these capitalized terms have the following meanings:

The Service	This means all the services selected by the Service Recipient as established and described in the Service Order Form and provided by the Service Provider either directly or indirectly
The Service Order Form	The form where the scope of selected Services and the pricing is described and added to this Contract as an annex. If the Service

	Recipient wishes to add more Services during the duration of this Contract, this form shall be modified by a separate agreement in writing, depending on the scope of selected Services
Development environment/period	Environment for any of the Services integration. This environment doesn't include a manual review service. The Development period shall in no case exceed 1 (one) month
Testing environment	Environment for identity verification service testing. This environment includes a manual review service
Inflation	means the Euro Area Inflation (HICP All Items Euro Area) as found on http://ec.europa.eu/eurostat/web/main/home (or such future replacement website as may be used by Eurostat)
Data Subject	identified or identifiable natural person[s]
Entity	Legal person
Intellectual Property	This means any and all patents, copyrights (including future copyrights), design rights, trademarks, service marks, domain names, trade secrets, know-how, database rights, and all other intellectual property rights, whether registered or unregistered, including applications for any of the foregoing and all rights of a similar nature which may exist anywhere in the world

Scope of services

Subject to the Service Recipient's compliance with the Terms, the Service Provider shall provide the Services to the Client with reasonable skill and care, including the Service levels set out in the Service Level Agreement. The specification of the Services shall be defined in the links provided in the Service Order Form

Scope and purpose of data processing

Data shall be processed based on this Agreement, and the Services selected, Data processor and Data Controller obligations, and other conditions related to the data processing are defined in the Data Processing Agreement.

Representations, obligations, and warranties of the Parties

The Service Provider acknowledges and assures that the Service Provider's employees and individuals recruited by the Service Provider on a different basis and engaged in Service provision will maintain the secrecy of data and information both in the presence of employment or civil relationships with the Service Provider and their absence due to the termination of such relationships.

The Service Provider acknowledges and assures that Services are performed in accordance with this Agreement and the instructions given by the Service Recipient to the Service Provider with regard to the Service provision.

The Service Provider has a valid insurance policy regarding cyber-security threats, which covers all the losses that could arise from possible cyber attacks on the Service Provider. The

terms, conditions, limits, and terms of the insurance shall be provided, and updates can be followed at the following link https://www.idenfy.com/cyber-insurance/.

The Service Recipient agrees to specify the Service Provider as the entity supplying the Services and indicating the Service Provider's name, logotype, or other identifying mark when rendering Services to the end users; and

The Service Recipient commits to provide permission for the Service Provider to use Service Recipient's name and logo for marketing purposes on the Service Provider's webpage or social media channels;

The Service Recipient must comply with all applicable laws and regulations with respect to its use of the Service and its activities under the Agreement;

Parties must notify each other in writing if there are any changes to any of its contact details;

Limitation of liability

In no event shall either Party have any liability to the other Party for any damages whatsoever, including but not limited to direct, indirect, special, incidental, punitive, or consequential damages, or damages based on lost profits, data, or use, however, caused and whether in contract, tort or under any other theory of liability, whether or not the Party has been advised of the possibility of such damages.

Both Parties shall indemnify and defend each other and their respective agents and contractors from and against any and all losses, damages, claims, liabilities, or expenses (including reasonable lawyer's fees) arising out of a claim brought by an end user or any other third party relating to the use of the Services, except to the extent caused by the indemnifying Party's negligence. The aggregate liability of either Party due to the above-mentioned exception shall in no case exceed the amount of fees paid to the Party in the 6 (six) month period immediately preceding the date on which the direct and only direct loss arises.

The Limitation of liability articles shall not apply to breaches of data protection regulations; the liability for such breaches is provided in the Data Processing Agreement.

Financial conditions

The price of Services consists of the price charged for each credit of selected Service multiplied by the number of the credits purchased. The total price of Services is subject to VAT and shall be provided in the Service Order Form and the Invoice.

The Service Recipient shall also pay a one-time set-up fee. The amount of the set-up fee shall be provided in the Service Order Form. This set-up fee includes 40 (forty) hours of the Service Provider's consultations during the implementation of the Services.

The Service Recipient commits to paying for the Services in accordance with the procedure established in the Service Order Form, Invoice, and this Agreement.

VAT invoices (hereinafter – the Invoice) shall be presented by the Service Provider to the

Service Recipient by sending an e-mail (given in the Service Order Form) after the Service Order Form has been signed by the Parties.

The price of Services shall be paid no later than 3 (three) calendar days after the Invoice is received. The Service Provider shall only provide the Services if the Invoice is paid up-front. The Invoice shall be an integral part of this Contract.

The Service Provider shall be entitled to annually increase its fees for the Service to adjust for Inflation to a maximum of last year's published Inflation or inflation in Lithuania, however in any case not higher than 10 % (ten percent) unless Parties have expressly agreed otherwise in writing. The fees for the Service shall only be increased after a notice in writing a month before the increase.

The Parties reach an agreement that when mutual settlement deadlines are violated, the Party that has failed to fulfill its obligations in a proper manner is obliged to pay the other Party a late payment fee of 0.02 % for each delayed day if the set amount is not paid on time. If the Service Recipient fails to pay any sum due to Service Provider and such sum remains unpaid for more than 5 (five) business days, Service Provider may immediately suspend all the Services provided to the Service Recipient without any additional notice to the Service Recipient until the unpaid amounts will be paid to the Service Provider in full. For the avoidance of doubt, suspension of the Services does not dismiss the Service Recipient from paying the owed amounts.

If the Service Receipt fails to pay any sum due to the Service Provider and such sum remains outstanding from the Invoice date for a further thirty (30) days, Service Provider may immediately terminate the Contract without any form of liability.

Validity and expiry of the agreement

This Contract shall become effective as of the date of signature and shall remain in effect for a period of 1 (one) year, commencing from the end of the Development period or until all of the Service credits have been used, whichever happens first.

The Parties reach an agreement that the term of this Agreement (as provided above) is automatically extended for the next calendar year if at least 14 (fourteen) days before the end of the period of time for which Services are supplied, none of the Parties expresses the wish to terminate the Agreement in writing. The number of such extensions of the Agreement is not subject to limitations.

Each Party is entitled to terminate the Agreement without any reason by sending a written notification to the other Party 90 (ninety) days in advance. If the Service Provider exercises its right to terminate the Agreement pursuant to this clause, the Service Recipient shall be entitled to a refund of the amount paid for any unused Service credits that remain, which shall be provided within 10 (ten) business days following the date of termination. However, if the Service Recipient exercises its right to terminate the Agreement pursuant to this clause, the Service Provider shall have no obligation to provide any refund.

Confidentiality and Intellectual property

Each party may be given access to confidential information from the other Party in order to perform its obligations under the Agreement. A Party's confidential information shall not be deemed to include information that:

- is or becomes publicly known other than through any act or omission of the receiving party;
- was in the other party's lawful possession before the disclosure;
- is lawfully disclosed to the receiving party by a third party without restriction on disclosure;
- is independently developed by the receiving party, which independent development can be shown by written evidence; or
- is required to be disclosed by law, by any court of competent jurisdiction, or by any regulatory or administrative body.

Each party shall hold the other Party's confidential information in confidence and, unless required by law, shall not make the other party's confidential information available for use for any purpose other than as needed to perform the terms of the Agreement.

Each party shall take all reasonable steps to ensure that the other party's confidential information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of the Agreement.

Each party shall take a backup of its own confidential information and shall not be responsible to the other party for any loss, destruction, alteration, or disclosure of confidential information.

The Service Provider is the owner or licensee of all Intellectual Property rights of the Services (except those Services where the Service Provider acts as an intermediary). These works are protected by copyright and other laws and treaties around the world. All such rights are reserved. Except as expressly set out in this Agreement, the Service Provider does not grant the Service Recipient any rights to or licenses in respect of the Service.

The "iDenfy" logo and any other "iDenfy" product or service names, logos, or slogans that may appear on the Services are trademarks of "iDenfy" and may not be copied, imitated, or used, in whole or in part, without the prior written permission of "iDenfy" or the applicable trademark holder. You may not use any metatags or other "hidden text" utilizing "iDenfy" or any other name, trademark, or product or service name of "iDenfy" without our prior written permission. In addition, the look and feel of the Services, including all page headers, custom graphics, button icons, and scripts, is the service mark, trademark, and/or trade dress of "iDenfy" and may not be copied, imitated or used, in whole or in part, without our prior written permission. All other trademarks, registered trademarks, product names, and company names or logos mentioned in the Services are the property of their respective owners. Reference to any products, services, processes, or other information by name, trademark, manufacturer, supplier, or otherwise does not constitute or imply endorsement, sponsorship, or recommendation by "iDenfy".

The Client shall not be entitled to use the Intellectual Property for any other purpose except for the purpose of this Agreement. In particular and without limitation, the Client shall have no right to copy, translate, reproduce, adapt, reverse engineer, decompile, disassemble, or create derivative works of the Intellectual property as permitted by applicable law. Further, the Client shall have no right to sell, rent, lease, transfer, assign, or sub-license the Services or its rights under this Agreement without the Service Provider's prior written consent.

Force majeure

The Party is not held responsible for the failure to fulfill or to partially fulfill any obligations under this Agreement if this failure has occurred as a result of exceptional circumstances that could not be envisaged, escaped, or eliminated by the Parties with the help of any measures (hereinafter referred to as Force Majeure Circumstances), for example, government decisions and acts that have affected the activities of the Parties, political unrest, strikes, declared and undeclared wars, other armed clashes, fires, floods, and other natural disasters. In such cases, the Parties extend the period established for the fulfillment of their obligations.

The party that requests for its release from responsibility is obliged to inform the other Party about Force Majeure Circumstances in writing within 3 (three) calendar days of the occurrence of such circumstances by providing evidence that it took all reasonable precautions and exerted all necessary efforts in order to reduce costs or negative consequences, and in addition, it shall notify the other party of the possible period for the fulfillment of their obligations. The notification is also required when the basis allowing the Party not to fulfill its obligations ceases to exist.

The basis for exempting the Party from responsibility comes into existence as soon as Force Majeure Circumstances emerge or if the notification has not been presented on time, as soon as the notification is presented. If the Party fails to send the notification or to inform the other Party on time, it is obliged to reimburse the other Party for damage sustained due to the fact that the notification was not presented on time or due to the fact that there was no notification.

Final conditions

Should a part or provision of this Agreement be recognized as invalid, the rest of the parts and provisions of this Agreement will remain valid in all respects.

The scope of Service shall be selected by the Service Recipient, and the Service Provider shall submit to the Service Recipient only the amount of information required by the Service Recipient. Therefore, the Service Provider shall not be liable for cases where the Service Recipient has not selected to verify mandatory information for its activities or has not collected all the information required for its activities.

The Parties agree that the rights and/or duties arising under this Agreement cannot be assigned to third parties without the prior approval of the Party.

This Agreement is concluded and shall be interpreted in accordance with the laws of the Republic of Lithuania.

The Parties reach an agreement that any dispute and/or claim arising from or in connection with this Agreement or arising from the breach, termination, and expiration of the Agreement will be resolved by negotiation.

If the Parties fail to settle the dispute through negotiations, it will be resolved in the courts of the Republic of Lithuania pursuant to the procedure established by the laws of the Republic of Lithuania.

Service Level Agreement

The Service Provider warrants that the Services provided by the Service Provider directly, and not as an intermediary, will be available to the Customer for at least 99.40% of the time during any given year of the term. The warranty excludes any downtime resulting from scheduled maintenance or repairs, as well as any downtime resulting from factors outside of the Service Provider's control, including but not limited to force majeure events, acts or omissions of third parties, or the Customer's own internet connectivity issues. The Service Provider's sole liability for any failure to meet this warranty shall be to use commercially reasonable efforts to restore the Services to their full functionality promptly.

The parties agree that the Service Level Agreement ("SLA") does not apply to any of the Services provided by the Service Provider when acting as an intermediary, and the availability and performance of such intermediary Services are subject to the terms and conditions of the third-party provider that provides those Services to the Service Provider. The Service Provider shall use reasonable commercial efforts to ensure that such intermediary Services are available to the Customer, but the Service Provider shall have no liability for any unavailability, interruption, or delay in the provision of such intermediary Services. The Customer acknowledges that any warranty, representation, or guarantee with respect to such intermediary Services is provided solely by the third-party provider and not by the Service Provider.

Service Provider’s regular working hours are 09:00 a.m. – 06:00 p.m., working days (GMT+3).
Consultations are provided free of charge by the Service Provider during the time of working hours (09:00 a.m. – 06:00 p.m., working days GMT+3):

- The Service Provider fulfills prevention work from 01:00 to 07:00 a.m. A service provider must inform customers about prevention work within 24 hours.
- The Service Provider undertakes obligations to inform a customer about any unauthorized login or attempt to connect to the service provider's systems immediately if login influences (or can influence) the fulfillment of suitable service performance on both Sides' commitments.
- The Service Provider undertakes obligations to present a report of the last month about the information on preventions and service malfunction (date, time, preventions, the date when malfunction ends, time a brief explanation).

Management of incidents and problems

The priority is established according to the level of influence and urgency of a problem or incident:

Priority	Characteristics
"High"	Malfunction of "iDenfy" services, due to which the system becomes malfunctioned, and it is impossible to carry out tasks. The service of specialists is necessary.
"Normal"	Mistake or breakdown that can determine the malfunction of the Client's technological process operation: however, permitting to use of the iDenfy services. Such a mistake does not change the Client's technological processes, and financial loss is insignificant. The following mistakes can occur: Mistake or breakdown in the process of sending e-mail reports about the iDenfy service; Mistake or breakdown limiting the usage of "Back Office"; Mistake or breakdown limiting communication with client's service or technical department; Other analogical mistakes and breakdowns;
"Low"	Mistake or breakdown that can determine a slight malfunction of the client's technological processes. Such malfunctions have no influence on iDenfy service and the review of results.

The time of reaction and order of breakdown elimination:

Priority	Time of reaction to client's application	Order of the process of breakdown elimination
"High"	30 minutes during working time or 2 hours during the off hours	Service Provider undertakes the obligation to work continuously till the elimination of a breakdown or alternative solution offer.
"Normal"	3 hours during working time	Service Provider undertakes the obligation to work continuously during working hours till the elimination of a breakdown.
"Low"	5 hours during working time	Service Provider undertakes the obligation to work continuously during working hours till the elimination of a breakdown.

Data Processing Agreement

between the Data Controller (Service Recipient) and the Data Processor (Service Provider)

THIS DATA PROCESSING AGREEMENT (herein defined as the “DPA”) entered into between Service Recipient (hereinafter "Company" /" Service Receipt" or/and "Data Controller") and Service Provider (hereinafter "Service Provider"/"iDenfy" or, "Data Processor");

SUBJECT MATTER:

In connection with the Terms, SLA, and the Service Order Form**,** certain Personal Data concerning Data Subjects (both as defined below) will be transferred from the Company to the Service Provider. **This DPA governs such transfers.**

The term Applicable Data Protection Law shall mean 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) and, to the extent applicable, the data protection or privacy laws of any other country in regard to Company.

The term Applicable Law shall mean any other EU or National State law with respect to the Personal Data Processed in respect of which the Data Controller or Data Processor is subject to.

Any capitalized terms not otherwise defined in this Data Processing Agreement shall have the meaning given to them in the Terms. Other terms used in this Data Processing Agreement that have meanings ascribed to them in the Applicable Data Protection law, including but not limited to "Processing," "Personal Data/Data," "Third Party," "Data Controller" and "Processor," shall carry the meanings set forth under Data Protection Law.

The details of the data processing (as well as the Personal Data covered) are specified in **Schedule 1 hereto.**

Terms

The parties agree that:

When the Service Provider process Personal Data subject to Applicable Data Protection Law under the performance of the Agreement, it will act in the role of Data Processor, and the Company will act in the role either as Data Controller or Data Processor.

Service Provider shall process Personal Data only for the purposes of carrying out their obligations arising under the Agreement.

The Data Controller shall give documented instructions to the Data Processor on how to process the Personal Data in any manner that may reasonably be required in order for the Service Provider to carry out the processing in compliance with this DPA and in compliance with Applicable Data Protection law.
The Data Controller shall refrain from providing instructions that are not in accordance with applicable laws, including Applicable Data Protection Law, and, in the event that such instructions are given, the Data Processor is entitled to resist carrying out such instructions.

The transfer details and Personal Data details are specified in Schedule 1. The parties agree that Schedule 1 may contain confidential business information which they will not disclose to Third Parties, except as required by Applicable Data Protection Law or in response to a competent regulatory or government agency, or as required by Applicable Law. The parties may execute additional annexes/schedules to cover additional transfers or may include multiple transfers in Schedule 1, which will be submitted to the Supervisory Authority if required.

This DPA shall continue for no less than the terms of the Contract.

The rights and obligations of the Parties with respect to each other under this Clause 1 shall survive any termination of the Agreement.

Regulatory compliance

To the extent required by Applicable law or Applicable Data Protection law:

The Data Processor shall cooperate with the Supervisory Authority in connection with any activities performed by the Data Processor (the Service Provider shall allow the Supervisory Authority to enter it's premises when required by Data Protection laws)

Service Provider shall provide reasonable assistance to Company with any DPIAs and prior consultation with Supervisory Authorities;

The Data Controller, its auditors, and the Supervisory Authority shall have effective access to data related to such activities, as well as effective access to the Service Provider's business premises;

Service Provider shall give prompt notice to the Company of any development that may have a material impact on Service Provider's ability to perform Services effectively under this DPA and Agreement and in compliance with Applicable Data Protection laws, Applicable laws, and regulatory requirements.

Obligations of the company as data controller

Company warrants and undertakes that:

The Personal Data, which will be transferred to Service Provider, has been collected, processed, and transferred in accordance with all Applicable Data Protection Laws.

It has used reasonable efforts to determine that the Service Provider is able to satisfy its legal obligations under this DPA.

It will respond to inquiries from Data Subjects and the Supervisory Authority concerning the processing of the Personal Data by the Data Controller unless the parties have agreed that the Service Provider will so respond, in which case the Data Controller will still respond to the extent reasonably possible and with the information reasonably available to it if Service Provider is unwilling or unable to respond. Responses will be made within a reasonable time and in accordance with the Applicable Data Protection Law.

It will make available, upon request, a copy of this DPA to Data Subjects who are relevant to the processing, the subject matter of this DPA, unless this DPA contains confidential information, in which case it may redact such information. The Data Controller shall abide by a decision of the Supervisory Authority regarding access to the full text of this DPA by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. Company shall also provide a copy of this DPA to the Supervisory Authority where required.

Obligations of the service provider as data processor

Service Provider warrants and undertakes that:

It will comply with all Applicable Laws, including Applicable Data Protection Laws, in its performance of this Agreement.

It will only Process the Personal Data on the documented instructions of the Data Controller. This DPA and Agreement. The Agreement constitutes the documented instructions

It shall immediately notify the Company if, according to its opinion, any instruction infringes this DPA or other Applicable Law, including Applicable Data Protection Law. Such notification will not constitute a general obligation on the part of the Service Provider to monitor or interpret the laws applicable to the Company, and such notification will not constitute legal advice to the Company.

It will not transfer Personal Data to a Third Country without the prior written approval of the Data Controller and only if the Third Country is recognized by the European Commission as providing an adequate level of protection for Personal Data, and if not, only transfer Personal Data under Standard Contractual Clauses (SCC) or to an organization that has adopted Binding Corporate Rules.

It will not appoint sub-processors to Process the Personal Data on its behalf if the Data Controller objects. Service Provider is authorized to engage the sub-processors and for the Data Processing activities described in Schedule 1. Service Provider shall inform Company of any additions or replacements of such sub-processors giving the Data Controller an opportunity to object to such changes. If Company timely sends the Service Provider a written objection notice detailing a reasonable ground for objection, the Parties will make a good-faith effort to resolve Data Controller's objection. In the absence of a resolution, Service Provider will make commercially reasonable efforts to provide the Data Controller with the same level of service described in the Agreement without using the sub-processor to process the Data Controller's, Personal Data. If Service Provider's efforts are not successful within a reasonable time, each Party may terminate the portion of the service which cannot be provided without the sub-processor, and the Company will be entitled to a pro-rated refund of the applicable service fees.

Once approved by the Data Controllers, sub-processors will only process the Personal Data on the documented instructions of the Data Controller, and the Data Processor will put in place a legal agreement in writing to govern the sub-processing with the same contractual obligations that Service Provider has under this DPA.

It will have in place appropriate technical and organizational measures, and all measures pursuant to Article 32 of the GDPR, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

It will have in place procedures so that any individual party it authorizes to have access to the Personal Data, including employees of the Service Provider, will respect and maintain the confidentiality and security of the Personal Data. It shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality. This

provision does not apply to persons authorized or required by law or regulation to have access to the Personal Data.

It will not disclose any Personal Data to a Third Party in any circumstances other than at the specific written request of the Data Controller unless such disclosure is necessary in order to fulfill the obligations of the Service Agreement or is required by Applicable Law, including Applicable Data Protection Law.

It will notify the Company of any request for information by the Supervisory Authority and will not disclose any Personal Data without the prior consent of the Data Controller.

It will notify the Company of any complaint, notice, or communication received which relates directly or indirectly to the processing of the Personal Data or other connected activities or which relates directly or indirectly to the compliance of the Data Processor and/or the Data Controller with relevant applicable law including Applicable Data Protection law.

Service Provider shall assist the Data Controller, whenever reasonably required, in so far as possible, to fulfill the Data Controller's obligation to respond to requests for exercising the Data Subject's rights as provided under Applicable Data Protection Law, and Service Provider will have the appropriate organizational and technical measures in place to deal with Data Subject requests.

It will give the Data Controller prompt notice of a Personal Data breach or a potential data breach once becoming aware of the same, and the Data Processor will cooperate with the Company in implementing any appropriate action concerning the breach or the potential breach as the case may be, including corrective actions.

It has no reason to believe, at the time of entering into this DPA, of the existence of any reason that would have a substantial adverse effect on the guarantees provided for under this DPA, and it will inform the Data Controller (which will pass such notification on to the Supervisory Authority where required) if it becomes aware of any such reason.

It will process the Personal Data for purposes described in Schedule 1 and has the legal authority to give the warranties and fulfill the undertakings set out in this DPA.

It will identify to Company a contact person within its organization authorized to respond to inquiries concerning the processing of the Personal Data and will cooperate in good faith with the Company, the Data Subject, and the Supervisory Authority concerning all such inquiries within a reasonable time.

Service Provider responsible Data protection officer direct e-mail: dpo@idenfy.com.

It will be capable of demonstrating its compliance with the obligations of Applicable Data Protection law.

Audit

Upon reasonable request of the Company, the Service Provider will submit it, and/or as appropriate, its sub-processors will submit data processing facilities, data files, and

documentation used for processing, reviewing, auditing, and/or certifying by Company (or any independent or impartial inspection agents or auditors, selected by Company and not reasonably objected to by Service Provider) to ascertain compliance with the warranties and undertakings in this DPA, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Data Controller. If the Company acts as Data Processor, it shall only access Personal Data when instructed so by the Data Controller for the purpose of an audit.

Liability and indemnity

Service Provider will not be liable for any claim brought by a Data Subject arising from any action by Service Provider to the extent that such action resulted directly from the Data Controller's instructions.

Except as provided for in the clause above, Service Provider shall indemnify the Company for any monetary fine or penalty imposed on the Company by the Supervisory Authority that results from the Service Provider's breach of its obligations under this DPA if they will be proved.

In the event that any claim is brought against the Company by a Data Subject arising from any action by Service Provider, to the extent that such action did not result directly from the Data Controller's instructions, Service Provider shall indemnify and keep indemnified and defend at its own expense Company against all costs, claims, damages or expenses incurred by Company or for which Company may become liable due to any failure by Service Provider or its directors, officers, employees, agents or contractors to comply with any of its obligations under this DPA.

In the event that any claim is brought against Service Provider by a Data Subject arising from any action or omission by Service Provider to the extent that such action or omission resulted directly from the Data Controller's instructions, Company shall indemnify and keep indemnified and defend at its own expense Service Provider against all costs, claims, damages or expenses incurred by Service Provider for which the Service Provider may become liable due to any failure by the Data Controller or its directors, officers, employees, agents or contractors to comply with any of its obligations under this DPA.

Either party will provide the other party with evidence of financial resources to confirm it has sufficient such resources to fulfill its responsibilities under Limitation and Indemnity clauses as appropriate (which may include proof of insurance cover).

Law applicable to this agreement

This DPA shall, in all respects, be governed by and interpreted in accordance with the laws of the Agreement.

Resolution of disputes with data subjects or the supervisory authority

In the event of a dispute or claim brought by a Data Subject or the Supervisory Authority concerning the processing of the Personal Data against either or both of the parties, the

parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or the Supervisory Authority. If they participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation, or other dispute resolution proceedings developed for data protection disputes.

Termination

In the event that either the Service Provider or the Company is in breach of its obligations under this DPA, then either Service Provider or the Company may temporarily suspend the transfer of Personal Data to the Service Provider until the breach is repaired or the Agreement is terminated.

In the event that:

- The transfer of Personal Data to the Service Provider has been temporarily suspended by the Company for longer than one month due to the breach of the DPA;
- Compliance by the Company with this DPA would put it in breach of its legal or regulatory obligations in the country of import;
- Service Provider or Company is in substantial or persistent breach of any warranties or undertakings given by it under this DPA;
- A final decision against which no further appeal is possible of a competent court or of the Supervisory Authority rules that there has been a breach of this DPA by the Company or Service Provider, Or
- A petition is presented for the administration or winding up of the Company, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Processor is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs, then the Company, without prejudice to any other rights which it may have against Service Provider, shall be entitled to terminate this DPA, in which case the Supervisory Authority shall be informed where required.

The parties agree that the termination of this DPA at any time, in any circumstances, and for whatever reason (except for termination under Clause above) does not exempt them from the obligations and/or conditions under this DPA as regards the processing of the Personal Data transferred.

Upon the termination of this DPA, the Data Controller's written request, or upon fulfilment of all purposes agreed in the context of the Agreement termination or any part of the Agreement whereby no further processing is required, the Service Provider shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies after an agreed time between Controller and Processor The only exception to this shall be where Service Provider shall have a legitimate reason, which is confirmed by the Company, to continue to process particular data or where it is

legally required to maintain a copy according to Applicable Data Protection Law or Applicable Law.

Variation of this DPA

The parties may not modify this DPA except to update any information in **Schedule 1**, in which case they will inform the Supervisory Authority where required. Any update shall be approved by the Data Controller before being applied. This does not preclude the parties from adding additional commercial clauses where required and does not affect the Service Agreement between the Company and the Service Provider. In cases where any conflict arises in the interpretation of these agreements, this DPA shall take precedence.

Brexit

To the extent necessary, the Parties agree to cooperate in good faith and to execute all necessary documents to ensure that the Services can be delivered irrespective of the effect that Brexit may have on the treatment of personal data. Such documents may include but are not limited to, standard contractual clauses relating to transfers of Personal Data outside the EU and power of attorneys giving the Data Processor the right to, on behalf of the Data Controller, sign standard contractual clauses with any sub-processor on the Data Controller's behalf. All documents will be modified after the ICO or European Commission publishes UK SCCs or similar.

Sub-processors (schedule 1)

Sub-processor / System managed	**Tasks to be done by the sub-processor**
Amazon AWS Dublin	Servers and datacenters
Google Ireland Limited	Machine learning algorithms for data processing

Categories of data subjects and personal data

Shall be established in the Service Order form, depending on the Services selected.

Data Retention periods

Shall be established in the Service Order form.

Data breach notification by the processor (schedule 2)

NOTIFICATION IS TO BE MADE BY THE PROCESSOR'S DATA PROTECTION OFFICER TO THE CONTROLLER'S DATA PROTECTION OFFICER OR RELEVANT EMPLOYEE.

Notification will be made by email and/or phone call.

Notification will be sent not later than 4 hours after the incident is registered in Service Provider Information Security Management System - Incident Report Log.

Data Processor will Assign the responsible Data Controller's employee (DPO) to the program to investigate the incident and continuously collect all the necessary information from the incident point (Processor's employee).

Security controls (schedule 3)

Description of the technical and organisational security measures which has to be followed by the Data processor and data processors sub-processors (Third Party Security Controls).

For the purposes of this Exhibit, the "Service Provider" means Service Provider or Data Processor.

For the purposes of this Exhibit, the "Service Provider" means Service Provider or Data Processor.

(An 'X' in any square below means: the mentioned Activity will be secured by the highest level of Data Classification. A blank square means the applicable technical measure Activity is not required for the applicable Data Classification.)

Activity 3.2 Policies and Training	**Public**	**Internal**	**Restricted**	**Secret**
Information Security and Privacy Polices and standards must be formalised and documented, reviewed at least every one year, and updated as needed.		X	X	X
Personnel must be required to sign a document or electronic acknowledgment indicating their understanding of, and agreement to abide by, all policies and standards at least annually.			X	X
Training and awareness activities must be conducted to heighten workforce understanding of the importance of data security. The Service Provider must document existence of and participation in training and awareness activities.		X	X	X
3.3 Human Resources				

Where permissible by law, all Services Personnel must clear screening and/or background checks (i.e., employment verification, professional references, academic/professional credentials) prior to handling Company data.			
b. The Service Provider shall ensure any subcontractor, business partner, or other Services Personnel involved in performing the services or who have access to Company data comply with the applicable Company Information Security requirements defined within this Exhibit and will provide evidence of compliance upon request.	X	X	X
3.4 System Authentication and Authorisation			
All users of information systems must be given a unique User Account and password.	X	X	X
The use of a User Account by multiple individuals is prohibited.	X	X	X
Sharing of User Account passwords is prohibited.	X	X	X
The Service Provider must have controls in place to detect and prevent repetitive “brute force” attempts and temporarily suspend the involved end-user account.		X	X
There must be a password policy available for Company review, which requires all of the following (i., through iii.):			
At least eight (8) characters in length.	X	X	X
At least two (2) complexity controls (e.g., uppercase letter, number, special character).	X	X	X
NOTE: if the required complexity cannot be achieved, a minimum password length of fifteen (15) characters is adequate mitigating control.			
Change at least every 180 days without the reuse of the previous six (6) passwords.	X	X	X
System and Service Accounts (e.g., operating system, application) must	X	X	X

have default passwords changed prior to Operational Use.			
Entities having access to Company data and resources must be appropriately identified. Access to a System, Service, or Shared Accounts by an individual must be accountable to that individual.	X	X	X
Embedded passwords (i.e., System Accounts, Service Accounts) must meet all of the following controls (i., through iii.):			
Be protected from unauthorised access and accidental disclosure.	X	X	X
Passwords must be changed in response to an event that creates exposure of the account password to unauthorised users	X	X	X
Have a complexity level requiring:	X	X	X
At least eight (8) characters in length.			
At least two (2) complexity controls (i.e., an uppercase letter, number, special character). NOTE: If the required complexity cannot be achieved, a minimum password length of fifteen (15) characters is adequate mitigating control.			
Change annually, without reuse of previous six (6) passwords			
Change the password in the event an individual's authorisation to use the account has been revoked.			
Credentials used for verification of identity or authentication must be encrypted at rest and in motion.	X	X	X
Third Parties must authorise and inventory devices that are owned or controlled by the Service Provider that access, process, or store Company data.		X	X
Access controls or other processes used to grant authorised access to Company data and Systems must be: 1) in place; 2) based on the Principle of Least Privilege access rights; and 3) role-based.	X	X	X
User access rights must be reviewed (i.e., recertification) based on the sensitivity of the information being accessed as follows:			

Privileged Users/Accounts	Not Required, unless regulatory requirement supersedes	Not Required, unless regulatory requirement supersedes	X (every 90 calendar days)	X (every 90 calendar days)
Standard Users/Accounts	Not Required, unless regulatory requirement supersedes	Not Required, unless regulatory requirement supersedes	X (every 12 months)	X (every 12 months)
When a Service Provider employee is terminated or otherwise ceases to provide services related to the Company, access must be terminated as follows:				
Effective access to Company data must be removed or disabled (e.g., disabling network access, remote connectivity).		X (72 hours)	X (48 hours)	X (48 hours)
User Accounts associated to an individual within an application or system that contains Company data must be deactivated or de-provisioned.		X (180 calendar days)	X (90 calendar days)	X (30 calendar days)
A process for an emergency, immediate removal of user access must exist.		X	X	X
Access, when a user is shifting departments/roles, must be reassessed within thirty (30) days of the user's job change completion.			X	X
Emergency access changes must be completed per a documented change control process.		X	X	X
3.5 Data Protection				
Company data in motion must be encrypted using industry-standard technologies.			X	X
Company data must be encrypted when at rest using industry-standard technologies.				X
A plan must be in place to address the secure return or destruction of Company data as part of contract termination.		X	X	X
All removable media with Company data must be encrypted using industry-standard technologies.			X	X

Company production data must be prevented from being used in non-production environments. If exceptions exist, sensitive information must be masked before use in non-production environments, and controls must be put in place to prevent the reintroduction of test data into production.		X	X
Devices that contain Company data must have screens that lock automatically after, at most, fifteen (5) minutes of inactivity.		X	X
Physical media containing Company data must be protected from unauthorised access during transport.		X	X
	(Sealed packaging)	(Locked container)	
Delivery tracking and signature are required for the transportation of physical media containing Company data.		X	X
3.6 Infrastructure Protection			
Standardised and current antivirus software or host-based intrusion prevention software must be deployed on all user systems. A standard policy must exist to ensure that systems containing Company data are actively scanned for malicious software.s	X	X	X
Antivirus software must be configured to prevent users from changing any settings or disabling the antivirus protection.	X	X	X
Firewall and content filtering logs must be created and saved for at least a 14-day period and be available for review in the event of an incident.		X	X
An Intrusion Detection/Prevention System must be in place, on all egress/ingress points to the internet, with active, automated alerts enabled and monitored.		X	X
Activity Event Logs recording important information security events related to Company data must be produced, retained, and reviewed in a risk-based manner as follows:			

The activity must be logged at a level of detail that maintains individual accountability for actions.			X	X
Log information must be protected against loss, tampering, and unauthorised access.			X	X
Identified vulnerabilities (e.g., patches, configuration) must be prioritised, based on a defined evaluation procedure, and remediated in an established timeframe.			X	X
Remote access to the Service Provider's network must have security controls in place to ensure authenticated and authorised access.		X	X	X
Wireless access points on the Service Provider's internal network must be encrypted and user authentication enabled in accordance with industry standards.		X	X	X
3.7 Incident Response				
A process must exist to establish, document, and annually assess for validity and effectiveness of an information security incident response plan.		X	X	X
A notification process must be in place to inform Company if the Service Provider experiences or suspects a Data Security Incident affecting Company data.		X	X	X
All reported Data Security Incidents must be documented by the Service Provider, and Company must be notified immediately and, in any event, no later than 24 hours upon discovery of a Data Security Incident involving Company data.	X	X	X	X
3.8 Physical Security				
Physical security and access control measures must be in place to ensure that only authorised personnel and visitors are allowed access, on a needed basis, to areas containing Company data.		X	X	X

Visitors must be escorted at all times in areas containing Company data. (e.g., data center).			X	X
Facilities containing Company data must be monitored (e.g., guard station, video recording, alarm service) for unauthorised access.			X	X
Auditing of physical access controls must occur once every twelve (12) months.			X	X
Access privileges, activity logs, and visitor logs must be reviewed for irregularities in a defined manner.			X	X
Physical security incidents must be documented and analysed with appropriate corrective actions implemented.			X	X
Ensure Company data is not viewable by personnel supporting non-Company systems in work areas performing Help Desk and/or Support services that are shared in support of other customers.			X	X
Physical security standards, policies, and procedures must be established, documented, and communicated to Service Provider Personnel.			X	X
Company data and computer access to Company data must not be left unsecured when an individual is away from their desk.			X	X
3.9 Disaster Recovery				
The Service Provider will develop and maintain appropriate Disaster Recovery Plans in alignment with Company business requirements specific to the solution.	X	X	X	X

Document History

- 2021-03-30 Document drafted and reviewed by Domantas Ciulde, CEO of UAB "iDenfy".
- 2021-04-01 Document assigned version is 1.0.0.
- 2021-04-01 Document reviewed and approved by Domantas Ciulde, CEO of UAB "iDenfy".
- 2022-01-05 Document updated.
- 2022-01-05 Document assigned version is 1.0.2.

- 2022-01-06 Document reviewed and approved by Domantas Ciulde, CEO of UAB "iDenfy".
- 2023-06-01 Document updated.
- 2023-06-12 Document assigned version is 1.0.3.
- 2023-06-12 Document reviewed and approved by Domantas Ciulde, CEO of UAB "iDenfy".
- 2023-06-13 Document updated.
- 2023-06-13 Document reviewed and approved by Domantas Ciulde, CEO of UAB "iDenfy".
- 2023-06-13 Document assigned version is 1.0.4.