

GlobalPass End-User Terms and Conditions

Last modified on 1 March 2022

GENERAL

1. These “GlobalPass End-User Terms and Conditions” (“Agreement”) governs your access to and use of the GlobalPass website and applications (collectively, the “Site”) and ID Verification Services (as defined below) offered on the Site. This is a legal agreement between you (the “Client”, “ID Verification User” or “you” or “your”) and GlobalPass AG (“GlobalPass”, “Service Provider”) which is an integral part of the Engagement Letter signed between you and GlobalPass.

When you registered, you either registered as an individual or as a company or other business organization. When registering, you provided information about yourself and/or an owner or principal of the business. You hereby represent and warrant that all information provided is true and correct and that you are authorized to act on behalf of the business and have authority to bind the business to this Agreement. The term “you” “your” and “ID Verification User” will mean you, the natural person, as well as the business.

When you register, we collect basic information such as your name, company name, location, email address, phone number and other information. We also may ask for a copy of an identity document such as a passport, national ID card or drivers’ license. You were also required to create a username and password to access the ID Verification Services. Any information you provided will be treated in accordance with our [Privacy Policy](#). Please also review our [Cookie Statement](#) to learn how this website uses cookies.

By checking the box on the registration page agreeing to these terms and conditions or by using the ID Verification Services, you are agreeing that you have read, understand, and agree to be bound by this Agreement.

If you do not agree or are unable to agree to be bound by this Agreement, do not use the ID Verification Services and exit the Site.

GlobalPass may modify this Agreement from time to time. When changes are made, GlobalPass will make the revised version available on this webpage and will indicate

the date that revisions were last made at the top of this page. Your use of the Site or the Services after such posting will constitute acceptance by you of such changes.

2. This Agreement is effective as of the date you first registered (the "Effective Date"). If you registered as a business entity, the ID Verification Services (as defined below) may also be utilized by Affiliates (as defined below) of the ID Verification User; provided that (i) the ID Verification User shall be the sole party responsible for making payments under this Agreement and (ii) the ID Verification User shall be responsible to GlobalPass for all Affiliates compliance with the terms and conditions of this Agreement. For purposes of this Agreement, the term "Affiliate" shall mean any entity in which the ID Verification User has direct or indirect ownership of greater than 50% of the voting shares of the relevant company.

3. As part of the ID Verification Services, GlobalPass grants to the ID Verification User a revocable, non-exclusive, non-transferable license to utilize the ID Verification Services for the lawful purposes and with consent (see "Permitted Purpose" and "User Consent"). This license allows the ID Verification User the right to submit data for verification through the ID Verification Services according to the Permitted Purpose (each submittal a "Transaction") to a maximum limit, as per separate agreement with the User.

Permitted Purpose - verifying an individual's identity, age or address information for lawful purposes of identity verification, fraud prevention or enforcement of laws designed to prevent money laundering but does not include determining a consumer's eligibility for credit or insurance for personal, family or household purposes, employment or a government license or benefit.

User Consent - ID Verification User agrees to obtain the appropriate, active, and informed consent from each individual consumer in accordance with all applicable laws for the collection, disclosure, and use of personal information prior to requesting any of the ID Verification Services. Additionally, a direct business need for the information in connection with a business transaction involving the consumer must exist. THE GLOBALPASS ID VERIFICATION SYSTEM MUST NOT BE USED FOR UNAUTHORISED USE.

4. The ID Verification User is responsible for:

- procuring any software or applications which it requires to use or view the ID Verification Services;
- the accuracy of the information input for the ID Verification Services; and
- assessing and setting the risk tolerance level according to its needs.

5. Subject to the terms of this Agreement, the parties agree to cooperate and provide reasonable assistance in joint marketing materials from time to time. No such

announcements shall be issued without both parties' prior written consent, such consent not to be unreasonably withheld or delayed.

6. Except as expressly set out herein, the ID Verification User will have no rights or interest with respect to the ID Verification Services. Nothing contained in this Agreement will constitute a license or grant of any rights to the ID Verification User with respect to any trademark, logo, service, mark, trade name, service name or patent.

PROVISION OF SERVICES

7. GlobalPass is providing electronic identity verification services ("ID Verification Services") to the ID Verification User pursuant to this Agreement. This Agreement shall remain in effect until terminated. ID Verification User or GlobalPass may terminate this Agreement, and/or suspend your access to the ID Verification Services, at any time.

8. The Client requests the Services via specified e-mail address.

9. Upon receiving the Client's request and the full information on the Customer needed for performing the Services, the Service Provider shall start performing the requested Services. The Service Provider shall render the Services within two (2) Business Days from the date when the Service Provider receives all the documents and the information needed to perform the Services and the fees for the Services. The timing for performing the Services may be reasonably extended if the process of verification of some or all of the information on a particular Customer turns to be significantly more complex than reasonably anticipated.

10. The Service Provider may engage to the Sub-Processors and/or other Sub-Processors for the provision of the Services and the Client hereby agrees to the same; provided that the Service Provider shall notify the Client in advance of the engagement of new sub-processors and their identity. Client may then object to Service Provider's use of a new sub-processor by notifying Service Provider in writing within ten (10) Business Days of the notification. In such event Service Provider will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Client. If Service Provider is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Client may terminate this Engagement Letter (and this Agreement) with respect only to those Services which cannot be provided by Service Provider without the use of new Sub-processors, by providing written notice to Service Provider.

11. After providing Service Provider with necessary information about the Customer, the Service Provider shall proceed with provision of the requested Services and verification shall be performed both automatically and manually by Service Provider's KYC analysts. The Result of the Services shall be provided to the Client in the form of a checklist reflecting the categories of the information on the Customer that was checked by the Service Provider upon the Client's request and the result of the process of verification (verified / not verified, confirmed / not confirmed, matching / not matching, Exact, Strong, Medium or Weak matches, etc.). The Client hereby confirms his Instructions to the Service Provider on the processes described in Schedule 1 to Appendix 1 and on the criteria and rules to be followed by Service Provider in the process of verification (including the content of the checklist) and issuance of the results thereof (i.e., verified/not verified or confirmed/not confirmed, matching / not matching, Exact, Strong, Medium or Weak matches, etc.) as hereby provided in Appendix 2. The Client may, subject to the Service Provider's acceptance, issue new or amend existing Instructions for the verification process. Service Provider undertakes not to contact Clients' Customers, including with regard to verification process.

12. When the Client required the Service Provider to transfer any documents or information on Client's Customers, the Service Provider shall proceed with such transfer in compliance with safety requirements established by applicable Data Protection Laws. The Service Provider shall keep the documents and / or information transferred to it in strict confidence and shall not transfer the received documents and / or information to any third parties, otherwise than provided herein, or use them for purposes other than those prescribed under this Engagement Letter (and this Agreement), without an explicit written authorization of the Client.

13. It shall be the Client's responsibility to determine whether the Services requested from the Service Provider are sufficient for the purpose of ensuring the Client's compliance with applicable anti-money laundering and countering the financing of terrorism regulation and, in particular, for the purpose of CDD. The Service Provider shall not provide to the Client (and nothing herein shall be construed as to constitute) any warranties or consultations in regard as to whether the requested Services suffice for the purpose of ensuring the Client's compliance with applicable anti-money laundering and countering the financing of terrorism regulation and, in particular, for acts the purpose of CDD.

14. The Service Provider only hereunder pursuant to the terms hereof and the Client's Instructions and to the extent and within the limits set by the Client, as the

15. Client represents that any Client's Instructions are and will at all times be in line with Applicable Laws.

16. Notwithstanding any type of Result provided by the Service Provider to the Client (whether positive, negative or otherwise) in respect of any Customer, it shall be the Client's responsibility to, and the Client shall in its sole and absolute discretion, determine whether it will establish or approve of any type of business relationship with such Customer.

17. The Service Provider represents to the Client that it makes all reasonable effort to ensure accurateness and completeness of the information provided to the Client as a Result of the provision of the Services, however, the Service Provider does not ensure that the Results of the Services and verified information including but not limited to information and / or documents of the Customer that is delivered to the Client is in all respects true, accurate and complete.

18. The Client shall not, without the prior written consent of the Service Provider reverse-engineer, reproduce, convert, modify, disassemble or decompile the Results (in any form) of the Services. For the sake of clarity, the Client must not distribute, market, re-license, sub-license, rent, lease, adapt, translate, enhance, modify, decompile, disassemble, reverse engineer, reproduce, create derivative works, or translate the whole or any part of the information included in the ID Verification Services, and must not merge the ID Verification Services into any other product or service without the prior written permission of the Service provider.

19. The Service Provider may, whether currently or in the future, have relationships with persons other than the Client, which persons may have interests, including adverse interests, with respect to the Client. The Service Provider will have no obligation to disclose such relationships or interests to the Client or to use such information on the Client's behalf.

20. The Service Provider confirms, and the Client expressly agrees that, given the nature of the Services, the sources of information collected to provide the Services, the development of the technical means used to provide the Services, the Services provided under the Engagement Letter or this Agreement do not guarantee accuracy of the Results of the Services (e.g., identification of the person, veracity of the document, etc.). The Parties confirm their common understanding that the Service Provider shall make reasonable efforts to render the Services specified in the contract properly but does not guarantee the accuracy of the result of the services in all cases of provision of the services.

21. The ID Verification Services are provided on the following terms:

- GlobalPass does not represent or warrant or guarantee that the databases used to provide the ID Verification Services are complete, accurate or correct and, accordingly, GlobalPass does not represent or warrant or guarantee that any information provided by GlobalPass to the ID Verification User as part of the ID Verification Services is complete, accurate or correct.

- Any information provided by GlobalPass to the ID Verification User as part of the ID Verification Services relies on the completeness, accuracy and correctness of data which is entered by the ID Verification User.
- The provision of the ID Verification Services by GlobalPass is contingent on data sources supplied by third parties, including government agencies, third-party suppliers of identity verification services and credit reference agencies. Those third parties may change or may, due to change in laws or other reasons, change their policies or services. Therefore, the provision and price of the ID Verification Services, and the Permitted Purpose, may be amended by GlobalPass (acting reasonably) where and to the limited and minimum extent required to comply with a change from a third-party supplier. Where possible, GlobalPass will provide ID Verification User at least 30 days' prior, written notice of such changes. If amendments in accordance with this clause (c) are not acceptable to ID Verification User (acting reasonably), the ID Verification User may cease their usage of the particular affected service.
- The ID Verification User hereby authorizes GlobalPass to engage the third parties described in clause 9(c), to provide the requested ID Verification Services. The ID Verification User agrees that GlobalPass may provide to such third parties any information necessary for the fulfilment of the ID Verification Services and GlobalPass may check the information provided by the ID Verification User against any databases supplied by such third parties for the purposes of performing the ID Verification Services.

COMPLIANCE WITH DATA PROTECTION LAWS

22. The Client and the Service Provider shall each, at their own cost, comply with all their obligations under the relevant rules, laws, regulations, directives and governmental requirements (the "Data Protection Laws") which are in effect, including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR") and Swiss Federal Data Protection Act („DPA“).

23. If GlobalPass processes EU Personal Data in the course of the provision or procurement of the ID Verification Services, the parties will abide by the requirements included in the EU Personal Data Schedule, attached as Schedule B, including notifying the data subject that their Personal Information will be transferred outside the European Economic Area ("EEA"), providing any other required information to the data subject, and offer the data subject the opportunity to object to the transfer.

24. The ID Verification User warrants and represents that it:

- will comply with all applicable laws and regulations, including but not limited to privacy and data protection laws;
- has all licenses, authorizations, consents and approvals necessary in order to perform its obligations under this Agreement;
- will maintain and enforce a privacy policy that at least complies with the [Swiss Federal Act on Data Protection](#) , and equivalent international legislation such as the GDPR).
- will only use the ID Verification Services for the Permitted Purpose and otherwise in accordance with the terms of this Agreement (including any obligations or restrictions set out in the Schedules);
- will comply with all requirements and additional obligations listed in paragraph 4, herein, including, where applicable, the implementation of consumer consent requirements and agreement to additional terms and conditions contained therein;
- will obtain the freely given specific and informed consent from the individual that is the subject of the ID Verification Services, in accordance with applicable laws;
- will utilize the ID Verification Services for its own purposes and will not forward, send or disseminate any data or information contained within the ID Verification Services to any other party (with the exception of any Affiliate of the ID Verification User, but only for such time as such ownership is held in the company); and
- will, upon request, provide all reasonable assistance to allow GlobalPass to monitor and audit the ID Verification User's compliance with this Agreement, and to otherwise enable GlobalPass to comply with its obligations to third parties (including but not limited to government departments and agencies).
- will not introduce any back door, drop dead device, time bomb, Trojan horse, virus, or worm (as such terms are commonly understood in the software industry) or any other code designed or intended to have, or capable of performing, any of the following functions: (i) disrupting, disabling, harming or otherwise impeding in any manner the operation of, or providing unauthorized access to, the ID Verification Services or GlobalPass's computer system or network; or (ii) damaging or destroying any data.

25. The Parties agree to be bound by provisions of Appendix 1 hereto for the purpose of Processing of Personal Data hereunder. The submission by the Client to the Service Provider of the request for the respective Services shall also be considered

as the Client's Instruction to the Service Provider to process the Personal Data as and to the extent prescribed by Appendix 1 hereof.

26. The Client undertakes to:

- (a) ensure that it always has, as a Data Controller, a proper and valid legal ground for Processing of the Personal Data hereunder (including, for avoidance of doubts, the Personal Data collected for the purpose of provision of the Services by the Service Provider); and specifically, that where a Customer's (or other Data Subject's) consent is required for the Processing of Personal Data (whether provided from the Client, and/or from the Customer on the Client's request, or to be collected from third party sources) as herein agreed, the Client will have obtained such consent conform to the Data Protection Laws;
- (b) ensure that at all times it complies with any other requirements imposed by Data Protection Laws on Data Controllers;
- (c) ensure, that the Instructions for the Processing of Personal Data, provided by the Client to the Service Provider under the Engagement Letter or this Agreement and throughout the term of validity hereof, shall be in compliance with Data Protection Laws;
- (d) protect the Personal Data or Results by making all reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information and communications technology measures) to prevent unauthorized or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Personal Data or Results, or other similar risks;
- (e) acting as Data Controller, must comply with its duties, under the Data Protection Laws, to notify Customers whether and how their personal data is being processed, the purpose of such Processing, categories of Personal Data being Processed, and any other parties involved in Processing (including the Processing by the Service Provider);
- (f) with the Service Provider assisting it, must enable Data Subjects to exercise their rights, such as subject access requests and requests for the rectification or erasure of personal data, and making objections to Processing;
- (g) be liable to Customers for the damage caused by processing which infringes the Data Protection Laws.

CONFIDENTIALITY

As used in this Agreement, "Confidential Information" means any information communicated by either party to the other party in the context of their business relationship (whether documented now or in the future or otherwise) and includes information regarding the ID Verification Services not generally known to the public, the identity of GlobalPass's data sources and vendors as well as any information relating to an identified or identifiable individual (including, without limitation, name, postal address, telephone number, date of birth, government identity card number, driver's license number, or any other unique identifier or one or more factors specific to the individual's physical, physiological, mental, economic or social identity, and whether confidential customer data or otherwise) provided by either party to the other ("Personal Information") and including user name and password information.

27. Notwithstanding the foregoing paragraph, a party may disclose Confidential Information:

- (a) to its Affiliates, the Agents of such Affiliates, its representatives in which case such party will inform such disclose of the terms of this Section 4 and will cause such disclose to comply with such terms as if it were bound by the provisions of this Agreement;
- (b) that (1) is in the public domain as of the Effective Date, or (2) enters the public domain after the Effective Date other than as a result of a breach of any duty of confidentiality by such party, its Affiliate or any Agent of the foregoing;
- (c) as required by law, or by a court or government agency of competent jurisdiction, or by the rules of any securities exchange, in which cases the party required to make such disclosure will promptly notify its counterparty of such requirement.

28. If, for any reason, GlobalPass is required to disclose any or all of its data vendors to ID Verification User, then ID Verification User agrees that it shall be prohibited from contacting or doing business with such data vendors, for the purpose of obtaining similar services as those provided through GlobalPass under this Agreement, at any time during the term of the Agreement and for a period of one (1) year after the termination of this Agreement.

29. Each party agrees that it will:

- not disclose, nor permit any person to disclose, to any other person or entity any Confidential Information except to those of its data vendors, directors, officers or employees with a strict need to know in order to perform the obligations under this Agreement. Such data vendors, directors, officers or employees shall be of the obligation of confidentiality hereunder and shall be subject confidentiality obligations at least as restrictive as those set forth in

this Agreement. Should either party be legally required to disclose Confidential Information, that party shall, unless prohibited by law, immediately notify the other party of such request or requirement for disclosure, and reasonably assist that party, prior to disclosure so that party may seek an appropriate protective order;

- protect the Confidential Information with the same degree of care it uses to safeguard its own information of a similar character, provided that such degree of care shall not be less than a reasonable degree of care implementing appropriate administrative, physical, technical and organizational measures, policies and procedures to protect Confidential Information against accidental or unlawful destruction or accidental loss, unauthorized alteration, disclosure or access, and other unlawful forms of processing;
- immediately notify the other party in writing if it suspects, has reason to believe or confirms that any Confidential Information is or has been lost, stolen, compromised, misused or used, accessed or acquired in an unauthorized manner or by any unauthorized person, or for any purpose other than legitimate business reasons;
- comply with all applicable privacy and data protection laws which may apply to the storage or transmission of any Confidential Information; and
- return or destroy Confidential Information to the other party within ten (10) days of notice from such party.

30. Except with respect to Personal Information, Confidential Information does not include information that is generally known to the public, information received in good faith from a third-party not subject to a confidential obligation to the source, or information that was independently developed by the recipient without the developing persons having access to or knowledge of the confidential information.

DURATION

31. Notwithstanding anything contained in the Engagement Letter or this Agreement and without prejudice to the other rights or powers under the Engagement Letter or this Agreement, a Party may terminate this Engagement Letter and Agreement with immediate effect by giving notice to the other Party (the “Defaulting Party”) upon any of the following:

- (a) if the Defaulting Party is in a serious breach of its contractual obligations set out of Engagement Letter or this Agreement;

- (b) if Defaulting Party goes into liquidation, whether compulsory or voluntarily;
- (c) if a petition is presented or an order is made for the appointment of an administrator in relation to the Defaulting Party or if an administrative receiver or judicial manager is appointed over any part of the assets of the Defaulting Party and such appointment is not revoked within 30 days from the date of such appointment; or
- (d) if the Defaulting Party makes a general assignment or any composition or arrangements with or for the benefit of its creditors.
- (e) Notwithstanding the foregoing sentence, the following provisions (the "Surviving Provisions") will survive termination for two (2) years from the Termination Date:
 - ("Indemnity");
 - ("Confidentiality");
 - ("Duration");
 - Miscellaneous provisions"); and
 - The definition of any defined term used but not defined in any Surviving Provision.

32. The Service Provider will retain the Results (including the Personal Data contained therein) in any form within the term of this Engagement Letter and 10 years after expiry of the Engagement Letter or this Agreement (unless retention period is modified by the applicable laws, rules, regulations or directives, including the Data Protection Laws, or an order of court or other competent institution or person). Without limitation of the foregoing, the Service Provider has a legal ground to retain the Personal Data and/or the Results where the Service Provider acts in the capacity of the data controller with regards to the Personal Data concerned or has other legal ground to retain the Personal Data (e.g., where the retention of the Personal Data and/or the Results are required for the defense against legal claims, where the Service Provider is required to retain the Personal Data and/or the Results under the applicable laws, etc.). The Client waives any of its claim rights and shall not be entitled to make any claims against the Service Provider with regards to the Services, the Results of which have not been retained by the Service Provider as a result of the requirements of the applicable laws or due to the actions of the Client.

33. At the termination of this Agreement and/or Engagement Letter, the Client can export and retain all Results (including the Personal Data contained therein) to its desired location in the supported format provided that the Client is not already in possession of the Results and the Personal Data (unless such retention is not supported by the applicable laws, rules, regulations, or directives, including the Data

Protection Laws, or an order of court or other competent institution or person). The Parties shall coordinate and agree on the implementation of the provisions hereof. The provisions of the present Section are without prejudice to the rights of the Service Provider.

MISCELLANEOUS PROVISIONS

34. GlobalPass, its contractors and sub-contractors, for the purposes of this Agreement, are not:

- a financial intermediary with the duty to report as set forth in Section 2, Article 9 (Duty to Report) by the [Swiss Federal Act on Combating Money Laundering and Terrorist Financing](#) (“**AMLA ACT**”) and as such do not have an obligation to retain any copies of an identification procedure as required under Article 7.
- a financial intermediary with the duty to report for the purposes of the requirement to retain copies of an identification procedure as required under Article 7 of the AMLA ACT.
- a financial intermediary with the duty to report as defined under Swiss cantonal and or federal laws;
- a Consumer Reporting Agency as defined by the U.S. Fair Credit Reporting Act 15 U.S.C. et seq (“**FCRA**”) and GlobalPass’s data or reports do not constitute “Consumer Reports” as that term is defined in the FCRA.

35. The ID Verification User must not distribute, market, re-license, sub-license, rent, lease, adapt, translate, enhance, modify, de-compile, disassemble, reverse engineer, reproduce, create derivative works or translate the whole or any part of the information included in the ID Verification Services, and must not merge the ID Verification Services into any other product or service without the prior written permission of GlobalPass.

36. In consideration of GlobalPass providing the ID Verification Services to the ID Verification User, the ID Verification User agrees to pay to GlobalPass the fees, which shall be set forth in separate agreement, including any related payment transmission fees or related bank charges. Unless otherwise expressly stated, all fees and charges referred to by separate agreement are exclusive of VAT. Payment will be made by charging your credit card on file. By providing credit card information or other payment method acceptable to GlobalPass, you represent and warrant that; i) the information provided is true and correct; ii) you are authorised to provide that information and to use the designated payment method; and iii) you authorise

GlobalPass (or GlobalPass's third-party payment processor) to charge your payment method for the total amount due. You agree to pay all credit card charges when due. You agree to pay all charges when due regardless of the number of transactions performed and regardless of the specific results or performance of the ID Verification Services.

37. Address for notices. Any notices delivered pursuant to this Agreement or Engagement Letter shall be delivered to the respective addresses of the parties indicated either in the beginning or in the signature block of this Engagement Letter.

38. Format of notices. A notice given under Agreement or Engagement Letter will be in writing in English and shall be:

- (a) Delivered personally, in which case it is deemed to have been received at the time of delivery;
- (b) Sent by prepaid first-class mail or recorded delivery, in which case it is deemed to have been received three Business Days after the date of posting, or, if the notice is served by mail from outside the country to which it is sent, sent by airmail, in which case it is deemed to have been received five Business Days after the date of posting; or
- (c) Sent by e-mail, in which case it is deemed to have been received at the time of delivery of such e-mail.

39. GlobalPass and its service providers will retain ownership of all intellectual property in the ID Verification Services (including any amendments, enhancements, modifications or updates of the ID Verification Services).

40. All documents referred to in this Agreement form part of this Agreement and may be amended from time to time by the parties in writing. Such amendments do not otherwise affect the rights and obligations howsoever under this Agreement.

41. This Agreement (including the Schedule and any other documents referred to in the Schedule or this Agreement) contains the entire Agreement between the parties and there are no other representations, promises or conditions.

42. This Agreement is governed by the laws of Switzerland. Both parties stipulate and agree that any litigation arising from or relating to this Agreement will be heard in a court of competent jurisdiction located in Zug, Switzerland.

LIST OF SUB-PROCESSORS

43. The Client hereby agrees to the use by the Service Provider of the following Sub-Processors for the Processing of Personal Data:

- (a) LexisNexis;
- (b) UAB Saulès sprendimai;

(c) Any other sub-processors as from time to time notified to the Client.

LIABILITY

44. IN NO EVENT WILL GLOBALPASS OR ITS REPRESENTATIVES, OR ANY DATA PROVIDER, BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES), ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT IN ANY MANNER, REGARDLESS OF THE FORM OF ACTION (INCLUDING STRICT LIABILITY OR NEGLIGENCE).

45. GLOBALPASS'S AGGREGATE LIABILITY DURING THE TERM FOR ANY OR ALL LOSSES OR INJURIES ARISING OUT OF ANY ACTS OR OMISSIONS UNDER THIS AGREEMENT WILL BE LIMITED TO A REFUND OF THE FEES PAID BY IDV USER UNDER THIS AGREEMENT DURING THE THREE (3) MONTH PERIOD IMMEDIATELY PRIOR TO THE OCCURRENCE OF THE FIRST EVENT GIVING RISE TO ALL OR PART OF THE LIABILITY.

45. Neither party will be liable for any delay or failure to perform its obligations under this Agreement if such delay is due to an act of God, fire, flood, earthquake, explosion, accident, acts of the public enemy, terrorist acts, war, rebellion, insurrection, sabotage, epidemic, quarantine restriction, transportation embargo, change of law or strike (each a "Force Majeure").

46. Notwithstanding any other term of this Agreement, GlobalPass accepts no liability for any inaccuracy, incompleteness or other error in any (i) inquiry information, (ii) other information, or (iii) data, provided by the ID Verification User to GlobalPass.

47. The ID Verification User will indemnify GlobalPass, its affiliates and agents from and against any and all claim, damages, losses, liabilities or fees arising in connection with any costs incurred as a result of a breach of any term of this Agreement by the ID Verification User.

48. The ID Verification User must not assign or transfer any rights or liabilities under this Agreement to any other person, except with written consent of GlobalPass.

49. The ID Verification User can contact GlobalPass at any time with questions or to cancel the ID Verification Services by sending an email to: support(at)globalpass.ch.

50. If any provision of this Agreement is found to be illegal or unenforceable by any court of competent jurisdiction then that provision will be deemed to be deleted, but without affecting the remaining provisions.

51. A failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence is not to be construed as a waiver of that party's rights under this Agreement.

52. GlobalPass may suspend the ID Verification Services or terminate this Agreement immediately, without further obligation to ID Verification User, in the event that (i) the ID Verification User commits a material breach of any of its obligations under this Agreement, (ii) for non-payment of services, or (iii) if there is a change of circumstances beyond GlobalPass's control which prevents GlobalPass from providing the ID Verification Services.

53. If a delay or failure of a party to perform its obligations is caused by, or anticipated because of, Force Majeure, the performance of that party's obligations will be suspended.

54. If a delay or failure by a party to perform its obligations because of Force Majeure exceeds 30 days, either party may immediately terminate this Agreement by giving written notice to the other party.

55. GlobalPass is not responsible:

- if the ID Verification User fails to use the ID Verification Services in accordance with the Permitted Purpose or any other term of this Agreement;
- if any equipment, browser, server or software utilised by the ID Verification User in accessing the ID Verification Services fails; or,
- for any damage to equipment, hardware, programs or data, whether stored or used with the ID Verification Services or otherwise, including the costs of repairing such equipment or hardware and the costs of recovering such programs or data.

56. To the extent permitted by law, other than to the extent expressly set out in this Agreement, GlobalPass makes no representations or warranties either express or implied:

- in relation to the suitability, quality, merchantability, performance or fitness for a particular purpose of the ID Verification Services;
- that the ID Verification Services will meet the ID Verification User's requirements;
- that the ID Verification User's use of the ID Verification Services will be uninterrupted or error-free or that any errors or defects in the ID Verification Services will be corrected; or
- regarding the interoperability, compatibility or coexistence of the ID Verification Services with the ID Verification User's operating system or particular network environment or hardware.

Schedule B - EU Personal Data Schedule

This EU Personal Data Schedule is only applicable if GlobalPass processes EU Personal Data in the course of the provision or procurement of the ID Verification Services. Capitalised terms used in this Schedule shall have the meaning ascribed to them in the Agreement including, without limitation, the definitions terms found in this EU Personal Data Schedule.

1. GlobalPass shall:

- process EU Personal Data in accordance with the ID Verification User's instructions as established in this Agreement or as provided in writing from time to time. Notwithstanding the foregoing, if GlobalPass is aware that such instructions are contrary to law, GlobalPass shall use reasonable efforts to inform the ID Verification User of the legal requirements prior to carrying out the processing, unless it is prohibited from doing so by law on important grounds of public interest;
- assist the ID Verification User, taking into account the nature of the processing and the information available to GlobalPass, in complying with the ID Verification User's obligations to respond to requests from individuals or supervisory authorities under applicable Data Protection Law, to the extent this is possible, or to carry out a data protection impact assessment;
- make available to the ID Verification User at the ID Verification User's request and cost all information necessary to demonstrate compliance with the obligations set out in this EU Personal Data Schedule and allow for any audits, including inspections, conducted by the ID Verification User or another auditor mandated by the ID Verification User, as requested by the ID Verification User on reasonable, legitimate grounds. Such audits shall be conducted no more than once per calendar year and at a mutually agreeable date and time;
- not provide EU Personal Data to any subcontractor utilised by GlobalPass to carry out data server hosting and other responsibilities on GlobalPass's behalf ("Subprocessor"), unless authorised, in writing, by the ID Verification User. The ID Verification User hereby authorises GlobalPass to engage such Subprocessors in the provision of the ID Verification Services. From 2 September 2019, GlobalPass will make available a list of Subprocessors if requested by ID Verification User in writing. GlobalPass can at any time at its discretion appoint a new Subprocessor provided that, from 2 September 2019, the ID Verification User is given fifteen (15) days' prior notice and does not object to such changes within that timeframe. If ID Verification User objects to such Subprocessor, it may terminate this Agreement on 30 (thirty) days'

written notice to GlobalPass. For the avoidance of doubt, notwithstanding this clause 1(d), GlobalPass may provide EU Personal Data to any third-party identity verification service provider acting as a data controller pursuant to GlobalPass's instructions under this Agreement to procure the ID Verification Services in accordance with clause 9(c);

- ensure that any Subprocessors to whom GlobalPass transfers EU Personal Data enter into written agreements with GlobalPass requiring that the Subprocessor abide by terms no less protective than those contained in this Agreement; and,
- For the purposes of this Agreement, "EU Personal Data" means Personal Information which is or has been subject to Data Protection Law and which has been provided by the ID Verification User to GlobalPass, together with the Personal Information which GlobalPass provides to ID Verification User confirming that it has matched a specific individual with a data source listed in 9(c) of this Agreement or 1(d) of this Schedule B. EU Personal Data does not include Personal Information which such a data source provides to GlobalPass on a general basis, irrespective of the ID Verification Services provided to ID Verification User. "Data Protection Law" means the European Directives 95/46 and 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation (EU) 2016/679) and the privacy and data protection laws of the European Economic Area, Switzerland and the United Kingdom (after it leaves the European Union), each as amended from time to time. The terms "process", "processing" "data controller" and "data subject" shall have the meanings accorded under applicable Data Protection Law. The subject-matter of the data processing under this EU Personal Data Schedule is the provision or procurement of the ID Verification Services and the processing will be carried out for as long as necessary to provide the ID Verification Services. Section 1 of this EU Personal Data Schedule sets out the nature and purpose of the processing, the types of EU Personal Data GlobalPass processes and the categories of data subjects whose personal data is processed.

2. This Clause 2 of EU Personal Data Schedule does not apply if the ID Verification User is located outside of the EU. GlobalPass agrees to comply with the obligations of a data importer as set out in the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission decision of 5 February 2010, published under document number C(2010) 593 2010/87/EU, or as updated thereafter (the "Standard

Contractual Clauses"). The ID Verification User agrees that it will be a data exporter under the Standard Contractual Clauses and will comply with the obligations imposed on data exporters. If the legal means by which adequate protection for the transfer is achieved ceases to be valid, GlobalPass will work with the ID Verification User to put in place an alternative solution. Each party's compliance with the Standard Contractual Clauses, as well as the provisions relating to data protection aspects for subprocessing, shall be governed by the law of the Member State in which the data exporter is established.

Section 1: Description of Personal Data Processing

The personal data transferred concern the following categories of data subjects:
Data subjects opening new accounts with the Customer

Categories of data

The personal data transferred concern the following categories of data:
Identifying information, such as contact details, date of birth, address, National ID, etc.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:
N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities:
For the provision of the ID Verification Services