PERSONAL DATA PROCESSING AGREEMENT

This Personal Data Processing Agreement is part of the Terms of Service concluded between you ("**Controller**") and Smartlook.com, s.r.o., Reg. no.: 09508830, with registered office at Šumavská 524/31, Veveří, 602 00 Brno, Czech Republic, registered in the Commercial Register administered by the Regional court in Brno under file No. C 119362 ("**Processor**"). This Agreement applies only to the extent to which Personal data are processed during your access to the Service, which depends solely on how you as a Controller setup the Service.

The Controller and the Processor are collectively referred to as the "**Parties**" and individually as a "**Party**".

The Parties hereto make this Agreement on Data Processing with the following content:

1. DEFINITIONS

1.1 For the purpose of this Agreement:

1.1.1 **Agreement** means this agreement and all underlying appendices.

1.1.2 **Data subject** means the identified or identifiable natural person to whom Personal data relates.

1.1.3 **GDPR** means the on the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

1.1.4 **Personal data** means any information relating to an identified or identifiable natural person as defined in the Article 4 of the GDPR, mainly any such information disclosed by the Controller to the Processor for purpose of Processing.

1.1.5 **Processing** or **Data processing** means any operation or set of operations which is performed on Personal data or on sets of Personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction as defined in the Article 4 of the GDPR.

1.1.6 **Security Breach** means any Personal data breach, which may potentially lead to accidental or unlawful destruction, alteration, unauthorised disclosure of, or access to, Personal data processed by the Processor for the Controller.

1.1.7 **Terms** means Terms of service available on the Processor´s website https://help.smartlook.com/en/articles/3244453-terms-of-service to which the Controller has agreed by accessing or using the services for which the Controller has signed up.

1.1.8 **Service** means worldwide, non-exclusive, non-transferable and time limited right to access and use Smartlook tools on a subscription basis in the form of Software as a Service (SaaS) provided by the Processor to the Controller as described in the Article 1.1. of the Terms.

1.1.9 **Data Retention Period** means a time frame for how long the data of the Controller, including Personal data, are stored by the Processor. Data Retention Period depends on the Service purchased by the Controller as further described in the Terms.

1.1.10 **Instructions** means any documented instructions issued by the Controller to the Processor in alignment with the Terms, this Agreement and the GDPR as to the nature, scope and method of Data processing.

2. Background and Purpose

2.1 The Parties have agreed to the provision of the Terms, which governs the Controller's limited, non-exclusive and terminable right to the use of the Service.

2.2 In this connection, the Processor processes Personal data on behalf of the Controller and by Controller's Instructions, and for that purpose the Parties have entered into this Agreement in accordance to the Article 28 of the GDPR.

2.3 The purpose of this Agreement is to ensure that the cooperation of the Processor and the Controller in the field of Processing of Personal data of Data subjects complies with the GDPR.

3. Appointment and Instructions

3.1 The Processor is authorised by the Controller to process Personal data disclosed to Processor by the Controller on behalf of the Controller on the terms and conditions set out in this Agreement.

3.2 The Processor may only process Personal data subject to the Instructions, including with regard to transfers of Personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 All Instructions shall comply with the GDPR and any other applicable law and the Processor reserves the right to refuse any Instruction noncompliant with the GDPR or any other applicable law or if such Instruction, in Processor's opinion, infringes the GDPR or other Union or Member State data protection provisions. In such case the Processor may postpone the execution of such an Instruction and shall immediately inform the Controller.

3.4 This Agreement, including appendices, constitutes the complete and final Instructions for the Processing of Personal data for purpose and in scope as set in this Agreement and in connection with the Service.

3.5 Any change of any Instruction shall be done by written and by both Parties signed amendment to this Agreement only. Before any changes are made to the Instructions, the Parties shall to the widest possible extent discuss and, if possible agree on, the implementation of the changes, including time and costs of implementation.

3.6 The Processor may process Personal data outside the scope of the Instructions in cases where required by EU law or national law to which the Processor is subject.

3.7 If Personal data are processed outside the scope of the Instructions, the Processor shall notify the Controller of the reason. The notification must be made before processing is carried out and must include a reference to the legal requirements forming the basis of the processing.

3.8 Notification should not be made if such notification would be contrary to EU law or national law.

3.9 By this Agreement Controller hereby appoints Processor to process Personal data disclosed to them by the Controller on behalf of the Controller in scope as is necessary to provide the Service or otherwise subsequently agreed to by the Parties in writing.

4. Duration

4.1 The Agreement applies until either (a) termination of the Agreement(s) on provision of the Service or (b) termination of this Agreement.

4.2 Regardless of the termination of the Agreement, clause 13 of the agreement regarding confidentiality as well as clauses 9, 10 and 11 will remain in force after termination of the Agreement.

5. Data Processing

5.1 The Processor shall process Personal data on behalf of the Controller solely for the purpose of providing the Service within the scope and for the purpose specified in Appendix 1 of this Agreement.

5.2 Subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects are specified in Appendix 1 of this Agreement.

5.3 Personal data of EU Data subjects processed on behalf of the Controller by the Processor will be processed within European Union, with the exception of certain server or technology infrastructure providers which the Processor is using to provide the Service. These providers are listed as sub-processors in Appendix 3 of this Agreement. Any sub-processors operating outside European Union process Personal data under EU Standard Contractual Clauses (SCCs).

5.4 All Personal data processed on behalf of the Controller by the Processor will be processed under appropriate technical and organisational security measures as specified in the Article 6.1. of this Agreement.

5.5 If a Data subject turns directly to the Processor to request the access, rectification, restriction, erasure or portability of Data Subject's Personal data, or if Data Subject objects to the Processing, or its right not to be subject to an automated individual decision making, the Processor shall forward such request to the Controller immediately.

5.6 The Processor shall not rectify, erase or restrict any Personal data processed on behalf of the Controller without documented Instruction of the Controller or unless Data Retention Period expires. The Processor shall not rectify, erase or restrict any Personal data processed on behalf of the Controller even if such Instruction is given in case any Union or Member State law requires storage of such Personal data.

5.7 The Processor shall not use any Personal data disclosed by the Controller for the Processing under this Agreement for any other purpose than specified in Appendix 1.

5.8 The Processor shall not disclose such Personal data to third parties, except sub-processors authorized by the Controller, specified in appendix 3 of this Agreement.

5.9 The Processor shall not make any copies or duplicate Personal data disclosed to them by the Controller without authorization of the Controller, except such copies or duplicates are part of backups described in the Terms or are required by the the GDPR or other Union or Member State law (i.e. statutory retention rules).

5.10 The Processor shall upon end of provision of the Service, fulfilment of contractual obligations as laid down in the Terms and this Agreement, or when requested by the Controller (mainly by the Instruction) delete all Personal data and delete existing copies unless Union or Member State law requires storage of the personal data.

5.11 The Processor shall not transfer Personal data to third countries or international organisations unless specifically stated in this Agreement.

5.12 The Processor has appointed a Data Protection Officer ("**DPO**"), who shall perform duties in compliance with the GDPR. The DPO can be contacted at dpo@smartlook.com.

6. Processor's Obligations

6.1 Technical and organisational security measures

6.1.1 The Processor has implemented necessary technical and organisational measures to ensure an appropriate security level. The measures must be implemented with due regard to the current state of the art, costs of implementation and the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity to the rights and freedoms of natural persons. The Processor shall take the category of Personal data described in appendix 1 into consideration in the determination of such measures.

6.1.2 Processor has implemented the technical and organisational security measures as specified in appendix 2 to this Agreement.

6.1.3 The Processor shall implement the suitable technical and organisational measures in such a manner that the processing by the Processor of Personal data meets the requirements of the applicable Personal data regulation.

6.1.4 Should the Processor implement any new technical or organizational security measures in the meaning of this Article, especially in connection with improvement and development of the Service, technical progress and development of technical and organizational security measures, changes in the organization of the Processor, changes in any applicable law etc., the specification in the appendix 2 will be updated if necessary. Any change in the technical or organizational security measures must not reduce the level of technical or organizational security measures as specified at the date of signature of this Agreement.

6.1.5 The Parties agree that the provided safeguards and all technical and organisational measures to ensure an appropriate security level of Personal data as specified in appendix 2 are adequate at the date of conclusion of this Agreement.

6.2 **Employee conditions**

6.2.1 The Processor shall ensure that employees who process Personal data for the Processor have undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

6.2.2 The Processor shall ensure that access to the Personal data is limited to those employees for whom it is necessary to process Personal data in order to meet the Processor´s obligations to the Controller under the Terms.

6.2.3 The Processor shall ensure that employees processing Personal data for the Processor only process such data in accordance with the Instructions.

6.3 **Documentation for compliance with obligations**

6.3.1 Upon written request, the Processor shall document to the Controller that the Processor:

a) meets its obligations under this Agreement and the Instructions.

b) meets the provisions of the GDPR, in respect of the Personal data processed on behalf of the Controller.

6.3.2 The Processor's documentation must be provided within reasonable time, but not later than within 30 days after receiving a written request.

6.4 **Records of processing activities**

6.4.1 The Processor shall maintain a record of the processing of Personal data.

6.4.2 The record must include the following information:

a) categories of processing carried out on behalf of the Controller;

b) a general description of technical and organisational measures in connection with the processing;

c) if relevant, specification of third countries or international organisations to which the personal data are transferred as well as documentation for appropriate safeguards;

d) contact details of the Processor's contact person and data protection officer.

6.4.3 Upon request, the Processor shall make the records available to the Controller or any relevant supervisory authority within reasonable time, but not later than within 60 days after receiving written request.

6.5 **Security breach**

6.5.1 The Processor shall notify the Controller of any Security Breach.

6.5.2 Security Breaches must be reported to the Controller without undue delay, but not later than within 48 hours from finding out Security Breach by the Processor. They must also be reported to the supervisory authority.

6.5.3 The Processor shall maintain a record of all Security Breaches. The record must as a minimum document the following:

a) the actual circumstances of the Security Breach;

b) the effects of the Security Breach; and

c) the remedial measures taken.

6.5.4 Upon written request, the record must be made available to the Controller or the supervisory authorities.

6.6 **Audits and Inspections**

6.6.1 The Processor allows for and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

6.6.2 Any audit or inspection by the Controller or auditor mandated by the Controller may be carried out by prior consultation with the Processor. In such consultation, duration, scope, subject and date and time of the respective audit or inspection must be mutually agreed. The Controller is obliged to send any request for an audit exclusively to the e-mail address of the Processor dpo@smartlook.com. If no agreement is reached even within 30 days from the date of receiving email according to this article, the Processor shall determine the terms of the audit.

6.6.3 The Processor may object in writing against any auditor who has been entrusted with the Controller, if the auditor is not sufficiently qualified in the opinion of the Processor, is not independent, is in a competitive position with the Processor or is otherwise obviously unsuitable. On the basis of the objection raised, the Controller is obliged to appoint another auditor or to carry out the audit themselves.

6.6.4 Due to the number of customers of the Processor, the Controller is entitled to carry out a maximum of 1 audit per year.

6.6.5 The right of audit or inspection stipulated in this Agreement does not extend to any facilities operated by sub-processors, sub-contractors or any third party, even if used in connection with providing the Service or Data Processing.

6.6.6 Any audit or inspection by the Controller or auditor mandated by the Controller may be carried out only to verify compliance of the Data Processing carried out by the Processor with this Agreement, the GDPR or other applicable law.

6.6.7 All information and documents disclosed by the Processor to the Controller in connection with audit or inspection are part of Processor’s trade secret and are subject to the confidentiality as stipulated in clause 13, if not stipulated otherwise. Such information and documents may be disclosed only to the authorized supervisory authority. The Controller shall ensure that any auditor it appoints is under an obligation of confidentiality in respect of any information it becomes aware of during the course of the audit.

6.6.8 All costs associated with the audit, including the work of the auditor or the cost of the Processor's workers, shall be borne by the Controller. Costs incurred by the Processor will be paid by the Controller within 14 days after the end of the audit based on an invoice issued by the Processor. The Processor shall have the right at its own discretion to request advance payment to cover related costs. The audit will not commence until the advance payment has been received.

6.7 **Assistance**

6.7.1 The Processor shall to the necessary and reasonable extent assist the Controller in the performance of its obligations in the processing of the Personal data covered by this Agreement, including in connection with:

a) responses to Data subjects on exercise of their rights, especially data subject's rights laid down in Chapter III of the GDPR;

b) ensuring compliance with the obligations of the Controller pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Processor;

c) Security Breaches;

d) impact assessments;

e) prior consultation of the supervisory authorities.

6.7.2 In this connection, the Processor shall obtain the information to be included in a notification to the supervisory authority provided that the Processor is best suited to do so.

6.7.3 The Processor is entitled to payment for time spent and materials consumed for assistance pursuant to clause 6.7.

6.7.4 Appropriate technical and organisational measures implemented by the Processor in order to assist the Controller with the fulfilment of their obligation to respond to requests for exercising the data subject's rights (right of access by the data subject, right to rectification, right to erasure, right to restriction of processing, right to data portability, Right to object and automated individual decision-making) laid down in Articles 15 to 22 of the GDPR are specified in appendix 2 of this Agreement.

7. Controller's Obligations

7.1 Lawfulness of processing

7.1.1 The Controller shall ensure and guarantees that during the whole duration of this Agreement:

a) all Personal data disclosed by the Controller to the Processor for Processing anyhow related to the Service were collected by legal and legitimate manners according to the GDPR, or any other applicable law;

b) consent of the Data Subject is given for Processing of the respective Personal data by the Processor, such consent is given freely and in accordance to the Article 7 of the GDPR and that the consent is valid for the whole time of Processing and was not withdrawn by the Data subject;

c) other conditions of lawful processing according to the Article 6 of the GDPR apply if consent of the Data Subject was not given;

d) no Personal data falling into the special category of Personal data as specified in the Article 9 of the GDPR were disclosed to the Processor.

7.1.2 In case any condition stipulated in the clause 7.1.1. is not met at any time of the Data Processing by the Processor or during the duration of this Agreement, Controller must notify the Processor in the most expedient time possible under the circumstances and without reasonable delay and, where feasible, not later than 72 hours after having become aware of such deficiency. The Controller must also exclude such Personal data from Processing by themselves (mainly by erasing such Personal data from the Controller's Service) and if not possible provide the Processor with all necessary assistance to exclude such Personal data from Processing.

7.1.3 In the event of a breach of any of the obligations set out in this Article 7, or of any other obligation of the Controller, the Controller is obliged to compensate the Processor for the damage caused to the Processor as a result of such breach of obligation, within 7 days upon the Processor's request by email.

7.1.4 The Controller shall indemnify and keep indemnified and defend at its expense the Processor against all costs, claims, damages, fines or expenses incurred by the Processor or for which the Processor may become liable in the event that the Controller does not obtain consent to the processing of Personal data in accordance with the Article 7.1.1 letter b) of this Agreement.

7.1.5 The Controller is solely responsible for its use of the Service, including backing up Personal data and securing accounts from which the Service is provided.

7.2 **Employee conditions and third parties**

7.2.1 The Controller shall ensure that employees who process Personal data and have access to the Service on behalf of the Controller have undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

7.2.2 The Controller shall ensure that any third party having access to the Service on behalf of the Controller undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

7.2.3 The Controller is fully liable to the Processor for the performance of any employee or third party to whom access to the Service is given by the Controller.

7.3 **Documentation for compliance with obligations**

7.3.1 Upon written request, the Controller shall document to the Processor that:

a) Controller meets its obligations under this Agreement and the Terms;

b) Controller meets the provisions of the GDPR or other applicable law, in respect of the Personal data disclosed to Processor;

c) Data Subject's consent is valid and was given for Processing of the respective Personal data by the Processor**,** such consent was given freely and in accordance to the Article 7 of the GDPR.

7.3.2 The Controller 's documentation must be provided within reasonable time.

7.4 **Security breach**

7.4.1 The Controller shall notify the Processor of any Security Breach.

7.4.2 Security Breaches must be reported to the Processor without undue delay.

7.4.3 The Controller shall maintain a record of all Security Breaches. The record must as a minimum document the following:

a) the actual circumstances of the Security Breach;

b) the effects of the Security Breach; and

c) the remedial measures taken.

7.4.4 Upon written request, the record must be made available to the Processor or the supervisory authorities.

7.5 **Assistance**

7.5.1 The Controller shall to the necessary and reasonable extent assist the Processor in the performance of its obligations in the processing of the Personal data covered by this Agreement, including in connection with:

a) responses to data subjects on exercise of their rights, especially data subject's rights laid down in Chapter III of the GDPR;

b) Security Breaches;

c) impact assessments;

d) prior consultation of the supervisory authorities.

7.5.2 In this connection, the Controller shall obtain the information to be included in a notification to the supervisory authority provided that the Controller is best suited to do so.

8. Sub-Processors

8.1 The Processor may only use a third party ("Sub-Processor") for the processing of Personal data for the Controller provided that it is specified in Appendix 3 of this Agreement.

8.2 The Processor and the Sub-Processor(s) have concluded a written agreement imposing the same data protection obligations on the Sub-Processor as those of the Processor (including in pursuance of this Agreement) as referred to in paragraph 3 of the GDPR regarding Data processing, ensuring protection of processed Personal data and compliance with the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Sub-processor also acts only under the Instructions of the Controller as stated in this Agreement.

8.3 Notwithstanding the provisions of article 3.5. of the Agreement, the Processor reserves the right to change or add Sub-Processors. The Processor shall notify the Controller of any such event via e-mail specified in the Controller's user account. The notification shall be done at least 30 days prior to the event and involvement of the new Sub-Processor. If the Controller doesn't agree to the new Sub-Processor, they have the right to terminate the Service immediately and are entitled to a refund for the remaining period of the Service. If the Controller does not send a written disagreement within 30 days upon receiving the notification, the Processor assumes that the Controller agrees with the involvement and shall involve these Sub-Processors.

8.4 All communication with the Sub-Processor is handled by the Processor, unless otherwise specifically agreed.

8.5 The Processor is directly responsible for the Sub-Processor's processing of Personal data in the same manner as had the processing been carried out by the Processor.

9. Liability and Limitation of Liability

9.1 The Parties are liable according to the general rules of applicable law, however, the Processor is liable according to limitations set out in the Terms. To the extent stipulated in these Terms, the Processor is not responsible for the Controller's use of the Service. The Processor is also not liable for any non-material damage incurred by the Controller in connection with this Agreement.

9.2 In the event of a claim for damages by the Controller, damages are limited to $2,000,000.

10. Force Majeure

10.1 The Processor cannot be held liable for situations normally referred to as force majeure, including, but not limited to, war, riots, terrorism, insurrection, strike, fire and natural disasters.

10.2 Force majeure may only be asserted for the number of working days for which the force majeure situation lasts.

11. Confidentiality

11.1 Information regarding the content of this Agreement, the underlying Service or the other Party's business which is either, in connection with the disclosure to the receiving Party, designated as confidential information, or which, by its nature or otherwise, should be considered as confidential, must be treated as confidential and subject to at least the same degree of care and discretion as the Party's own confidential information. Data, including Personal data, are always confidential information.

11.2 However, the duty of confidentiality does not apply to information, which is or becomes publicly available without this being the result of a breach of a Party's duty of confidentiality, or information, which is already in the possession of the receiving Party without any similar duty of confidentiality or information, which is developed independently by the receiving Party.

12. Termination

12.1 Termination for cause or breach

12.1.1 The Agreement may only be terminated according to the provisions on termination in the Terms or this Agreement.

12.1.2 Termination of this Agreement is subject to – and allows for – simultaneous termination of the parts of the Terms that concern Personal data processing pursuant to the Agreement.

12.2 **Effects of termination**

12.2.1 The Processor's authority to process Personal data on behalf of the Controller lapses on termination of the Agreement for whatever reason.

12.2.2 The Processor may continue to process Personal data for up to three months after the termination of this Agreement to the extent that this is necessary to take the required statutory measures. The Processing by the Processor during this period is assumed to comply with the Instructions.

12.2.3 The Processor is obliged to delete all Personal data disclosed by the Controller within 3 months from the termination of the Agreement. The Controller may request confirmation of such deletion. This confirmation contains signed information of the Processor, that all Personal data were deleted, unless they are necessary for fulfilment of the Processor's legal obligations.

13. Final Provisions

13.1 The regulation of dispute resolution specified in the Terms, including governing law and venue, also applies to this Agreement as were this Agreement an integral part thereof.

13.2 Natural person concluding and accepting this Agreement on Processor's website www.smartlook.com hereby declares that he or she acts on behalf of the Controller and is legally authorized to act on behalf of the Controller in the matter of this Agreement.

13.3 The Parties affirmatively declare that actions of the Parties made under the conditions agreed in this Agreement create the rights and duties for the Parties leading to creation of the legal relations between the Parties as assumed by the Agreement. The Parties also declare that all rights and duties and the agreed matters are considered definite adequately and capable to call the legal effects and impacts assumed by this Agreement. Provisions under the preceding phrases are valid even if actions of the Parties do not meet all prerequisites assumed by the binding legal regulations. In this case the Parties shall agree and meet such prerequisites without undue delay.

13.4 The rights and duties following from or connected to this Agreement may not be assigned or transferred anyhow by any Party without the prior written approval of the other Party.

13.5 Communication of the Parties concerning the Agreement (incl. Security Breach notification) shall be led through following email addresses:

a) Processor: dpo@smartlook.com

b) Controller: email address used to sign up for the Service

13.6 Notwithstanding the provisions of article 3.5. of the Agreement, the Processor reserves the right to change or update this Agreement with a 30 days prior notice. If the Controller does not agree with the changed or updated Agreement within this period, the relationship will be governed by the current Agreement, however the Processor has the right to terminate the Agreement. If the Controller does not send disagreement within the 30 day period, the Processor assumes that the Controller agrees to the change or update of the Agreement and the change or update becomes effective. By continuing to access or use the Service after those revisions become effective, the Controller agrees to be bound by the revised Agreement. If the Controller does not agree to the new Agreement after effectiveness, the Controller should stop using the Service. The rules set out in this Article shall not apply if the change is caused by a change in the legislation on the protection of personal data (in particular GDPR) and such addition is necessary to comply with the obligations caused by this change. In this case, the Controller automatically agrees with the change. The latest version of this Agreement, which is legally in effect, can always be found at www.smartlook.com/dpa.

APPENDIX 1
NATURE, SCOPE, DURATION AND PURPOSE OF PERSONAL DATA PROCESSING

1. Nature, Scope, Duration and Purpose of Personal Data Processing

1.1 **Nature of processing**: Personal data are processed in an automated way via a script of the Processor that the Controller inserts into their website(s). The script is tracking activity and behavior of visitors on the Controller's website(s). The Controller can import additional Personal data for processing via API of the Processor or by using integrations with 3rd party services as part of the Service.

1.2 **Scope of processing:** Depending on how the Controller is using the Service, particularly following types of Personal data may be processed in connection with the delivery of the Service:

a) browsed pages on the Controller's website and referring URL;

b) date and time of visits to the Controller's website;

c) mouse movement and mouse clicks;

d) technical information as screen resolution, operating system, browser type and device type;

e) geolocation data (country and city);

f) IP address;

g) first name and/or last name;

h) email address;

i) additional types of Personal data depend on the Controller's use of the Service.

1.3 Controller shall NOT disclose to the Processor any Personal data falling into a special category of Personal data as specified in the Article 9 of the GDPR. Example of such data types:

a) information about race and/or religious beliefs;

b) information about sexual behavior and/or sexual preferences;

c) sensitive medical information and/or information about health and illnesses.

1.4 **The categories** of data subjects covered by this Agreement:

a) visitors of Controller's website(s) where the Service is used.

1.5 **Duration of processing:** All processed Personal data are automatically deleted according to the Data Retention Period based on the purchased Service.

1.6 **Purpose of the processing** is to provide the Controller insights to:

a) improve their website or web product;

b) improve user experience on their website;

c) improve customer support and speed up support case resolution;

d) improve bug discovery and bug fixing.

2. Tools to Limit Processing of Personal Data and Improve Privacy of Users

2.1 As part of the Service, the Processor offers the Controller following tools to limit processing of Personal data and to improve privacy of Data Subjects. All tools are further described on Processor's website at www.smartlook.com/help.

2.2 Certain types of sensitive data may automatically be excluded from processing. The automatic exclusion is mainly focused on input HTML elements and emails within the text content of websites. This measure is based on the assumption that the Controller is using best practises for building websites and labelling fields with sensitive information in the website source code.

2.3 Option to disable tracking of data filled in form inputs on Controller's website. Tracking of form inputs is located in the Controller's account at www.smartlook.com and is disabled by default.

2.4 Option to anonymize IP addresses of visitors of Controller's website. IP address anonymization is located in the Controller's account at www.smartlook.com and is enabled by default.

2.5 API to exclude certain pages or elements on the Controller's website from being tracked. The API is documented at Processor's website www.smartlook.com/docs/recording.

2.6 Processor provides to the Controller an option to collect consent from visitors via a pop up window on Controller's website. If this option is used, the visitor is asked to give consent for processing of Personal data via the Service. If a visitor doesn't give the consent in this pop up, he is automatically excluded from the Personal Data Processing via Service.

APPENDIX 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1.1 The Processor implemented following technical security measures to maximize protection of Personal data:

a) SSL/TLS encryption (secure sockets layer / transport layer security) for all data transfers in all parts of the Service;

b) Processor's website and web software runs on secured https protocol;

c) Processor offers the Controller multiple tools, described in point 2 in Appendix 1, to limit processing of Personal data and improve privacy of Data subjects;

d) all employees of the Processor with access to Personal data have signed a confidentiality agreement with the Processor;

e) Processor appointed a Data Protection Officer to ensure that Personal data are protected. The DPO can be contacted at dpo@smartlook.com;

f) Processor chose Amazon Web Services as its server and data storage provider. Amazon Web Services is one of the world's most advanced server infrastructure providers with state of the art security and data protection, which is further described in this appendix.

1.2 The Processor is using servers and cloud infrastructure of Amazon Web Services to store Personal data (see Appendix 3 - Sub-processors).

1.3 Information about security of Amazon Web Services:

a) Information about security of Amazon Web Services

aws.amazon.com/security

b) Information about physical security of Amazon AWS data centers:

aws.amazon.com/compliance/data-center/controls

c) Information about GDPR compliance of Amazon Web Services:

aws.amazon.com/compliance/gdpr-center

1.4 The Controller can manage and delete any Personal data in their account used to access the Service at www.smartlook.com. This allows the Controller to meet their obligations regarding requests of Data subjects for Personal data information or deletion.

APPENDIX 3
SUB-PROCESSORS

1. SUB-PROCESSORS

1.1 The Controller hereby approves that the Processor uses following Sub-Processors to process Personal data:

a) Amazon Web Services EMEA SARL, 5 rue Plaetis, L-2338 Luxembourg

1.2 Any sub-processors operating outside European Union process Personal data under EU Standard Contractual Clauses (SCCs) or under any other condition set out in the articles 44 – 49 of the GDPR (especially under adequacy decision).