Personal Data Processing Agreement

Parties:

Business name: _____

Registered office: _____

Company ID: _____

E-mail: _____

Registered
in the Business Register: _____

(hereinafter as "**Controller**")

and

Business name: **UXtweak j.s.a.**

Registered office: Cajakova 18, 811 05 Bratislava - Stare Mesto, Slovakia

Company ID (ICO): 52344932

Represented by:: Eduard Kuric, board member
eduard.kuric@uxtweak.com

Lubomir Lajos, board member
lubomir.lajos@uxtweak.com

Registered
in the Business Register: City Court Bratislava III, section: Sja, registration No.: 80/B

(hereinafter as "**Processor**")

(The Controller and the Processor are collectively referred to as the "Parties" and individually as the "Party")

have entered into the Personal Data Processing Agreement (hereinafter as ”**Contract**“) with the following content:

1. Definitions

For the purpose of this Contract, the following definitions apply:

”Contract“ means this Contract including all its annexes.

“CCPA” means the California Consumer Privacy Act of 2018, a state statute of the state of California, United States, intended to enhance consumer privacy rights and protection.

”Directive“ means the General Data Protection Regulation – GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)).

“DORA” means the Digital Operational Resilience Act (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector).

”Terms“ mean Terms of the Website and/or Service available on the Processor's website: uxtweak.com/legal/terms-and-conditions to which the Controller has agreed by accessing the website and/or using the service.

”Service“ means the service provided by the Processor to the Controller as described in the Terms.

”Website“ means the website of uxtweak.com including all its subwebsites.

”Personal data“ means any information about an identified or identifiable natural person as defined in the Article 4 of the Directive, mainly any such information disclosed by the Controller to the Processor for the purpose of processing.

”Data subject“ means the identified or identifiable natural person to whom personal data relates.

”Processing“ and **“Data processing“** mean 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 Directive.

”Data retention period“ means a time for how long Controller's data, including personal data, are stored by the Processor. The data retention period depends on the service purchased by the Controller as further described in the Terms.

”Instructions“ means any additional instructions issued by the Controller to the Processor in alignment with Terms as to the nature, scope and method of data processing.

2. Basic provisions and purpose of the Contract

2.1 Parties have agreed to the provisions of the terms, which govern the Controller's limited, non-exclusive and terminable right to use the service and/or websites.

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 Contract in accordance with the Article 28 of the Directive.

2.3 The purpose of this Contract is to ensure that the cooperation between the Processor and the Controller in the field of personal data processing complies with the Directive.

3. Duration of the Contract

3.1 Provisions of this Contract shall apply until either **a)** termination of provision of the service; or **b)** termination of this Contract.

3.2 Regardless of the termination of the Contract, Article 13 of the Contract regarding confidentiality, as well as Articles 9, 10, and 11 shall apply.

4. Appointment and Instructions

4.1 The Controller authorizes the Processor to process personal data disclosed to the Processor by the Controller on behalf of the Controller on the terms stipulated in this Contract.

4.2 This Contract, including all its annexes, constitutes the complete and final instructions for the processing of personal data for purpose and in scope defined for the service under this Contract.

4.3 All instructions shall comply with the Directive and any other applicable law. The Processor reserves the right to refuse any instruction which is not compliant with the Directive or any other applicable law or, if such instruction, in Processor's opinion, infringes the Directive or any other applicable law on personal data protection of the European Union or its Member State. In such a case, the Processor can postpone the execution of the instruction and shall immediately inform the Controller.

4.4 Any change of any instruction shall be done in writing as a supplement to the Contract, and such supplement shall be signed by both Parties. Prior to any change of the instructions, Parties shall mutually discuss the change in details and exert maximum effort to agree on the change, including time and costs for implementation.

4.5 The Processor shall process personal data in compliance with instructions. This shall apply to Processor's personal data transfer to any third country or international organization, unless such Processor's duty arises from the law of the European Union or its Member States. In such case the Processor shall immediately notify the Controller thereof prior to the processing, unless the respective law prohibits such notification for serious reasons of public interest.

4.6 Provided that the law of the European Union or its Member State or the local law would require the processing beyond the limits of Controller's instruction, the Processor can exceed the limits of Controller's instruction.

4.7 Provided that personal data is processed beyond the limits of the instructions, the Processor shall immediately inform the Controller about the reason for doing so. The notification shall be made prior to the processing and shall contain references to the respective law according to which such processing is applicable.

4.8 Provided that such notification would infringe with the law of the European Union or its Member state, the notification shall be omitted.

4.9 By this Contract, the Controller instructs and authorizes the Processor to process personal data disclosed by the Controller to the Processor in scope necessary to provide the service or otherwise subsequently agreed by the Parties in writing.

5. Data processing

5.1 The Processor solely processes personal data on behalf of the Controller in scope and for the purpose set in this Contract.

5.2 Subject, character, purpose and duration of the processing, type of personal data and categories of data subjects are further defined under par. 5.3 – 5.13 and the Annex No. 1 to this Contract.

5.3 Personal data of data subjects which are on the territory of the European Union being processed by the Processor on behalf of the Controller, shall solely be processed in one of the Member States of the European Union. The exemption is the processing of personal data by the services (sub-processors) listed in Annex No. 3. Any sub-processors operating outside the European Union process Personal Data under EU Standard Contractual Clauses (SCCs). We no longer rely on the Privacy Shield as a data transfer mechanism given that the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield are no longer valid as a result of the Schrems II decision issued by the European Court of Justice on July 16, 2020. We continue to commit to the principles of the Privacy Shield framework given it can still provide privacy protections to users.

5.4 All personal data processed by the Processor on behalf of the Controller, shall be processed under adequate technical, organizational and security measures defined under par. 6.1 of this Contract.

5.5 The Processor shall not alter, erase or restrict any personal data processed on behalf of the Controller without any additional Controller's instruction or prior to expiration of the data retention period. The Processor shall not alter, erase or restrict any personal data processed on behalf of the Controller even if the respective additional instruction has been issued, provided that the law of the European Union and/or its Member State requires retention of the respective personal data.

5.6 Provided that a data subject requests access, alteration, restriction, erasure or portability of his personal data and provided that the data subject raises objections against processing of his/her personal data or asserts his/her right not to be the subject of automated decision-making, the Processor shall forward such request to the Controller without undue delay.

5.7 Personal data made available by the Controller for the purpose of data processing by the Processor in accordance with provisions of this Contract, shall be not used by the Processor for any other purpose than for the purposes defined in this Contract.

5.8 The Processor shall not disclose personal data to any third parties except of subprocessors approved by the Controller as specified in the Annex No. 3 to this Contract.

5.9 The Processor shall not make any copy or duplicate of personal data disclosed by the Controller prior to Controller's approval with the exception of copies or duplicates made according to the Directive or the law of the European Union or its Member State, and with the exception of copies or duplicates made as backup and precaution against data loss due to server errors, in order to fulfil the duty arising from the Directive, i.e. to prevent any casual or intentional data destruction. For prevention, backup data shall be stored for at least the next 240 hours (10 days). The Processor provides the Controller with no other archiving or backup services, unless otherwise agreed upon.

5.10 The Processor may anonymise personal data collected from the Controller and/or data subjects such that the data cannot be linked to an individual, directly or indirectly, by any means. The Processor reserves the right to use such anonymised data for purposes that include developing and testing the Processor's systems and processes, research, data analysis, improving the Processor's website and software, and developing new products and features.

5.11 After service termination in accordance with the Terms and this Contract or upon request by the Controller (based on the Controller's instruction in particular), the Processor shall erase all personal data and their copies unless otherwise stipulated by the law of the European Union or its Member State.

5.12 The Processor shall not disclose personal data to any third countries and international organizations unless otherwise expressively stipulated in provisions of this Contract.

5.13 The Processor appointed a person authorized to protect personal data (hereinafter as **„POOOU**") and this person shall supervise processor's observation of duties. The POOOU can be contacted at info@uxtweak.com.

6. Processor's obligations

6.1 Technical and organizational safeguards

6.1.1 The Processor shall make technical and organizational safeguards necessary to ensure the adequate level of security. Designing the safeguards, the Processor shall consider the current condition of the used technology, safeguard costs and the nature, scope, context and purposes for data processing, as well as differentiation of various risks and effects on rights and freedoms of natural persons. The Processor shall consider categories of personal data as specified in the Annex No. 1.

6.1.2 The Processor shall comply with the applicable law governing personal data and with provisions of the Directive when designing his technical and organizational safeguards.

6.1.3 The Processor has introduced his own technical and organizational safeguards, as stipulated in the Annex No. 2 to this Contract.

6.1.4 Should the Processor introduce new technical or organizational safeguards according to this Article, in order to improve and develop the service and due to the technical progress and development of technical and organisational security measures, and due to changes of the Processor's organization, or due to the amended applicable law, or due to other circumstances, the safeguards stipulated in the Annex No.2 shall be amended accordingly. No change shall affect the level of organizational safeguards set at the time of entering into this Contract.

6.2 Terms and conditions of employees

6.2.1 The Processor shall ensure that employees processing personal data undertake to maintain confidentiality or they are subject to confidentiality obligation according to the applicable law.

6.2.2 The Processor shall solely ensure the access to personal data to the employees which need the access to process personal data in order to meet the Processor's obligation to the Controller under the Terms.

6.2.3 The Processor shall ensure that employees processing personal data for the Processor solely process personal data according to the instructions and the Directive.

6.3 Proof of meeting the obligations

6.3.1 Upon Controller's request in writing, the Processor shall prove that:

a) the Processor meets his obligations arising from this Contract and instructions;

b) the Processor acts in compliance with the Directive with regard to the processing of personal data being processed on behalf of the Controller.

6.3.2 The Processor's documentation shall be forwarded in the adequate period of time.

6.4 Records on processing activities

6.4.1 The Processor shall maintain a record on processing of personal data.

6.4.2 His records shall contain the following information

a) category of processing made on behalf of Controllers;

b) general description of technical and organizational safeguards made due to processing of personal data;

c) Processor's employees who process personal data;

d) information on any possible subprocessor who process personal data;

e) specification of any third country or international organization the personal data are transferred to and a proof of adequate guarantee;

f) contact details of the contact person, or the Processor's POOOU, or subprocessor, if applicable.

6.4.3 The Processor shall forward such records to the Controller or respective supervisory authority upon request.

6.5 Security breach

6.5.1 In case of security breach, the Processor shall immediately notify the Controller about each case which potentially could result in casual or intentional data destruction, change, disclosure or access to personal data processed by the Processor on behalf of the Controller (hereinafter as "**security breach**").

6.5.2 The Processor shall record all cases of security breach. The records shall include at least the following information:

a) True circumstances and probable reason of security breach;

b) Consequences of security breach;

c) Adopted corrective measures to improve safety.

6.5.3 Records on security breach shall be forwarded to the Controller or supervisory bodies upon request in writing.

6.6 Inspections and security audits

6.6.1 The Processor shall enable the Controller or the auditor appointed by the Controller to conduct inspections and security audits, and the Processor shall take part in such inspections and audits.

6.6.2 Inspections and security audits by the Controller or by the auditor appointed by the Controller shall be conducted upon prior consultation with the Processor. Duration, scope, subject matter, purpose, date and time of the respective inspection or security audit shall be settled during the consultation.

6.6.3 Inspections and security audits by the Controller or auditor appointed by the Controller shall be conducted for the sole purpose of verifying whether the Processor processes personal data in accordance with this Contract, the Directive, as well as the applicable law.

6.6.4 The right of audit or inspection stipulated under this Contract shall not apply to facilities operated by subprocessors, subcontractors or other third persons even if used for providing the service of data processing.

6.6.5 All information and documents disclosed by the Processor to the Controller due to the inspection or security audit belong to the Processor's trade secret. Unless otherwise stipulated, such information and documents are subject to confidentiality and may only be disclosed to the authorized supervisory authority.

6.7 Assistance

6.7.1 The Processor shall, to the necessary and reasonable extent, assist the Controller to perform his obligations arising from this Contract regarding personal data processing including:

a) responses to data subjects on exercise of their rights as affected persons and, in particular, the data subject's rights laid down in the Chapter III of the Directive;

b) ensuring compliance with the obligation of the Controller pursuant to the Articles 32 to 36 of the Directive and in consideration of the nature of data processing and information available to the Processor;

c) security breaches;

d) impact assessments;

e) consultations with supervisory authorities.

6.7.2 In relation to the subject matter of this Article, the Processor collects information to be reported to the respective supervisory authority provided that the Processor is the most adequate person to do so.

6.7.3 The Processor is entitled to claim payment for his time spent and efforts exerted to assist, as well as compensation for any material used for assistance pursuant to par. 6.7.

6.7.4 Adequate technical and organizational measures taken by the Processor to assist the Controller with the fulfilment of his obligation of responding to requests by data subjects exercising their rights (access right, 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 the Articles 15 to 22 of the Directive and specified in the Annex No. 2 to this Contract.

7. Controller's obligations

7.1 Lawfulness of processing

7.1.1 The Controller shall ensure and secure that during the whole duration of this Contract:

(a) all personal data disclosed by the Controller to the Processor for processing and with any relation to the service, have been collected in legal and legitimate manner in accordance with the Directive or any other applicable law;

(b) consent by the data subject is given for processing of the respective personal data by the Processor, and the consent is given freely and pursuant to Article 7 of the Directive, and that the consent will be valid for the whole period of data processing and will be not cancelled by the data subject;

(c) other terms of lawful processing pursuant to Article 6 of the Directive shall apply provided that the Data subject refuses to agree;

(d) no personal data falling into the special category of personal data as specified in Article 9 of the Directive will be disclosed to the Processor..

7.1.2 Should the Processor fail to meet any obligation specified in par. 7.1.1. during data processing or in the course of the duration of this Contract, the Controller shall inform the Processor thereof without undue delay and not later than up to 72 hours after he learns about the deficiency. The Controller shall exclude such personal data from the processing (mainly by erasing such personal data from the Controller's service), and if not possible, the Controller shall provide the Processor with all necessary assistance and cooperation to exclude such personal data from processing.

7.2 Terms for employees and third persons

7.2.1 The Controller shall ensure that his employees processing personal data on behalf of the Controller and having access to the service, will be obliged to maintain confidentiality or their obligation to maintain confidentiality arises from the applicable law.

7.2.2 The Controller shall ensure that any third party having access to the service on behalf of the Controller, will be obliged to maintain confidentiality or the obligation to maintain confidentiality arises from the applicable law.

7.2.3 The Controller is fully liable to the Processor for any action of his employees or third persons provided with access to the service by the Controller.

7.3 Proof of meeting the obligations

7.3.1 Upon Processor's request in writing, the Controller shall prove that:

(a) the Controller meets his obligations arising from this Contract and the Terms;

(b) in relation to personal data disclosed to the Processor, the Controller acts in compliance with the respective provisions of the Directive or any other applicable law;

(c) consent by the data subject is valid and given for processing specific respective personal data by the Processor and the consent was given freely and in compliance with Article 7 of the Directive.

7.3.2 The Controller shall forward the documentation in the adequate period of time.

7.4 Security breach

7.4.1 The Controller shall, without undue delay, notify the Processor on each security breach of personal data pursuant to par. 6.5.1.

7.4.2 The Controller shall maintain a record on all cases of security breach. The records shall include the following facts at least: **(a)** real circumstances and probable reason of security breach; **(b)** impacts of security breach; a **(c)** adopted corrective measures to improve safety.

7.4.3 Upon a request in writing, the records shall be forwarded to the Processor or the supervisory authorities.

7.5 Assistance

7.5.1 The Controller shall, to the necessary and reasonable extent, assist to the Processor to perform his obligations arising from this Contract regarding personal data processing including: **(a)** responses to data subjects on exercise of their rights as affected persons and in particular data subject's rights laid down in the Chapter III of the Directive; **(b)** security breach; **(c)** impact assessments; **(d)** consultation with supervisory authorities.

7.5.2 In this regard, the Controller will get information to be reported to the supervisory authority provided the Controller is the most adequate person to do so.

8. Subprocessors

8.1 The Processor may only use a third party (hereinafter as "**subprocessor**") for personal data processing provided that the third party is specified in the Annex No. 3 to this Contract.

8.2 The Processor and the subprocessor have concluded a written contract imposing the same data protection obligations on the subprocessor as the Processor's obligations are (also in pursuance of this Contract) stipulated in par. 3 of the Directive regarding data processing, ensuring protection of processed personal data and in compliance with the Directive, in particular providing sufficient guarantees for implementation of technical and organizational measures in order to ensure that the processing will comply with the Directive. A subprocessor shall only act in accordance with instructions of the Controller and this Contract.

8.3 The Processor reserves the right to change or add subprocessors. The Processor shall notify the Controller about each case at least 30 days prior to his action. Should the Controller disagree to the new subprocessor, the Controller has the right to terminate the service with immediate effect and the Controller can also claim refund for the remaining paid period of using the service and/or the website.

8.4 The Processor shall handle the whole communication with subprocessors unless otherwise specifically agreed.

8.5 The Processor is accountable for data processing by subprocessors in the same manner as if the Processor did it himself.

9. Fees and costs

9.1 The Parties can claim payment for the service provided in accordance with the Terms, unless otherwise stipulated under this Contract.

10. Confidentiality of information

10.1 Any information regarding the content of this Contract, or the related service or business activities of the other Party to the Contract, which are designated as confidential when disclosing them to the other Party to the Contract, or which should be handled as confidential due to their character or for any other reason, shall be considered as confidential information requiring at least the same degree of care and discretion as the receiving Party's own confidential information. Any data being subject matter of this Contract, including personal data, shall be classified as confidential information.

10.2 The obligation to maintain confidentiality shall not apply to information, which is publicly known or which will become publicly known without any breach of the obligation to maintain confidentiality by the receiving Party, and to information which is already in the possession of the receiving Party, whereas this Party has been not obligated to maintain confidentiality, and to information elaborated by the receiving party itself and independently.

11. Breach of the Contract

11.1 Breach specified under the Terms and Conditions for the Service shall fully apply to any breach of the Contract, as if the Contract were an inseparable part thereof. Provided that the breach is not specified under the Terms and Conditions for the Service, general remedies for breach laid down in the applicable law shall apply.

12. Liability and limitation of liability

12.1 The Processor is liable for any damage in accordance with general rules of the applicable law. The Parties have explicitly agreed that the Processor's liability for damages incurred to the Controller shall be limited to terms under this Article of the Contract.

12.2 The Processor rejects liability for any direct or indirect loss or damages including profit loss, reputation damage, loss of savings or earnings including costs for renewal of loss of earnings, loss of interests and loss of data.

12.3 Parties have explicitly agreed that any liability of the Processor for any damages incurred to the Controller or any compensation claim based on this Contract shall be limited to the amount of total payments for the three last calendar months paid by the Controller to the Processor prior to the event establishing the Processor's obligation to compensate damages incurred to the Controller. Should this Contract be not effective in the period of the three months, the Processor shall pay compensation in the amount of total payments paid by the Controller to the Processor in the period of duration of this Contract divided by the number of months in which this Contract was in effect.

13. Force majeure

13.1 The Processor cannot be held liable for damages arising from situations usually referred to as force majeure, including but not limited to: war, riots, terrorism, rebellions, strikes, fire and natural disasters.

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

14 Termination of the Contract and its consequences

14.1 Termination of the Contract giving reasons for the termination or for its violation

14.1.1 This Contract can solely be terminated pursuant to clauses on termination stipulated in the Terms or in this Contract.

14.1.2 Termination of this Contract is subject to – and enables – simultaneous termination of the parts of the Terms which govern processing of personal data pursuant to this Contract.

14.2 Effects of termination

14.2.1 Processor's authorization to process personal data on behalf of the Controller shall cease by contract termination for whatever reason.

14.2.2 The Processor can process personal data for up to three months after the termination of the Contract in the scope necessary to take necessary legal measures. Processing by the Processor in this period shall be considered as complying with the instructions.

14.2.3 The Processor shall erase all personal data disclosed by the Controller up to 3 months after the termination of the Contract. The Controller can request adequate proof of data erasure.

14.2.4 The Processor shall never process personal data which are not available to the Controller and all personal data are forwarded to the Processor by the Controller.

15. Final provisions

15.1 The regulation of dispute resolution specified in the Terms, including the governing law and venue shall apply to this Contract as if the Contract were an integral part thereof.

15.2 Natural person concluding and accepting this Contract on the Processor's website uxtweak.com (hereinafter as "**natural person**") hereby declares to act on behalf of the Controller and is legally authorized to act on behalf of the Controller in the matter of this Contract. Provided that such legal authorization will be found as invalid, the Contract shall

be binding for the natural person which shall be liable for fulfilment of all obligations stipulated in this Contract.

15.3 The Parties explicitly declare that their actions made under conditions agreed in this Contract create rights and duties of the Parties leading to creation of the legal relations as assumed by the Contract. The Parties also declare that all rights and duties and other agreed matters are considered as definite, adequate and produce legal effects and impacts as assumed by this Contract. Provisions set in the previous phrases are valid even if action of the Parties do not comply with all requirements laid down in binding legal regulations. In such case, the Parties shall immediately agree and meet requirements without undue delay

15.4 Both Parties shall not transfer and assign its rights and obligations arising from or related to this Contract without prior written approval of the other Party.

15.5 Communication of the Parties concerning the Contract, including security breach notification, shall be made in writing through the following e-mail addresses:

a) Processor: info@uxtweak.com;

b) Controller: e-mail address used to sign up for the Service.

15.6 UXtweak j.s.a. reserves the right to modify or update this Contract without prior notification. By continuing to access or use the service after the revisions become effective, you agree to be bound by the revised Contract. Should you disagree to the new Contract, you must immediately stop using the service. The latest version of this Contract, which is legally in effect, is always available at uxtweak.com/legal/dpa.

In _____, on _____._____._____

_____

Controller

In Bratislava, on _____. _____. _____

_____

Eduard Kuric, CEO
UXtweak j.s.a.
Processor

Annex No. 1: Purpose, nature, scope and time of personal data processing

1. Purpose, nature, scope, categories and time of personal data processing

1.1 Purpose of the processing is to provide the Controller with the following advantages:

a) improvement of user experience of websites/applications/services (hereinafter as "**software**");

b) overall improvement of the software quality (information architecture, etc.);

c) provision of better customer service;

d) support for detection of software errors and their fixing.

1.2 Nature of processing is automated processing of personal data imported and/or entered by the Controller into the Service manually or via a script that is integrated by the Controller into the code of his software. The Controller can import additional personal data via interface for Processor's applications programming (API) or via integrations with services of third parties.

1.3 Scope of processing depends on how the Controller is using the Service and/or the website and particularly the 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, including datum and time of browsing;

b) mouse movement and clicks;

c) technical data as screen resolution, device type, operating system and browser type;

d) geolocation data (country and town, approximate location);

e) IP address;

f) name and surname;

g) e-mail address and phone number;

h) audio (voice / microphone), video (face / webcam) and screen recordings;

i) other types of personal data depending on the Controller's use of the Service and/or the website.

1.4 The Controller shall not disclose to the Processor any personal data falling into special category of personal data as specified in Article 9 of the Directive. Such data include the following examples:

a) information about race and/or religious beliefs;

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

c) health information and information about diseases;

d) other kinds of sensitive information as e.g. credit card numbers, passwords, etc.

1.5 Categories of the processing include:

a) visitors of Controller's websites where the Service is used;

b) users of Controller's software where the Service is used;

c) participants of Controller’s studies created using the Service;

d) other registered identified or identifiable natural persons covered by this Contract.

1.6 Processing time depends on the Contract's duration and all processed data are deleted pursuant to terms on data retention arising from the purchased service.

2. Tools for limitation of personal data processing and for a better privacy protection

2.1 As a part of the service and/or website, the Processor offers the Controller the following tools to limit the personal data processing and to improve privacy protection of the affected persons. All tools are described in detail at: uxtweak.com/legal/gdpr-compliance.

2.1.1 Some sensitive data of EU residents are excluded by default from processing, e.g. data stated under par 1.3 letter d). This measure is based on the assumption that the Controller uses defaults and best procedure in the field of creation of HTML websites, including marking the fields with sensitive information in the source code of his websites.

2.1.2 The service enables anonymization of IP addresses of visitors of Controller's websites. The function was turned on by default for visitors from the EU and its Member States..

2.1.3 The service enables to block recording of data given into the forms on websites/in the application of the Controller. The function is turned on by default for visitors from the European Union and its Member States.

2.1.4 The service provides an API to disable tracking of some websites, i.e. elements on Controller's websites. The API is documented on the Processor's website uxtweak.com/help/privacy-and-security-sensitive-data-protection-api.

2.1.5 The Processor provides the Controller with a possibility to get a consent by visitors to data processing via popups on the Controller's websites. Using this possibility, the visitor will be asked to agree to the personal data processing via the service. Should the visitor reject to agree, the visitor will be automatically excluded from the personal data processing.

Annex No. 2: Technical and organizational safeguards

1. Technical and organizational safeguards

1.1 To ensure the possibly best protection of personal data, the Processor has introduced the following technical safeguards:

a) secure sockets layer use for the overall data exchange in all parts of the service and/or website;

b) use of secure HTTPS for websites and Processor's web software;

c) the Processor provides the Controller with a toolkit described in par. 2.1 of Annex No. 1 to restrict the personal data processing and to improve privacy protection of affected persons;

d) all Processor's employees provided with access to personal data have signed the confidentiality agreement with the Processor;

e) the Processor appointed a person authorized to protect personal data ("**POOOU**") in order to secure protection of personal data. The POOOU can be contacted at info@uxtweak.com.

1.2 The Processor uses the servers and cloud infrastructure by Amazon Web Services (AWS) for storage of personal data (see Annex No. 3). All data collected by the processor is stored electronically in Ireland, Europe in the AWS infrastructure, data center eu-west-1. Our application servers and database servers function within Amazon VPC (Virtual Private Cloud). The database containing data of the subjects is accessible only from the application servers and completely inaccessible to any other sources. For more information regarding the security of AWS, see the following links:

a) https://aws.amazon.com/security
b) Information about the physical security of AWS data centers: https://aws.amazon.com/compliance/data-center/controls

c) Information about GDPR compliance on the part of AWS: https://aws.amazon.com/compliance/gdpr-center

Certifications and audit reports for AWS:

a) ISO-27001 Certification for AWS: https://aws.amazon.com/compliance/iso-27001-faqs/
b) SOC2 third-party audit reports for AWS: https://aws.amazon.com/compliance/soc-faqs/

1.3 The Processor passed a self-evaluation process in accordance with the SAQ A standard (Self Assessment Questionnaire) and is eligible to accept so-called card-not-present payments (CNP) by entrusting all operations related to payments to the company Stripe (see Appendix n. 3) which conforms to the standard PCI DSS (Payment Card Industry Data Security Standard).

1.3 The Controller is enabled to edit or to delete personal data at his account used by him to access the service at the website uxtweak.com, whereby it is enabled to the Controller to fulfil his obligations concerning requests by affected data subjects to provide information on personal data, or to delete personal data.

Annex No. 3: Subprocessors

1. Subprocessors

1.1 The Controller acknowledges and agrees that the Processor hires the following subprocessors for purpose of personal data processing:

a) Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg;

b) Sendinblue SAS, 106 boulevard Haussmann, 75008 Paris, France;

c) Tawk.to, Inc., 187 East Warm Springs Rd, SB298, Las Vegas, NV 89119, USA;

d) Mailgun Technologies, Inc., 112 E Pecan St. #1135 San Antonio Texas 78205, USA;

e) Stripe Payments Europe, Limited is registered in Ireland, company number IE513174. Registered Office: The One Building, 1 Grand Canal Street Lower, Dublin 2, Co. Dublin, Ireland;

f) Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland;

g) Zoom Video Communications, Inc., 55 Almaden Blvd, Suite 600 San Jose, CA 95113, USA.

h) HubSpot Ireland Limited, HubSpot House, One Sir John Rogerson's Quay, Dublin 2, Ireland.

1.2 For the purposes of data storage, provisioning of server infrastructure (cloud computing), sending transactional e-mails (e.g., a user registration message), implementation and operation of security and monitoring measures, and providing other functionality necessary for provisioning the service, the Processor utilizes cloud hosting services provided by AWS. For the purposes of securing effective distribution of content while providing services as a data processor, as well as optimal functioning of the server infrastructure on part of the data processor, the Processor utilizes the service AWS CloudFront as a content delivery network (CDN) service. AWS CloudFront processes geolocation data of subjects and stores it in its anonymized form for the purposes of securing effective provisioning of services and data delivery to subjects.

1.3 The Processor uses Brevo (formerly Sendinblue) (https://www.brevo.com) for sending promotional newsletters by e-mail. If the data subject subscribes to the Processor's newsletter, the Processor needs their explicit permission that they agree to receive the newsletter. The data the subject provides to subscribe to the Processor's newsletter will be stored on Brevo servers. If the subject wants to cancel their subscription, they may do so at any time either through the "Unsubscribe" link in one of the Processor's newsletter emails or by using the Processor's contact form (https://uxtweak.com/contact-us). Data processing is based on Art. 6 (1) (a) GDPR. The subject may revoke their consent at any time. The data provided when registering for the newsletter will be used to distribute the newsletter until the subject cancels their subscription, at which point said data will be deleted from servers of Brevo. The data the Processor has stored for other purposes (e.g., email addresses of registered users) remains unaffected.

1.4 Tawk.to (live chat support service) is only being used for live communication with the site's visitors of the Processor, in order to provide customer support as per the Processor's request, and in no way comes into contact with Processor's internal data or services.

1.5 The Processor utilizes the service Mailgun for sending invitations to studies using the Own Database participant recruitment tool. Within Mailgun, the metadata of a message is indexed and maintained for 30 days and the message body is stored for up to seven days. Processing of private data by Mailgun is handled in the USA (https://www.mailgun.com/gdpr/).

1.6 All operations related to payments are processed by Stripe, which conforms to the PCI DSS (Payment Card Industry Data Security Standard). The Processor's servers do not process, transfer or store any data of the card holder (https://stripe.com/payments/elements).

1.7 The Processor uses the service Google Analytics for monitoring user activity on UXtweak's website for the purposes of providing relevant information. For this purpose, Google collects anonymized statistical data about usage of the website. The Processor uses GSuite as an email provider, which means that e-mails delivered to email addresses belonging to UXtweak or sent by UXtweak's employees can be stored on Google's servers. The Processor uses Google Drive for shared files. In rare cases the Processor maintains lists of contact information in Google spreadsheets, but the Processor is continuously working on removing all such data. The Processor also uses the following: (a) Google reCAPTCHA protection for enhancing security of the Service, (b) Google Tag Manager (GTM) for deploying UXtweak code snippet used in conjunction with the Session Recording and (optionally) Website Testing tools, (c) Google Sign-In for providing a secure sign-up / sign-in method.

1.8 The Processor uses the service Zoom to provide live meeting functionality (online video calls) as part of the Live Interviews toolset (moderated research studies) of the Service, which is purchasable as a separate subscription package, or may be part of a custom plan offering as defined by a separate agreement.

1.9 The Processor uses the service HubSpot to facilitate customer relationship management (CRM) processes, including evidence of customers, providing customer support and sending promotional e-mails.

1.10 The Controller agrees that the Processor's employees use the standard office software by Microsoft (e.g., MS Office) and Google (e.g., Google Docs) and, due to this fact, Microsoft and Google may process some personal data of the Controller.

Annex No. 4: Additional legislation

1. California Consumer Privacy Act (CCPA)

1.1 In addition to compliance with the Directive (GDPR) and any other applicable law as stipulated in this Contract, to ensure compliance with the CCPA, for affected Controllers, the Processor shall not retain, use, or disclose any personal data that is subject to the CCPA ("CCPA Personal Data") for any purpose other than for the limited and specific purpose of providing the Service to the Controller as stipulated by this Contract, or as otherwise permitted by applicable law and the CCPA.

1.2 The Processor shall not:

a) sell or share CCPA Personal Data. "Sharing" for purposes of the CCPA means the disclosure, transfer, or otherwise making available personal information to a third party for cross-context behavioral advertising, whether or not money or other valuable consideration is exchanged;

b) except as allowed under the CCPA, retain, use, or disclose CCPA Personal Information other than for providing the Service, or for any business outside the direct business relationship between the Controller and the Processor;

c) except as allowed under the CCPA, combine CCPA Personal Data received from the Controller with personal information that the Processor receives from, or on behalf of, another person or persons, or collects from its own interaction with consumers.

1.3 The Processor shall notify the Controller if the Processor can no longer meet its obligations under the CCPA. Upon such notice from the Processor, the Controller may direct the Processor to take reasonable and appropriate steps to stop and remediate any unauthorized use of CCPA Personal Data by deleting all or the relevant portion of CCPA Personal Data from the Service or by such other means as reasonably agreed between the parties.

2. Digital Operational Resilience Act (DORA)

2.1 The Processor provides software in the form of a web application, allowing for improvement of user experience (UX) and quality of websites/applications/services, and does not offer financial services as defined under Regulation (EU) 2022/2554 (DORA). Furthermore, based on the current understanding of the Processor, the Processor's services are not considered critical ICT services to entities within the financial sector as outlined within DORA. Therefore, the direct obligations of DORA are not considered applicable to the Processor. However, the Processor remains committed to adhering to applicable laws and regulations, as well as maintaining cybersecurity standards as per the industry best practices.