Privacy policy

Effective on: 13 June 2022. This Privacy Policy completely replaces the previous version.

OWOX is committed to protecting your safety and privacy, and takes its responsibilities regarding the security of information very seriously.

This privacy policy explains what data OWOX collects about you, how and why OWOX uses it, who OWOX discloses it to, and how OWOX protects your privacy.

If you do not agree to this Privacy policy, please do not use our website and our services.

1. Who is collecting and/or processing your data?

OWOX, Inc., a company established under the laws of California, United States of America, with registration number C3725260, (referred to as "OWOX", "we", "us", "our" in this Privacy Policy) is a company that collects and/or processes your data.

Data controller. OWOX collects some personal data from you, for example when you use OWOX website, provide feedback on OWOX services or contact OWOX. In this case, OWOX is the data controller for purposes of European data protection legislation and OWOX takes on the obligations and responsibilities of data controllers, particularly described in General Data Protection Regulation.

Data processor. You may decide to transfer OWOX with your clients' personal data by using our services. In this case, you are the data controller and OWOX stands out as the data processor for purposes of European data protection legislation. You are solely responsible for the accuracy of clients' personal data and obtaining the legal grounds for their processing. You shall inform your clients about the use of data processors to process their personal data and that their personal data may be processed outside of the European Economic Area.

2. What personal data OWOX collects and processes?

The term "personal data" in this Privacy Policy is the information that relates to you and allows OWOX to identify you, either directly or in combination with other information that OWOX may hold. Your personal data may include for example your name, your contact details (email, telephone number), your payment details or information on how you use our website.

The personal data you provide us with is only processed and used in the manner adequate for the purpose for which it was collected. OWOX does not combine personal data that was obtained for a variety of purposes.

When providing the personal data through OWOX website, you consent to the OWOX usage of provided data in accordance with this Privacy Policy and/or any additional agreement between you and OWOX.

OWOX may collect and process the following categories of information about you:

Your contact details (name, surname, telephone number, email, company name, company website)	When you log in or create an account or project in OWOX services When you choose an offer OWOX makes available on its website When you request an OWOX services demonstration or trial When you subscribe for OWOX newsletters

	When you register for OWOX webinars When you send a request for OWOX technical support When you send a request for third-party services information (e.g. Google Analytics 360)
Your payment details (credit card number, expiry date, etc.)	When you purchase OWOX products or services When you validate your payment details
Your IP, cookies	When you visit our website When you use our services
The communications you exchange with OWOX (for example, your emails, letters, calls, or your messages on OWOX online chat service)	When you contact OWOX or you are contacted by OWOX messages on our online chat service)
Your posts and messages on social media directed to OWOX	When you interact with OWOX on social media
Your feedback	When you reply to our requests for feedback or participate in our surveys
Information about how you use our website	When you navigate on our website
Aggregated data statistics (for personalization of user experience in services)	When you provide your access to Google Analytics account

By using our services, you may be providing us with your clients' personal data. You should therefore ensure that you have collected your clients' respective consents and approval in order to process their data in accordance with applicable data protection law and the Terms of use. We shall be entitled to: obtain, collect, distribute, record, organise, adapt or alter, retrieve, consult, align, combine, transfer, use, store, block, destroy, and conduct the international transfer (including countries that do not ensure adequate level of protection of personal data) of the personal data you provide us with. Your clients' personal data belongs to you and OWOX will follow your instructions in the regard of your client's personal data. It will be stored at Google BigQuery tables and at your Google Cloud Platform project.

We do not knowingly collect personal data from children under 16 without the consent of parents or legal guardians. You must be of age of majority in your jurisdiction to use our website or services. If you are under the age of 16, you may only use our website with the permission of your parents or legal guardian.

We do not knowingly collect personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, or biometric data data concerning health or data concerning a natural person's sex life or sexual orientation.

2. Rights of data subjects

You have certain legal rights to access certain personal data we hold about you and to obtain its correction, amendment, portability or deletion.

You may exercise those rights in your account, in the “Settings” chapter, or by contacting us via data-protection@owox.com. We will respond to your request at the soonest, but in any case within 30 calendar days from the date we receive your request.

According to California Consumer Protection Act, consumers from California has the following rights:

- Right to request from OWOX:
  (1) The categories of personal data that OWOX has collected about you,
  (2) Categories of sources from which personal data are collected,
  (3) Business or commercial purpose for the collection or sale of personal data,
  (4) Categories of third parties to whom OWOX provides personal data,
  (5) Categories of your personal data that has been sold, and categories of third parties to whom personal data has been sold,
  (6) The specific personal data that OWOX has collected about you,
  You can exercise this right by using the method described above.
- The right to non-discrimination in the event you exercise your rights under the California Consumer Privacy Act.

4. How and why OWOX uses your data?

We use your personal data for the following purposes:

4.1. To provide our services to you and technical support

OWOX uses your information to perform OWOX services in relation to your project. For example, to automatically import data into your Google Analytics account, collect Google Analytics unsampled data in your Google BigQuery project, store frequently used queries for Google BigQuery, make transactions, or when you ask for the technical assistance.

4.2. To communicate with you and manage our relationship with you

When you provide your details to submit the request for information on our website, download any material or presentation from our website, request a demo of our services, register for webinar, start a trial or services usage, contacted us on social media, or in any other way express your interest in our services and products, we will communicate with you to respond on your request and subscribe you to our newsletter. You may unsubscribe from us or request to stop any communication with you by clicking the "unsubscribe" link on our email or by replying "unsubscribe" for any emails from our sales or marketing team (if "unsubscribe" link is unavailable). We will honor your request.

Occasionally we may need to contact you by email and/or telephone for administrative or operational reasons, for example in order to send you the confirmation regarding webinar registration, the reply for your request on the technical assistance, to remind you about trail expiry date or pending invoices.

Please be aware that these communications are not made for marketing purposes and as such, you will continue to receive them even if you opt-out from receiving marketing communications.

4.3. To personalize and improve your customer experience

OWOX may use your personal data in order to tailor our services to your needs and preferences and to provide you with a personalised customer experience.

OWOX may also collect information on how you use our website, which pages of our website you visit most, what products you buy, in order to understand what you like. OWOX may use this information to tailor the content and offers that you see on our website and, if you have agreed to receiving marketing communications, to send you relevant messages that we think you like.

4.4. To inform you about our news and offers that you may like

OWOX may send you marketing communications, if you have indicated your interest in our product and services: submitted the request for information on our website, downloaded any material or presentation from our website, requested a demo of our services, registered for webinar, started a trial or services usage, contacted us on social media, or in any other way expressed your interest in our services and products..

Please note that OWOX does not share your contact details and other personal data with other companies for marketing purposes, unless OWOX has obtained your consent to do so.

If you do not want to receive marketing communications from us, you can at any time opt out from receiving marketing communications by updating your account settings or by clicking on the relevant "unsubscribe" link at the bottom of any email you received from us, or by replying "unsubscribe" for any emails from our sales or marketing team (if "unsubscribe" link is unavailable).

4.5. To improve our services, fulfil our administrative purposes and protect our business interests and for marketing purposes

The business purposes for which OWOX will use your information include lead's evaluation, marketing among leads and customers, accounting, billing and audit, credit or other payment card verification, fraud screening, safety, security and legal purposes, systems testing, maintenance and development.

OWOX may use anonymous data, which will not include personally identifiable information or information that identifies or would reasonably be expected to identify you, to collect the OWOX service statistics and to improve and enhance the OWOX services (the data is collected in anonymized form, e.g. in the form of derived metrics and coefficients).

4.6. To showcase the results of using OWOX services or your feedback, only upon prior agreement with you and to the agreed extent

4.7. To comply with our legal obligations and compliance reasons, such as the prevention, detection, or investigation of a crime; loss prevention; or fraud.

OWOX may also use personal information to meet its internal and external audit requirements, information security purposes, and as OWOX otherwise believe to be necessary or appropriate: (a) under applicable law, which may include laws outside your country of residence; (b) to respond to requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities, which may include such authorities outside your country of residence; (c) to enforce our terms and conditions; and (d) to protect our rights, privacy, safety, or property, or those of other persons, court order, law or governmental request.

We use your personal data based on:

your consent,

agreement concluded with you, or to take action at your request before concluding an agreement,

compliance with our legal obligations,

based on our legitimate interests, for example, when we use cookies on our website or when we receive your data from advertising campaigns, from open public sources or as a result of communications with you.

5. Security of your data

We are committed to taking appropriate technical and organisational measures to protect your personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.

Your personal information is stored behind secured networks and is only accessible by a limited number of people who have special access rights to such systems, and are required to keep the information confidential. In addition, all information you supply is encrypted using Secure Socket Layer (SSL).

Our services use official APIs from Google, Bing, Facebook, Yandex, Vkontakte and others, where it is technically applicable to access the data that you provide.

To provide access to Google services, we use OAuth authentication. This is an open authorization protocol, which provides us with limited access to protected resources for our services without passing your data for authorization in your account.

You can limit access to your data in your Google account settings at any time.

We will protect your data in the following ways:

using cryptography, where necessary;

using password, where necessary; and

restricting access to your data (i.e. access to your personal data is granted only to those of our employees or contractors for whom the access is necessary).

6. International transfer of data

6.1. As described in this Privacy Policy, OWOX may in some instances disclose your personal data to third parties. Where OWOX discloses your personal data to a third party, we require that the third party has appropriate technical and organisational measures in place to protect your personal data.

6.2. The information that you provide to us will be held in our systems, which are located on our premises or those of an appointed third party.

6.3. We and some of our subprocessors are based outside the EEA. That is why your personal data may be accessed by and processed outside the European Economic Area, Switzerland and/or United Kingdom.

6.4. When we act as data controller, the transfer of personal data outside the EEA, Switzerland and/or United Kingdom is based on this Privacy Policy. In this case, we check if there is a European authorities decision that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection, and/or in the absence of this decision we will rely on one or more of the appropriate safeguards, referred to in Article 46 of the GDPR.

6.5. When you are (a) an EU-based controller (or a processor for an EU-based controller), (b) OWOX is engaged as a processor (or a subprocessor), (c) the conditions set forth under Article 3 of the GDPR are met, and (d) only to the extent that any processing of personal data by OWOX takes place in any country outside the EU (except if the country ensures an adequate level of protection as defined in Article 45 of the GDPR), the parties agree that the Standard Contractual Clauses, attached as annex to this Privacy Policy, will apply in respect to that processing, and OWOX will comply with the obligations of the ‘data importer’ and you will comply with the obligations of the 'data exporter'.

6.6. The following additional conditions shall apply during the international transfer of personal data (hereinafter — Client's Personal data) based on the Standard Contractual Clauses:

6.6.1. Legal basis. If you provide us with Client's Personal Data, you should comply with the applicable EU data protection laws and regulations. As between the parties, OWOX is responsible for the lawfulness of the processing of Client's Personal Data in its capacity as a processor (or subprocessor), and you are responsible for the processing of Client's Personal Data in your capacity as a controller (or a processor for an EU-based controller).

6.6.2. Subprocessor's engagement. You provide OWOX with the authorization to engage sub-processors for processing of Client's Personal Data, including transfer to third country or an international organization, provided the provisions of Standard Contractual Clauses are fulfilled. OWOX hereby confirms that it requires all of its personnel and engaged subcontractors authorized to process Client's Personal Data to commit themselves to confidentiality, or ensures that they are under an appropriate statutory obligation of confidentiality, and not to process Client's Personal Data for purposes other than as described in this Privacy Policy. This authorization should be considered as a prior written consent.

6.6.3. Integration with Third Party services. OWOX may provide links to integrations with Third Parties services, including, without limitation, certain Third Party services, which may be integrated directly into OWOX Services. If you elect to enable, access or use such Third Party Services, the access and use of such Third Party services is governed solely by the terms and conditions and privacy policies of such Third Party services, and OWOX does not endorse, is not responsible or not liable for, and makes no representations as to any aspect of such Third Party services, including without limitation their consent or the manner in which they handle Client's Personal Data or any interaction between you and the provider of such Third Party services. The provider of Third Party services shall not be deemed subprocessors for any purpose under this Privacy Policy.

6.6.4. International Transfer. You acknowledge that OWOX and its subprocessors may maintain data processing operations in countries that are outside of the EEA, Switzerland and the UK.

1.1.1. Limitation of Liability. Notwithstanding anything to the contrary, will either party of this Privacy Policy, their affiliates, officers, directors, employees, agents, service providers, suppliers or licensors be liable to the other party or any third party for any lost profits, lost sales, lost data (being data lost in the course of transmission via Your system or over

the internet through no fault of OWOX), loss of goodwill, or for any type of indirect, incidental loss or damages, incurred by the other party in connection with this Privacy Policy. For the avoidance of doubt, this provision shall not be construed as limiting the liability of either party with respect to claims brought by data subjects.

7. Term for data storage

OWOX will not store your personal data for longer than is necessary for the purpose for which it was provided or collected. OWOX will only retain the personal data that serves a legitimate purpose (e.g. applicable legal regulations may require the retention of data, or some data may be necessary for the purposes of billing outstanding amounts).

After 2 years from the moment of last visit of OWOX website, your account and your unsubscription from OWOX newsletters, OWOX at its sole discretion delete your personal data or anonymize it.

OWOX will also delete your personal data within 30 calendar days upon receiving your request for data erasure.

OWOX reserves its right to retain a part of personal data, which are required by applicable law and for the term, required by applicable law (e.g. applicable law may require that some personal data shall be retained for tax accounting or for issues of the invoice for unpaid fees).

8. Sharing your personal data

OWOX uses a limited number of third party providers to assist us in providing the services to our customers. Third parties may access, process or store personal data in the framework and upon our instructions only. OWOX may share your information with the following persons:

Affiliates. OWOX may disclose your information to its affiliates or subsidiaries, which may use your information to provide services to you or to communicate with you regarding services provision on OWOX behalf.

*Service Providers***.** OWOX may disclose the information it collects from you to third party vendors, service providers, contractors or agents who perform functions on OWOX behalf.

Other Third Parties. OWOX may disclose your information to third parties upon your instructions to do so. For example, when you ask OWOX to transfer the data from your CRM to your Google BigQuery project.

Credit and debit card companies. OWOX may disclose your payment details strictly to the companies that process the card payments for the purposes of processing of payment for OWOX services.

Business Transfers. If OWOX is acquired by or merged with another company, if substantially all of OWOX assets are transferred to another company, or as part of a bankruptcy proceeding, OWOX may transfer the information it has collected from you to this company.

9. Cookies or other tracking technologies

In order to improve our services, to provide you with more relevant content and to analyse how visitors use our website, or for direct marketing purposes, we may use technologies, such as cookies, local storage and pixels. Please be aware that in most cases we will not be able to identify you from the information we collect using these technologies.

For example, we use software to monitor customer traffic patterns and website usage to help us develop the design and layout of the website in order to enhance the experience of the visitors to our website. In addition, in order to understand how our customers interact with the emails and the content that we send, we use pixels that allow us to know if the emails we send are opened.

We use cookies and local storage on our website. These technologies are small pieces of information stored by your browser on your computer's hard drive. On your further visits to that website, the information stored in the cookie is sent back to the website. This allows the website to recognise you and tailor its content to your needs.

What cookies does OWOX use?

We use the following types of cookies:

(i) essential cookies, which are essential for the provision of access to our websites and Services;

(ii) functionality cookies, which are used to personalize the content in accordance with your actions on our website;

(iii) performance cookies, which do not identify you individually (until you enter your identification details in any of our forms) but help us to evaluate the website performance and its statistics; and

(iv) targeting/advertising cookies, which help advertise OWOX offers and services on the other sites.

We also use analytics and similar services that collect third-party cookies:

1. Google Analytics, Google Optimize, and Google AdWords (Google Privacy Policy is available at https://policies.google.com/technologies/ads?hl=en, text and URL may be changed by Google sole discretion),

2. Intercom (Intercom Privacy Policy is available at https://www.intercom.com/terms-and-policies#privacy, text and URL may be changed by Intercom sole discretion),

3. Facebook (Facebook Privacy Policy is available at https://www.facebook.com/policy.php, text and URL may be changed by Facebook sole discretion),

4. Twitter (Twitter Privacy Policy is available at https://twitter.com/en/privacy, text and URL may be changed by Twitter sole discretion),

5. LinkedIn (LinkedIn Privacy Policy is available at https://www.linkedin.com/legal/preview/privacy-policy, text and URL may be changed by LinkedIn sole discretion).

6. Yandex.Metrics (Yandex Privacy Policy is available at https://yandex.ru/support/legal/confidential/index.html?lang=en, text and URL may be changed at Yandex sole discretion),

7. AdMixer (AdMixer Privacy Policy is available at https://sales.admixer.ua/privacy, text and URL may be changed by AdMixer sole discretion),

8. Zendesk (Zendesk Privacy Policy is available at https://www.zendesk.com/company/customers-partners/privacy-policy/, text and URL may be changed by Zendesk sole discretion),

9. Albacross (Albacross Privacy Policy is available at https://albacross.com/privacy-policy/, text and URL may be changed by Albacross sole discretion),

10. Other services.

How to reject or delete cookies?

Most web browsers automatically accept cookies. However, you do not have to accept cookies and you can, should you choose to at any time, reject or block the use of cookies and delete all cookies currently stored on your device. You can find out how to do this for your particular browser by clicking "help" on your browser's menu, or by visiting: www.allaboutcookies.org, http://www.youronlinechoices.com/uk/your-ad-choices, http://optout.networkadvertising.org/.

However, if you turn off cookies, the functionality of our Services may be limited (i.e. in the case of essential cookies you may not be able to access our websites, your account and services).

10. Links

OWOX websites may contain links to others websites, which are owned and operated independently of OWOX. Therefore, any information you provide to those websites will be governed by their own privacy policy principles and data collection practices. OWOX assumes no responsibility or liability for information handling procedures and/or policies of such independent websites.

11. Revisions

OWOX may make changes to this Privacy Policy from time to time, without the advance notice and any modifications are effective when they are posted at our website.

OWOX may make changes to this Privacy Policy including as part of the new European data protection legislation which will start to apply on 25 May 2018 (the "General Data Protection Regulation") and Privacy Shield program.

12. Privacy Shield notice

Starting from 13 June 2022 OWOX withdrew from participating in the Privacy Shield Program.

13. Contact information

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to data-protection@owox.com.

You may also send your request to our data protection officer – Maksym Voloshyn, email: data-protection@owox.com.

For EU and EEA citizens — you may also contact our EU Data Representative: OWOX limited, Boumpoulinas 11, 1st floor, 1060 Nicosia Cyprus.

Statement for the performance of California Consumer Protection Act:

Based on Article 1278.130 California Consumer Protection Act we inform you on the following actions, performed in the past 12 months:

1. OWOX collected the following categories of personal data: personal data, listed in paragraph 2 of OWOX Inc Privacy Policy,
2. OWOX did not sell personal data to third parties,
3. OWOX disclosed for business purposes to its contractors and processors: personal data, listed in paragraph 2 of OWOX Inc Privacy Policy.

EU Standard Contractual Clauses

Module Two: (controller to processor)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also

notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[1] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 5 working days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[2] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller

under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(a) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[3];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) For Module Two: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Cyprus.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f) The Parties agree that those shall be the courts of Cyprus.

(g) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(h) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): You, when You act as an EU-based Controller (or a Processor for an EU-based Controller)

1. Name: Shall be filled in by You in OWOX BI Project settings

Address: Shall be filled in by You in OWOX BI Project settings

Contact person's name, position and contact details: Shall be filled in by You in OWOX BI Project settings

Activities relevant to the data transferred under these Clauses: providing personal data to the Data importer necessary for the provision of services by the Data importer to the Data exporter.

Signature and date: On the date of creating and filling in the data in the OWOX BI Project you agree to these SCC

Role (controller/processor): Controller

Data importer(s):

1. Name: **OWOX, Inc.**

Address: Suite 340 S Lemon Ave Ste 2021 Walnut CA 91789 United States

Contact person's name, position and contact details: DPO Maksym Voloshyn, data-protection@owox.com

Activities relevant to the data transferred under these Clauses: processing personal data of the Data exporter in accordance with the instructions of the Data exporter in order to deliver services to the Data exporter.

Signature and date: On the date when You create and fill in the data in the OWOX BI Project OWOX agrees to these SCC

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Natural persons employed or otherwise engaged by the data exporter, customers of the data exporter and other users of data exporter products or services, employees of the data exporter.

Categories of personal data transferred

Names, email address, phone number, username, cookies, IP address, first name, last name, subscription information.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing

The personal data transferred will be subject to activities necessary to provide the data exporter with products and services, such as: collection; recording; organisation; structuring; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission; dissemination or otherwise making available; alignment or combination; restriction; erasure or destruction.

Purpose(s) of the data transfer and further processing

Provision of services of Data importer to Data exporter

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

OWOX will not store your personal data for longer than is necessary for the purpose for which it was provided or collected. OWOX will only retain the personal data that serves a legitimate purpose (e.g. applicable legal regulations may require the retention of data, or some data may be necessary for the purposes of billing outstanding amounts).

After 2 years from the moment of last visit of OWOX website, your account and your unsubscription from OWOX newsletters, OWOX at its sole discretion delete your personal data or anonymize it.

OWOX will also delete your personal data within 30 calendar days upon receiving your request for data erasure.

OWOX reserves its right to retain a part of personal data, which are required by applicable law and for the term, required by applicable law (e.g. applicable law may require that some personal data shall be retained for tax accounting or for issues of the invoice for unpaid fees).

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The same as for Data importer

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

DPA of Cyprus

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Measures of pseudonymisation and encryption of personal data
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Measures for user identification and authorisation
Measures for the protection of data during transmission
Measures for the protection of data during storage
Measures for ensuring limited data retention
Measures for allowing data portability and ensuring erasure

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

OWOX hereby confirms that it requires all of its personnel and engaged subcontractors authorized to process Client's Personal Data to commit themselves to confidentiality, or ensures that they are under an appropriate statutory obligation of confidentiality

Where OWOX discloses your personal data to a third party, we require that the third party has appropriate technical and organisational measures in place to protect your personal data.