Name doc. : **Oxygis - Subscription agreement**

Version : 18/08/2022

Summary: By subscribing to the Oxygis Enterprise services (the "*Services*") provided by Oxygis Partners SRL and its affiliates (collectively, "*Oxygis*") in connection with Oxygis (the "*Software*"), hosted on the Oxygis Cloud Infrastructure ("*Cloud Infrastructure")* or on-premises ("*Self-Hosting*"), you (the "*Customer*") agree to be bound by the following terms and conditions (the "*Agreement*").

1. Duration of the agreement

The term of this agreement (the "Term") shall be specified in writing at the time of entering into this agreement, commencing on the date of entering into it. It shall automatically renew for an equal term unless either party provides written notice of termination to the other party at least 30 days before the end of the Term.

2. Definitions

User

Each user wishing to use Oxygis must be named and have a licence, which is nominative, corresponding to their user type. Disabled user accounts are not counted as Users.

Types of users

In an Oxygis environment, user types are determined by the roles and privileges granted to them.

Oxygis integrator

An Oxygis integrator is a third party company or individual, chosen by the Client, who works with the Client for its Oxygis related services. The Client may decide at any time to work with another Oxygis integrator, or to work directly with Oxygis (subject to notice).

Additional module

An additional module adds functionality or modifies the standard behaviour of the software. It may have been developed by Oxygis or by an Oxygis integrator on behalf of the Client, or by third parties.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Additional covered module

A covered add-on module is an add-on module for which the Customer chooses to pay a maintenance fee in order to receive support, upgrade and bug fix services.

Bug

A Bug is any failure of the Software or a Covered Add-on that results in a complete shutdown, error escalation, or security breach, and is not directly caused by faulty installation or configuration. Failure to meet specifications or requirements will be considered a Bug at Oxygis' discretion (typically, where the Software does not produce the results or performance for which it was designed, or where country-specific functionality no longer meets legal accounting requirements).

Versions covered

Unless otherwise specified, the Services provided under this Agreement are applicable only to Covered Versions of the Software, which include the last 3 major releases.

3. Access to the software

The Client may use the Software hosted on the Oxygis Cloud Infrastructure, or choose the "Self-Hosting" option. The Oxygis Cloud Infrastructure is hosted and fully managed by Oxygis, and is accessed remotely by the Client. With the "Self-Hosting" option, the Client hosts the Software on computer systems of their choice, which are not under the control of Oxygis.

For the duration of this Agreement, Oxygis grants the Client a non-exclusive, non-transferable license to use (execute but not modify) the Oxygis software.

The Client agrees to take all necessary measures to ensure the execution of the Software that verifies the validity of the use of Oxygis and collects statistics for this purpose, including, but not limited to, the execution of an instance, the number of Users and the modules installed.

Oxygis agrees not to disclose individual or nominative data to third parties without the Client's consent, and to treat all data collected in accordance with its ***privacy policy.***

Upon expiration or termination of this Agreement, this license is revoked immediately and the Client agrees to cease using the Oxygis software.

If the Client breaches the terms of this section, the Client agrees to pay Oxygis an additional fee equal to 300% of the applicable list price for the actual number of users or calculated on the last annual license amount.

4. Services

4.1 Bug fixing service

During the term of this Agreement, Oxygis agrees to make all reasonable efforts to remedy any bugs in the Software and Covered Add-On Modules submitted by the Client through the appropriate channel (typically the web form or phone numbers listed on *https://oxygis.eu/contact-us/,* or in the case of collaboration with an Oxygis integrator, the channel provided by the integrator), and to begin processing Client submissions within 2 business days.

As soon as the bug is corrected, an appropriate remedy will be communicated to the Customer. If the Customer is using a Covered Version, the Customer will not be required to upgrade to a newer Covered Version of the Software to remedy a bug.

When a bug is fixed in a Covered Version, Oxygis agrees to fix the bug in all more recent Covered Versions of the Software.

Both parties acknowledge that, as specified in the Software license and in section **7.3 Limitation of Liability of** this Agreement, Oxygis is not responsible for bugs in the Software or in the Covered Add-On Modules.

4.2 Security Update Service

Self-Hosting

During the term of this Agreement, Oxygis agrees to send a "Security Advisory" to the Client for any security bugs discovered in the Covered Versions of the Software (this excludes Additional Modules), at least 2 weeks prior to making the Security Advisory public, unless the bug has already been publicly disclosed by a third party. Security Notices include a full description of the bug, its cause, its possible impact on the Customer's systems and the corresponding solution for each Covered Version.

The Customer understands that the Bug and the information contained in the Security Notice shall be treated as Confidential Information as described in **Section 6.4 Confidentiality during** the embargo period prior to public disclosure.

Cloud infrastructure

Oxygis agrees to apply security remedies for any Security Bug discovered in a version of the Software hosted on its Cloud Infrastructure, on all systems under its control, as soon as the remedy is available, with a minimum of manual action by the Client.

4.3 Software upgrade services

During the term of this Agreement, the Client may submit upgrade requests through the appropriate channel (typically the Oxygis Help Desk), to convert a database of the Software from any version of the Software to a newer covered version (the "Target Version"). In most

cases, this operation is performed spontaneously by our team with prior notification to the Client.

For self-hosting, upgrade requests must include a copy of the Customer's database and associated data (usually obtained from the Software Backup menu). In most cases, our Clients provide secure remote access to their infrastructure to enable our teams to assist the Client with the upgrade.

The upgrade service is limited to the technical conversion and adaptation of the Customer's database to make it compatible with the target version, the correction of any bugs directly caused by the upgrade operation and not normally occurring in the target version, and the conversion of the source code and data of the additional modules covered for the target version.

It is the Customer's responsibility to check and validate the upgraded database for bugs, to analyse the impact of changes and new features implemented in the target version, and to convert and adapt to the target version any third party extensions to the software that were installed in the database prior to the upgrade (e.g. unconverted add-on modules). The Customer may submit multiple upgrade requests for a database until an acceptable result is achieved.

4.4 Cloud hosting services

During the term of this Agreement, when the Client chooses to use the Cloud Infrastructure, Oxygis agrees to provide at least the following services

- Choice of multiple hosting regions (not included in standard licences)
- Hosting in Tier III or equivalent data centres with 99.9% network availability.
- Class A SSL (HTTPS) Communication encryption
- Fully automated, verified backups (replication across multiple regions is on demand and subject to additional costs).
- Disaster recovery plan, tested regularly

Details of cloud hosting services are described in the document ***Cloud Hosting - Service Level Agreement***

4.5 Support services

Scope
During the term of this Agreement, the Customer may open an unlimited number of support tickets free of charge, exclusively for questions concerning Bugs (see **4.1 Bug Resolution Service**).

Other support requests, such as development or customization issues, may be covered by the purchase of a separate service contract called a "Success Pack". In the event that it is unclear whether a request is covered by this contract, the decision is at the discretion of Oxygis.

Availability
Tickets can be submitted via the web form or phone numbers listed on https://oxygis.eu/contact-us/ , or, if you are working with an Oxygis integrator, via the channel provided by the partner, subject to local business hours.

4.6 Success Pack Distinct Service Agreement

To ensure a successful and personalised implementation, Oxygis and/or its integrators offer a set of premium à la carte services in the form of "Success Packs". These services can be, for example: remote or on-site training, customised development, customised data import, etc.

The hours of a **Success Pack remain valid for a period of two years** after acceptance of the offer. At the end of the two years, any unused hours are lost and the Client may acquire a new Success Pack if necessary.

The Client may at any time request/receive a detailed account of the hours used and still available in his Success Pack.

Once ordered, Success Packs are non-refundable, even in the event of termination of the contract with Oxygis.

4.7 Working with an Oxygis Integrator

For bug fixes, support and upgrade services, the Client can either work with an Oxygis integrator as their primary point of contact, or work with Oxygis directly.

If the Client decides to work with an Oxygis Integrator, Oxygis will subcontract services related to the additional modules covered to the Oxygis Integrator, who becomes the Client's primary point of contact. The Oxygis Integrator may contact Oxygis on behalf of the Client for second level support regarding the standard functionality of the Software.

If the Client chooses to work directly with Oxygis, the services related to the Additional Modules covered are provided *if and only if* the Client is hosted on the Oxygis Cloud Infrastructure.

5. Taxes and fees

5.1 Standard fees

Standard fees for Oxygis subscription and services are specified in writing at the time of contract conclusion. They may be based on the number of Users and the version used, a number of citizens for public entities (e.g. cities, provinces, ...) or based on a geographical area.

If, during the term of the contract, the Customer exceeds the metrics agreed upon at the time of the signature of the contract and determining the price of the licenses (e.g.: number of users, number of citizens for cities and municipalities...), the Customer agrees to pay additional fees equivalent to the list price applicable at the beginning of the contract or at the time of the last renewal for exceeding these metrics for the remainder of the contract term.

5.2 Taxes

All fees and charges are exclusive of any federal, provincial, state, local or other governmental taxes, fees or charges (collectively, "Taxes"). The Customer is responsible for the payment of all Taxes associated with purchases made by the Customer under this Agreement, except to the extent that Oxygis is legally required to pay or collect Taxes for which the Customer is responsible.

6. Terms of service

6.1 Obligations of the Customer

The Client undertakes to :

- pay to Oxygis all fees applicable to the Services under this Agreement, in accordance with the payment terms specified upon execution of this Agreement
- immediately inform Oxygis when the actual number of Users exceeds the number specified at the conclusion of the Agreement, and in this case, pay the applicable additional fees as described in Article **5.1 Standard Fees** ;
- take all necessary measures to ensure the execution of the part of the Software that verifies the validity of the use of Oxygis Cloud, as described in **3. Access to the Software** ;
- appoint 1 dedicated contact person at Oxygis for the duration of the Contract;
- provide 30 days written notice to Oxygis before changing their primary point of contact to work with another Oxygis integrator, or to work with Oxygis directly.

Where the Customer chooses to use the Cloud Infrastructure, the Customer further agrees to :

- take all reasonable steps to ensure the security of their user account, including choosing a strong password and not sharing it with anyone else;

- make reasonable use of the hosting services, excluding any illegal or abusive activity, and strictly abide by the rules described in the acceptable use policy.

When the Client chooses the "Self-Hosting" option, he/she also agrees to :

- take all reasonable steps to protect the Client's files and databases and to ensure that the Client's data is safe and secure, recognizing that Oxygis cannot be held responsible for any loss of data;
- grant Oxygis the access necessary to verify the validity of the use of the Oxygis Cloud upon request (for example, if the automatic validation proves inoperative for the Client);

6.2 No soliciting or hiring

Unless the other party consents in writing, each party, its affiliates and representatives agree not to solicit or offer employment to any employee of the other party who is involved in the performance or use of the services under this contract, for the duration of the contract and for a period of 12 months from the date of termination or expiration of this contract. In the event of a breach of the terms of this section resulting in the dismissal of the said employee for this purpose, the breaching party agrees to pay to the other party an amount of 30,000.00 Euros (thirty thousand Euros).

6.3 Advertising

Unless otherwise notified in writing, each party grants to the other a worldwide, non-transferable, non-exclusive, royalty-free license to reproduce and display the other party's name, logos and marks solely for the purpose of referring to the other party as a Customer or supplier on websites, press releases and other marketing materials.

6.4 Confidentiality

Definition of "confidential information" :

> Any information disclosed by one party (the "disclosing party") to the other party (the "receiving party"), whether orally or in writing, which is designated as confidential or which ought reasonably to be considered confidential given the nature of the information and the circumstances of its disclosure. In particular, any information relating to the activities, business, products, developments, trade secrets, know-how, personnel, Customers and suppliers of either party shall be treated as confidential.

For all Confidential Information received during the term of this Agreement, the receiving Party shall exercise the same degree of care as it uses to protect the confidentiality of its own similar Confidential Information, but not less than reasonable care.

The Receiving Party may disclose the Disclosing Party's Confidential Information to the extent required by law, provided that the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure, to the extent permitted by law.

6.5 Data protection

Definitions

"Personal Data", "Controller", "Processing" shall have the same meanings as in Regulation (EU) 2016/679 and Directive 2002/58/EC, and any regulations or legislation amending or replacing them (hereinafter referred to as "Data Protection Legislation").

Processing of personal data

The parties acknowledge that the Client's database may contain Personal Data, for which the Client is the Controller. This data will be processed by Oxygis when requested by the Client, using any of the services that require a database (for example, cloud hosting services or database upgrade service), or if the Client transfers its database or a portion of its database to Oxygis for any reason related to this Agreement.

This processing will be carried out in accordance with data protection legislation. In particular, Oxygis undertakes to:

- (a) process Personal Data only when and as directed by the Client, and for the purpose of performing any of the services contemplated by this Agreement, except as required by law, in which case Oxygis will provide prior notice to the Client, unless prohibited by law;
- (b) ensure that all persons within Oxygis authorised to process personal data have undertaken to respect confidentiality;
- (c) implement and maintain appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure;
- (d) promptly forward to the Client any data protection requests that have been submitted to Oxygis regarding the Client's database;
- (e) inform the Customer as soon as possible upon becoming aware of and confirming any accidental, unauthorised or unlawful processing, disclosure or access to personal data;
- (f) inform the Client if the processing instructions violate applicable data protection legislation, as determined by Oxygis;
- (g) make available to the Customer all information necessary to demonstrate compliance with the Data Protection Legislation and to permit and reasonably assist with audits, including inspections, conducted or commissioned by the Customer;
- (h) permanently delete all copies of the Client's database in the possession of Oxygis, or return such data, at the Client's option, upon termination of this Agreement, subject to the time limits specified in the ***Oxygis Privacy Policy;***

With respect to items (d) through (f), the Client agrees to provide Oxygis with accurate contact information at all times as necessary to notify the Client's data protection officer.

Subprocessors
The Client acknowledges and agrees that in order to provide the Services, Oxygis may use third party service providers (Subcontractors) to process Personal Data. Oxygis undertakes to use Subcontractors only in accordance with data protection legislation. Such use will be covered by a contract between Oxygis and the Subcontractor who provides guarantees to that effect. The ***Oxygis Privacy Policy***, published at provides updated information regarding the names and purposes of the Subcontractors currently used by Oxygis to perform the Services.

6.6 Termination

If either party fails to perform any of its obligations hereunder, and if such breach has not been cured within 30 calendar days of written notice of such breach, this Agreement may be terminated immediately by the non-breaching party.

In addition, Oxygis may terminate the contract immediately in the event that the Client fails to pay the applicable fees for the services within 21 days of the due date specified on the corresponding invoice, and after a minimum of 3 reminders.

6.7 Survival provisions

Sections "**6.4 Confidentiality**", "**7.2 Disclaimer**", "**7.3 Limitation of Liability**" and "**8. General Provisions**" shall survive any termination or expiration of this Agreement.

7. Warranties, waivers, liability

7.1 Guarantees

Oxygis holds the copyright to 100% of the code of the Software, and confirms that all software libraries necessary to use the Software are available under a license compatible with the Software license.

During the term of this Agreement, Oxygis agrees to use commercially reasonable efforts to perform the Services in accordance with generally accepted industry standards, provided that:

- the Customer's computer systems are in good working order and, for Self-Hosting, that the Software is installed in an appropriate operating environment;
- the Client provides adequate troubleshooting information and, for Self-Hosting, any access that Oxygis may need to identify, reproduce and address problems;
- all amounts due to Oxygis have been paid.

The Client's sole and exclusive remedy and Oxygis' sole obligation for any breach of this warranty is for Oxygis to resume performance of the Services at no additional charge.

7.2 Disclaimer

Except as expressly provided herein, neither party makes any warranty of any kind, whether express, implied, statutory or otherwise, and each party specifically disclaims all implied warranties, including any implied warranties of merchantability, fitness for a particular purpose or non-infringement, to the maximum extent permitted by applicable law.

Oxygis does not warrant that the Software complies with any local or international law or regulation.

7.3 Limitation of liability

To the maximum extent permitted by law, the aggregate liability of each party, together with its affiliates, arising out of or in connection with this Agreement shall not exceed 50% of the total amount paid by the Customer under this Agreement in the 12 months immediately preceding the date of the event giving rise to such claim. Multiple claims do not extend this limitation.

In no event shall either party or its affiliates be liable for any indirect, special, exemplary, incidental or consequential damages of any kind, including, but not limited to, loss of revenue, profits, savings, loss of business or other financial loss, downtime or delay costs, loss or corruption of data, arising out of or in connection with this Agreement, regardless of the form of action, whether in contract, tort (including strict negligence) or any other legal or equitable theory, even if a party or its affiliates have been advised of the possibility of such damages, or if a party's or its affiliates' remedy does not serve its essential purpose.

7.4 Force Majeure

Neither party shall be liable to the other for delay in performance or failure to perform under this Agreement where such delay or failure is caused by *force majeure*, such as government regulation, fire, strike, war, flood, accident, epidemic, embargo, appropriation of plant or product in whole or in part by any government or public authority, or any other cause or causes, whether or not such force majeure exists, flood, accident, epidemic, embargo, appropriation of plant or product in whole or in part by any government or public authority, or any other cause or causes, whether of a similar or different nature, beyond the reasonable control of such party so long as such cause or causes exist.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

8. General provisions

8.1 Applicable law

This contract and all orders of the Customer are subject to Belgian law. Any dispute arising out of or in connection with this contract or any of the Customer's orders shall be subject to the exclusive jurisdiction of the Brussels Business Court.

8.2 Divisibility

In the event that one or more of the provisions of this Agreement or its application is invalid, illegal or unenforceable in any respect, the validity, legality and enforceability of the remaining provisions of this Agreement and its application shall not in any way be affected or impaired. Both parties undertake to replace any invalid, illegal or unenforceable provision of this Agreement with a valid provision having the same effect and purpose.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Name doc. :	**Oxygis - Acceptable Use Policy**
Version:	18/08/2022
Summary:	Use of Oxygis Cloud Services is subject to this Acceptable Use Policy (AUP). This AUP is incorporated by reference into and governed by the ***Oxygis Subscription Agreement*** between you (Client) and Oxygis Partners SRL. Clients who violate these rules may have their subscription **suspended without notice**. Subscription fees will generally **not be** refunded.

I. Illegal or harmful use

You may not use the Oxygis Cloud Services to store, display, distribute or otherwise deal with illegal or harmful content. This includes:

- **Illegal activities:** promotion of sites or services related to gambling or child pornography.
- **Harmful or fraudulent activities:** Activities harmful to others, promotion of fraudulent goods, services, schemes or promotions (e.g., get-rich-quick schemes, Ponzi and pyramid schemes, phishing or pharming), or other deceptive practices.
- **Illegal content:** Content that infringes the intellectual property of others.
- **Offensive content:** Content that is defamatory, obscene, abusive, invasive of privacy or otherwise objectionable, including content that constitutes child pornography, relates to bestiality or depicts non-consensual sexual acts.
- **Harmful content:** Malicious and malware content, such as viruses, Trojan horses, worms, etc.
- **Spam Content:** Content published for "black hat SEO" purposes, using tricks such as link building / link spam, keyword spam, in order to exploit the reputation of Oxygis services to promote third party content, goods or services.

II. Security breaches

You may not attempt to compromise Oxygis Cloud services, access or modify content that does not belong to you, or engage in other malicious actions:

- **Unauthorized Access:** Accessing or using any Oxygis Cloud system or service without authorization.
- **Security Research:** Conducting any security research or audit on Oxygis Cloud systems without written permission, including via scanners and automated tools. Please see our ***Responsible Disclosure*** document for more information on Oxygis security research.
- **Listening:** listening to or recording data that does not belong to you without permission.
- **Other attacks:** non-technical attacks such as social engineering, phishing or physical attacks against any person or system.

III. Abuse of networks and services

You may not abuse the resources and systems of Oxygis Cloud. In particular, the following activities are prohibited:

- **Network abuse:** causing a denial of service (DoS) by flooding systems with network traffic that slows down the system, makes it inaccessible or has a significant impact on the quality of service.
- **Unthrottled RPC/API calls**: sending a large number of remote RPC or API calls to our systems without proper throttling, with the risk of impacting the quality of service for other users. Note: Oxygis provides batch APIs for imports, which should not be necessary. Limited calls are generally acceptable for non-sustained use, at a rate of one call per second, with no parallel calls. Exceptions may be allowed on a case-by-case basis for Oxygis Cloud (please **contact us** if you think you need them), dedicated hosting mode may be considered as an alternative to this restriction.
- **Overload:** deliberate impact on the performance or availability of systems with abnormal content such as very large amounts of data, or a very large number of items to be processed, such as electronic bombs.
- **Crawling:** Automatically crawling resources in a way that has an impact on system availability and performance.
- **Attack:** Use Oxygis Cloud Services to attack, crawl, or otherwise impact the availability or security of third party systems.
- **Abusive Registrations:** Use of automated tools to repeatedly register or subscribe to Oxygis services.

Name doc. :	**Oxygis - Cloud Hosting - Service Level Agreement**
Version:	18/08/2022
Summary:	Databases & services hosted on the Oxygis Cloud Infrastructure benefit from the following service level at all times:

I. Operating time - 99.9%.

- Customer databases are hosted in the Azure Western Europe region
- We work with Microsoft Azure services which offer a guarantee of at least 99.95% availability

II. Backups and disaster recovery

- Weekly backups kept for 1 year
- Backups stored on / and following Microsoft Azure policies within an availability zone with replication to multiple data centres.

III. Security

The security of your data is very important to us, and we design our systems and procedures to ensure this. Here are some examples:

- **HTTPS -** Use of the secure HTTPS protocol to encrypt exchanges between Clients and the server.
- **Reliable platform** - Hosting of the application on Azure which provides the guarantee of hardware, data storage, network.
- **Passwords** - Client passwords are protected by industry-standard PBKDF2+SHA512 encryption (salted + stretched for thousands of rounds).
- **Isolation -** Client data can be stored in dedicated databases - no sharing of data between Clients, no access from one database to another.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

IV. Service continuity plan

Perimeter covered by Oxygis

Oxygis designs and develops its applications by systematically striving to :

- Minimise the need for system and infrastructure administration by using managed services provided by the world's leading cloud providers (e.g. Microsoft Azure, Amazon Web Services);
- Minimise dev ops operations through automated deployment and testing dev ops systems.

This is done with a view to maintaining a human-sized, highly agile operational team that can devote most of its time to developing new features.

In doing so, Oxygis transfers responsibility for the lower layers of the architecture to the cloud provider, offering an unparalleled level of service and minimising the multitude of risks encountered in a more traditional approach.

This does not detract from the fact that Oxygis retains a degree of responsibility which it is keen to honour.

Oxygis continually evolves the architecture of the cloud infrastructure it uses to minimize security and downtime risks to its services by following best practices recommended by the cloud service provider and the community.

Our scope of responsibility includes at least :

- Endpoints
- All data necessary for the execution of our applications. Excluded from this scope: data entered by the Client.
- The management of the accesses and accounts of its employees and the administrator accounts of its Clients. The Client remains responsible for the non-disclosure of its login and password to third parties, as well as for the management of the access rights it grants to its users through the Oxygis administration user interface.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

The diagram below illustrates the concept of shared responsibility between Oxygis, its Cloud Service Provider (Microsoft Azure) and the Client.

Responsibility	Oxygis Cloud Infrastructure - SaaS (hosted on a Paas infrastructure)		Self-hosting : Customer Infrastructure**.
Information and data			
Terminals (Mobile and Personal Computers)*			
Accounts and identities			
Identity and directory infrastructure			
Applications			
Network control			
Operating system			
Physical hosts			
Physical network			
Physical data centre			

* A distinction is made here between information, data, terminals and accounts/identities belonging to the Client or to Oxygis. More explicitly and by way of example, the Client remains responsible for the veracity and quality of the information and data that it encodes in Oxygis. Oxygis is responsible for the information and data it integrates into its applications.
**Applicable only if the Client decides to use Oxygis on its own infrastructure

	Microsoft Azure
	Oxygis
	The Client

Level of service continuity provided and back-up solutions :

Most of the service continuity provided is covered by the Cloud Service Provider on which the Oxygis architecture is deployed. The infrastructure and managed services used by Oxygis (e.g. Azure App Service, Azure SQL Database, ...) are designed to provide high availability, very low risk of data loss and low risk of service interruption.

These managed services come with options for security, performance (e.g. auto-scaling of instances or auto-tuning of db) and replication to other regions. Some options are systematically activated by us. Other options (e.g., multi-region replication, multi-zone deployment, specific backups, etc.) are reviewed in collaboration with the Client and are activated upon request. However, Oxygis reserves the right to pass on the additional cost generated by the activation of these options.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

In addition to this, Oxygis has organised its team so that every day two people are responsible for ensuring a presence for the helpdesk, which is accessible by telephone, email and through the Oxygis ticket management system available at https://oxygis.odoo.com/helpdesk/.

In the event of partial or total unavailability of personnel, a back-up procedure is implemented so that the teams of our sister company Aloalto, sharing the same offices, are able to react without delay. In the event that Aloalto is completely unavailable, Oxygis can still rely on its network of integrator partners.

The possible unavailability of Oxygis' premises does not affect the continuity of the service. Oxygis does not host any infrastructure on its premises that could affect the proper functioning of its applications. 100% of the infrastructure is in the cloud.

Maximum Allowable Interruption Duration (MAD) and Maximum Allowable Data Loss (MADL):

DIMA and PDMA are defined on a service-by-service basis by Microsoft Azure:

Example: Azure SQL DB Service: https://docs.microsoft.com/en-us/azure/azure-sql/database/business-continuity-high-availability-disaster-recover-hadr-overview

Name doc. : **Oxygis -** Privacy **Policy**

Version: 18/08/2022

I. How we protect your privacy

- on Oxygis.eu and when you use our services -

Oxygis Partners SRL and its affiliates offer a number of services to help you run your business, including a platform to host your own Oxygis database. As part of these services, we collect data about you and your business. This data is not only essential for the operation of our services, but also for the security of our services and all of our users. This policy explains what information is collected, why it is collected and how we use it.

II. Information we collect

Most of the personal data we collect is provided directly by our users when they register and use our services. Other data is collected by recording interactions with our services.

- **Account and contact details**

When you register on our website to use or download one of our products, or to subscribe to one of our services (Oxygis applications, free trial, etc.), or when you fill out one of our contact forms, you voluntarily provide us with certain information. This information typically includes your *name, company name, email address, and* sometimes *your phone number, mailing address* (when an invoice or delivery is required), your *industry* and *interest in Oxygis, and* a *personal password*.

We never record or store our Customers' credit card information, and we always rely on trusted third-party **PCI-DSS compliant payment processors** for credit card processing, including recurring payment processing.

- **Data on job applications**

When you apply for a job on our website or through an employment agency, we generally collect your contact information (*name, email address, telephone number*) and any information you choose to provide in your *cover letter* and *resume*. If we decide to send you a job offer, we will also ask you to provide additional personal information in order to meet our legal obligations and

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

personnel requirements.
We will **not** ask you to provide information that is not necessary for the recruitment process. In particular, we will **never** collect information about your racial or ethnic origin, political opinions, religious beliefs, trade union membership or sex life.

- **Navigation data**

When you visit our website and access our online services, we detect and store your *browser*'s *language and geolocation in* order to tailor your experience to your country and language preference. Our servers also passively record a summary of information sent by your browser for statistical, security and legal purposes: your *IP address*, the *time and date of your visit*, your *browser version and platform,* and the *web page that referred you* to our website.

Your browser may also be used to store and retrieve your current session data, using a session cookie (see also the **Cookies** section for more details).

Form protection: Some forms on our website may be protected by Google reCAPTCHA. This technology relies on heuristics based on the technical characteristics of your browser and device, and may also use specific Google cookies. See also Google's privacy policy and terms of use in the **Third Party Service Providers** section below.

- **Client databases**

When you subscribe to an Oxygis Cloud service and create your own Oxygis database (e.g. by starting a free trial), any information or content you submit or upload to your database is yours to keep and control.

Similarly, when you ask us to upload an on-premises database to the Oxygis Cloud, you own the data it contains. This data will often include personal information, for example: *your employee list, your contacts and Clients, your messages, photos, videos, etc*. We only collect this information on your behalf, and **you always retain full ownership and control of this data**.

III. How we use this information

- **Account and contact data**

We use your contact information to provide our services, to respond to your requests and for billing and account management purposes. We may also use this information for marketing and communication purposes (our marketing messages are always accompanied by an option to opt-out at any time). We also use this data in aggregate/anonymised form to analyse trends in the service.
If you have registered to participate in an event published on our website, we may transfer your *name, email address, telephone number* and *company name* to our local organiser and event sponsors for direct marketing purposes and to facilitate event preparation and booking.
If you have expressed interest in using Oxygis or have requested to be contacted by an Oxygis service provider, we may also transfer your *name, email address, phone number* and *company*

name to one of our official **partners** in your country or region to contact you for local support and services.

- **Data on job applications**

We will only process this information as part of our recruitment process, to assess and monitor your application, and as part of the preparation of your contract, should we decide to send you a job offer. You may contact us at any time to request that we delete your information.

- **Browser data**

This automatically recorded data is analysed anonymously in order to maintain and improve our services. Google reCAPTCHA may also be used for security purposes to prevent abuse of our services. In this case, we only process the anonymous score that reCAPTCHA determines based on your browser and device.
We will only correlate this data with your personal data when required by law or for security purposes if you have violated our acceptable use policy.

- **Customer database**

We collect and process this data only on your behalf, in order to perform the services you have subscribed to, and based on the instructions you explicitly gave when registering or setting up your Oxygis service and database. Our support staff and engineers may access this information in a limited and reasonable manner to resolve any problems with our services, or at your explicit request for support purposes, or as required by law, or to ensure the security of our services in the event of a breach of our acceptable use policy in order to maintain the security of our services.

IV. Access, update or delete your personal information

- **Account and contact data**

You have the right to access and update the personal data you have previously provided to us. You may do so at any time by logging into your personal account on Oxygis. If you wish to permanently delete your account or personal data for a legitimate purpose, please contact our **helpdesk** to request this. We will take all reasonable steps to permanently delete your personal information, unless we are required to retain it for legal reasons (typically, for administrative, billing and tax reporting purposes).

- **Data on job applications**

You may contact us at any time to request access to, update or delete your application information. The easiest way to do this is to reply to the last message you exchanged with our human resources staff.

- **Client database**

You can manage all data collected in your Oxygis hosted databases at any time, using your administration credentials, including modifying or deleting any personal data stored there. At any time, you can export a complete backup of your database by simply requesting it from our Helpdesk, in order to transfer it, or to manage your own backups/archives. You are responsible for the processing of this data in compliance with all confidentiality rules. You can also request the deletion of all your data via our helpdesk at any time.

- **Security retention period**

we keep a copy of your data in our backups for security reasons, even after it has been deleted from our active systems. See **Data retention** for more details.

V. Security

We are aware of the importance and sensitivity of your personal data, and we take a large number of measures to ensure that this information is processed, stored and preserved securely against data loss and unauthorised access. Our technical, administrative and organisational security measures are described in detail in our ***security policy***.

VI. Third party service providers / subcontractors

To support our operations, we rely on several service providers. They help us provide various services such as payment processing, web analytics, cloud hosting, marketing and communication, etc.

Whenever we share data with these service providers, we ensure that they use it in accordance with data protection legislation and that the processing they carry out for us is limited to our specific purpose and covered by a specific data processing contract.

Below is a list of the service providers we currently use, why we use them and the type of data we share with them.

A. Sub-processors

These third party service providers process data for which Oxygis is the controller or processor, on behalf of Oxygis.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Important: Due to the wide variability of resources and services provided by these sub-processors, Oxygis Clients cannot choose which sub-processor will be used to process their data. They can, however, choose their primary *hosting region* (see **Data Location** section).

Subprocessors	Objective	Shared data
Microsoft Azure **Privacy and security**	Infrastructure and hosting of Oxygis. eu (production + backups), Oxygis SaaS (production + backups), DDOS protection.	**Currently hosted on Microsoft Azure**: Production data from Oxygis and its affiliated services, including shared and individual Oxygis Online (SaaS) client databases; Backup data for all Oxygis cloud services. **Data Center Certifications**: **ISO 27001, SOC 1 TYPE II, SOC 2 TYPE II, PCI-DSS, CISPE, SecNumCloud, CSA STAR**.
Amazon Web Services, Inc. **Privacy and Security**	Infrastructure and hosting of Oxygis Infocenter (cadastral and shapefile database)	**Currently hosted by AWS**: Production data from Oxygis.eu and its affiliated services, including Oxygis Infocenter, Backup data for all Oxygis cloud services. **Data centre certifications**: **ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC3, PCI-DSS, HIPAA, CISPE, CSA STAR**.
Kinsta.com **Privacy and security**	Infrastructure and hosting of the Oxygis website	**Currently hosted by Kinsta:** Oxygis WordPress website and database. Kinsta is hosted on Google Cloud Platform.

B. Subcontractors and third party auditors

These third party service providers process the data for which Oxygis is a controller, as processors, on behalf of Oxygis, or they receive such data as controllers, for the specific purpose of performing the services for which they have been engaged.

Service provider	Objective	Shared data
Google's reCAPTCHA **Privacy and security**	Protection of the form.	**Used by Google reCAPTCHA**: browser and device characteristics, Google cookies.
Calendly **Privacy and security**	Programming of the demo/meeting on Oxygis.eu.	**Shared with Calendly** : All personal information entered by the user in the planning form: name and contact details, reason for the request, etc.
CloudFlare **Security and privacy** **Cookie Policy**	Distributed caching of static resources and images of Oxygis.eu	**Used by CloudFlare:** Browser and device characteristics, CloudFlare cookies.

Service provider	Objective	Shared data
MailChimp / Intuit **Privacy and security**	Mail campaigns	**Used by MailChimp:** Email campaigns to inform our Customers about new features, updates, security issues or for marketing purposes. It is always possible to unsubscribe from these campaigns.

VII. Data retention

- **Account and contact data**

We will only retain such data for as long as is necessary to fulfil the purpose for which it was collected, as set out in this policy, including any legal retention period, or for as long as is necessary for the legitimate and reasonable promotion of our products and services.

- **Data on job applications**

If we do not hire you, we may retain the information you have provided for up to 3 years in order to contact you again for any new job opportunities that may arise, unless you ask us not to do so. If we do employ you, your personal information will be retained for the duration of your employment contract with us, and thereafter for the legal retention period applicable in the country where we have employed you.

- **Browser data**

We may retain this data for a maximum of 12 months, unless we need to retain it as part of a legitimate concern relating to the security or performance of our services, or if required by law. Any server-side session information is only retained for 3 months when actively used, otherwise it is deleted after 7 days.

- **Customer database**

We only keep this data for as long as it is needed to provide the services you have subscribed to. For databases hosted on the Oxygis Cloud, if you cancel the service, your database is kept deactivated for 3 weeks (the grace period during which you can change your mind) and then destroyed.

Security retention period :

As part of our ***security policy***, we always try to protect your data from accidental or malicious deletion. Therefore, after we have deleted any of your personal information (account and contact data) from our database at your request, or after you have deleted any personal information from your database (Customer database), or if you delete your entire database, it is not immediately

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

deleted from our secure and unalterable backup systems. Personal data may remain stored in these backups for up to 12 months until they are automatically destroyed.

We will not use these backups of your deleted data for any purpose other than to maintain the integrity of our backups, unless you or the law requires us to do so.

VIII. Physical location of data / Data transfers

Hosting services

- **Places of accommodation**

Clients' databases are hosted in the Oxygis Cloud region closest to their place of residence. They may request a change of region (subject to availability):

  - Europe (Netherlands, France, Belgium, Germany, Ireland)

- **Backup locations**

Backups are replicated to multiple data centres within an availability zone to meet our disaster recovery objectives. Customers may request replication to other availability zones in the following countries, **regardless of the region of origin**:

  - Netherlands, France, Belgium, Germany, Ireland

- **International staff**

In some cases, the personal data referred to in this Privacy Policy may be accessed by staff members of Oxygis Partners SRL subsidiaries in other countries. Such access will always be carried out for the same purposes and with the same confidentiality and security precautions as if it were carried out by our own local staff, so that all the guarantees we provide remain applicable.

We use the **EU standard contractual clauses** to bind our subsidiaries in a way that provides sufficient data protection safeguards for the limited and temporary data transfers that take place for this access.

IX. Disclosure to third parties

Except as explicitly stated above, we do not sell, trade, or otherwise transfer your personal data to third parties. We may share or disclose aggregated or de-identified information, for research purposes, or to discuss trends or statistics with third parties.

X. Cookies

Cookies are small pieces of text sent by our servers to your computer or device when you access our services. They are stored in your browser and later sent back to our servers so that we can provide contextual content. Without cookies, using the web would be a much more frustrating experience. We use them to support your activities on our website, for example your session (so you don't have to log in again) or your shopping cart.

Cookies are also used to help us understand your preferences based on your previous or current activity on our website (the pages you have visited), your language and your country, enabling us to provide you with improved services. We also use cookies to help us compile aggregate data about site traffic and interaction so that we can provide better site experiences and tools in the future.

We also use third party services such as Google Analytics, which set and use their own cookies to identify visitors and provide their own contextual services. For more information about these third party providers and their cookie policies, please see the relevant references in the **Third Party Service Providers** section.

To date, Oxygis records a very limited number of cookie categories when visiting our website. Our website will function properly even if the visitor rejects or discards the cookies.

This may change in future versions of our website as follows:

Cookie category	Objective
Session and security	Authenticate users, protect user data and enable the website to provide the services users expect, such as maintaining the contents of their shopping cart or enabling file downloads. The website will not function properly if you reject or delete these cookies.
Preferences	Store information about the preferred look and feel of the website, such as your preferred language, region and time zone. Your experience may be degraded if you delete these cookies, but the website will still function.
History of interaction	Used to collect information about your interactions with the website, the pages you have visited and any specific marketing campaigns that brought you to the website.

Cookie category	Objective
	We may not be able to provide you with the best service if you refuse these cookies, but the website will work.
Advertising and marketing	Used to make advertising more attractive to users and more valuable to publishers and advertisers, for example by providing more relevant ads when you visit other websites that display ads or to improve reporting on the performance of advertising campaigns. Note that some third party services may set additional cookies on your browser to identify you. You can opt out of the use of third party cookies by visiting the **Network Advertising Initiative opt-out page**. The website will continue to function if you reject or delete these cookies.
Analytical	To understand how visitors use our website, via Google Analytics. Learn more about **Analytics cookies and privacy information.** The website will continue to function if you refuse or delete these cookies.

You can instruct your computer to notify you each time a cookie is sent, or you can choose to disable all cookies. Every browser is a little different, so check your browser's help menu to learn the correct way to change your cookies, or check the links below:

- Chrome: **https://support.google.com/chrome/answer/95647?hl=en**
- Advantage : https:**//support.microsoft.com/en-us/help/4468242/microsoft-edge-browsing-data-and-privacy**
- Firefox: **https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer**
- Safari: **https://support.apple.com/guide/safari/manage-cookies-and-website-data-sfri11471/mac**

We do not currently support Do Not Track signals as there is no industry standard for compliance.

XI. Policy updates

We may update this privacy policy from time to time to clarify it, to reflect any changes to our website or to comply with legal requirements. The "Last updated" notice at the top of the policy indicates the last revision, which is also the effective date of those changes.

XII. Contact us

If you have any questions about this privacy policy, or if you would like information about your personal data, please contact the **Oxygis** helpdesk or contact us by phone at +32 (0)2 736 10 17 or by e-mail at **info@oxygis.eu** or by mail :

Oxygis Partners SRL
Eikelenbergstraat, 20
1700 Dilbeek
Belgium
VAT : BE 0872.350.989

Or

Oxygis Partners (Foreign company registered with the RCS)
130, Boulevard de la Liberté
59800 Lille
France

SIREN : 811593730
VAT: FR 13 811 593 730

Name doc. :	**Oxygis - General Data Protection Regulation (GDPR)**
Version:	18/08/2022
Summary :	Oxygis' guide to European data protection rules. Overview of new privacy laws and best practices with Oxygis

As of 25 May 2018, the **General Data Protection Regulation (GDPR)** came into force, ushering in a new era of data protection and privacy for all. While you've certainly heard and read a lot about the GDPR, it can be difficult to understand exactly **what it means for your business**, in practical terms, and what **you need to do** to comply with the new rules.

At Oxygis, we are committed to following best practices in security and privacy. We strive to provide the same level of protection to all users and Clients, regardless of location or nationality. And we apply these best practices to all data, not just personal data.

Oxygis Partners SRL and its subsidiaries are therefore GDPR compliant.

I. What you need to know about the GDPR

Advice
If you can, the best way to understand the GDPR is to **read the official text**. It is a bit long (99 articles on 88 pages), but quite readable for non-experts.

It is a European **regulation** that aims to **harmonise** and **modernise** existing privacy legislation, such as the European Data Protection Directive, which it replaces. It establishes rules for the protection of individuals with regard to the processing of their personal data, and the free movement of personal data within Europe.

It is a **regulation**, not a directive, and is therefore immediately applicable in all EU Member States, without the need to transpose it into national law in each country. EU countries have limited room for interpretation on finer points, but **the basic rules will be the same for everyone**, everywhere in the EU.

The GDPR also **brings legislation into the next millennium**, taking into account social media, cloud computing, cybercrime and the major challenges they pose to the privacy and security of personal data.

In a word: Don't panic!
The GDPR is not a revolutionary new legislation, and it is basically a good thing for citizens and businesses.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

This is positive!
We would like to stress that the GDPR can be great for you and your Customers. Complying with the GDPR may initially be a lot of work, but there are benefits to the new rules:

- Increased confidence from your customers and users
- Simplification: the same rules are applied in all EU countries.
- Streamlining and centralising your organisational processes

The aim of the GDPR is to give individuals more control over their personal data. If your business has the right strategies and systems in place, it will be easier to manage, safer and more secure for years to come.

What are the risks if you are not compliant?

The maximum penalty for non-compliance is an administrative fine of €20 million or 4% of your annual worldwide turnover, whichever is higher. 10 million or 2% of your annual worldwide turnover, whichever is lower.

These caps are intended to be a **deterrent** for companies of all sizes, but the GDPR also requires that fines remain **proportionate**.

The supervisory authorities (also known as data protection authorities: DPAs) must take into account the circumstances of each case, including the nature, seriousness and duration of the infringement. These authorities also have the power to **investigate** and **impose remedies**, including the restriction of unlawful activities, without necessarily imposing a fine.

Another risk if you don't comply is that your customers and prospects will lose confidence in how you handle their data!

Key principles of the GDPR

- ***Scope***

The Regulation applies to all **processing of personal** data **by any organisation**:

  - If the monitoring or processing organisation **is located in the EU**

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

- If the organisation **is not located in the EU**, but the processing involves personal data of data subjects located in the EU, and is related to commercial offers or behavioural monitoring.

The scope therefore includes non-EU companies, which was not the case with the previous legislation.

- ***Roles***

The Regulation distinguishes between two main types of entities:

- **Controller:** any entity that **determines the purposes and means of** the processing of personal data, alone or jointly. As a general rule, each organisation is a controller of its own data.
- **Data processor**: any entity that processes data on behalf of a data controller.

For example, if your company has a database hosted on **the Oxygis Cloud Infrastructure**, you are the **controller of** that database, and **Oxygis Partners SRL** is only a **data processor**. If, on the other hand, you use **Oxygis for self-hosting**, you are both the **controller and the** data **processor.**

- ***Personal data***

The GDPR gives a broad definition of personal data: **any information relating to an identified or identifiable natural person.** An identifiable person is a person who can be identified, **directly or indirectly**, by means of his or her name, email, telephone number, biometric information, location data, financial data, etc. Online identifiers (IP addresses, device identifiers, ...) are also concerned.

This **also** applies in **business contexts**: *info@oxygis.eu* is not considered personal, but *john.smith@oxygis.eu is,* as it can be used to identify a natural person within a company.

The GDPR also requires a higher level of protection for **sensitive data**, which includes specific categories of personal data such as health, genetic, racial or religious information.

- ***Data processing principles***

To be compliant, processing activities must comply with the following rules: (
as listed in Article 5 of the GDPR)

1. **Legality, fairness and transparency**: to collect data, you must have a *legal basis*, a clear *purpose* and you must *inform* the subject.
    - Have a simple and clear privacy policy and refer to it wherever you collect data.

- Check the legal basis for each of your data processing activities

2. **Purpose limitation**: once you have collected data for one purpose, ask permission if you wish to use it for a different purpose.

   For example, you cannot decide to sell your Customer data if it has not been collected for that purpose.

3. **Minimisation**: you should only collect the data you need for your purpose.

4. **Accuracy**: reasonable steps must be taken to ensure that the data is kept up to date, having regard to the purpose.

   For example, make sure you deal with bounced emails, and correct or delete addresses.

5. **Limitation of storage**: personal data should only be kept for as long as is necessary to fulfil its primary purpose.

   Set deadlines for deleting or reviewing the personal data you process, depending on their purpose.

6. **Integrity and confidentiality:** data controllers must implement appropriate access control, security and data loss prevention measures, depending on the type and extent of the data processed.

   For example - Make sure your backup system is working, put in place appropriate security controls, use encryption to protect sensitive data such as passwords, ...

7. **Accountability**: Data controllers are responsible for compliance with all the above-mentioned processing principles and must be able to demonstrate this.

   - Establish and maintain a data mapping reference for your organisation, describing the compliance of your processing activities.
   - Inform your customers with a clear privacy policy

- ***Legal basis***

To be lawful under the GDPR (*first principle*), the processing of personal data must be based on **one of the 6 possible legal grounds** listed in Article 6 (1):

1. **Consent.** Valid when the data subject has *explicitly* and *freely* given his or her consent after having been properly *informed*, in particular by a *clearly stated* and *specific purpose*. The burden of proof of all this lies with the controller.

2. **Necessary for the performance of a contract**, or to respond to requests from the data subject, in preparation for a contract.
3. **Compliance with a legal obligation** imposed on the controller.
4. **Protection of a vital interest**. Where treatment is necessary to save a life.
5. **Public interest or official authority**.
6. **Legitimate interest.** Applicable where the controller has a legitimate interest which is not overridden by the interests and fundamental rights of the data subject.

One of the major changes brought about by the GDPR compared to the previous data privacy regulation is the strengthening of the requirements for obtaining valid **consent.**

- ***Rights of the persons concerned***

Existing data privacy rights of individuals are further expanded by the GDPR. Organisations must be prepared to deal with data subjects' requests in a timely manner (within one month), free of charge:

1. **Right of access** - Individuals have the right to know *what* and *how* their personal data is being processed in a transparent manner;
2. **Right of rectification** - Individuals have the right to have their personal data *rectified* or *completed*;
3. **Right to erasure** - Individuals have the right to have their personal data *erased* for legitimate reasons (withdrawal of consent, data no longer necessary for the purpose, etc.).
4. **Right to restrict** - Individuals can ask the controller to *stop processing their* personal data, if they are unwilling or unable to request complete deletion;
5. **Right to object** - Individuals have the right to *object* at any time *to* certain processing of their personal data, for example for direct marketing purposes;
6. **Data portability** - Individuals have the right to request that personal data held by one controller *be provided to them*, or to another controller.

II. How to prepare for the GDPR

Disclaimer of liability

We cannot provide legal advice, this section is for information purposes only. Please speak to your legal advisor to determine exactly how the GDPR affects your business.

Here are the key steps we suggest for a GDPR compliance roadmap:

1. **Map** your organisation's data processing **activities to** *get a clear picture of the situation*. Data protection authorities often provide template spreadsheets to help you with this task. For each process, document the type of personal data and how it was

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

collected; the *purpose*, *legal basis* and *erasure policy* of the processing; the technical and organisational *security measures implemented,* and the *processors* involved.

You will need to maintain this data map regularly as your processes evolve.

2. Based on step 1, choose a **remediation strategy** for any processing for which you do not have a legal basis (e.g. missing consent) or for which you have not put in place appropriate security measures. Adapt your processes, internal procedures, access control rules, safeguards, monitoring, etc.
3. Update and publish a clear **privacy policy** on your website. Explain what personal data you process, how you do it, and what rights individuals have regarding their data.
4. Review your **contracts** with a legal advisor and adapt them to the GDPR.
5. Decide how you will respond to the different types of **requests from the people involved**.
6. Prepare your **incident response procedure in** case of a data breach.

Depending on your situation, other items could be added to the list, such as the appointment of a data protection officer. Consult your internal processing experts and legal advisors to determine any other relevant measures.

Don't forget!

By establishing a clear mapping of your processes, everything will be easier on the way to compliance!

III. How does Oxygis comply with the GDPR?

At Oxygis, implementing privacy and security best practices is not a new idea. As a cloud-based software company, we are constantly reviewing and improving our systems, tools and processes in order to maintain a high-performance and secure platform.

Our roles in GDPR

Our data protection responsibilities depend on our different data processing activities:

Our roles	Data processing	Type of data
Controller and data processor	**On Oxygis.eu**	Personal data provided to us by our Clients and direct prospects, our partners and all **direct users of**

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Our roles	Data processing	Type of data
		Oxygis.eu (names, emails, addresses, passwords, etc.).
Data **Processor**	**On Oxygis Cloud** (Oxygis Online, Oxygis Mobile and other Oxygis enterprise services)	Any personal data stored in our Clients' databases, hosted in the Oxygis Cloud or transferred to us for the purpose of using any of our services. The owner of the database is the **data controller**.
No role	**On site**	Any data located in Oxygis databases hosted on site or in any hosting not operated by us.

Our GDPR documents

As a **data controller**, our activities are covered by our ***Privacy Policy*** which has been updated for the GDPR. This policy explains as clearly as possible *what* data we process, *why* we process it and *how* we process it. Closely related to this, our ***Security Policy*** explains the best security practices we have implemented at Oxygis, at all levels (technical and organisational) to ensure that your data is processed safely and securely.

In addition to these policies, our activities as a **Data Processor** are subject to the acceptance of our ***Oxygis Subscription Agreement*****.** This agreement has been updated to add the necessary data protection clauses (often referred to as a "data processing agreement") as required by the GDPR.
As an Oxygis Customer you do not need to do anything to agree to these changes, **you already benefit from the new safeguards**, and we will assume you agree if we do not hear anything from you!

In addition to these documents, we have also updated our website to include privacy notices in all relevant places, in order to keep our users informed at all times.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

IV. How does Oxygis help you implement GDPR best practices?

Using Oxygis to manage your business **may not be sufficient for GDPR compliance**, *as the regulation applies to your entire organisation.* However, because Oxygis centralises your data, reduces data redundancy and implements granular access rights and security controls, it can be a great help in complying with the GDPR.

Here are some of the ways we believe Oxygis can help you in the context of GDPR, for both on-premises and cloud-hosted Oxygis databases.

Disclaimer: As always, consult your legal counsel to determine how you should comply with the GDPR and data subject requests. At all times, keep in mind that you may also process personal data outside of Oxygis.

Right of access (Art. 15) and right to data portability (Art. 20)

- Oxygis provides tools that allow individuals to access and update their personal information in a self-service mode.
- If you need to export all data, or to communicate private data that are not accessible via the portal, some manual steps are necessary.
  You can export all information using the "Print as PDF" function in your browser or the "*Export*" menu. Both options provide GDPR compliant electronic formats.

Reminder: In addition to the ability to export to PDF via your browser, Oxygis has a tool that allows you to export certain records, or a list of records, to a CSV or Excel file, along with the documents associated with that record. To use it, go to the list view of any screen, select the record(s) and click on Export, then choose "Export all data".

Our helpdesk is available for more important exports.

Right to be forgotten (art. 17)

The GDPR gives data subjects the right to request the erasure of their personal data, under specific conditions, such as:

- **The data is no longer necessary for the** *purpose*;
- **They withdraw their consent for a treatment that was based on** *consent alone;*
- **The treatment is also** *illegal*.

If you determine that the request is legitimate, and you have confirmed the identity of the subject, you may attempt to delete the corresponding *contact* in Oxygis. In this case, you must decide whether you have any other obligations to retain these records, and must deny the deletion request.

If you have no legal reason to keep personal information, but cannot or do not want to delete a document or contact, consider making it anonymous. You can rename the contact and change their recognisable data (email, address, etc.), or you can reassign the documents to a generic *anonymous* contact. Once properly anonymised, this data will no longer be *personal data*.

Restriction of processing (Art. 18) and withdrawal of consent (Art. 7)

Users often request to be unsubscribed from commercial emails. Users can unsubscribe themselves by using the unsubscribe link in the footer.

Right to rectification (Art. 16) and accuracy of data (Art. 5(1)(d))

In terms of rectification, Users and Clients can correct their own personal data (name, email) via the Oxygis Resources / Personal Screen tab. They can also contact our helpdesk at any time.

Consent (Art. 7)

When you collect personal data using Oxygis custom fields (for example, by creating your own contact form, subscribing to a mailing list, or registering for an event), you must establish a *purpose* and a *legal basis* for the processing. This largely depends on how you will use the data.

If the purpose is specific and obvious (e.g. storing registered participants in an event to keep them informed about the event; subscribing a person to a mailing list they have chosen), you do not need to ask for their explicit consent (personal data is *necessary for the performance of a contract* - art. 6(1) b). However, you should always specify the purpose to the user and refer to your privacy policy page where you give more information.

However, if you intend to use the data collected for other purposes, you must obtain the user's explicit consent for each purpose.

Privacy by design (Art. 25)

Security by design is at the heart of our R&D work at Oxygis, and we apply best security practices to make our software **safe, robust and resilient** for all.

- **Access Control -** Oxygis' default group access control mechanism allows you to limit access to personal data based on each user's role and needs. If you review user group assignments and maintain them properly as roles change in your organization, you have a solid privacy foundation. You can easily add or change user groups to suit your organisation.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

- **Passwords -** Oxygis stores user passwords with an industry standard secure hash.
- **Employee Data -** One area where Oxygis databases may include personal data is the *Resource / Personal Page tab* which collects employee usernames.

Security of treatment (Articles 25 and 32)

If you use Oxygis Cloud services, we implement best practices in security and privacy at all levels. You can read more about this in our ***security policy.***

If you use Oxygis on site, you are responsible for adhering to best security practices.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Name doc. :	**Oxygis - Responsible disclosure of security vulnerabilities**
Version:	18/08/2022
Summary:	Help us keep Oxygis safe

Responsible disclosure policy

The security of Oxygis systems is very important to us, and we consider security issues with the highest priority. We do our best every day to protect Oxygis users from known security threats, and we welcome all reports of security vulnerabilities discovered by our users and contributors.

We undertake to treat reports of vulnerability with the utmost care, provided that the following rules are observed.

I. Report a problem

Please share the details of your security vulnerability privately by emailing our security team at info@oxygis.eu . Be sure to include as much information as possible, including detailed steps in reproducing the issue, the versions involved, expected and actual results, and any other information that may help us respond more quickly and effectively. We tend to prefer text-based **bug descriptions with a proof-of-concept script/explanation,** rather than long videos.
Vulnerability reporting via third party websites is not acceptable, with the exception of the use of https://drop.aloalto.com for password sharing, as it violates the terms of our policy.

Please note: we receive a majority of security reports that have little or no impact on the security of Oxygis and we must ultimately reject them. To avoid a disappointing experience when you contact us, try to implement a **proof-of-concept attack** and critically examine what is **really at risk**. If the proposed attack scenario turns out to be **unrealistic**, your report will probably be rejected. Also, be sure to check the list of **ineligible issues** below.

You can send this report from an anonymous email account, but we promise not to disclose your identity if you do not wish to.

You can also use https://drop.aloalto.com to share critical information (e.g. API keys, passwords, etc.).

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

II. Incident response procedure

A. Procedure

- You can share details of the security breach with our security team by reporting a problem (see above).
- We acknowledge receipt of your request and check for vulnerability. Our first response usually arrives within 48 hours.
- If the vulnerability is valid and within the scope, we work with you to correct it.
- We write a detailed safety opinion describing the problem, its impacts, possible workarounds and the solution, and ask you to review it.
- We have privately distributed the security notice and correction to stakeholders and Clients with an Oxygis Subscription contract.
- We allow stakeholders and Customers a reasonable period of time to implement the correction, before disclosing it publicly (e.g. 2-3 weeks).
- We disclose and broadcast the safety notice and correction on **our public channels**.

B. Rules

We ask you to respect the following rules at all times:

- Test vulnerabilities exclusively on your own deployments, on demo.oxygis.eu, or on your own Oxygis Cloud trial instances.
- Never attempt to access or modify data that does not belong to you.
- Never attempt to carry out denial of service attacks or compromise the reliability and integrity of services that do not belong to you.
- Do not use scanners or automated tools to find vulnerabilities, as their effects may violate the above rules (unless you can guarantee that they will be limited to less than 5 requests/second and will not violate any other rules).
- Never attempt non-technical attacks, such as social engineering, phishing or physical attacks, against anyone or any system.
- Do not publicly disclose vulnerabilities without our prior consent (see also the disclosure procedure above). During the non-disclosure period, you are allowed to use/test any fix we have provided, provided you do not emphasise the fix and do not publish it as a security report (i.e. you can use it on production servers).

C. In return :

- We will not take legal action against you if you have complied with the rules.
- We will process your report and respond as soon as possible.
- We will provide a fix as soon as possible
- We will work diligently with stakeholders and Customers to help them restore the security of their systems.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

- We will not publicly disclose your identity if you do not wish to be credited for your discovery.

III. What to report?

Qualifying vulnerabilities - REPORT!

- SQL injection vectors in public API methods
- XSS vulnerabilities work in supported browsers
- Faulty authentication or session management, allowing unauthorised access.

Non-qualifying vulnerabilities - DO NOT REPORT!

- XSS vulnerabilities only work in unsupported or deprecated browsers, or require less stringent security settings.
- Auto-XSS attacks requiring the user to actively copy/paste malicious code into their own browser window.
- XSS attacks" by administrators, e.g. via file uploads (SVG, HTML, JS, ...) or script injection. Administrators are webmasters, the security restrictions do not apply to them, this is a feature.
- Speed limitation / brute force / scripting of components working as intended (e.g. password authentication, password reset, etc.)
- User registration (possibility to check that a user name exists). Does not carry much risk and cannot be avoided without deteriorating the user experience.
- File path disclosures, which do not pose a significant risk and do not allow for attacks that would otherwise be impossible.
- Clickjacking or phishing attacks, which use social engineering tricks to trick users into using the system as intended.
- Tabnapping or other phishing attacks carried out by browsing in other browser tabs
- CSRF disconnection (no plausible attack + cannot be prevented, e.g. via cookie throwing or cookie box overflow)
- Reflexive file downloads, another attack technique that requires social engineering and is not very practical.
- Leakage of referrers (including sensitive tokens) via social media links or advertising/analysis requests - very unlikely to be clicked, or exploited during the validity period by these mainstream companies!
- More generally, attacks based on physical or social engineering techniques will generally be rejected.
- Non-permanent Denial of Service (DoS) and Distributed DoS (DDoS) that maintain resource (cpu/network/memory) exhaustion via a sustained stream of requests/packets.
- Password policies (length, format, character classes, etc.)
- Missing or partial verification of e-mail addresses
- Disclosure of public information or information that does not carry significant risk (the directory listing on our download archive is a mandatory feature! ;-))

- Anti-spam policies and systems, such as DKIM, SPF or DMARC.
- Lack of HTTP Strict Transport Security (HSTS) headers, HSTS preloading and HSTS policies.
- Attack scenarios including a takeover of users' email accounts

If you have any doubts, ask us first!

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Name doc. : **Oxygis Security**

Version: 18/08/2022

Summary: Your security is very important to us! Here is a summary of what we do every day to ensure that your data is safe with Oxygis and that we apply the best security practices on our hosted version, the Oxygis Cloud.

1 - Oxygis Cloud (Oxygis Cloud Infrastructure)

I. Backups / disaster recovery

- Weekly backups kept for 1 year
- Backups are stored on Microsoft Azure
- Backups are replicated in at least 3 different data centres in an availability zone in Western Europe. On request, automatic replicas can be made in other availability zones (this may incur additional costs, which are passed on to the Customer).
- You can contact our helpdesk to restore any of these backups to your active database (or to the side).
- The actual locations of our data centres are specified in our ***Privacy Policy***.
- **Hardware failover:** no services are hosted directly on baremetal, but only on virtual servers or managed services from Microsoft Azure or Amazon Web Services.
- **Disaster recovery: In the** event of a complete disaster, with a data centre *completely out of service for an extended period of time,* preventing failover to our local hot-standby (this has never happened so far, it is the worst case plan), we have the following objectives:
    - **RPO** (Recovery Point Objective) = 24 hours. This means that you can lose a maximum of 24 hours of work if the data cannot be recovered and we have to restore your last daily backup.
    - **RTO** (Recovery Time Objective) = 24h for paid subscriptions, 48h for free trials, educational offers, freemium users, etc. This is the time needed to restore service in another data centre if a disaster occurs and one data centre is completely down.
    - How it's done: We actively monitor our daily backups, and they are replicated to multiple data centres in an availability zone. We have an automated provisioning system to deploy our services to a new hosting site. Data restoration based on our previous day's backups can then be completed within hours (for larger clusters).

II. Database security

- Client data can be stored in a dedicated database - no data sharing between Clients.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

III. Password security

- Client passwords are protected by industry-standard PBKDF2+SHA512 encryption (salted + stretched for thousands of rounds).
- Oxygis staff do not have access to your password and cannot recover it for you, the only option if you lose it is to reset it.
- Login credentials are always transmitted securely via HTTPS.
- Password policies: passwords must be at least 10 characters long and must contain at least one upper case letter, one lower case letter, one number and one special character.

IV. Staff access

- Oxygis Help Desk staff can log into your account to access the settings related to your support issue. They do this using their own credentials, not your password (which they have no way of knowing).
- This special staff access improves efficiency and security: they can immediately reproduce the problem you encounter, you never have to share your password, and we can audit and monitor staff actions separately!
- Our helpdesk staff strive to respect your privacy as much as possible and only access the files and settings necessary to diagnose and resolve your problem.

V. Physical security

Oxygis Cloud servers are hosted on Microsoft Azure, no physical access is possible

VI. Communications

- All data communications to Client instances are protected by state-of-the-art 256-bit SSL (HTTPS) encryption.

2 - Oxygis (the software)

I. Software security

Oxygis is coded in C# for the backend and in AngularJS for the frontend.

Oxygis' R&D processes include code review steps that include the security aspects of new code elements as well as existing elements.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

II. Safety by design

Oxygis is designed to prevent the introduction of the most common security vulnerabilities:

- SQL injections are avoided by using a top-level API that does not require manual SQL queries.
- XSS attacks are prevented by using a high-level modelling system that automatically escapes injected data.

See also the **OWASP Top Vulnerabilities** section to see how Oxygis is designed from the ground up to prevent such vulnerabilities from occurring.

III. OWASP Top Vulnerabilities

Here is Oxygis' position on the main web application security issues, as listed by the **Open Web Application Security Project** (OWASP):

- **Injection flaws:** Injection flaws, including SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data causes the interpreter to execute unwanted commands or modify data.

  Oxygis uses an ORM that abstracts the construction of queries and prevents SQL injections. Normally, developers do not manually build SQL queries, which are generated by the ORM, and the parameters are always correctly escaped.

- **Cross Site Scripting (XSS):** XSS flaws occur when an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface websites, possibly introduce worms, etc.

  Oxygis escapes all data which prevents XSS.

- **Cross Site Request Forgery (CSRF):** A CSRF attack forces a logged-in victim's browser to send a fake HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests that the vulnerable application thinks are legitimate requests from the victim.

  Oxygis includes a built-in CSRF protection mechanism. It prevents any HTTP controller from receiving a request without the corresponding security token. This is the recommended technique for CSRF prevention.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

- **Malicious file execution:** Remote File Inclusion (RFI) vulnerable code allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise.

  Oxygis does not expose functions for remote file inclusion.

- **Insecure direct object reference:** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate these references to gain unauthorised access to other objects.

  Access control to Oxygis is not implemented at the user interface, so there is no risk of exposing references to internal objects in URLs. Attackers cannot bypass the access control layer by manipulating these references, as each request must always pass through the data access validation layer.

- **Insecure cryptographic storage:** Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to commit identity theft and other crimes, such as credit card fraud.

  Oxygis uses a standard secure hash for user passwords (by default PKFDB2 + SHA-512, with key stretching) to protect stored passwords. It is also possible to use external authentication systems to avoid local storage of user passwords.

- **Unsecured communications:** Applications often fail to encrypt network traffic when it is necessary to protect sensitive communications.

  Oxygis works with HTTPS.

- **Lack of URL access restriction:** Often, an application protects sensitive functionality only by preventing links or URLs from being displayed to unauthorised users. Attackers can use this weakness to access and perform unauthorised operations by directly accessing these URLs.

  Oxygis access control is not implemented at the user interface, and security does not rely on hiding special URLs. Attackers cannot bypass the access control layer by reusing or manipulating a URL, as each request must pass through the data access validation layer. In the rare cases where a URL provides unauthenticated access to sensitive data, such as special URLs that Customers use to confirm an order, these URLs are digitally signed with unique tokens and sent only via email to the intended recipient.

IV. Reporting security vulnerabilities

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

If you need to report a security vulnerability, please report it to our Help Desk as soon as possible. These reports are treated with high priority, the issue is immediately assessed and resolved by the Oxygis security team, in collaboration with the reporter, and then responsibly disclosed to Oxygis Clients and users.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu