Nom doc. : **Oxygis - Règlement général sur la protection des données (RGPD)**

Version mise à jour le : 18/06/2025

Résumé : Le guide d'Oxygis sur les règles européennes de protection des données. Aperçu des nouvelles lois sur la protection de la vie privée et des meilleures pratiques avec Oxygis

Depuis le 25 mai 2018, le **règlement général sur la protection des données (GDPR)** est entré en vigueur, ouvrant une nouvelle ère de protection des données et de la vie privée pour tous. Si vous avez certainement entendu et lu beaucoup d'informations sur le GDPR, il peut être difficile de comprendre exactement **ce qu'il signifie pour votre entreprise**, en termes pratiques, et **ce que vous devez faire** pour vous conformer aux nouvelles règles.

Chez Oxygis, nous nous engageons à suivre les meilleures pratiques en matière de sécurité et de confidentialité. Nous nous efforçons d'offrir le même niveau de protection à tous les utilisateurs et Clients, sans distinction de lieu ou de nationalité. Et nous appliquons ces meilleures pratiques à toutes les données, et pas seulement aux données personnelles.

Oxygis fournit des outils facilitant la conformité RGPD, mais chaque client reste seul responsable de l'évaluation de sa propre conformité, notamment pour ce qui concerne ses activités hors de la plateforme.

Oxygis Partners SRL et ses filiales sont donc conformes au GDPR.

I. Ce que vous devez savoir sur le GDPR

Conseil
Si vous le pouvez, la meilleure façon de comprendre le GDPR est de **lire le texte officiel**. Il est un peu long (99 articles sur 88 pages), mais tout à fait lisible pour les non experts.

Il s'agit d'un **règlement** européen qui vise à **harmoniser** et à **moderniser la** législation existante en matière de protection de la vie privée, telle que la directive européenne sur la protection des données qu'il remplace. Il établit des règles pour la protection des personnes physiques à l'égard du traitement de leurs données personnelles, et la libre circulation des données personnelles en Europe.

Il s'agit d'un **règlement**, et non d'une directive, qui est donc applicable immédiatement dans tous les États membres de l'UE, sans qu'il soit nécessaire de le transposer dans le droit national de chaque pays. Les pays de l'UE disposent d'une marge d'interprétation limitée pour les

points plus fins, mais **les règles fondamentales seront les mêmes pour tous**, partout dans l'UE.

Le GDPR **fait** également **passer la législation au prochain millénaire**, en prenant en compte les médias sociaux, l'informatique en cloud, la cybercriminalité et les défis majeurs qu'ils posent en termes de confidentialité et de sécurité des données personnelles.

En un mot : Ne paniquez pas !
Le GDPR n'est pas une nouvelle législation révolutionnaire, et c'est fondamentalement une bonne chose pour les citoyens et les entreprises.

C'est positif !
Nous tenons à souligner que le GDPR peut être excellent pour vous et vos Clients. Se conformer au GDPR peut initialement représenter beaucoup de travail, mais il y a des avantages à ces nouvelles règles :

- Une confiance accrue de la part de vos Clients et utilisateurs
- Simplification : les mêmes règles sont appliquées dans tous les pays de l'UE.
- Rationalisation et centralisation de vos processus organisationnels

L'objectif du GDPR est de donner aux individus plus de contrôle sur leurs données personnelles. Si votre entreprise met en place les bonnes stratégies et les bons systèmes, elle sera plus facile à gérer, plus sûre et plus sécurisée pour les années à venir.

Quels sont les risques si vous n'êtes pas conforme ?

La sanction maximale en cas de non-conformité est une amende administrative de 20 millions d'euros ou de 4 % de votre chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Une amende plus faible, de 10 millions d'euros ou de 2 % de votre chiffre d'affaires annuel mondial, est applicable pour les infractions de moindre importance.

Ces plafonds sont censés être **dissuasifs** pour les entreprises de toutes tailles, mais le GDPR exige également que les amendes restent **proportionnées**.

Les autorités de contrôle (également connues sous le nom d'autorités de protection des données : APD) doivent tenir compte des circonstances de chaque cas, notamment de la nature, de la gravité et de la durée de l'infraction. Ces autorités ont également le pouvoir d'**enquêter** et d'**imposer des mesures correctives**, notamment la limitation des activités illicites, sans nécessairement imposer une amende.

Un autre risque si vous ne vous conformez pas est la perte de confiance de vos Clients et prospects, qui se soucient de la manière dont vous traitez leurs données !

Principes clés du GDPR

- ***Portée***

Le règlement s'applique à tout **traitement** de données **personnelles par toute organisation** :

  - Si l'organisation de contrôle ou de traitement **est située dans l'UE**
  - Si l'organisation **n'est pas située dans l'UE**, mais que le traitement concerne des données à caractère personnel de personnes concernées situées dans l'UE, et qu'il est lié à des offres commerciales ou à la surveillance du comportement.

Le champ d'application inclut donc les entreprises non européennes, ce qui n'était pas le cas avec l'ancienne législation.

- ***Rôles***

Le règlement distingue deux grands types d'entités :

  - **Responsable du traitement :** toute entité qui **détermine les finalités et les moyens** du traitement des données à caractère personnel, seule ou conjointement. En règle générale, chaque organisation est un responsable du traitement de ses propres données.
  - **Processeur de données** : toute entité qui traite des données pour le compte d'un contrôleur de données.

Par exemple, si votre entreprise possède une base de données hébergée sur **l'Infrastructure Cloud d'Oxygis**, vous êtes le **contrôleur de** cette base de données, et **Oxygis Partners SRL** n'est qu'un **processeur de données**. Si, au contraire, vous utilisez **Oxygis en self-hosting**, vous êtes à la fois le **contrôleur et le processeur** des données.

- ***Données personnelles***

Le GDPR donne une définition large des données personnelles : **toute information relative à une personne physique identifiée ou identifiable.** Une personne identifiable est une personne qui peut être identifiée, **directement ou indirectement**, au moyen de ses noms, emails, numéros de téléphone, informations biométriques, données de localisation, données financières, etc. Les identifiants en ligne (adresses IP, identifiants d'appareils, ...) sont également concernés.

Cela s'applique **également dans les contextes professionnels** : *info@oxygis.eu* n'est pas considéré comme personnel, mais *john.smith@oxygis.eu* l'est, car il peut être utilisé pour identifier une personne physique au sein d'une entreprise.

Le GDPR exige également un niveau de protection plus élevé pour les **données sensibles**, qui comprennent des catégories spécifiques de données personnelles telles que les informations sur la santé, la génétique, la race ou la religion.

- ***Principes de traitement des données***

Pour être conformes, les activités de traitement doivent respecter les règles suivantes : (telles qu'énumérées à l'article 5 du GDPR)

1. **Légalité, équité et transparence** : pour collecter des données, vous devez disposer d'une *base juridique*, d'une *finalité* claire et vous devez en *informer* le sujet.

    - Disposez d'une politique de confidentialité simple et claire, et faites-y référence partout où vous collectez des données.
    - Vérifier la base juridique de chacune de vos activités de traitement des données

2. **Limitation de la finalité** : une fois la collecte effectuée dans un but précis, demandez l'autorisation si vous souhaitez l'utiliser dans un but différent.

    Par exemple, vous ne pouvez pas décider de vendre vos données Clients si elles n'ont pas été collectées dans ce but.

3. **Minimisation** : vous ne devez collecter que les données nécessaires à votre objectif.

4. **Exactitude** : des mesures raisonnables doivent être prises pour s'assurer que les données sont mises à jour, eu égard à la finalité.

    Par exemple, assurez-vous de traiter les courriels rebondis, et corrigez ou supprimez les adresses.

5. **Limitation du stockage** : les données personnelles ne doivent être conservées que pendant la durée nécessaire à la réalisation de leur finalité première.

    Définissez des délais d'effacement ou de révision des données personnelles que vous traitez, en fonction de leur finalité.

6. **Intégrité et confidentialité :** les responsables du traitement des données doivent mettre en œuvre des mesures appropriées de contrôle d'accès, de sécurité et de prévention des pertes de données, en fonction du type et de l'ampleur des données traitées.

Par exemple - Assurez-vous que votre système de sauvegarde fonctionne, mettez en place des contrôles de sécurité appropriés, utilisez le cryptage pour protéger les données sensibles telles que les mots de passe, ...

7. **Responsabilité** : les responsables du traitement des données sont responsables du respect de tous les principes de traitement susmentionnés et doivent être en mesure de le démontrer.

    - Établir et maintenir une référence de cartographie des données pour votre organisation, décrivant la conformité de vos activités de traitement.
    - Informez vos Clients par le biais d'une politique de confidentialité claire

- ***Base juridique***

Pour être licite en vertu du GDPR (*premier principe*), le traitement des données à caractère personnel doit être fondé sur l'**une des 6 bases juridiques possibles**, énumérées à l'article 6 (1):

1. **Consentement.** Valable lorsque la personne concernée a *explicitement* et *librement* donné son consentement après avoir été correctement *informée*, notamment par une *finalité clairement énoncée* et *spécifique*. La charge de la preuve de tout cela incombe au responsable du traitement.
2. **Nécessaire à l'exécution d'un contrat**, ou pour répondre aux demandes de la personne concernée, en préparation d'un contrat.
3. **Le respect d'une obligation légale** qui s'impose au responsable du traitement.
4. **Protection d'un intérêt vital**. Lorsque le traitement est nécessaire pour sauver une vie.
5. **Intérêt public ou autorité officielle**.
6. **Intérêt légitime.** Applicable lorsque le responsable du traitement a un intérêt légitime qui n'est pas supplanté par les intérêts et les droits fondamentaux de la personne concernée.

L'un des changements majeurs apportés par le GDPR par rapport à la réglementation précédente sur la confidentialité des données est le renforcement des exigences relatives à l'obtention d'un **consentement** valide.

- ***Droits des personnes concernées***

Les droits existants des personnes en matière de confidentialité des données sont encore élargis par le GDPR. Les organisations doivent être prêtes à traiter les demandes des personnes concernées en temps utile (dans un délai d'un mois), sans frais :

1. **Droit d'accès** - Les personnes ont le droit de savoir *ce que* leurs données personnelles sont traitées et *comment elles le* sont, en toute transparence ;

2. **Droit de rectification** - Les personnes ont le droit d'obtenir que leurs données personnelles soient *rectifiées* ou *complétées* ;
3. **Droit à l'effacement** - Les personnes ont le droit d'obtenir l'*effacement* de leurs données à caractère personnel pour des motifs légitimes (retrait du consentement, données qui ne sont plus nécessaires à la finalité poursuivie, etc ;)
4. **Droit de restriction** - Les personnes peuvent demander au responsable du traitement de *cesser de traiter leurs* données à caractère personnel, si elles ne veulent pas ou ne peuvent pas demander la suppression complète de celles-ci ;
5. **Droit d'opposition** - Les personnes ont le droit de *s'opposer* à tout moment à certains traitements de leurs données personnelles, par exemple à des fins de marketing direct ;
6. **Portabilité des données** - Les personnes ont le droit de demander que les données personnelles détenues par un responsable du traitement *leur soient fournies*, ou soient fournies à un autre responsable du traitement.

II. Comment vous préparer au GDPR

Clause de non-responsabilité

Nous ne pouvons pas fournir de conseils juridiques, cette section est uniquement fournie à titre informatif. Veuillez-vous adresser à votre conseiller juridique afin de déterminer exactement comment le GDPR affecte votre entreprise.

Voici les étapes clés que nous suggérons pour une feuille de route de conformité au GDPR :

1. Établissez une **cartographie des activités** de traitement des données de votre organisation pour *obtenir une image claire de la situation*. Les autorités de protection des données fournissent souvent des modèles de feuilles de calcul pour vous aider dans cette tâche. Pour chaque processus, documentez le type de données personnelles et la manière dont elles ont été collectées ; la *finalité*, la *base juridique* et la *politique d'effacement* du traitement ; les *mesures de sécurité* techniques et organisationnelles mises en œuvre, et les *sous-traitants* (processeurs) impliqués.

   Vous devrez maintenir cette cartographie des données régulièrement, au fur et à mesure de l'évolution de vos processus.

2. Sur la base de l'étape 1, choisissez une **stratégie de remédiation** pour tout traitement pour lequel vous ne disposez pas d'une base juridique (par exemple, un consentement manquant) ou pour lequel vous n'avez pas mis en place de mesures de sécurité appropriées. Adaptez vos processus, vos procédures internes, vos règles de contrôle d'accès, vos sauvegardes, votre surveillance, etc.

3. Mettez à jour et publiez une **politique de confidentialité** claire sur votre site web. Expliquez quelles données personnelles vous traitez, comment vous le faites, et quels sont les droits des individus concernant leurs données.
4. Révisez vos **contrats** avec un conseiller juridique et adaptez-les au GDPR.
5. Décidez comment vous allez répondre aux différents types de **demandes des personnes concernées**.
6. Préparez votre **procédure de réponse aux incidents** en cas de violation des données.

En fonction de votre situation, d'autres éléments pourraient être ajoutés à la liste, comme la désignation d'un délégué à la protection des données. Consultez vos experts internes en matière de traitement et vos conseillers juridiques pour déterminer toute autre mesure pertinente.

N'oubliez pas !

En établissant une cartographie claire de vos processus, tout sera plus facile sur la voie de la conformité !

III. Comment Oxygis se conforme-t-il au GDPR ?

Chez Oxygis, la mise en œuvre des meilleures pratiques en matière de confidentialité et de sécurité n'est pas une idée nouvelle. En tant qu'éditeur de logiciels hébergés dans le cloud, nous révisons et améliorons constamment nos systèmes, nos outils et nos processus, afin de maintenir une plateforme performante et sécurisée.

Nos rôles en matière de GDPR

Nos responsabilités en matière de protection des données personnelles dépendent de nos différentes activités de traitement des données :

Nos rôles	Traitement des données	Type de données
Contrôleur et processeur de données	**Sur Oxygis.eu**	Les données personnelles qui nous sont fournies par nos Clients et prospects directs, nos partenaires et tous les **utilisateurs directs d'Oxygis.eu**

Nos rôles	Traitement des données	Type de données
		(noms, emails, adresses, mots de passe...).
Processeur de données	**Sur Oxygis Cloud** (Oxygis Online, Oxygis Mobile et autres services d'entreprise Oxygis)	Toute donnée personnelle stockée dans les bases de données de nos Clients, hébergée dans le Cloud Oxygis ou transférée vers nous dans le but d'utiliser l'un de nos services. Le propriétaire de la base de données est le **contrôleur de données**.
Aucun rôle	**Sur site**	Toute donnée située dans les bases de données d'Oxygis hébergées sur place ou dans tout hébergement non exploité par nous.

Nos documents GDPR

En tant que **contrôleur de données**, nos activités sont couvertes par notre ***Politique de Confidentialité*** qui a été mise à jour pour le GDPR. Cette politique explique aussi clairement que possible *quelles* données nous traitons, *pourquoi* nous les traitons et *comment* nous le faisons. Étroitement liée à cela, notre ***Politique de Sécurité*** explique les meilleures pratiques de sécurité que nous avons mises en œuvre chez Oxygis, à tous les niveaux (technique et organisationnel) afin de garantir que vos données sont traitées de manière sûre et sécurisée.

En plus de ces politiques, nos activités en tant que **Responsable du traitement des données** sont soumises à l'acceptation de notre ***Contrat d'Abonnement à Oxygis*****.** Voir également la section 6.5 du contrat d'abonnement pour les clauses contractuelles relatives au traitement de données personnelles. Ce contrat a été mis à jour afin d'ajouter les clauses de protection des données nécessaires (souvent appelées "contrat de traitement des données"), comme l'exige le GDPR. En tant que Client d'Oxygis vous n'avez rien à faire pour accepter ces changements, **vous bénéficiez déjà des nouvelles garanties**, et nous considérerons que vous êtes d'accord si nous n'entendons rien de votre part !

En plus de ces documents, nous avons également mis à jour notre site web afin d'insérer des avis de confidentialité à tous les endroits pertinents, dans le but de tenir nos utilisateurs informés à tout moment.

IV. Comment Oxygis vous aide-t-il à mettre en œuvre les meilleures pratiques du GDPR ?

L'utilisation d'Oxygis pour gérer votre entreprise **ne peut pas être suffisante pour la conformité au GDPR**, *car le règlement s'applique à l'ensemble de votre organisation.* Cependant, comme Oxygis centralise vos données, réduit la redondance des données et met en œuvre des droits d'accès et des contrôles de sécurité granulaires, il peut être d'une grande aide pour se conformer au GDPR.

Voici quelques façons dont nous pensons qu'Oxygis peut vous aider dans le contexte du GDPR, pour les bases de données Oxygis sur site et hébergées dans le Cloud.

Avertissement : comme toujours, consultez votre conseiller juridique afin de déterminer comment vous devez vous conformer au GDPR et aux demandes des personnes concernées. À tout moment, gardez à l'esprit que vous pouvez également traiter des données personnelles en dehors d'Oxygis.

Droit d'accès (art. 15) et droit à la portabilité des données (art. 20)

- Oxygis fournit des outils permettant aux personnes concernées d'accéder à leurs informations personnelles et de les mettre à jour en mode libre-service.
- Si vous avez besoin d'exporter toutes les données, ou de communiquer des données privées qui ne sont pas accessibles via le portail, certaines étapes manuelles sont nécessaires.
  Vous pouvez exporter toutes les informations à l'aide de la fonction "Imprimer en PDF" de votre navigateur ou du menu "*Exporter*". Ces deux options fournissent des formats électroniques conformes au GDPR.

Rappel : En plus de la possibilité d'exporter en PDF via votre navigateur, Oxygis dispose d'un outil permettant d'exporter certains enregistrements, ou une liste d'enregistrements, dans un fichier CSV ou Excel, ainsi que les documents liés à cet enregistrement. Pour l'utiliser, allez dans la vue liste de n'importe quel écran, sélectionnez le ou les enregistrements et cliquez sur Exporter, puis choisissez "Exporter toutes les données".

Notre Helpdesk reste à votre disposition pour les exportations plus importantes.

Droit à l'oubli (art. 17)

Le GDPR accorde aux personnes concernées le droit de demander l'effacement de leurs données personnelles, dans des conditions spécifiques, telles que :

- **Les données ne sont plus nécessaires en fonction de la** *finalité* ;
- **Ils retirent leur consentement pour un traitement qui était fondé sur le** *seul consentement ;*
- **Le traitement est par ailleurs** *illégal*.

Si vous déterminez que la demande est légitime, et que vous avez confirmé l'identité du sujet, vous pouvez tenter d'effacer le *contact* correspondant dans Oxygis. Dans ce cas, vous devez décider si vous avez d'autres obligations de conserver ces documents, et devez refuser la demande d'effacement.

Si vous n'avez aucune raison légale de conserver les informations personnelles, mais que vous ne pouvez ou ne voulez pas supprimer un document ou un contact, envisagez de le rendre anonyme. Vous pouvez renommer le contact et modifier ses données reconnaissables (courriel, adresse, etc.), ou vous pouvez réaffecter les documents à un contact *anonyme* générique. Une fois correctement anonymisées, ces données ne seront plus des *données personnelles*.

Restriction du traitement (art. 18) et retrait du consentement (art. 7)

Les utilisateurs demandent souvent à être désinscrits des courriers électroniques commerciaux. Les utilisateurs peuvent se désabonner eux-mêmes en utilisant le lien de désabonnement du pied de page.

Droit à la rectification (art. 16) et à l'exactitude des données (art. 5, paragraphe 1, point d))

En termes de rectification, les utilisateurs et les Clients peuvent corriger leurs propres données personnelles (nom, email) via l'onglet Ressources Oxygis / écran personnel. Ils peuvent également s'adresser à tout moment à notre helpdesk.

Consentement (art. 7)

Lorsque vous collectez des données personnelles à l'aide des champs personnalisés d'Oxygis (par exemple, en créant votre propre formulaire de contact, en vous inscrivant à une liste de diffusion ou en vous inscrivant à un événement), vous devez établir une *finalité* et une *base juridique* pour le traitement. Cela dépend largement de l'utilisation que vous ferez des données.

Si la finalité est spécifique et évidente (par exemple, stocker les participants inscrits à un événement pour les tenir informés du déroulement de l'événement ; inscrire une personne à

la liste de diffusion qu'elle a choisie), vous n'avez pas besoin de demander son consentement explicite (les données à caractère personnel sont *nécessaires à l'exécution d'un contrat* - art. 6 (1) b). Cependant, vous devez toujours préciser la finalité à l'utilisateur et renvoyer à la page de votre politique de confidentialité où vous donnez de plus amples informations.

Toutefois, si vous envisagez d'utiliser les données collectées à d'autres fins, vous devez obtenir le consentement explicite de l'utilisateur pour chaque finalité.

Vie privée dès la conception (art. 25)

La sécurité par la conception est au cœur de notre travail de R&D chez Oxygis, et nous appliquons les meilleures pratiques de sécurité pour rendre nos logiciels **sûrs, robustes et résilients** pour tous.

- **Contrôle d'accès -** Le mécanisme de contrôle d'accès par groupe par défaut d'Oxygis vous permet de limiter l'accès aux données personnelles en fonction du rôle et des besoins de chaque utilisateur. Si vous révisez les attributions des groupes d'utilisateurs et les maintenez correctement lorsque les rôles changent dans votre organisation, vous disposez d'une base de confidentialité solide. Vous pouvez facilement ajouter ou modifier des groupes d'utilisateurs pour les adapter à votre organisation.

- **Mots de passe -** Oxygis stocke les mots de passe des utilisateurs avec un hachage sécurisé conforme aux normes industrielles.

- **Données sur les employés -** Un domaine dans lequel les bases de données d'Oxygis sont susceptibles d'inclure des données personnelles est l'*onglet Ressource / page personnelle* qui recueille les noms d'utilisateur des employés.

Sécurité du traitement (articles 25 et 32)

Si vous utilisez les services Oxygis Cloud, nous mettons en œuvre les meilleures pratiques en matière de sécurité et de confidentialité à tous les niveaux. Vous pouvez en savoir plus à ce sujet dans notre ***politique de sécurité.***

Si vous utilisez Oxygis sur site, vous êtes responsable du respect des meilleures pratiques de sécurité.