

<b>DOCUMENT</b>	Niveau de service pour compatibilité RGPD
<b>SCOPE</b>	Infrastructure IT mise à disposition des clients – stockage et services

1	Introduction.....	1
2	Definitions.....	2
3	Cadre du service.....	3
4	Engagement et positionnement de THELIS.....	3
	En tant que sous-traitant, Thelis s’engage à:.....	4
	Propriété des données.....	4
	Accès aux données hébergées .....	5
	Localisation géographique des données.....	5

## 1 INTRODUCTION

Ce document décrit le niveau de service et les procédures mises en œuvre par THELIS dans le cadre de la réglementation RGPD et concerne les activités suivantes :

- L’infrastructure IT mise à disposition de ses clients sous forme de service (avec abonnement récurrent).
- Logiciels développés par Thelis (pour le compte du client ou mis à disposition du client)

Ce document n’a pas de valeur contractuelle, il est fourni à titre indicatif et décrit les procédures appliquées par Thelis dans le cadre du traitement des données stockées dans son infrastructure ‘as a service’ et logiciels et/ou serveurs qui remplissent les conditions décrites ci-dessous.

---

## 2 DEFINITIONS

### Définitions :

- Un '*client*' est défini comme une entité pour laquelle THELIS a réalisé des développements spécifiques (dans le cadre THELIS Engineering) ou fourni des solutions logicielles développées par Thelis (dans le cadre de THELIS ICT / solution Kiwix)
- *Architecture et Logiciel couverts* par ce document : Logiciels développés par THELIS Engineering pour le compte du client (logiciel spécifique) ou logiciels développés par Thelis et mis à disposition du client dans le cadre d'un abonnement (solution Kiwix)
- *Infrastructure couverte* par ce document : Infrastructure IT hébergeant les logiciels tels que définis ci-dessus et faisant part explicite d'un contrat entre le client et Thelis.
- *Datacenter*: Lieu physique où sont situés les serveurs physiques et l'infrastructure correspondante. Si l'infrastructure est hébergée par le client, cette infrastructure n'est pas considérée comme Datacenter au sens de ce document, son intégrité physique n'étant pas garantie par le contrat Thelis. Les data-center sont en général opérés par des sous-traitants de Thelis. Dans ce cas, Thelis informe le client du sous-traitant et le cas échéant de toute contradiction qui pourrait intervenir avec le niveau de service offert par Thelis dans le cadre de la protection des données à caractère privé.
- *Utilisateur final* : l'utilisateur final ayant une relation commerciale ou non avec le client. Thelis n'est pas en contact direct avec l'utilisateur final.
- *Données à caractère personnel* : toute information se rapportant à une personne physique identifiée ou identifiable.
- *Traitement* : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel (collecte, enregistrement, transmission, stockage, conservation, extraction, consultation, utilisation, interconnexion, etc.).
- *Responsable du traitement* : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.
- *Sous-traitant* : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

---

### 3 CADRE DU SERVICE

Ce document s'applique à l'architecture couverte par celui-ci et aux services hébergés sur cette infrastructure. Tout usage autre n'est pas couvert par ce document.

Par défaut, uniquement les serveurs et services de "production" sont inclus. Les environnements de test doivent être explicitement spécifiés pour être couverts par ces procédures.

Toute demande émanant du client en vue de fournir un accès bas-niveau (p.ex. administrateur) sur l'infrastructure à des tiers ou ses propres employés ouvre des brèches de sécurité au regard de la RGPD. Le client est seul responsable et doit dans ce cas s'assurer de l'intégrité des données et du bon traitement de celles-ci. Etant donné que les actions réalisées dans le cadre d'un accès bas-niveau ne sont en général pas traçables, tout accès de ce type rendra caduque la possibilité pour Thelis de détecter une éventuelle fraude.

### 4 ENGAGEMENT ET POSITIONNEMENT DE THELIS

Le règlement de RGPD décrit les entités traitant des données en deux catégories : « responsables de traitement (data controller) » et les « sous-traitants (data processor) ». Les définitions de ces termes sont reprises dans le paragraphe précédent.

Les responsables du traitement doivent donc répondre aux principes de la RGPD, et notamment en termes de transparence et légalité du traitement. Les sous-traitants agissent en suivant les instructions du responsable de traitement, et notamment sécuriser les données.

THELIS ainsi que les data-center sous-traitants est un "sous-traitant" au sens de la RGPD et dans le cadre de l'infrastructure et logiciels décrits dans ce document.

Les clients sont responsables du traitement pour les données maintenues dans les infrastructures Thelis étant donné que nous traitons les données suivant leurs instructions. Notre charte de sous-traitance décrit notre responsabilité et obligations en tant que sous-traitant.

En résumé, THELIS s'engage sur les points suivants :

- Traiter les données personnelles uniquement sur base des instructions transmises par notre client qui agit en tant que responsable du traitement
- Implémenter des mesures de sécurité adéquates
- Garantir que nos employés sont liés à des obligations de confidentialité

- Notifier nos clients en cas de détection d'un accès non autorisé à des données à caractère privé.
- Accompagner nos clients afin de les aider à répondre aux exigences du règlement de RGPD

*En tant que sous-traitant, Thelis s'engage à :*

- Traiter les données à caractère personnel aux seules fins de la bonne exécution des services : THELIS ne traitera jamais vos informations à d'autres fins (marketing, etc.).
- Ne pas transférer vos données hors UE ou hors pays reconnus par la Commission européenne comme disposant d'un niveau de protection suffisant : sous réserve que vous ne sélectionniez pas un datacenter dans une zone géographique hors UE.
- Vous informer de tout recours à des sous-traitants qui pourraient traiter vos données à caractère personnel.
- Appliquer des mesures techniques et organisationnelles adaptées afin de protéger vos données de destruction accidentelle, perte, altération, fuite, ou d'accès à des données à caractère privé.
- Vous notifier dans les meilleurs délais en cas de violation de données.
- Vous aider à respecter vos obligations réglementaires en fournissant une documentation adéquate de nos services.
- D'appliquer ces engagements au travers de notre chaîne de sous-traitants

### *Propriété des données*

Les données stockées par le client dans le cadre des services souscrits auprès de Thelis restent la propriété du client.

Thelis ne va jamais utiliser ou accéder à ces données, excepté dans le cas où cette opération est nécessaire afin de fournir les services souscrits ou demandés.

Thelis s'interdit de vendre ou utiliser ces données pour son usage personnel

### *Accès aux données hébergées*

Thelis et/ou ses sous-traitants peuvent être amenés à accéder à ces données dans deux cas bien précis :

- Afin de fournir un niveau de service, par exemple lorsque le client contacte le support client.
- Afin de répondre à des obligations légales, dans le cadre de demandes officielles et mandatées (légales ou administratives)

#### Dans le cadre du support au client :

Lorsqu'un client contacte l'équipe de support technique ou administrative, deux catégories de données peuvent être accédées en fonction de la nature de la demande.

Afin de traiter de manière efficace la demande du client, le service de support aura accès aux données fournies par le client (nom, prénom, n° de téléphone, adresse e-mail ...)

Dans un deuxième temps et uniquement avec l'accord du client, et de manière technique restreinte en fonction du type de service, le service de support au client peut accéder aux données stockées par le client ou ses utilisateurs finaux sur l'infrastructure de Thelis, et ce, avec l'objectif de déterminer l'origine du problème rencontré, et de tenter de le résoudre.

#### Accès dans le cadre de demande officielles judiciaires et/ou administratives :

Afin de répondre aux règles et lois en vigueur, Thelis peut être amené à répondre à des demandes émanant d'instances judiciaires et/ou administratives. Ces requêtes sont couvertes par un cadre juridique strict. Thelis n'autorisera pas ces requêtes sans qu'elles n'aient été validées. De plus, et à moins que ce ne soit interdit par la requête ou la loi, Thelis informera le client de cette requête.

### *Localisation géographique des données*

Thelis informera son client (le responsable de traitement) du data-center utilisé et du pays hébergeant celui-ci.

Thelis s'engage à ne pas déplacer le service dans un pays différent sans approbation préalable du client. Pour des raisons techniques, les services peuvent être déplacés sans accord préalable du

client dans un autre data-center ou vers un sous-traitant différent pour autant que la destination reste dans l'Union Européenne et que les conditions de services ne soient pas modifiées.

Thelis ne stocke pas de données en dehors de l'Union Européenne sans une demande ou accord explicite du client.