

CODE DE CONDUITE SWIPO POUR LA COMMUTATION ET LA TRANSMISSION DE DONNEES

DECLARATION DE TRANSPARENCE DE THESEE DATACENTER

Chez Thésée Data Center, nous avons à cœur d'instaurer une relation de confiance et de transparence avec nos clients. Nous nous engageons à répondre à leur besoin en hébergement d'infrastructures informatiques et de performance en lien avec les niveaux de service. La liberté de choix de son prestataire est un élément essentiel de la souveraineté des organisations, et c'est pourquoi nous souhaitons mettre en œuvre l'ensemble des bonnes pratiques du secteur.

Ainsi, la présente déclaration de transparence vise à aider nos clients lorsqu'ils envisagent de changer de prestataire, et ce avant même de conclure un contrat avec Thésée Data Center. Cette déclaration est en conformité avec le Code de Conduite sectoriel SWIPO IaaS, développé par la communauté des fournisseurs et clients d'infrastructures Cloud sous l'égide de la Commission Européenne afin de permettre la mise en œuvre de l'Article 6 Portabilité des Données du Règlement Européen sur la libre circulation des données.

Même si ce Code a été développé initialement pour les acteurs d'infrastructure Cloud qui ne sont pas ceux de la colocation, Thésée Data Center a souhaité répondre à ses attentes afin de permettre à ses clients de bénéficier à la fois des meilleures pratiques du secteur développées dans le cadre européen, mais aussi de leur garantir l'utilisation de prestataires et contrats conformes aux attentes de labels définis par des projets structurant tels que Gaia-X.

Exigences du Code de conduite SWIPO	Réponse de Thésée Datacenter
2.1 Exigences	
<i>Les exigences suivantes doivent être complétées par le CSP.</i>	
2.1.1 Exigences procédurales	
PR01 - Procédures pour initier la commutation et le portage à partir du service en nuage lorsqu'il s'agit d'une source de portage.	Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client. C'est pourquoi, les procédures pour initier la commutation et le portage relèvent de la responsabilité exclusive du client.
PR02 - Procédures pour initier la commutation et le	Les données, applications et serveurs informatiques

portage vers le service en nuage lorsqu'il s'agit d'une destination de portage.	relèvent de la responsabilité exclusive du Client. C'est pourquoi, les procédures pour initier la commutation et le portage à destination du service en nuage relève de la responsabilité exclusive du client.
PR03 – Portage et formats disponibles y compris les protections disponibles et les restrictions et limitations techniques connues.	Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client. C'est pourquoi, le portage et les choix de formats de données sont à la charge du client.
PR04 – Frais et conditions associées au portage	Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client. Les seuls frais en relation avec le portage tiennent à la continuité du service d'hébergement de Thésée et au choix par le client du prestataire de son choix pour ses liens de communication, y compris leur dimensionnement et leur coût.
PR05 – Procédure d'activation d'un nouveau service en nuage lorsqu'il est la destination du portage	Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client. Il convient que le client souscrive les contrats et mette en place les infrastructures nécessaires.
PR06 – Processus de sortie d'un service en nuage existant, lorsqu'il est la source de portage et que le CSC souhaite mettre fin à son utilisation du service en nuage une fois le portage terminé.	Dans la mesure où le client est responsable de ses données et de ses choix de liens de communication, il lui reviendra de mettre en œuvre le portage de ses données en tenant compte du délai de préavis prévu dans le contrat d'hébergement.
PR07 – Capacités de gestion disponibles pour le processus de portage et de commutation (par exemple, gestion de bout en bout pour éviter la perte de service pour le client).	Thésée Data Center ne fournit pas de services de portabilité des données ou des infrastructures. Le client est libre de se faire accompagner par le prestataire de son choix. Thésée s'engage à poursuivre le contrat dans les conditions prévues au contrat.
2.1.2 Exigences en matière de portabilité	
DP01 – Le service en nuage doit être capable d'importer et d'exporter des artefacts d'infrastructures du CSC, de manière simple et sécurisée, en prenant en charge les scénarios suivants : CSC vers service en nuage et service en nuage vers CSC. L'infra CSP doit fournir le support nécessaire pour permettre le transfert des artefacts d'infrastructure dans un format structuré, couramment utilisé et lisible par machine.	Thésée fournit exclusivement des services d'hébergement physique. Les données et les artefacts d'infrastructure sont de la responsabilité exclusive du client. Thésée ne fournit pas de support additionnel pour transférer les données ou les artefacts d'infrastructure.
DP03 – Le CSP déclare tout soutien à faciliter l'interopérabilité entre les capacités du CSC, y compris la fonction d'utilisateur, la fonction d'administrateur et la fonction commerciale liées au service en nuage.	Thésée fournit exclusivement des services d'hébergement physique. L'interopérabilité entre les capacités du CSC, y compris la fonction d'utilisateur, la fonction d'administrateur et la fonction commerciale liées au service en nuage relèvent de la responsabilité exclusive du client.

DP07 – Lorsque les données du CSC impliquent des artefacts d'infrastructure qui reposent sur une caractéristique ou une capacité du service en nuage, l'Infra. CSP doit fournir une description appropriée de l'environnement pour leur exécution et de la manière dont les dépendances du service peuvent être satisfaites.	Thésée fournit une documentation complète au client exclusivement sur le périmètre du service d'hébergement d'infrastructures informatiques proposé par Thésée. Aucune autre documentation n'est fourni au client.
DP09 – L'Infra CSP doit prendre des mesures raisonnables pour permettre à un CSC de maintenir la continuité de ses services lors du transfert de données entre fournisseurs, lorsque cela est techniquement possible.	Afin d'éviter toute interruption des services pendant la phase de transfert de données entre fournisseurs, Thésée s'engage à assurer, en fonction de la durée et de la rémunération prévues par le contrat, et maintenir la continuité des services jusqu'à ce les équipements informatiques du client soient repris par celui-ci ou son prestataire.
2.1.3 Champ d'application et exigences de compatibilité	
SCR01 – La déclaration de transparence mentionne les capacités nécessaires pour un changement efficace de service en nuage, afin de minimiser la perte de fonctionnalité, en particulier la fonctionnalité de sécurité. La déclaration définit les données dérivées soumises aux mêmes exigences de portage. Toute capacité de portage relative à des données dérivées de services en nuage désignés doit être clairement décrite dans la déclaration de transparence du CSP.	La sécurité et le transfert des données sont de la responsabilité du client. Thésée assure la continuité des services tout au long du transfert (accès réseau, refroidissement, alimentation) en fonction de la durée et de la rémunération prévues par le contrat.
SCR02 – La déclaration de transparence doit préciser ce qui suit : a) L'étendue des artefacts d'infrastructure disponible pour le transfert ; b) Toute revendication sur les droits de propriété intellectuelle que l'Infra CSP sur les données de la CSC et la manière dont ces droits sont exercés après changement de fournisseur.	a) Le client seul est responsable du transfert de ses artefacts d'infrastructure et en détermine lui-même l'étendue. b) Le Client est seul propriétaire de ses artefacts et peut en disposer sous sa responsabilité.
2.1.4 Exigences en matière de planification	
DPP01 – La déclaration prévoit une procédure visant à déterminer la mise à l'essai des mécanismes et le calendrier d'un transfert, sur la base des besoins opérationnels du CSC, des risques de sécurité et des capacités techniques et de soutien attendues de chacun des Infra CSP et du CSC. Les tests doivent porter à la fois sur les mécanismes utilisés pour le portage des données vers et depuis un service en nuage et sur les API utilisés pour accéder aux données et les gérer lorsqu'elles sont stockées dans le service en nuage.	Le transfert des données sont la seule responsabilité du client. Il effectue lui-même les mises à l'essai des mécanismes et le calendrier des transferts.
DPP02 – Ce qui constitue une durée appropriée pour le transfert de données en utilisant les meilleures pratiques actuelles et la technologie disponible, y compris toute solution n'utilisant pas un réseau.	Le transfert de données et la reprise des équipements par le client sont sous la responsabilité du client qui détermine la durée appropriée pour le transfert de ses données. Une documentation indicative sur le dimensionnement des réseaux nécessaire en fonction de la volumétrie de données est disponible pour le client.
PLR03 – Le CSP doit déclarer s'il existe différents mécanismes pour différents volumes d'artefacts	Les mécanismes de transfert sont à prévoir et à mettre en œuvre par le client.

d'infrastructure et les détails de chaque mécanisme y compris les prédictions de disponibilité et le coût.	Les coûts associés au transfert des données ont à la charge du client. Une documentation indicative sur le dimensionnement des réseaux nécessaire en fonction de la volumétrie de données est disponible pour le client, lui permettant d'estimer les coûts auprès du prestataire réseau de son choix.
DPP04 – Attribution de la responsabilité respectives en matière de sécurité des données afin de garantir, par exemple, le contrôle d'accès, l'authentification des utilisateurs, la confidentialité et l'intégrité tout au long du processus.	Le client est seul responsable des données qu'il exploite et stocke. Lors du transfert, il assume l'entière responsabilité en matière de sécurité et de confidentialité. Thésée est responsable de la disponibilité des services d'hébergement prévus au contrat et du contrôle d'accès physique aux équipements du client.
DPP05 – La période pendant laquelle le CSC a le droit de transférer ses données une fois que le contrat est résilié pour quelque raison que ce soit et la nature des avertissements claires et opportuns émis avant que les données du CSC ne soient supprimées.	Le client gère seul la période pendant laquelle il transfère ses données. Les données sont sous la seule responsabilité et sous la garde du client. A la fin du contrat, les serveurs sont coupés et repris par le client.
2.1.5 Exigences du contrat de service en nuage	
FR1 – Le contrat doit être documenté et juridiquement contraignant entre le prestataire et le client.	Tous les services sont délivrés dans le cadre d'un contrat négocié et signé par les deux parties ayant force obligatoire. Les contrats sont documentés d'annexes RGPD et de clauses réversibilité permettant aux clients d'avoir une visibilité.
FR2 – Le contrat de prestation de services peut prendre n'importe quelle forme, y compris, mais sans s'y limiter : a) Un contrat unique ; b) Un ensemble de documents tels qu'un contrat de services de base avec les annexes pertinentes (accord sur le traitement des données, accord de niveau de service, conditions de service, politiques de sécurité, etc.) c) Conditions générales d'utilisation en ligne. Note : Les différentes formes et le contenu d'un contrat sont abordés dans la partie 1 de l'ISO 19086.	Nos contrats clients comportent : - Un contrat de service d'hébergement d'infrastructures informatiques, - Annexes pertinentes : offre et conditions financières, niveaux de service, plan assurance sécurité, plan de réversibilité, RGPD et sécurité des données personnelles, règlement intérieur des sites, la présente déclaration de transparence.
2.1.6 Exigences de transparence	
TRO1 – Les termes et conditions nécessaires pour respecter le présent Code doivent être décrits au client potentiel en termes claires et avec un niveau de détails approprié dans une déclaration de transparence du prestataire précontractuelle entre le prestataire et son client. Veuillez noter que la mise à disposition des informations précontractuelles aux CCF potentiels n'exige pas une divulgation publique et peut se faire dans la stricte confidentialité.	La présente déclaration de transparence est annexée aux contrats. Elle est communiquée préalablement à tout prospect dans le cadre des négociations commerciales.
TRO2 – Le prestataire doit fournir une déclaration de transparence en utilisant le modèle de la version de la déclaration de transparence du Client pour les services	La présente déclaration répond à l'ensemble des critères formels posés par le Code.

IaaS Cloud et ne doit pas modifier l'ordre et la structure de ce modèle.	
TR03 – La description prévue dans TR01 doit fournir un niveau approprié de détails, y compris : a) Tous les aspects du respect du présent code ; b) Toute la documentation, le support disponible et les outils pour transférer les données CSC d'un Infra CSP à un autre ; c) Une description de l'ensemble du processus de portage des données et des capacités prises en charge, y compris les processus de sauvegarde et de récupération des données adoptés pour protéger les données pendant le portage des données, les mesures de sécurité, la gestion des dossiers et, si cela a été convenu, la suppression des données du CCF une le portage des données terminé avec succès. Si la capacité d'effacement est fournie au CSC par le fournisseur de services d'infonuagique, le CSC peut procéder à l'effacement des données du CSC. CSP, le CSC peut procéder lui-même à l'effacement. L'effacement doit être effectué par le fournisseur infra CSP source, dans le cas où cette capacité n'est pas fournie au CSC ; d) L'état et les procédures de traitement des données du CSC sur l'infrastructure infra ; après la résiliation, y compris les instructions du CSC sur les points suivants toute obligation de conservation, de préservation ou de restauration des données prévue par la loi ou la réglementation applicable ; e) Une description claire de tous les tiers qui ont accès aux données dans le cadre du processus ; f) Une description claire des politiques et procédures d'accès aux données en cas de faillite ou d'acquisition par une autre entité d'Infra CSP en cas de faillite ou d'acquisition par une autre entité. Ces politiques et procédures doivent inclure les informations du SCS sans délai excessif dès lors qu'une procédure de faillite a été engagée auprès des autorités publiques compétentes ; g) Si un prestataire de services tiers est nécessaire pour convertir, traduire ou transférer les artefacts d'infrastructure du CSC, il doit être explicitement mentionné dans la déclaration de transparence du CSP.	Thésée fournit des descriptions par le biais de la présente déclaration de transparence : a) Le présent code est annexé aux contrats de service d'hébergement ; b) Le transfert des données sont sous la responsabilité du client qui en assure seul l'exécution. Une note spécifique est disponible pour le client ; c) Le client est pleinement responsable du processus de portage des données et des capacités prises en charge, y compris : ▪ Les processus de sauvegarde et de récupération des données disponibles pendant le portage, ▪ Les mesures de sécurité, toute gestion de dossier, ▪ Des suppressions de données – Thésée n'ayant pas d'accès aux serveurs et données des clients, ne saurait être tenu responsable d'une quelconque suppression ou perte des données du CSC. d) Le client a la charge de la conservation, de la préservation et de l'utilisation de ses données. e) Le client est seul responsable de ses données vis-à-vis des tiers. f) Une option de résiliation du contrat de services est ouverte au client en cas de changement de contrôle du groupe ou en cas de faillite. g) Le client est seul responsable de l'intervention des tiers sur ses infrastructures informatiques que cela soit pour convertir, traduire ou transférer les artefacts d'infrastructure. Les tiers interviennent à la demande exclusive du client.
TR04 – Avant que le CSC n'accepte le contrat, l'infra CSP doit fournir au CSC une déclaration de transparence du CSP décrivant le(s) mécanisme(s) lié(s) au portage des données du CSC : a) Des installations sur site d'un CSC vers un service en nuage d'Infra CSP cloud service, b) D'un autre service en nuage vers le service en nuage d'Infra CSP cloud,	Toutes les informations pertinentes et requises sont fournies dans la présente déclaration de transparence annexé au contrat d'hébergement.

c) Vers les installations sur site du CSC à partir du service en nuage d'Infra CSP cloud, d) Vers un autre service en nuage à partir du service en usage de l'Infra service en nuage du CSP. La description doit fournir un niveau de détail approprié, y compris : e) Les procédures, les conditions, les politiques et les coûts associés à un tel portage de données, f) Des informations appropriées sur les mesures techniques, physiquement organisationnelles pertinentes pour réaliser ce portage de données, g) Le cas échéant, une explication du modèle de données, du schéma de données et de la sémantique des données, ainsi que de toutes les considérations relatives aux facettes de la politique adoptées par l'infra CSP dans la mesure où celles s'appliquent aux données du CSC, et la manière dont ces aspects sont traités lors de l'examen de la portabilité des données, h) Tous les domaines des coûts connexes qui seraient facturés par l'Infra CSP. L'Infra CSP veille à ce que les informations relatives à la portabilité des données soient mises à la disposition du CSC, y compris en ligne et/ou incorporés par référence dans d'autres documents contractuels et à ce que ces informations soient tenues à jour.	
TR05 – L'Infra CSP doit informer les CSC en temps utile de toute modification des mécanismes et des conditions, y compris des coûts identifiés, qui modifierait sensiblement la portabilité des données du CSC. Le CSC doit avoir le droit de résilier l'accord à l'avance.	A revoir quid si modification des ontrats – consensuel – enaggement auprus de clients à les informaer en amont et possibilité de r&silier Aucune modification contractuelle n'est faite par Thésée avant la fin du contrat (ou Toute modification contractuelle est présentée au client au moins 90 jours avant son entrée en vigueur, le client disposant de 60 jours pour résilier son contrat en cas de modification substantielle du contrat)
TR06 – L'Infra CSP informe le CSC dans les meilleurs délais en cas de modification permanente de sa déclaration d'adhésion.	Thésée informera le client des mises à jour de la Déclaration d'adhésion dans les meilleurs délais.
2.2 Recommandations	
<u>Les recommandations suivantes ne doivent être complétées que si elles sont soutenues.</u>	
2.2.1 Recommandations en matière de portabilité	
DP02 – Lors de l'exportation d'artefacts d'infrastructure du CSC d'un CSC vers un service en nuage, l'Infra CSP doit fournir un support pour faciliter l'interopérabilité entre les capacités du CSC, y compris la fonction utilisateur, la fonction administrateur et la fonction métier liées au service en nuage.	Non soutenue par Thésée. Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client.

DP04 – L'infra CSP doit fournir des interfaces de programmation d'application liées au service en nuage et, si elles sont fournies, elles doivent être entièrement documentées. Ces API doivent permettre le transfert d'artefacts d'infrastructure entre les parties participantes. S'il existe des dépendances associées à des bibliothèques de code, elles doivent être déclarées, documentées et mises à disposition.	Non soutenue par Thésée. Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client.
DP05 – Le service en nuage n'est pas tenu, en vertu du présent code, de transformer les artefacts d'infrastructure du CSC lorsque l'environnement de destination exige que les artefacts d'infrastructure soient dans des formations différents de ceux proposés par l'environnement source. Les parties peuvent en convenir autrement dans le contrat.	Non soutenue par Thésée. Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client.
DP06 – Le transfert des artefacts d'infrastructure du CSC vers et depuis le service en nuage doit utiliser des normes et des protocoles ouverts pour le mouvement des artefacts d'infrastructure.	Non soutenue par Thésée. Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client.
DP08 – Le CSP doit fournir une interface en libre-service qui permet au CSC d'extraire périodiquement ses données. Cette fonctionnalité peut faire l'objet d'un contrat et peut entraîner des coûts supplémentaires.	Non soutenue par Thésée. Les données, applications et serveurs informatiques relèvent de la responsabilité exclusive du Client.

