

HDS Representation of Safeguards

Last update: June 2026

PLENIT

Mapping of actors and representation of safeguards

Actor legal name	Role in the hosting service	HDS certified	SecNumCloud qualified	Hosting activities performed by the actor	Access to DSCP from third countries outside the EEA (HDS requirement no. 29)	Risk of access imposed by third-country legislation and safeguards (HDS requirement no. 30)
PLENIT TECHNOLOGY, S.L. (PLENIT HQ)	Host / main technical operator. Technical sub-processor of PLENIT FRANCE when PLENIT FRANCE enters into the Service Contract with the end customer.	Yes (PLENIT, subject to the HDS certificate scope)	No	Underlying infrastructure, hosting, storage, identity management, backups, operations, security, technical support and maintenance of the platform.	No. HDS activities are operated from the EEA and DSCP are not transferred outside the EEA by PLENIT HQ.	No third-country legislation risk identified for PLENIT HQ. Measures include RBAC, MFA, logging, monitoring, encryption, change management and security governance.
PLENIT FRANCE SAS	Contracting host / French local entity where the Service Contract is entered into with French customers. Acts as Data Processor towards the end customer for Customer Data.	Yes (PLENIT, subject to the HDS certificate scope)	No	Local commercial relationship, contracting, invoicing, customer management and local coordination. Does not provide technical infrastructure services to PLENIT HQ.	No. No access to DSCP from a third country outside the EEA is performed by PLENIT FRANCE.	No third-country legislation risk identified. Applicable HDS, GDPR and contractual obligations are reflected in the customer-facing and intragroup documentation.
JOTELULU S.L. SUCURSAL EM PORTUGAL (Portuguese branch of the PLENIT Group)	Portuguese local entity of the group. Sub-processor only where it effectively accesses Customer Data or provides local customer support for the relevant services.	Yes (PLENIT, subject to the HDS certificate scope)	No	Local commercial activities, customer relationship management, invoicing/local administration and first-level customer interaction. Does not provide technical infrastructure services to PLENIT HQ and does not operate independent data centres.	No. No access to DSCP from a third country outside the EEA.	No third-country legislation risk identified. Any processing is performed in the EEA and is subject to the group's common security measures.
PLENIT TECHNOLOGY, S.A. de C.V. (PLENIT MEXICO)	Potential sub-processor for out-of-hours operational support, acting exclusively under documented instructions from PLENIT HQ.	No	No	Limited technical support for infrastructure and platform operations. No logical access to customer content or DSCP. Interventions only when necessary and under internal procedures validated by PLENIT HQ.	No logical access to DSCP from Mexico. Any possible access is limited to infrastructure and platform administration tools and does not allow access to customer content. All access is subject to prior authorization by an authorized member located in the European Union. Permission assignment and VPN access are controlled from the European Union.	PLENIT MEXICO is established in Mexico, a third country outside the EEA. A theoretical risk linked to non-European legislation cannot be completely excluded. However, this risk is strongly limited by: absence of logical access to DSCP; least privilege; MFA; VPN controlled from the EU; logging and monitoring; segregation of duties; confidentiality undertakings; prior EU-based authorization. Any change to permissions, VPN access or sensitive configuration requires approval by two authorized members and validation by the CAB, located and operated in the EU. Residual risk: limited.

Actor legal name	Role in the hosting service	HDS certified	SecNumCloud qualified	Hosting activities performed by the actor	Access to DSCP from third countries outside the EEA (HDS requirement no. 29)	Risk of access imposed by third-country legislation and safeguards (HDS requirement no. 30)
INTERXION FRANCE SAS	Host / data centre provider in France.	Yes	No	Activity 1 - provision and operational maintenance of physical sites hosting the hardware infrastructure of the information system used for DSCP processing.	No. No access to DSCP from a third country outside the EEA.	Interxion France belongs to a US-based group and may therefore be exposed to certain US extraterritorial laws. The risk is limited because the provider has no logical access to PLENIT infrastructure or DSCP and PLENIT controls encryption, logical administration and access control mechanisms. Residual risk: limited.
INTERXION ESPAÑA SAU	Host / data centre provider in Spain.	No	No	Activity 1 - provision and operational maintenance of physical sites hosting the hardware infrastructure of the information system used for DSCP processing.	No. No access to DSCP from a third country outside the EEA.	Interxion Spain belongs to a US-based group and may therefore be exposed to certain US extraterritorial laws. The risk is limited because the provider has no logical access to PLENIT infrastructure or DSCP and PLENIT controls encryption, logical administration and access control mechanisms. Residual risk: limited.
DATA 4 Spain	Host / data centre and remote hands provider in Spain.	Yes	No	Physical site provision, hardware hosting and remote hands for Servers and Remote Desktop where applicable.	No. No access to DSCP from a third country outside the EEA.	No third-country legislation risk identified. The provider has no logical access to DSCP. Interventions are limited to physical/remote hands operations governed by PLENIT procedures.

Additional organizational safeguards

For HDS activities, PLENIT applies an access governance model based on control from the European Union. Any operational access from a third country is subject to prior authorization by an authorized member located in the European Union.

Permission assignment, rights revocation, privileged account management and VPN access are controlled from the European Union. Access is individual, limited to need-to-know, protected by strong authentication and logged.

Any change to access rights, VPN access, sensitive configuration or parameters that may affect the HDS environment must be approved by two authorized members and validated by the Change Advisory Board (CAB). The CAB is located and operated from the European Union.

Représentation des garanties HDS

Dernière mise à jour : juin 2026.

PLENIT

Cartographie des acteurs et représentation des garanties

Raison sociale de l'acteur	Rôle dans le cadre de la prestation d'hébergement	Certifié HDS	Qualifié SecNumCloud	Activités d'hébergement réalisées par l'acteur	Accès aux DSCP depuis des pays tiers hors EEE (exigence HDS n°29)	Risque d'accès imposé par la législation d'un pays tiers et garanties (exigence HDS n°30)
PLENIT TECHNOLOGY, S.L. (PLENIT HQ)	Hébergeur / opérateur technique principal. Sous-traitant technique de PLENIT FRANCE lorsque PLENIT FRANCE conclut le Contrat de Service avec le client final.	Oui (PLENIT, sous réserve du périmètre du certificat HDS)	Non	Infrastructure sous-jacente, hébergement, stockage, gestion des identités, sauvegardes, opérations, sécurité, support technique et maintenance de la plateforme.	Non. Les activités HDS sont opérées depuis l'EEE et les DSCP ne sont pas transférées en dehors de l'EEE par PLENIT HQ.	Aucun risque lié à une législation de pays tiers n'est identifié pour PLENIT HQ. Les mesures comprennent notamment RBAC, MFA, journalisation, supervision, chiffrement, gestion des changements et gouvernance de la sécurité.
PLENIT FRANCE SAS	Hébergeur contractant / entité locale française lorsque le Contrat de Service est conclu avec des clients français. Agit en tant que sous-traitant du client final pour les Données Client.	Oui (PLENIT, sous réserve du périmètre du certificat HDS)	Non	Relation commerciale locale, contractualisation, facturation, gestion client et coordination locale. Ne fournit pas de services d'infrastructure technique à PLENIT HQ.	Non. Aucun accès aux DSCP depuis un pays tiers hors EEE n'est réalisé par PLENIT FRANCE.	Aucun risque lié à une législation de pays tiers n'est identifié. Les obligations HDS, RGPD et contractuelles applicables sont reflétées dans la documentation client et intragroupe.
JOTELULU S.L. SUCURSAL EM PORTUGAL (succursale portugaise du groupe PLENIT)	Entité locale portugaise du groupe. Sous-traitant uniquement lorsqu'elle accède effectivement aux Données Client ou fournit un support client local pour les services concernés.	Oui (PLENIT, sous réserve du périmètre du certificat HDS)	Non	Activités commerciales locales, gestion de la relation client, facturation/administration locale et interaction client de premier niveau. Ne fournit pas de services d'infrastructure technique à PLENIT HQ et n'exploite pas de centres de données indépendants.	Non. Aucun accès aux DSCP depuis un pays tiers hors EEE.	Aucun risque lié à une législation de pays tiers n'est identifié. Tout traitement est réalisé dans l'EEE et soumis aux mesures de sécurité communes du groupe.
PLENIT TECHNOLOGY, S.A. de C.V. (PLENIT MEXICO)	Sous-traitant potentiel pour le support opérationnel hors horaires ouvrés, agissant exclusivement sous instructions documentées de PLENIT HQ.	Non	Non	Support technique limité aux opérations d'infrastructure et de plateforme. Aucun accès logique au contenu client ni aux DSCP. Les interventions sont réalisées uniquement lorsque cela est nécessaire et conformément aux procédures internes validées par PLENIT HQ.	Aucun accès logique aux DSCP depuis le Mexique. Tout accès éventuel est limité aux outils d'administration d'infrastructure et de plateforme et ne permet pas d'accéder au contenu client. Tous les accès sont soumis à une autorisation préalable par un membre autorisé situé dans l'Union européenne. L'attribution des permissions et l'accès VPN sont contrôlés depuis l'Union européenne.	PLENIT MEXICO est établie au Mexique, pays tiers hors EEE. Un risque théorique lié à une législation extra-européenne ne peut être totalement exclu. Toutefois, ce risque est fortement limité par : l'absence d'accès logique aux DSCP ; le principe du moindre privilège ; la MFA ; le VPN contrôlé depuis l'UE ; la journalisation et la supervision ; la séparation des tâches ; les engagements de confidentialité ; l'autorisation préalable depuis l'UE. Toute modification des permissions, de l'accès VPN ou d'une configuration sensible nécessite l'approbation de deux membres autorisés et la validation du CAB, situé et opéré dans l'UE. Risque résiduel : limité.
INTERXION FRANCE SAS	Hébergeur / fournisseur de centre de données en France.	Oui	Non	Activité 1 - mise à disposition et maintien en condition opérationnelle de sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des DSCP.	Non. Aucun accès aux DSCP depuis un pays tiers hors EEE.	Interxion France appartient à un groupe basé aux États-Unis et peut donc être exposée à certaines lois extraterritoriales américaines. Le risque est limité car le fournisseur ne dispose d'aucun accès logique à l'infrastructure de PLENIT ni aux DSCP, et PLENIT maîtrise le chiffrement, l'administration logique et les mécanismes de contrôle d'accès. Risque résiduel : limité.
INTERXION ESPAÑA SAU	Hébergeur / fournisseur de centre de données en Espagne.	Non	Non	Activité 1 - mise à disposition et maintien en condition opérationnelle de sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des DSCP.	Non. Aucun accès aux DSCP depuis un pays tiers hors EEE.	Interxion Spain appartient à un groupe basé aux États-Unis et peut donc être exposée à certaines lois extraterritoriales américaines. Le risque est limité car le fournisseur ne dispose d'aucun accès logique à l'infrastructure de PLENIT ni aux DSCP, et PLENIT maîtrise le chiffrement, l'administration logique et les mécanismes de contrôle d'accès. Risque résiduel : limité.
DATA 4 Spain	Hébergeur / fournisseur de centre de données et de remote hands en Espagne.	Oui	Non	Mise à disposition de site physique, hébergement matériel et remote hands pour les services Servers et Remote Desktop lorsque applicable.	Non. Aucun accès aux DSCP depuis un pays tiers hors EEE.	Aucun risque lié à une législation de pays tiers n'est identifié. Le fournisseur ne dispose d'aucun accès logique aux DSCP. Les interventions sont limitées aux opérations physiques / remote hands régies par les procédures de PLENIT.

Garanties organisationnelles complémentaires

Pour les activités HDS, PLENIT applique un modèle de gouvernance des accès fondé sur un contrôle depuis l'Union européenne. Tout accès opérationnel depuis un pays tiers est soumis à une autorisation préalable par un membre autorisé situé dans l'Union européenne.

L'attribution des permissions, la révocation des droits, la gestion des comptes privilégiés et l'accès VPN sont contrôlés depuis l'Union européenne. Les accès sont individuels, limités au besoin d'en connaître, protégés par une authentification forte et journalisés.

Toute modification des droits d'accès, de l'accès VPN, d'une configuration sensible ou des paramètres susceptibles d'affecter l'environnement HDS doit être approuvée par deux membres autorisés et validée par le Change Advisory Board (CAB). Le CAB est situé et opéré depuis l'Union européenne.