Accusé de réception en préfecture
091-219106614-20250225-DEC_2025_027b-CC
Date de télétransmission : 28/02/2025
Date de réception préfecture : 28/02/2025

CONTRAT DE MAINTENANCE OXALIS

GESTION DES DOSSIERS D'APPLICATION DU DROIT DES SOLS

GESTION DU CADASTRE ET DE L'URBANISME

CONTRAT N° 2025CM0417

Entre :

OPERIS, Société par actions simplifiées, au capital de 1000 000 €uros, immatriculée au registre du commerce et des sociétés d'Evry, sous le numéro 453 874 687 RCS, ayant son siège social situé au

130 Avenue Claude Antoine PECCOT, 44700 ORVAULT,

Représentée par Madame LE BRIS, en qualité de Dirigeant,

ci-après dénommée « ***OPERIS*** »,

et :

Villebon-sur-Yvette (91)
7 place Gérard-Nevers
BP 1
91141 VILLEBON-SUR-YVETTE
FRANCE

ci-dessous dénommé(e) « le Client »

OBJET

OPERIS assure au Client la réalisation des services de Maintenance et Support de base pour le Logiciel objet du présent Contrat, selon les conditions particulières et générales spécifiées dans ce contrat.

Operis propose également des prestations optionnelles associées au présent contrat.

L'intégralité des prestations proposées sont décrites dans l'article **« Description des prestations ».**

CONDITIONS PARTICULIERES

DATE D'EFFET DES PRESTATIONS

Les prestations de services prendront effet le 01/01/2025, puis à la date de mise en service de chaque module.

TARIF ANNUEL DU CONTRAT

Maintenance	Qté	5 429,84 € HT
[OXA-SVW-MLS] Serveur WEB	ilimité	
[OXA-DII-MLU] DIA /I - Gestion des dossiers DIA	1	
[OXA-TXI-MLU] ADS TAXES - Taxes et participations des dossiers Droit des Sols	2	
[OXA-VPO-MLU] VECPRO - Lien SIG côté OPERIS	2	4 161,65 € HT
[OXA-ADI-MLU] ADS /I - Instruction des dossiers du Droit des Sols	2	
[OXA-SVW-JAH] Assistance Annuelle	1	
[OXA-DGI-MLU] Mise à jour et intégration des données DGI	1	
[OXA-CAD-MLU] CADASTRE - Gestion du cadastre MAJIC et Règlement PLU	5	
[OXA-SVE-MLS] SVES - GNAU Module Saisine et Suivi Site	ilimité	691,74 € HT
[OXA-LEG-MLS] LEGA/PLAT'AU - GNAU Module Éditions Légales-PLAT'AU	ilimité	576,45 € HT

Montant total du Contrat	**5 429,84 € HT**

CONDITIONS FINANCIERES DE LA MAINTENANCE DU LOGICIEL

La première redevance sera réglée sur présentation de facture, à la société OPERIS, pour la période de douze mois à échoir à compter de la date d'effet.

Les redevances suivantes seront dues à la société OPERIS sur présentation de facture, chaque année à la date d'anniversaire, pour une période de douze mois.

INTERLOCUTEUR CLIENT POUR LA PARTIE ADMINISTRATIVE

Le Client désigne une personne comme unique interlocuteur auprès d'OPERIS pour la partie administrative des contrats. (A remplir par le client)

Site	Civilité-Nom-Prénom	Fonction	E-mail

INTERLOCUTEURS CLIENT POUR LES PRESTATIONS DE MAINTENANCE ET DE SUPPORT

Support inclus au contrat de base : Interlocuteur unique pour les Prestations de Maintenance

Conformément à l'article « Collaboration du Client » des Conditions Générales de Maintenance, le Client désigne une personne comme unique interlocuteur et coordonnateur auprès d'OPERIS concernant les Prestations de Maintenance du Logiciel. Un suppléant, du même site, peut être nommé pour pallier aux périodes d'absence de l'interlocuteur principal. (A remplir par le client)

Site	Civilité-Nom-Prénom	Fonction	E-mail

PERIMETRE DU DROIT D'USAGE DU LOGICIEL

Commune/Collectivité
Villebon-sur-Yvette (91)

DESCRIPTION DES PRESTATIONS

PRESTATIONS DU CONTRAT

Maintenance du logiciel

La maintenance de base des logiciels OPERIS couvre les corrections, les évolutions fonctionnelles et les adaptations du produit dues aux évolutions réglementaires.

Le logiciel fait l'objet de plusieurs révisions ou versions, en fonction du changement de réglementation ou de la technologie, fournies à l'ensemble des clients dans le cadre du contrat de maintenance.

Support

Le support (Hotline) est accessible aux personnes désignées dans le présent contrat afin de remédier aux problèmes d'utilisation ou d'exploitation courants du logiciel, à savoir:

- Dysfonctionnement du logiciel
- Accès au logiciel
- Assistance au diagnostic sur la compatibilité du logiciel à l'environnement d'exploitation du site
- Assistance à l'utilisation du logiciel
- Assistance en cas d'anomalies constatées durant la mise en œuvre d'une nouvelle version

L'interlocuteur désigné par le client dans le présent contrat soumettra à OPERIS sa demande via l'extranet Operis ou par téléphone.

Les dysfonctionnements doivent être reproductibles et constatés par l'interlocuteur désigné par le client avant signalement à OPERIS. Ce dernier devra associer à sa demande tout élément permettant de décrire l'anomalie constatée et le cheminement permettant de la reproduire.

PRESTATIONS ANNUELLES OPTIONNELLES (INCLUSES SI LISTEES DANS LE TABLEAU ARTICLE 2 : TARIF ANNUEL)

Assistance Sérénité

Elle a pour objet d'assister le client pour toute opération relevant de l'exploitation du logiciel :

- Installation par OPERIS des mises à jour du logiciel
- Paramétrage de l'environnement OPERIS du serveur sur lequel sont implémentés le logiciel et la base de données associée
- Diagnostic technique de l'environnement sur lequel est implémenté le logiciel

Assistance Annuelle

Cela consiste en une intervention d'une ou plusieurs journées par an sur le site du client afin de l'assister à une meilleure utilisation du logiciel.

Il peut s'agir aussi bien d'un complément de formation (y compris pour de nouveaux utilisateurs) que d'une assistance au paramétrage du logiciel.

Le contenu de la prestation est défini en commun avec le client.

Extension du support à d'autres interlocuteurs du site client

Cette option permet à tous les utilisateurs du site de contacter directement le support pour la prise en charge et le traitement de leurs demandes.

Cette option répond au client qui souhaite désigner plusieurs interlocuteurs auprès d'OPERIS pour son site.

Mise à jours et intégration des données DGI (MAJIC)

Cette prestation consiste à intégrer annuellement les nouvelles données MAJIC 3 (données textuelles du cadastre) dans la base du client.

Cette prestation sera réalisée dans un délai d'un mois à compter de la réception par Operis des données MAJIC3 transmises par le client.

Mise à jours et intégration des plans vectoriels du cadastre (EDIGEO)

Cette prestation consiste à intégrer annuellement dans la base du client les nouvelles données cartographiques du cadastre fournies au format EDIGEO.

Cette prestation sera réalisée dans un délai d'un mois à compter de la réception par Operis des données EDIGEO transmises par le client.

Intégration des données PLU dans le référentiel du logiciel via un fichier Excel

Cette prestation consiste à intégrer dans la base du client les données PLU associées aux données parcellaires. La structure du fichier Excel est fournie par Operis et renseignée par la collectivité.

La qualité des informations intégrées reste sous la responsabilité de la collectivité.

La première redevance sera réglée à terme à échoir sur présentation de facture, à la société OPERIS, pour la période de douze mois débutant à compter de la date d'effet.

Les redevances suivantes seront dues à la société OPERIS sur présentation de facture, chaque année à la date d'anniversaire, pour une période de douze mois, puis pour les périodes succédant à la reconduction du Contrat.

Les présentes Conditions Particulières complètent les Conditions Générales de Maintenance 07 2024 . Ainsi toute signature des présentes emporte application desdites Conditions Générales Maintenance 07 2024 qui ont été fournies au Client avant cette signature, ce que le Client reconnait expressément.

Fait à Villebon-sur-Yvette

le __/__/____ le 11/02/2025

Le Client

MAIRIE DE VILLEBON SUR YVETTE 91 ESSONNE

Victor DA SILVA

Maire de Villebon-sur-Yvette

OPERIS

Elodie LE BRIS

Signature numérique de Elodie LE BRIS
Date : 2025.02.10 17:00:04 +01'00'

CONDITIONS GENERALES MAINTENANCE 07.2024

Les présentes Conditions Générales, les Conditions Particulières qui s'y rattachent et les conditions spécifiques au règlement sur la protection des données à caractère personnel, définissent les termes et conditions des Prestations de Maintenance par OPERIS portant sur le Logiciel, dont le Client doit avoir précédemment acquis par licence un droit d'utilisation.

La signature des Conditions Particulières de Maintenance vaut acceptation des présentes Conditions Générales ainsi que des conditions spécifiques au règlement sur la protection des données à caractère personnel.

ARTICLE-1 DEFINITIONS

Chacun des termes mentionnés ci-dessous, avec une majuscule, au singulier ou au pluriel, aura la signification suivante :

- **« Logiciel »** désigne le logiciel **cité en objet**
- **« Erreur de fonctionnement »** désigne tout défaut d'exécution imputable au Logiciel et reproductible en présence d'OPERIS, se traduisant par des résultats non conformes aux fonctionnalités décrites dans la Documentation associée au Logiciel. Une Erreur de fonctionnement est **bloquante** si elle rend totalement impossible l'utilisation du Logiciel ou d'une fonctionnalité essentielle du Logiciel, pour tous les utilisateurs. Une Erreur de fonctionnement est **Majeure** si elle a un impact significatif sur l'activité du client ou rend indisponible l'utilisation d'une fonctionnalité importante pour un seul utilisateur ou un groupe limité d'utilisateurs. Toute autre Erreur de fonctionnement est **Mineure**. Toute demande d'évolution est exclue du contrat et fera l'objet d'une étude pour intégration éventuelle dans une version ultérieure.
- **« Mise à Jour »** désigne les versions du Logiciel intégrant les solutions apportées par OPERIS aux dysfonctionnements éventuels rencontrés par le Client. Elles comprennent la Mise à Jour éventuelle de la Documentation associée.
- **« Nouvelles Versions »** désigne (i) l'ensemble des Mises à Jour apportées par OPERIS depuis les précédentes versions du logiciel livrées au Client et (ii) les évolutions requises par la législation en vigueur étant précisé que dans l'hypothèse où ces évolutions entraîneraient pour OPERIS des frais disproportionnés par rapport à la redevance visée aux Conditions Particulières, les Parties se concerteront pour examiner les modalités d'intégration de cette évolution dans le Logiciel. Il est précisé qu'une Nouvelle Version peut modifier et/ou supprimer certaines fonctionnalités mineures de la Nouvelle Version précédente.
- **« Solution »** désigne le logiciel, le système d'exploitation, les serveurs web et d'application et la base de données nécessaire à l'exploitation du logiciel, celle-ci contient les données du client
- **« Parties »** désigne la société Operis (RCS B 453 874 687) et le client désigné dans le présent contrat

ARTICLE-2 DUREE ET FIN DE CONTRAT

La Maintenance du Progiciel prend effet à la date indiquée dans les Conditions Particulières de Maintenance pour une durée de douze (12) mois et sera reconduite de manière tacite tous les ans et ce au maximum 4 fois, sauf en cas de résiliation par l'Editeur ou par le Client par lettre recommandée avec demande d'avis de réception 3 mois avant la date de fin.

Lors de l'ajout d'un nouveau module la maintenance prendra effet à la date de formation ou à la date d'installation si aucune formation n'est associée à la livraison du module. Lors de l'ajout d'un nouveau module la maintenance prendra effet à la date de formation ou à la date d'installation si aucune formation n'est associée à la livraison du module.

ARTICLE-3 COLLABORATION DU CLIENT

Le Client s'engage à collaborer avec OPERIS, ou tout tiers qu'il mandatera, afin de faciliter l'exécution des Prestations de Maintenance et, plus particulièrement, à :

- Désigner un interlocuteur unique et privilégié auprès d'OPERIS, coordonnateur des demandes de prestations de maintenance et responsable de la mise en œuvre des instructions d'OPERIS et de la collaboration du Client. Cet interlocuteur aura été préalablement formé à l'utilisation du Logiciel et centralisera les demandes de Maintenance en décrivant avec précision l'erreur de fonctionnement rencontrée et les conditions de leur survenance ;
- Assurer aux utilisateurs du Logiciel un niveau de compétence et de formation permettant une utilisation du Logiciel conforme à la Documentation associée ;
- Tenir un registre détaillé de toutes les difficultés et Erreurs de fonctionnement du Logiciel en décrivant notamment les conditions exactes de leur survenance et les interventions d'OPERIS ;
- Fournir toute information de nature à faciliter la recherche des causes d'une Erreur de fonctionnement ;
- Fournir et rappeler, à chaque intervention sur le Site d'OPERIS ou de tout tiers qu'il mandatera, les procédures spécifiques (sécurité, normes d'exploitation...) en vigueur sur son Site ;

- Donner à OPERIS ou à tout tiers qu'il mandatera, le libre accès à ses locaux et à son système informatique aux jours et heures ouvrés, notamment dans le cadre de la télémaintenance et des interventions sur Site ;
- S'assurer de l'existence de sauvegardes récentes du logiciel et de toutes les données du Client, préalablement à toute intervention d'OPERIS ou de tout tiers qu'il se substituera, et le cas échéant, procéder à ces opérations de sauvegarde avant toute Prestation de Maintenance ;
- Prendre toutes les mesures nécessaires afin de permettre un bon déroulement de l'installation des Mises à Jour et/ou Nouvelles Versions dans les conditions décrites aux présentes Conditions Générales Prestations de Maintenance du logiciel.
- Le Client autorise expressément OPERIS ainsi que les membres de son groupe à se connecter sur le(les) serveur(s) du client afin de réaliser toute opération d'assistance-maintenance-installation.
- Le Client autorise expressément Operis ainsi que les membres de son groupe à transférer vers le(s) serveurs et le(s) datawarehouse(s) de son groupe toute donnée nécessaire à l'installation, l'utilisation et la maintenance des objets liés aux contrats, ainsi que la communication entre eux.

ARTICLE- 4 PRESTATION DE MAINTENANCE DU LOGICIEL

OPERIS s'engage à faire ses meilleurs efforts pour fournir au Client la Maintenance corrective et évolutive du logiciel selon les règles de l'art et l'état de la technique lors de chaque intervention.

OPERIS se réserve seule le droit d'assurer ou de faire assurer la Maintenance du logiciel. Pour toute difficulté d'utilisation du logiciel, le Client s'engage à informer en premier lieu OPERIS, et s'interdit de corriger/adapter ou de faire corriger/adapter le logiciel par un tiers.

Les Mises à Jour et Nouvelles Versions sont livrées en un (1) seul exemplaire par OPERIS, à charge au Client d'en effectuer une (1) copie de sauvegarde.

ARTICLE-5 MAINTENANCE EVOLUTIVE ET CORRECTIVE DU LOGICIEL

La maintenance du Logiciel comprend également les services de fourniture des mises à jour du Logiciel sous réserve des dispositions du présent article. La nécessité de réaliser une mise à jour est décidée unilatéralement par Operis au regard des évolutions légales et technologiques. Les mises à jour peuvent intégrer, selon les cas :

- la correction des Anomalies sous forme de patchs,
- les modifications rendues nécessaires par l'évolution des textes législatifs ou réglementaires applicables aux fonctions traitées par le Logiciel, sauf si ces modifications nécessitent une modification substantielle du Logiciel qui fera alors l'objet de notification par Operis au Client,
- l'apport d'améliorations des fonctions existantes.

Les Prestations de Maintenance corrective ne sont pas dues par OPERIS en cas :

- Anomalie qu'Operis ne peut reproduire sur la version standard en cours
- de manquement du Client à ses obligations au titre des présentes, notamment si le Logiciel a fait l'objet d'une utilisation ou modification sans l'autorisation expresse d'OPERIS ou n'est pas utilisé conformément aux recommandations ou instructions de celle-ci ;
- et plus généralement en cas de difficultés ou Erreurs de fonctionnement n'étant pas directement imputables au Logiciel.
- La fourniture d'un logiciel nouveau qui viendrait se substituer dans la gamme à un Logiciel existant, ce logiciel nouveau présentant des différences sensibles de conception et/ou de programmation et/ou de fonctionnalités ;
- les travaux rendus nécessaires sur les Adaptations ou tout développement spécifique, par l'installation de la mise à jour,
- tous travaux ou fournitures non explicitement mentionnés dans le présent contrat, y compris la formation par téléphone du personnel du Client.

ARTICLE-6 LE SUPPORT

Le support permet au Client de bénéficier pour les Erreurs de fonctionnement d'une assistance dans un premier temps par téléphone, puis dans un second temps par télémaintenance, du lundi au jeudi, sauf jours fériés, de 9 heures à 12 heures et de 14 heures à 18 heures et le vendredi sauf jour férié de 9 heures à 12 heures et de 14 heures à 17 heures.

Pour bénéficier de la télémaintenance, le Client devra se doter au préalable des éléments techniques nécessaires tels que définis dans la Documentation du Logiciel.

À compter de la réception par OPERIS du signalement d'une Erreur de fonctionnement, OPERIS s'engage à fournir :

- Pour les erreurs de fonctionnement Bloquantes, une solution de contournement dans les huit (8) jours ouvrés, et un correctif logiciel dans les quinze (15) jours ouvrés ;
- Pour les Erreurs de fonctionnement Majeures, une solution de contournement dans les quinze (15) jours ouvrés, et un correctif logiciel au plus tard dans la Mise à Jour suivante du Logiciel ;
- Pour les Erreurs de fonctionnement Mineures, un correctif logiciel dans une Mise à Jour suivante du Logiciel.

ARTICLE-7 EXECUTIONS DE PRESTATIONS DE MAINTENANCE

Les Prestations de Maintenance corrective ne sont pas dues par OPERIS en cas :

- Anomalie qu'Operis ne peut reproduire sur la version standard en cours
- de manquement du Client à ses obligations au titre des Conditions Générales et/ou Particulières de Maintenance et/ou de Licence, notamment si le Logiciel a fait l'objet d'une utilisation ou modification sans l'autorisation expresse d'OPERIS ou n'est pas utilisé conformément aux recommandations ou instructions de celle-ci ;
- d'implantation de tous logiciels, logiciels ou système d'exploitation non compatibles avec le Logiciel ;
- et plus généralement en cas de difficultés ou Erreurs de fonctionnement n'étant pas directement imputables au Logiciel
- d'utilisation par le Client d'une version antérieure à la version courante du logiciel, ou à la version précédente si la version courante est diffusée depuis moins de douze (12) mois ;
- La fourniture d'un logiciel nouveau qui viendrait se substituer dans la gamme à un Logiciel existant, ce logiciel nouveau présentant des différences sensibles de conception et/ou de programmation et/ou de fonctionnalités ;
- les travaux rendus nécessaires sur les Adaptations ou tout développement spécifique, par l'installation de la mise à jour,
- tous travaux ou fournitures non explicitement mentionnés dans le présent contrat, y compris la formation par téléphone du personnel du Client.
- et plus généralement en cas de difficultés ou Erreurs de fonctionnement n'étant pas directement imputables au logiciel.
- En pareils cas, la responsabilité d'OPERIS ne pourra pas être engagée, et toute intervention d'OPERIS, ou de tout tiers qu'elle se serait substituée, donnera lieu à une facturation spécifique pour le temps passé au tarif d'OPERIS en vigueur à la date de son intervention et pour les éventuels frais engagés.

ARTICLE-8 CONFIDENTIALITE

Pendant la durée du présent Contrat et pendant cinq (5) ans après sa cessation, chacune des Parties s'engage à conserver strictement confidentiels, les données, informations, et/ou documents de toute nature concernant l'autre Partie, à l'exclusion de ceux qui étaient notoirement et publiquement divulgués avant leur obtention et/ou réception. Les Parties considèreront comme strictement confidentiels et s'interdisent de divulguer toute information de quelque nature que ce soit, qui pourra leur être révélée lors de l'exécution du contrat. En particulier Operis s'engage à conserver secrètes toutes les informations sur le Client qui lui auront été communiquées aux fins de traitement. Le Client reconnait que le logiciel constitue le savoir-faire d'Operis. Le client s'interdit , sans autorisation préalable et écrite d'Operis, de communiquer ou révéler, de quelques manières que ce soit, tout ou partie du Solution, de la Documentation, des programmes ou autres éléments concernant le logiciel, ainsi que toute reproduction totale ou partielle. Le client s'engage également à prendre toutes les mesures nécessaires pour que le Logiciel et la Documentation ne soient pas mis à disposition de tiers et s'engage à ce que ses collaborateurs ou son personnel, respecte ces obligations. Les obligations imposées aux parties par le présent article ne s'appliquent toutefois pas aux informations dont la partie réceptrice peut prouver :

- Qu'elles étaient connues d'elle antérieurement à la date de leur communication
- Qui étaient dans le domaine public à la date de leur communication
- Qui après communication, deviendraient accessibles au public par publication ou tout autre moyen, sauf si ce fait résulte d'une faute ou d'un négligence de la part de la partie réceptrice

Chaque partie s'engage à ne laisser accès aux informations confidentielles qu'à ceux de ses dirigeants, employés, conseils, sociétés de son groupe, sous-traitants, devant y avoir accès pour la bonne exécution et sous réserve du respect par ceux-ci d'une obligation de confidentialité au moins équivalente à la présente.

ARTICLE-9 CONDITIONS FINANCIERES

Toutes prestations supplémentaires (intervention sur site : assistance/formation, installation…), non couvertes dans le contrat de maintenance, feront l'objet d'une proposition commerciale et seront facturées au Client selon les tarifs OPERIS.

Sauf indication contraire, les factures sont payables par mandat administratif dans les trente (30) jours après leur date d'émission. Tout retard de paiement fera courir, de plein droit, des intérêts de retard au taux légal en vigueur majoré de huit (8%) par mois de retard.

A chaque reconduction du contrat, les redevances forfaitaires sont révisées pour l'annuité suivant la date de fin d'un premier contrat. Si la maintenance du logiciel devait être interrompue faute de cadre contractuel pour en assurer la continuité, une redevance de rétablissement serait due par la personne publique, et calculée de la manière suivante : (R/360)*N où,

R=redevance annuelle

N= nombre de jours non couverts entre le présent contrat et l'ancien contrat.

En l'absence de cette rémunération, une mise à niveau équivalente sera calculée pour la fourniture de la première mise à jour de version

OPERIS, révisera à chaque date anniversaire du contrat, le montant de la redevance annuelle en appliquant la variation de l'indice SYNTEC; par application de la formule « R = Ro x Im / Io ». Pour les besoins de la formule, « Rm » désigne le montant de la redevance après révision, « Ro » désigne le montant de la redevance initiale, « Im » désigne le dernier indice SYNTEC connu à la date d'anniversaire du contrat et « Io » l'indice SYNTEC connu à la date de prise d'effet du contrat de maintenance et ne pourra être inférieure à 2%.

ARTICLE-10 RESPONSABILITES

Les Parties ne peuvent être tenues pour responsables de l'inexécution de leurs obligations en cas de force majeure, étant entendu que chacune des Parties s'engage à en limiter au maximum les conséquences dommageables pour l'autre.

OPERIS ne saurait en aucun cas être tenue pour responsable des éventuels préjudices indirects revendiqués, même prévisibles, et notamment de pertes de données et de marchés, de manque à gagner ou augmentation de coûts et dépenses.

L'utilisation du Logiciel, de ses Mises à Jour et Nouvelles Versions, ainsi que le traitement des données et leur sauvegarde, reste sous les seules directions, contrôle et responsabilité du Client. Il lui appartient de prendre toute mesure appropriée contre toute conséquence dommageable due à l'utilisation du Logiciel.

La responsabilité d'OPERIS envers le Client ne pourra en aucun cas excéder le montant annuel des redevances du présent contrat ou de prestation effectivement payées par le Client et à l'origine de la réclamation. Aucune action ne pourra être intentée à l'expiration d'une durée de six (6) mois après la survenance de l'événement à l'origine de l'action.

L'obligation pesant sur OPERIS est une obligation de moyens, la preuve de manquement incombant à la collectivité.

OPERIS s'efforce d'assurer la confidentialité et la sécurité des données.

OPERIS ne pourra en aucune circonstance encourir de responsabilité au titre des pertes ou dommages indirects ou imprévisibles de la collectivité ou de tiers.

OPERIS ne saurait en outre être tenu responsable de destruction des données par la collectivité ou un tiers ayant accédé au service au moyen des identifiants remis par la collectivité.

OPERIS ne pourra en aucun cas être tenu pour responsable de tout dommage en cas de préjudice causé par une interruption ou baisse de service de l'opérateur de télécommunications ou du fournisseur d'électricité. Ces cas étant considérés comme des cas de force majeure.

ARTICLE-11 RESILIATION DU CONTRAT DE MAINTENANCE

En cas de manquement par l'une des Parties à une obligation lui incombant, le contrat de Maintenance pourra être résilié de plein droit, sans qu'aucune formalité judiciaire ne soit nécessaire, trente (30) jours calendaires après une mise en demeure par lettre recommandée avec accusé de réception, restée en tout ou en partie sans effet.

En cas de résiliation qu'elle qu'en soit la cause, les sommes versées par le Client resteront acquises à OPERIS et les sommes dues lui seront versées.

La résiliation du contrat de Maintenance ne donne aucun droit au Client de faire effectuer ou d'effectuer lui-même la maintenance du logiciel.

ARTICLE-12 DISPOSITIONS DIVERSES

Les présentes Conditions Générales et les Conditions Particulières s'y rattachant constituent l'intégralité des dispositions liant les Parties quant à leurs objets.

Si une disposition est jugée nulle ou non applicable, toutes les autres dispositions resteront en vigueur.

Chacune des Parties agit en son nom et pour son compte. Aucune clause des Conditions Générales et des Conditions Particulières s'y rattachant ne pourra être interprétée comme créant entre les parties une relation de mandat, d'associés ou un lien de subordination.

Le Client ne pourra céder les présentes Conditions Générales et les Conditions Particulières s'y rattachant sans l'accord préalable et exprès d'OPERIS.

ARTICLE-13 LITIGES

Les présentes Conditions Générales et les Conditions Particulières s'y rattachant sont régies par la loi française.

A défaut d'une solution amiable dans un délai de trente (30) jours ouvrables à compter de la notification du différend par l'une des parties, tout litige de la formation, l'interprétation, l'exécution ou la résiliation des présentes Conditions Générales et Conditions Particulières s'y rattachant sera soumis aux tribunaux compétents de Nantes, y compris en cas de référé, de pluralité de défendeurs ou d'action en garantie.

CONDITIONS SPECIFIQUES RELATIVES A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Les présentes dispositions contractuelles relatives strictement à la protection des données à caractère personnel viennent compléter les conditions générales et les conditions particulières du présent contrat (ci-après le « Contrat »).

Elles s'appliquent quel que soit le type d'hébergement choisi (hébergement interne, ou confié au prestataire, ou confié à un sous-traitant ultérieur).

Les présentes Conditions ont pour objet de définir les conditions dans lesquelles le Prestataire mettra en œuvre pour le compte du Client, le traitement des données personnelles.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la règlementation applicable en matière de traitement des données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après dénommé "Règlement Général sur la Protection des Données" ou RGPD).

Dans le cadre du RGPD, le Client agit en qualité de responsable de traitement tandis que le Prestataire agit en qualité de sous-traitant.

Les termes et concepts utilisés dans ce contrat de sous-traitance des données personnelles ont la même signification que dans le RGPD.

Le Prestataire est autorisé à traiter les données à caractère personnel, pour le compte du Client et pour fournir le service suivant : la maintenance de l'application OXALIS et les traitements des données personnelles liées, et le cas échéant l'hébergement de l'application et des données.

ARTICLE 1- OBLIGATIONS DE COLLABORATION ENTRE LES PARTIES

ARTICLE 1.1 Interlocuteurs des deux parties

Dans le cadre du RGPD, une forte obligation de collaboration est nécessaire entre le Client et le Prestataire eu égard notamment au régime de responsabilité qu'il entraîne. Aussi, les Parties doivent nommer un interlocuteur privilégié au titre du Contrat et s'engage à informer l'autre Partie en cas de changement d'interlocuteur.

Cet interlocuteur privilégie peut-être le DPO ou une autre personne référente qui rendra compte au DPO.

Pour le Prestataire

Operis a désigné un Délégué à la Protection des Données en la personne de : Monsieur Damien LE ROUX, joignable sur rendez-vous au 01 69 10 00 00 ou par courriel, exclusivement dédié à la communication concernant le RGPD : dpo@operis.fr

Pour le Client

Informations à compléter par le Client

DPO (le cas échéant) : …Clarice Chalier : c.chalier@villebon-sur-yvette.fr, 01 69 93 59 00

(Compléter ci-dessus nom, prénom, adresse email et numéro de téléphone)

Interlocuteur privilégié : ……

(Compléter ci-dessus nom, prénom, adresse email et numéro de téléphone)

Personne autorisée à donner des instructions pour le compte du Client : ……

(Compléter ci-dessus nom, prénom, adresse email et numéro de téléphone)

ARTICLE 1.2 Instructions

Conformément à l'article 28 du RGPD, le Prestataire est tenu d'informer le Client de toute instruction qu'il recevrait de sa part et qui serait apparemment, et en l'état des connaissances du Prestataire, en violation du droit à la protection des données. Cette information sera délivrée sous forme écrite au Client. En cas de désaccord sur le caractère illicite ou non d'une instruction, il pourra être fait appel à la Commission Nationale de l'Informatique et des Libertés (CNIL).

ARTICLE 2 - DESCRIPTION DES TRAITEMENTS FAISANT L'OBJET DE LA SOUS-TRAITANCE

ARTICLE 2.1 Collecte de données personnelles

Les données à caractère personnel sont les informations qui permettent, de façon directe ou indirecte, d'identifier une personne physique, que celle-ci ait confié les informations la concernant dans le cadre de son activité professionnelle ou à titre privé.

Aucune donnée personnelle relevant de la catégorie « données particulières » des articles 9 ou 10 du RGPD ne sont en principe collectées.

En cas de collecte de ces données, le Client s'engage à informer le Prestataire, sans délai, de manière que celui-ci indique les procédures à mettre en œuvre et notamment au titre d'une sécurité renforcée. Un devis pourra être proposé au préalable au Client.

ARTICLE 2.2 Traitement des données personnelles

Le Sous-traitant est autorisé à traiter pour le compte du Responsable du Traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) prévus dans le Contrat.

La nature des opérations réalisées par le Prestataire, en qualité de sous-traitant, sur les données personnelles sont liées aux fonctionnalités de l'application.

Les modalités de traitement des données à caractère personnel sont liées aux prestations de maintenance pouvant être réalisées pour le compte du Client, responsable de traitement, à savoir notamment :

- les mises à jour des données dans la base du Client au titre d'un traitement se basant sur des fichiers intégrant des données à caractère personnel, transmis par le Client au Prestataire.

- l'analyse de la base de données du logiciel ou une simple consultation de ces données afin d'identifier tout dysfonctionnement éventuel signalé par ce dernier. Lors de cette opération, le Prestataire peut être amené à accéder à des données à caractère personnel ;

- l'intégration ou suppression de données de la base du Client, données qui devront être communiquées par ce dernier au Prestataire. Lors d'une telle intervention, le Prestataire peut être amené à accéder à des données à caractère personnel afin de les intégrer dans la base du Client ou de les supprimer ;

- la sauvegarde/restauration, réplication de la base de données OXALIS du Client y compris tout éventuel traitement de sécurisation portant sur cette base ;

• tout éventuel autre usage lié aux obligations de maintenance pouvant amener le Prestataire à avoir accès à des données à caractère personnel, présentes dans la base OXALIS du Client.

Les finalités du traitement des données à caractère personnel sont transmises par le Client dans le cadre des instructions écrites qu'il communique au Prestataire.

Les catégories de données traitées sont décrites dans l'Annexe au présent document.

Les modalités de traitement des données employées par le Prestataire en qualité de sous-traitant sont indiquées en Annexe au présent document.

ARTICLE 3- ENGAGEMENTS DU CLIENT

ARTICLE 3.1 Respect des obligations au titre du RGPD

Le Client garantit le Prestataire du respect de l'ensemble de ses obligations au titre du RGPD en sa qualité de responsable de traitement.

A ce titre, le Client garantit le Prestataire contre tout recours, plainte ou réclamation, d'une personne physique dont les données personnelles seraient collectées par le Client et confiées au Prestataire dans le cadre du Contrat.

En conséquence, le Client assurera à ses frais la défense du Prestataire pour toute procédure diligentée contre ce dernier aux motifs qu'une action de la part du Prestataire sur une donnée à caractère personnel porte atteinte aux droits des personnes concernées sous réserve que :

- le Prestataire notifie au Client rapidement toute assignation ou mise en demeure,
- Le Prestataire apporte à la demande raisonnable du Client toute assistance ou information et éléments utiles en sa possession.

ARTICLE 3.2 Répertoire des instructions

En tant que responsable de traitement, le Client s'engage à toujours documenter par écrit toute instruction concernant le traitement des données par le Prestataire et à informer immédiatement le Prestataire de toute erreur ou irrégularité dont il a connaissance en relation avec les mesures de protection des données ou de ses instructions.

ARTICLE 3.3 Information de collecte de données

Pour l'exécution du service objet du présent Accord, le Client s'engage à communiquer au Prestataire toutes informations nécessaires.

A ce titre, il appartient au Client de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données personnelles,(art. 13 du RGPD) ou par la suite en cas de collecte indirecte (art. 14 du RGPD) notamment en ce qui concerne les modalités de leurs droits d'accès, de rectification, de l'effacement et d'opposition, droit à la limitation du traitement et droit à la portabilité et aussi, droit de ne pas faire l'objet d'une décision individuelle automatisée.

A la demande du Client, le Prestataire pourra intervenir ou assister le Client pour permettre l'exercice des droits des personnes concernées. Ces mesures ne relevant pas des prestations prévues au présent Contrat elles seront facturées au Client selon la grille tarifaire en vigueur au moment de la réception de la demande par le Prestataire. Dans tous les cas, le Prestataire bénéficiera d'un délai de 15 jour calendaire pour exécuter ces mesures, à compter de la date de réception de la demande. Ce délai pourra être prorogé de 8 jours calendaires, selon la complexité, la période de l'année, et le nombre de demandes en cours de traitement par le Prestataire.

ARTICLE 3.4 Supervision du traitement

En qualité de responsable de traitement, le Client doit également superviser le traitement, y compris réaliser les audits et les inspections auprès du Prestataire. La personne autorisée à donner des instructions pour le compte du Client, la personne chargée d'appliquer ces instructions pour le compte du Prestataire et les Délégués à la Protection des Données responsables dont la nomination est imposée par la loi seront listés en ARTICLE 1. Dans l'hypothèse d'un changement de contact d'un responsable, la Partie cocontractante devra être notifiée du nom du nouveau contact sans délai.

ARTICLE 4 – ENGAGEMENTS DU PRESTATAIRE

ARTICLE 4.1 Respect des obligations au titre du RGPD

Dans le cadre de la réalisation des prestations prévues au Contrat, le Prestataire s'engage à :

- traiter les données uniquement selon les modalités rappelées à l'article 2.2 ci-dessus
- traiter les données conformément aux instructions documentés et écrites du Client. Cette documentation devra comprendre un détail des prestations demandées, ainsi que des informations relatives aux types de données traitées et aux traitements envisagés. Si le Prestataire considère qu'une instruction constitue une violation du RGPD, il en informe immédiatement le Client et n'exécutera ledit traitement que dans le cas où il aurait obtenu la garantie du Client du caractère licite du traitement demandé ;
- garantir la confidentialité des données à caractère personnel traitées ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
- mettre en œuvre les mesures de sécurité suivantes garantissant la bonne exécution de toute prestation portant sur des données à caractère personnel :
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes de ses systèmes et de ses services de traitement portant sur des données à caractère personnel ;
- détruire de l'ensemble de son système d'information toutes les données qui lui ont été mises à disposition par le Client pour l'exécution de la prestation, une fois la demande d'intervention terminée et validée par Client ou une fois le Contrat terminé pour quelque raison que ce soit
- tenir par écrit un registre de toutes les catégories d'activités de traitement portant sur des données à caractère personnel effectuées pour le compte du Client.

ARTICLE 4.2 Lieu du traitement des données personnelles

Tout transfert de données vers un Etat tiers ou vers une organisation internationale requiert l'accord préalable et écrit du Client et ne sera autorisé qu'à condition d'avoir rempli les conditions prévues aux articles 44 et 50 du RGPD.

Le Prestataire ne procèdera pas au transfert de données personnelles vers un pays tiers ou une organisation internationale sans avoir fourni au Client des garanties appropriées. Par garantie appropriée, on entend notamment la signature de clauses contractuelles types de protection des données, entre le Client et le sous-traitant ultérieur (tel que ce terme est défini à l'article 4.4 ci-dessous) importateur des données personnelles dans le pays tiers, et, la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

Par conséquent, en signant le présent Contrat, le Client en tant qu'exportateur de données, donne au Prestataire un mandat explicite et clair de signer, en son nom et pour son compte, les clauses contractuelles avec l'importateur de données, situé dans un Etat tiers et agissant en tant que sous-traitant ultérieur.

ARTICLE 4.3 Rectification, suspension et effacement des données

1. Le Prestataire ne peut rectifier, suspendre ou effacer les données objet du traitement que sur instruction écrite du Client. Les copies nécessaires au traitement des données, à la fourniture des services conformément au Contrat, et au respect des exigences légales, ne nécessitent pas l'accord préalable du Client.
2. En cas de demande de rectification ou d'effacement des données personnelles effectuée auprès du Prestataire par la personne concernée, le Prestataire devra transférer ladite requête au Client dans les meilleurs délais.
3. Ces deux engagements sont applicables seulement si l'hébergement des données personnelles collectées par le Client est assuré par le Prestataire.
4. Les prestations spécifiques commandées par le Client dans le cadre de ses obligations de conformité au RGPD qui nécessitent la mise en œuvre de services supplémentaires par le Prestataire, feront l'objet d'une tarification aux conditions applicables à la date de la demande.

ARTICLE 4.4 Sous-traitance ultérieure

Pour répondre à ses obligations contractuelles, le Prestataire est autorisé à solliciter les services d'une autre société. Cette société partenaire est désignée ci-après « sous-traitant ultérieur ».

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant le Client de l'exécution par l'autre sous-traitant de ses obligations.

Dans la mesure où le Prestataire peut solliciter un sous-traitant ultérieur pour le traitement ou l'utilisation des données personnelles du Client, les conditions suivantes s'appliquent :

- Le Prestataire peut faire appel à un autre sous-traitant ultérieur pour mener des activités de traitement spécifiques. Dans ce cas, le Prestataire informe le Client de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants ultérieurs par courriel ;
- Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant ultérieur et les dates du contrat de sous-traitance.
- En signant cet Accord, le Client approuve les sous-traitants ultérieurs du Prestataire ;
- Le Client dispose d'un délai maximum de sept jours à compter de la date de réception de cette information pour présenter ses objections ;
- Le sous-traitant ultérieur est tenu de respecter les obligations du présent Contrat pour le compte et selon les instructions du Client ;
- Il appartient au Prestataire de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD ;
- Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant le Client de l'exécution de ses obligations.

ARTICLE 4.5 Analyse d'impacts

En cas de besoin et notamment dans le cadre de la collecte et du traitement de données à caractère personnel relevant des article 9 et 10 du RGPD, le Prestataire pourra aider le Client pour la réalisation d'analyses d'impact relative à la protection des données. Une telle prestation sera exécutée à la suite de la validation par le Client du devis correspondant à cette prestation.

De la même manière, le Prestataire pourra aider le Client pour la réalisation de la consultation préalable de l'autorité de contrôle. Une telle prestation sera exécutée par le Prestataire à la suite de la validation par le Client du devis correspondant à cette prestation.

ARTICLE 4.6 Audit

Le Client pourra réaliser des audits, directement ou par l'intermédiaire de tout prestataire externe indépendant (non concurrent du Prestataire), afin de s'assurer du respect des obligations du Prestataire.

Dans ce cadre, le Client communiquera préalablement au Prestataire, et au plus tard 30 jours calendaires avant le démarrage de l'audit : toute demande d'opération d'audit, la date de l'audit, la période au cours de laquelle l'audit interviendra, ainsi que les noms et les références des personnes en charge de l'audit qui auront préalablement signé un accord de confidentialité.

Le Prestataire ne pourra pas refuser, sans motif légitime, l'entreprise choisie par le Client pour cet audit ou les personnes désignées pour le réaliser.

En cas de refus, le Prestataire devra le notifier sous un délai de 15 jour calendaire suivant la notification faite par le Client. A défaut d'accord sur la personne de l'auditeur, le Prestataire pourra proposer un cabinet externe.

Le Prestataire communiquera à l'auditeur toutes informations ou documents nécessaires à la réalisation de l'audit, dans le respect des politiques de sécurité et de confidentialité du Prestataire.

Le temps passé par le personnel du Prestataire, dans le cadre de la réalisation de ces audits, sera à la charge du Client. Le Prestataire sera en droit d'établir une facture au Client, selon la grille tarifaire en vigueur à la date de l'audit.

Le rapport de l'audit sera adressé gratuitement au Prestataire par les auditeurs, afin qu'il puisse formuler toute observation ou objection dans un délai de 15 jours calendaires, à partir de la date de réception, par le Prestataire, dudit rapport. Ce rapport est confidentiel et strictement réservé au Prestataire et au Client. Toutefois, dans le cadre de ses missions et pouvoirs, toute autorité de contrôle qui le souhaite dispose d'un droit d'accès et de consultation dudit rapport.

Si le rapport fait apparaître un manquement significatif aux obligations du Prestataire, ce dernier s'engage à mettre en œuvre, à ses frais, toute mesure corrective appropriée dans un délai de 3 mois. En cas de contestation du rapport d'audit par le Prestataire, le Prestataire proposera un nouvel audit par un autre cabinet de son choix.

En toute hypothèse, le Client ne pourra pas réaliser plus d'un audit du Prestataire sur une période glissante de 12 mois, sauf accord de ce dernier.

ARTICLE 4.7 Information au Client

Le Prestataire s'engage à informer le Client dans le plus rapidement possible en cas de découverte d'une violation de données à caractère personnel. Cette information pourra prendre la forme d'un email, suivi d'un courrier recommandé avec accusé de réception. Elle contiendra la description des circonstances de la violation ainsi que les informations que le Prestataire aura réunies sur celle-ci.

Le Prestataire devra fournir ses meilleurs efforts aux fins de mettre un terme à la violation observée et s'engage à assister, si nécessaire le Client afin de notifier ladite violation à l'autorité de contrôle compétente ainsi qu'à la ou aux personnes concernées.

ARTICLE 4.8 Mesures techniques et organisationnelles

Le Prestataire prendra les mesures techniques et organisationnelles adéquates permettant d'assurer un niveau de sécurité approprié au risque tel que déterminé par le Client et doit maintenir ces mesures pendant toute la durée du Contrat. Le Prestataire garantit au Client qu'il a pris les mesures techniques et organisationnelles spécifiées dans l'Annexe au présent document.

Les mesures techniques et organisationnelles doivent être conformes à l'état de l'art et aux évolutions techniques. Le Prestataire peut, par conséquent prendre des mesures alternatives adéquates. Le niveau de sécurité de ces mesures ne doit pas être en deçà de celui des mesures techniques et organisationnelles. Toute modification substantielle doit être documentée.

ARTICLE 5 Responsabilité

Les stipulations suivantes concernent les relations contractuelles entre le Prestataire et le Client. Elles ne sont pas opposables aux dispositions relatives aux droit des personnes dont les données sont traitées, régies par l'article 82(1) du RGPD.

Le Prestataire et ses représentants légaux ou ses agents, ne verront pas leur responsabilité engagée en cas de manquement mineur. Toutefois, cette exonération de responsabilité pour manquement mineur, ne s'appliquera pas en cas de violation d'une obligation contractuelle essentielle. Par obligation essentielle, les Parties entendent, l'obligation dont la mise en œuvre par le Prestataire est nécessaire à la bonne exécution des présentes conditions, notamment les obligations dont la violation compromettrait la réalisation de l'objet des présentes tel qu'il est défini dans l'article 1. Dans ce cas, l'exonération de responsabilité du Prestataire en cas de manquement mineur est exclue.

Si et dans la mesure où le Prestataire et ses représentants légaux sont reconnus responsables pour manquement mineur, leur responsabilité doit être limitée aux dommages prévisibles en cas de dommages matériels et de pertes financières. La responsabilité pour toute autre dommage notamment les dommages indirects, est exclue.

En tout état de cause, le montant de l'indemnisation à verser par le Prestataire dans le cas où sa responsabilité serait engagée, tous motifs confondus, ne pourra excéder la somme totale effectivement perçue par le Prestataire au titre du contrat de maintenance de l'application OXALIS dans l'année où est constaté l'incident.

En cas de perte ou de détérioration des données ou fichiers du Client, et si cette perte ou détérioration a été causée par le Prestataire, la responsabilité du Prestataire sera limitée à la réinstallation de la dernière sauvegarde effectuée par le Client.

Toute action judiciaire du Client introduite pour obtention de dommages et intérêts, deux années après la survenance du dommage sera prescrite. Le présent délai de prescription ne s'applique pas en cas de responsabilité délictuelle ou en cas de dommages intentionnellement causés.

ARTICLE 6 DISPOSITIONS FINALES

Si une stipulation des présentes Conditions est réputée nulle au regard d'une règle de droit ou d'une loi en vigueur, sa nullité n'affectera pas les autres stipulations. Les Parties s'engagent à remplacer la stipulation inapplicable avec une stipulation légale qui poursuivrait le même objectif que la stipulation inapplicable.

En cas de contradiction entre les présentes conditions et d'autres accords entre les Parties en particulier le contrat de maintenance de l'application OXALIS, les présentes conditions prévalent pour tous les sujets relatifs aux données personnelles.

Toute modification accessoire, avenants et ajouts aux présentes Conditions se fera par écrit.

Les présentes conditions et toutes les transactions réalisées dans le cadre de sa réalisation sont régies par la loi française et le RGPD.

En cas de différend entre les Parties, compétence exclusive est donnée aux tribunaux de Nantes, qu'il y ait ou non pluralité de défendeurs ou appel en garantie.

Fait à Villebon-sur-Yvette,

Le 11../02/ 2025 En deux exemplaires originaux,

Victor DA SILVA
Maire de Villebon-sur-Yvette

ANNEXE AUX CONDITIONS SPECIFIQUES RELATIVES A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

La présente annexe a pour objet de détailler ce qu'OPERIS s'engage à mettre en œuvre en matière :

- de mesures de sécurité
- d'outils de traçabilité des données
- de modalités de traitement des données personnelles

1 Mesures de sécurité

Les mesures de sécurité mise en place chez OPERIS sont définies dans le Plan d'Assurance Sécurité (PAS) d'OPERIS dont vous trouverez ci-dessous un extrait de ses mesures.

ADMINISTRATION

Aucun utilisateur d'Operis ne peut disposer de droits d'administration du système. L'administration et la configuration sont à la charge exclusive du personnel habilité, et s'effectuent avec les outils centralisés adéquats permettant d'en garder le contrôle. Si l'intervention ne peut se faire à distance, une intervention physique sera opérée par une personne habilitée.

L'intervention non prévue et non encadrée de tiers (en particulier extérieurs) sur les systèmes est absolument exclue.

Les droits des utilisateurs doivent être restreints selon le principe du « moindre privilège », et ils doivent être juste suffisants au regard des tâches à effectuer.

CONFIGURATION

La configuration des systèmes est durcie autant que possible :

- Les services et fonctions inutiles sont désactivées
- Sauf dérogation justifiée et validée :
- Toute fonction d'exécution automatique de programmes est désactivée
- Toute session ouverte est mise en veille automatiquement au bout d'une certaine durée d'inactivité (définie en fonction du contexte d'utilisation)

Les horloges de tous les systèmes sont synchronisées sur la même base de temps interne.

La politique de sécurité Windows est déployée à partir de l'ajout de la machine dans le domaine.

Politique en matière d'appareils mobiles et télétravail

Les informations systèmes sensibles permettant de se connecter à des ressources internes d'OPERIS sont protégées par firewall, traçabilité des accès et VPN. Les comptes sensibles sont protégés par des systèmes de connexion double facteur.

SECURITE DES RESSOURCES HUMAINES

Recrutement

Dès son recrutement, tout nouveau collaborateur d'OPERIS est informé des mesures de sécurité en place et s'engage contractuellement à les respecter.

Operis fait porter sur le contrat des salariés un engagement de confidentialité et de discrétion.

Gestion des arrivées et départs

Les responsables, épaulés par le service RH et des outils semi automatisés, ont à suivre une procédure lors de l'arrivée ou le départ de personnel. En particulier :

- L'aspect nomade de la personne recrutée via une procédure de *checkin*

- Les accès relatifs à son niveau d'habilitation dans ses missions
- Les ressources matérielles requises
- La désactivation du ou des comptes lors de sa sortie d'Operis via des alertes automatiques de *checkout*
- La remise du matériel professionnel à un responsable
- La purge éventuelle de la boite mail et de l'ordinateur

Sensibilisation et formation à la PSSI

Globalement, tout le personnel d'Operis est responsable d'une partie de la sécurité du Système d'Information, et est sensibilisé en ce sens. Le MOOC RGPD fourni par la CNIL constitue l'élément principal de sensibilisation des agents qui interagissent avec les données personnelles confiées par nos clients. Nos responsables sont également formés par un cabinet d'avocats spécialisé RGPD.

La sécurité étant l'affaire de tous, l'effort doit être constant et la sensibilisation est primordiale. Dès son embauche, tout nouveau salarié d'Operis reçoit les éléments du livret d'accueil, et doit être particulièrement vigilant sur le respect de la charte et des règles d'usage du SI. Ces règles pouvant évoluer, des réunions spécifiques aux nouveautés sont organisées en conséquence.

Chacun reçoit en complément une formation interne en fonction de son niveau d'interaction avec le SI. Les procédures d'arrivée et de départ encadrent l'intégration et la suspension d'un utilisateur du système. Ces procédures doivent prévoir les modalités d'information de la DSI par la DRH, ou le service concerné, lorsque surviennent ces événements, ou en cas d'absence prolongée de l'agent. Elles doivent également intégrer les dispositions adéquates pour les cas des personnels temporaires ou des stagiaires ou en formation.

Le manquement aux règles édictées dans la charte et les règles d'usage peuvent faire l'objet de rappel aux règles, et dans les cas les plus graves de sanctions disciplinaires en fonction de la gravité du manquement.

GESTION ET CONTROLE DES ACCES LOGIQUES

Identification

- Tout personne accédant au SI est identifiée de manière unique ou différentiable,
- Les accès administrateurs sont tracés par le système,
- Seuls les agents expérimentés peuvent avoir des droits élevés sur les serveurs,
- Les autres agents d'Operis ayant un accès ont des droits restreints,
- Les accès des agents peuvent être révoqués,
- Les comptes inutiles sont désactivés et archivés sur une durée suffisamment longue, en lien avec le rôle et le temps passé dans l'entreprise par l'employé.

Authentification

L'authentification est suffisamment forte pour respecter les préconisations de la CNIL. Un mot de passe étant personnel, pour des raisons de service ce dernier peut être modifié temporairement soit par l'agent pour le transmettre à son supérieur ou à un collègue, avec approbation du supérieur, soit modifié par un administrateur sur demande hiérarchique écrite ou de l'utilisateur lui-même (oubli de mot de passe).

Cette authentification permet d'accéder aux ressources partagées, aux serveurs d'applications, et à Internet.

Un mot de passe :

- doit être changé annuellement
- ne peut être changé plus de deux fois par jour, sauf par un administrateur

Le système verrouille le compte au bout d'un nombre trop important de connexions.

Les pratiques suivantes sont mises en place pour contrôler l'accès aux actifs :

- Les données des clients ne sont ni accessibles sans droits appropriés sur le réseau en cas de transit, ni sur les serveurs de production clients sans les accès adéquats. Les clés d'accès aux serveurs sont individuelles, révocables, identifiables dans les logs, via un processus de supervision et management des accès.
- Les droits par défaut sont minimisés, et attribués sur validation des managers ou responsables de service. Des audits d'appartenances aux groupes d'habilitation sont effectués régulièrement, à minima une fois par an.
- Une automatisation des vérifications des droits est effectuée sur les serveurs pour rapporter les droits abusifs.
- Les mots de passe des utilisateurs doivent être changés une fois par an, et respecter la politique de sécurité des mots de passe.
- Les comptes sensibles sont paramétrés en double facteur pour les accès 365. Une authentification double facteur est à l'étude pour le VPN pour ces mêmes comptes.

- Le disque C:\ des postes Operis est chiffré.
- Les supports de données (disques, clés) sont analysés et purgés avant réutilisation. Operis rappelle à ses salariés qui traitent des données, que si les données personnelles doivent transiter sur un support physique, celui-ci doit être chiffré. A défaut, les données doivent être chiffrées dans une archive avec un mot de passe fort en AES 256.

Gestion des droits d'accès (politique d'habilitation)

Un utilisateur ne doit pas pouvoir s'auto-habiliter. L'affectation d'un profil d'accès à une ressource relève exclusivement du responsable de cette ressource ou de son représentant, et via les procédures réalisées par un administrateur du système ou du responsable directement.

L'accès au SI s'effectue selon le principe du « moindre privilège » : chaque utilisateur doit être doté des privilèges minimums pour accéder aux ressources dont celui-ci a besoin afin d'effectuer les tâches qui lui incombent. Ce principe vaut aussi bien pour les logiciels métier que les partages réseau de nature bureautique.

Au travers du référentiel des utilisateurs, sont définis pour chaque profil les droits d'accès au SI global. Cela s'effectue en fonction du rôle qui lui est attribué, en fonction du ou des postes qu'il occupe et de l'organisation d'Operis.

Les responsabilités « clé » sont chacune associée à un rôle différent. Afin de prévenir toute exploitation abusive, le cumul de ces rôles par une même personne doit être proscrit.

La liste des utilisateurs du SI ayant le pouvoir de créer des comptes et d'affecter des droits à tous niveaux est strictement limitée et contrôlée.

La matérialisation informatique des profils est protégée contre toute modification abusive par le biais de serveurs d'annuaires sécurisés.

Revue des politiques d'habilitation

L'activation du compte d'accès d'un agent au SI global, et de l'authentification associée, l'habilite à utiliser au minimum les services d'infrastructure de base :

- La station de travail physique ou virtuelle qui lui est affectée
- La ressource réseau sécurisée liée à ce compte
- Les partages réseau adéquats au regard de ses fonctions
- La messagerie
- L'accès au Web
- Le « Portail Operis » et les applications qu'il met à disposition.

L'affectation d'un profil d'accès à un utilisateur pour le SI doit être validée par son responsable et par le responsable de la ressource, selon la procédure définie.

Tous les mouvements de salariés (arrivées, mutations internes ou départs) sont signalés à la DSI par la DRH ou les Directions ou Services concernés.

A l'occasion de la mutation ou du départ d'une personne, la hiérarchie d'origine doit faire procéder au retrait des droits antérieurs correspondant à l'ancienne situation de celle-ci, et vérifier son caractère effectif auprès de la DSI.

Gestion des sessions inactives

Les serveurs TSE sont relancés régulièrement pour purger la mémoire et les connexions fantômes. Les postes clients doivent être verrouillés par l'utilisateur en cas d'absence, et se verrouille d'eux-mêmes en cas d'absence prolongée et d'oubli. Il n'y a pas de système de clé ou de badge permettant un verrouillage physique.

CRYPTOGRAPHIE

Politique d'utilisation des mesures de chiffrement

Lorsque le protocole le permet, Operis active le chiffrement. Toute connexion au système est chiffrée, aussi bien pour l'administration que l'utilisation. Le stockage des fichiers lorsque nécessaire est également chiffré. Pour le FTP, le chiffrement étant optionnel, dépend de la configuration du tiers s'y connectant. Il est nécessaire de rappeler alors d'activer le support des protocoles chiffrés standards.

Gestion des certificats et des clés

Spécifiquement, les systèmes de chiffrement mis en œuvre doivent systématiquement prévoir des dispositifs de recouvrement, constamment maintenus en condition opérationnelle. Les clés de recouvrement sont conservées ou archivées de manière hautement sécurisée. Elles doivent permettre de garantir des possibilités d'accès aux fichiers chiffrés, sous le contrôle de la Direction Générale et de la DSI, même en cas d'absence ou de départ du propriétaire, en cas de nécessité absolue de service, ou d'intervention des services habilités de l'Etat (Police Judiciaire, etc.).

PROTECTION DE LA CONFIDENTIALITE DES DONNEES

Les répertoires ou espaces partagés sur le réseau doivent être chiffrés, **s'ils contribuent au stockage de fichiers sensibles**, fichiers bureautiques en particulier. Le moyen de chiffrement utilisé devra être techniquement cohérent avec ces infrastructures de stockage. A défaut d'un chiffrement natif, une archive compressée avec mot de passe sera utilisée, et le niveau de chiffrement adapté au contenu.

MESURES CONTRE LES LOGICIELS MALVEILLANTS

Les failles de sécurité connues affectant les systèmes et logiciels supportant le SI sont recherchées en permanence et corrigées dans les meilleurs délais dès lors que leur criticité est importante.

Tout système connecté au réseau d'Operis est protégé par un antivirus actif en permanence. Le pare-feu local est activé. Ces dispositifs sont paramétrés de façon la plus adéquate au regard des caractéristiques du système protégé.

Operis dispose d'un EDR sur tous ses postes clients et sur ses serveurs internes.

L'anti-Malware et l'EDR peut être rajouté sur proposition commerciale sur les serveurs hébergés des clients.

Les échanges avec Internet (messagerie, web, transferts de fichiers) sont contrôlés et protégés via les systèmes de sécurité appropriés gérés par la DSI ou ses fournisseurs et mis à jour en permanence, contre les usages illégitimes, et les codes ou sites malveillants.

SECURITE DES COMMUNICATIONS

Contrôle et cloisonnement des réseaux

Le réseau d'entreprise est séparé de tout réseau public, et les différents flux examinés par les passerelles de sécurité adéquates (« pare-feu » et autres). Des mesures sont prises pour que celles-ci ne puissent pas être contournées. Toutes les dispositions raisonnables sont prises pour que leur configuration corresponde aux bonnes pratiques généralement admises, et pour que ces dispositifs ne soient ni compromis, ni altérés, ni indisponibles.

Le réseau d'entreprise est lui-même cloisonné en sous-réseaux physiques ou logiques distincts.

Les flux observés entre les réseaux doivent être conformes (en source, destination et nature) à la matrice des flux autorisés.

Les différents sous-réseaux se voient appliquer une politique et des mesures de sécurité spécifiques à leur situation, examinées en commun par le RSSI et le Responsable des Infrastructures, sous le contrôle du Directeur des Systèmes d'Information. Les dérogations au cloisonnement (pour motif technique incontournable) doivent être très strictement contrôlées. Aucun dispositif ne doit remettre en question le cloisonnement adopté, en particulier au niveau des hyperviseurs (et des machines virtuelles).

Contrôle et cloisonnement des actifs clients hébergés

Le cloisonnement dépend de l'offre du client.

- SaaS : cloisonnement à l'habilitation métier
- Mutualisé : cloisonnement à la base de données quand deux clients sont sur le même serveur
- Dédié : cloisonnement au serveur
- Sur mesure : toute mesure supplémentaire souhaitée par le client, en mode projet et à façon

Politique et procédures de transfert de l'information

Les transferts de fichiers, en particulier ceux qui sont trop volumineux pour être transférés par la messagerie, doivent être effectués via les systèmes internes gérés par la DSI ou identifié par le client ou par un partenaire. Cette disposition vaut pour les transferts inter-direction comme pour les transferts vers et depuis les partenaires extérieurs.

Aucun autre système ne doit être utilisé, en particulier externe, public, ou hébergé en dehors de l'Europe (WeTransfert, DropBox, …).

Le système est réservé à l'utilisation professionnelle. Operis demande à ses clients de chiffrer les documents contenant des données personnelles lorsqu'ils sont déposés sur le FTP d'Operis. La préconisation est de compresser en Zip avec chiffrement AES.

GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

Veille et gestion des vulnérabilités techniques

Une veille technologique spécifique doit être assurée afin de vérifier en permanence l'adéquation des solutions retenues au regard de la situation sécuritaire, et de prévoir d'éventuelles mesures correctives.

Gestion des incidents et des alertes

En premier lieu, une chaîne d'alerte et de réaction doit être mise en place et connue de tous les intervenants.

Tout incident de sécurité, toute anomalie constatée, tout problème de sécurité avéré ou soupçonné doit être signalé dans les meilleurs délais à la DSI, au minimum par le canal de l'assistance aux utilisateurs, et la synthèse de ces événements transmise au RSSI.

Gestion de crise

Pour les incidents les plus graves, et sur décision du Directeur de la DSI, une cellule de crise doit pouvoir être réunie.

Toutes mesures conservatoires doivent être prises pour éviter une éventuelle propagation de l'incident ou de l'atteinte au reste du SI, en particulier par l'isolement des locaux, dispositifs ou systèmes impliqués. En fonction de la nature de l'incident, les actions et moyens prévus pour le régler sont mis en œuvre

2 Outils de traçabilité des données

Classification de l'information

Les données hébergées par Operis pour ses clients sont qualifiées de « notables » selon la classification de notre PSSI. Toute perte d'intégrité est à signaler par les clients, sachant que les bases clients sont sauvegardées tous les jours. Les accès sont limités aux membres du service support et exploitation, et sur dérogation au service réalisation. Les accès sont tracés.

Traçabilité des accès

Les accès sont tracés par application. L'accès aux traces est limité aux utilisateurs habilités à les consulter, et lui-même tracé :

- Les droits par défaut sont minimisés, et attribués sur validation des managers ou responsables de service. Des audits d'appartenances aux groupes d'habilitation sont effectués régulièrement, à minima une fois par an.
- Les accès aux serveurs sont tracés via le système de clés individuelles, et par les firewalls. Les logs d'accès sont conservés une année pour les firewalls.
- Il n'y a aucune pseudonymisation ou anonymisation lors des accès en production, ceci ne s'applique ni au métier de nos clients (sauf pour les bases de tests ou développement), ni à notre métier quand il s'agit d'intégrer ou corriger de la donnée.

Politique de journalisation des événements

Les journaux applicatifs opérés par Operis sont conservés un an. Les journaux système sont conservés en standard de l'OS. Les journaux des Firewalls des hébergeurs sont sauvegardés selon les délais prévus au contrat d'hébergement entre l'hébergeur et Operis, et selon la réglementation. Operis opère par Alsatis une conservation longue des accès en cœur de réseau.

La liste des événements ou succession d'événements à tracer ou à analyser au titre de la sécurité du SI doit être établie, précisant la nature des informations recueillies. Le cas échéant, et en fonction de la catégorie d'événements considérée, pourront être tracés aussi bien les réussites que les échecs.

Outre les phénomènes mentionnés dans la section « Supervision et surveillance du réseau » ci-dessus, cette liste devra notamment inclure :

- Les connexions au SI, et aux ressources ou machines sensibles
- Les actions affectant des droits sur le SI, en particulier des droits d'administration
- L'utilisation des comptes d'administration, en particulier à l'occasion des actions d'administration ou de mise en œuvre d'outils sensibles
- Les actions affectant des ressources critiques ou sensibles (en particulier : Données à Caractère Personnel)
- Les actions sur la configuration des systèmes, en particulier les systèmes de sécurité
- Le téléchargement d'outils et d'utilitaires pour l'administration des systèmes
- L'activité des programmes malveillants et les attaques logiques associées
- Les tentatives d'intrusion
- Les traces d'incidents de fonctionnement, en particulier pour les dispositifs de sécurité du SI
- Des accès aux comptes des personnes-clé (compte de messagerie et ressources spécifiques en particulier).

Les corrélations pertinentes au niveau des traces devront être définies et appliquées

3 Modalités des traitements des données personnelles effectués

Inventaire des traitements

Les services doivent communiquer au référent RGPD toute information adéquate sur les traitements de Données à Caractère Personnel qu'ils mettent en œuvre.

En fonction des caractéristiques du traitement dont il est informé, et en particulier des risques sur la vie privée, le référent RGPD procède à l'inscription du traitement au Registre des Traitements de Données à Caractère Personnel (DCP).

Conformité

Tout traitement de Données à Caractère Personnel doit être conforme à la Loi « Informatique et Libertés », ainsi qu'au Règlement Européen. Le référent RGPD doit procéder ou faire procéder à l'évaluation de la conformité de tout traitement dont il a connaissance, et ce en fonction des évolutions des textes réglementaires.

Finalité

Tout traitement de Données à Caractère Personnel doit avoir une finalité (raison d'être) déterminée explicite et légitime et ne doit pas être utilisé à d'autres fins.

Données à Caractère Personnel : proportionnalité

Pour tout traitement de Données à Caractère Personnel, il doit être possible de justifier à partir de ses finalités le caractère nécessaire et indispensable de chaque donnée recueillie et traitée, ainsi que leur exactitude et complétude, et le recueil de toute donnée non nécessaire doit être exclu.

Traitement de données prohibés

Sont prohibés les traitements suivants mettant en œuvre des données faisant apparaître directement ou indirectement :

- Les origines ethniques
- Les opinions politiques, philosophiques ou religieuses
- L'appartenance syndicale
- L'état de santé
- L'orientation sexuelle.

Durée de conservation

Les données à caractère personnel sont conservées pendant une durée définie, limitée et adaptée à la finalité du traitement.

Contrôle et sous-traitance des traitements

Le contrat de maintenance et d'hébergement régit les règles des traitements par Operis. Les traitements à « grande échelle » concernent les reprises de données, les extractions, les fusions de communes, les imports de données MAJIC.

Des documents d'analyse sont rédigés si la reprise de données est spécifique.

Le client est maître de la validation et du contrôle de la reprise dans les délais prévus au projet de reprise de données.

Operis ne fait pas appel à des sous-traitants pour ses actions de mise à jour ou reprise de données.

Contrôle des saisies

Dans nos applications, le responsable de traitement est responsable de la donnée saisie ou transmise à Operis. Le client a la main sur la complexité des mots de passe, et peut se rapprocher d'Operis pour durcir la politique, ou gérer des modes type SSO, LDAP/AD, France Connect.

Toute demande d'accès à la donnée par une personne non identifiée lève une alerte auprès de nos contacts Clients. Seuls les référents identifiés peuvent solliciter notre service support pour demander un accès privilégié. Ces demandes sont tracées dans l'outil de gestion du service support.

Evaluation et procédure de contrôle périodique :

Des audits sur les différents aspects évoqués précédemment sont effectués de manière régulière et par sondage. Le respect de la procédure est alors évalué. Tout manquement est remonté au responsable côté Operis, et au client en cas de fait le nécessitant. A titre d'exemple :

- Analyse de demande de réversibilité
- Analyse de demande d'accès applicatifs
- Retour d'expérience post crise et amélioration continue