SISTEC
Des solutions au cœur de votre gestion

DECLARATION ET POLITIQUE DE SECURITE ET DE CONFIDENTIALITE

Mise à jour du 02 janvier 2021

La confiance que nous portent nos clients constitue notre capital le plus important.

Le respect de la réglementation et de la confidentialité des données à caractère personnel revêt dès lors une importance essentielle pour nous.

La présente déclaration s'applique entre autres à nos sites Internet, aux services en ligne et logiciels que nous éditons à destination des collectivités et des citoyens, ainsi qu'à toutes les relations contractuelles existant entre SISTEC et ses clients, prospects, cotraitants, sous-traitants et salariés.

Réglement Général sur la Protection des Données

SOMMAIRE

RESPECT DE LA REGLEMENTATION RELATIVE A LA PROTECTION DES DONNEES PERSONNELLES

SISTEC s'engage à respecter pendant toute la durée de ses contrats, la règlementation applicable à la protection des données personnelles (ou DCP), telles que définies ci-dessous, comprenant la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et toutes ses versions ultérieures, incluant notamment le RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données applicable à partir du 25 mai 2018).

LES DONNEES PERSONNELLES, LES ROLES DE CHACUN

Données à caractère personnel, ou DCP

Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Responsable du Traitement

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Principes généraux

- Il est rappelé qu'au sens de la Réglementation Applicable et dans le cadre de l'exécution du Contrat :
  - -le Client agit en qualité de responsable du traitement de Données Personnelles ou, le cas échéant, de sous-traitant de ses clients ;
  - -SISTEC agit en qualité de sous-traitant uniquement pour le compte et sur les instructions documentées et licites du Client.
- SISTEC met à disposition du client, les registres des traitements visés par le contrat.
- Les Parties reconnaissent que la réalisation de l'objet du Contrat constitue les instructions documentées du Client (Objet, nature, finalité et durée du traitement).
- Toute instruction supplémentaire du Client devra être faite par écrit, préciser la finalité concernée et l'opération à effectuer.
- SISTEC s'engage à informer le Client par tout moyen dans un délai raisonnable à compter de la prise de connaissance par SISTEC de l'instruction si, selon elle, cette instruction constitue une violation de la Réglementation Applicable.
- Il est entendu que le Client est le seul à disposer de la maîtrise et de la connaissance, notamment de l'origine, des Données Personnelles traitées lors de l'exécution du Contrat. Le Client garantit ainsi respecter l'ensemble des obligations qui lui incombent en qualité de responsable du traitement.
- SISTEC supprimera ou restituera au Client les Données Personnelles et leurs éventuelles copies au terme du Service ou de la Prestation à moins que le droit applicable n'exige la conservation de ces Données Personnelles.
- Le Client s'engage à indiquer à SISTEC au moment de la signature du Contrat la personne à contacter pour toutes informations, communications, notifications ou demandes. À défaut d'indication par le Client, le signataire du Contrat sera considéré comme la personne à contacter.

Sous-Traitant

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

Dans le cadre de prestations telles que l'hébergement de données, le support, la maintenance de fichiers ou de systèmes, la prise de contrôle à distance, l'aide à la réalisation d'opération, la réalisation de travaux en régie pour le compte de ses clients (liste non exhaustive), SISTEC agit en tant que sous-traitant.

La collectivité agit donc dans ces cas en tant que Responsable du Traitement.

Sous-traitance:

- Conformément à l'article 28-2 du RGPD, le Client autorise SISTEC par la signature du contrat visé à faire appel à des sous-traitants pour mener les activités de traitement de Données à caractère personnelles pour le compte du Client strictement nécessaires à l'exécution du Contrat.
- SISTEC s'engage à faire appel à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à répondre aux exigences de la Réglementation Applicable.
- SISTEC s'engage à imposer à ses sous-traitants un niveau d'obligation au moins aussi équivalent en matière de protection des Données Personnelles à celui fixé dans la présente Politique de confidentialité et par la Réglementation Applicable.
  Évidemment comme l'indique l'article 28-3g du RGPD, SISTEC ou le sous-traitant doit respecter la confidentialité, et supprimer ou restituer toutes les données à l'échéance de la prestation.
- SISTEC pourra être amenée à transférer les Données Personnelles pour les stricts besoins de l'exécution du Contrat sous réserve d'en informer préalablement le Client. Dans tous les cas, SISTEC s'interdit de transférer les Données Personnelles, sans mettre en place les outils adéquats d'encadrement de ces transferts en application de l'article 46 du RGPD, en dehors :
  - de l'Union Européenne, ou
  - de l'Espace Economique Européen, ou
  - des pays reconnus comme disposant d'un niveau de sécurité adéquat par la Commission Européenne
- Cependant, si un sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, SISTEC demeure responsable devant le Client de l'exécution par ledit sous-traitant de ses obligations.
- SISTEC s'engage à faire appel uniquement à un sous-traitant :
  - établi dans un pays de l'Union Européenne ou de l'Espace Economique Européen, ou
  - établi dans un pays disposant d'un niveau de protection suffisant par décision de la Commission Européenne au regard de la Réglementation Applicable,
  - disposant des garanties appropriées en application de l'article 46 du RGPD.
- La liste des sous-traitants de SISTEC est fournie sur demande écrite du Client. SISTEC s'engage à informer le Client de tout ajout ou remplacement de sous-traitants dans les plus brefs délais
- Le Client pourra formuler ses objections par écrit dans un délai de dix (10) jours ouvrés à compter de la réception de l'information. Le Client reconnaît et accepte que l'absence d'objection dans ce délai équivaut à une acceptation de sa part du sous-traitant.

  En cas d'objection, SISTEC dispose de la possibilité de répondre au Client pour apporter des éléments de nature à lever ces objections. Si le Client maintient ses objections, les Parties s'engagent à se rencontrer et à échanger de bonne foi concernant la poursuite de leur relation.

NOS OBLIGATIONS, LA SECURITE DES DONNEES, LA CONFIDENTIALITE, LA NOTIFICATION DES VIOLATIONS DE DCP

SISTEC s'engage à prendre toutes précautions utiles afin de préserver la confidentialité et la sécurité des DCP et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés ; plus généralement SISTEC s'engage à mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les DCP contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés ; SISTEC s'engage en outre à faire respecter ces mesures par toutes les personnes amenées à traiter les DCP sous sa responsabilité (par exemple, et sans limitation, salariés, stagiaires, consultants, etc.) ;

SISTEC s'engage à :

1. ne pas concéder, louer, céder ou autrement communiquer à un tiers tout ou partie des DCP, que ce soit à titre onéreux ou gratuit ;
2. ne pas utiliser les DCP à d'autres fins que celles prévues par les termes de ses contrats et de la loi française, notamment à des fins de prospection commerciale, marketing ou autre ;
3. supprimer les DCP (ainsi que toutes leurs copies et instances) selon les fonctionnalités standards des logiciels et, en tout état de cause, à la demande du responsable du traitement ;
4. fournir à ses clients les moyens de répondre à ses obligations de responsable de traitement, et de permettre à ce dernier d'agir, dans les délais impartis, suites aux éventuelles requêtes des personnes concernées (droit d'accès, droit de rectification, droit de destruction, etc.) ;
5. informer immédiatement par écrit le responsable du traitement de toute modification ou changement le concernant pouvant avoir un impact sur le traitement des DCP ;
6. ne pas sous-traiter l'exécution des prestations à un tiers sans l'accord préalable et écrit du Responsable du Traitement. A toutes fins utiles, SISTEC utilise les services de l'hébergeur OVH sur un cloud Français;
7. en cas de sous-traitance autorisée, reporter sur son propre sous-traitant l'ensemble des obligations mises à sa charge par la présente déclaration de confidentialité au moyen de clauses contractuelles dont SISTEC peut exiger la production à première demande ;
8. ne pas transférer de DCP hors de l'Espace Economique Européen vers un pays qui n'est pas reconnu par la Commission Européenne comme disposant d'un niveau de protection suffisant, notamment en cas d'hébergement, sans l'autorisation préalable du Responsable du Traitement et sans l'en avoir averti préalablement avant la date envisagée du transfert ;
9. si SISTEC a des raisons de croire ou a acquis la conviction de l'existence d'une faille de sécurité, d'une perte ou d'une altération des DCP traitées pour le compte du Responsable du Traitement, SISTEC s'engage à :
    - notifier l'existence de cet incident au Responsable du Traitement dans les meilleurs délais,
    - s'abstenir de communiquer sur cet incident,
    - assister le Responsable du Traitement dans la mise en place des actions destinées à mettre fin à cette faille, et à réparer les éventuels dysfonctionnements que cette faille est susceptible d'avoir occasionné.
10. SISTEC notifie au Client dans les meilleurs délais après en avoir pris connaissance toute violation de la sécurité des Données Personnelles entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données Personnelles.
11. SISTEC fournit au Client dans les meilleurs délais à compter de la notification de la violation de la sécurité des Données Personnelles et dans la mesure du possible les informations suivantes :
    - les catégories et le nombre approximatif de personnes concernées par la violation ;
    - les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
    - la description des conséquences probables de la violation de données à caractère personnel ;
    - la description des mesures prises ou que SISTEC propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

COLLECTE DE DONNEES DEPUIS LES SITES ET SERVICES HEBERGES

La visite de notre site internet ou de nos services hébergés, la création de comptes ou l'abonnement à nos publications impliquent une approbation expresse de l'internaute au moyen de procédures d'inscription claires.

Les sites internet et services hébergés collectent en outre automatiquement des informations anonymes concernant l'utilisation faites du site web et des services de SISTEC. Ainsi, nous enregistrons automatiquement quelles parties du site web, de la Plateforme et/ou de l'Appli est visitée, quel navigateur web est utilisé, quel site web était visité avant d'accéder à notre site web, ainsi que l'adresse IP du terminal connecté.

Il ne nous est pas possible d'identifier un individu sur la base de ces données, mais celles-ci permettent à SISTEC d'établir des statistiques concernant l'utilisation de ses sites internet et services hébergés, ainsi que proposer des contenus et informations pertinentes aux visiteurs.

Les sites internet que nous éditons utilisent des cookies.

Ces fichiers stockés sur l'ordinateur des internautes nous servent à faciliter l'accès aux services que nous proposons et à personnaliser les contenus proposés afin d'améliorer l'expérience utilisateur. Les cookies de nos sites ne contiennent pas de données permettant d'identifier personnellement les visiteurs, et ils ne sont utilisés que pour la bonne marche des services en ligne.

Chaque internaute peut s'opposer à l'enregistrement de ces "cookies" en configurant son ordinateur.

L'ensemble des DCP recueillies par l'intermédiaire de nos sites internet, le sont par le remplissage d'un formulaire par l'internaute après avoir pris connaissance et avoir donné son autorisation sur le traitement de ses DCP.

TYPES ET COLLECTE DES DONNEES A CARACTERE PERSONNEL

Mode de collecte des données à caractère personnel

Les données à caractère personnel sont collectées par la collectivité en tant que responsable de traitement pour tout ce qui concerne les logiciels, hébergés ou non.

Elles sont collectées par SISTEC, en tant que Responsable de Traitement, pour tout ce qui concerne l'utilisation de certains services en ligne par les citoyens, ou l'utilisation de nos sites internet par les internautes.

Ces DCP sont collectées à l'occasion de :

- La visite sur nos sites internet (uniquement si l'internaute s'identifie de lui-même en complétant un formulaire)
- La création d'un compte
- L'utilisation de services hébergés au moyen de la plateforme
- La communication à SISTEC d'idées concernant l'amélioration des services, de la plateforme des logiciels
- La correspondance échangée avec et émanant de SISTEC

- L'abonnement à une newsletter
- La demande d'une offre, de brochures, d'informations ou d'une présentation commerciale
- La fourniture de données lors de salons et évènements
- L'inscription à une session de formation en ligne ou d'un webinaire
- L'inscription à l'un de nos extranets de support

L'Utilisation des données à caractère personnel

SISTEC peut être amené à utiliser les DCP collectées pour :

- La création d'un compte et la confirmation de cette création
- L'exécution d'une convention conclue avec SISTEC
- La fourniture de services
- La fourniture d'un support
- L'envoi de communications ciblées sur la base des préférences sélectionnées par l'usager
- L'envoi de factures et le recouvrement de paiements
- L'optimisation de la qualité, la gestion et le contenu du site web, de la plateforme d'hébergement et des logiciels
- À des fins statistiques
- L'élaboration d'une offre
- La réalisation d'études et d'enquêtes de satisfaction clients

Liste et types de données gérables dans nos logiciels et solutions

A des fins d'accompagnement et de simplification du travail de ses clients Responsables de Traitement, SISTEC met à disposition les « Registre de traitement », recensant l'ensemble des données personnelles pouvant être recueillies par les logiciels qu'elle édite.

Ces registres sont disponibles pour tous les logiciels qui gèrent des données à caractère personnel, ils sont récupérables à partir du logiciel concerné ou sur simple demande à adresser par email à dpo@jvs.fr.

Les données stockées, gérées et traitées par nos clients Responsables de Traitement, au moyen des logiciels que SISTEC édite et fournit en tant que Sous-Traitant ne sont en aucun cas exploitées par SISTEC pour quelque traitement que ce soit.

LA DIVULGATION DE DONNEES A CARACTERE PERSONNEL A DES TIERS

SISTEC ne divulgue pas de DCP à des tiers, sauf lorsque cela s'avère nécessaire dans le cadre de la fourniture de services et de leur optimisation (exemples non exhaustifs : Fourniture de listes de références, Déclarations de traitements aux autorités pour des opérations de télétransmission, la mise en œuvre de systèmes de connexion tels que France Connect, …) par ses éventuels sous-traitants. S'il est nécessaire que, dans ce cadre, SISTEC divulgue des données à caractère personnel à des tiers, la tierce partie concernée sera tenue de les utiliser conformément aux dispositions de la présente Déclaration de Confidentialité.

Dans ces cas, aucune divulgation de DCP ne sera exécutée sans que SISTEC n'ait obtenu un accord explicite de la part des propriétaires de ces données.

Il est également possible que SISTEC divulgue des DCP aux autorités compétentes lorsqu'elle y est tenue sur

la base de la loi ou dans le cadre d'une procédure judiciaire ou d'une procédure judiciaire future et pour garantir et défendre ses droits.

Dans tous les autres cas, SISTEC s'abstiendra de vendre, louer ou transmettre les DCP à des tiers, sauf quand elle a obtenu une autorisation explicite à cet égard et a conclu avec la tierce partie concernée un contrat de traitement de données, lequel contient les garanties nécessaires en matière de confidentialité et de protection de la vie privée.

STOCKAGE DES DONNEES A CARACTERE PERSONNEL

Sauf quand un plus long délai de conservation est requis ou justifié par le respect d'une obligation légale, SISTEC ne conserve les DCP collectées que pendant la période qui est nécessaire pour atteindre et remplir les objectifs tels que décrits dans la Déclaration de Confidentialité, sous le point « Types et collecte des données à caractère personnel ».

PROTECTION DES DONNEES A CARACTERE PERSONNEL

SISTEC s'engage à prendre les mesures de précaution raisonnables, physiques, technologiques et organisationnelles pour éviter l'accès non autorisé aux DCP stockées, ainsi que la perte, l'abus ou la modification de ces DCP.

SISTEC conservera son système d'information local ainsi que toutes les DCP collectées dans le cloud avec un (des) centre(s) d'hébergement de données situé(s) en France. Ainsi que sur son système d'information local.

Nonobstant la politique de sécurité de SISTEC, les contrôles qu'elle effectue et les actes qu'elle pose dans ce cadre, il ne peut être garanti un niveau infaillible de sécurité. Aucune méthode de transfert ou de transmission par le biais de l'Internet, ni aucune méthode de stockage électronique ne sont sûres à 100 %, de sorte que SISTEC ne peut, dans ce cadre, garantir une sécurité absolue.

La sécurité des comptes créés dépendra également de la confidentialité et du niveau de sécurité des mots de passe utilisés pour accéder à la Plateforme et/ou aux applications. SISTEC ne demandera ni ne communiquera jamais un mot de passe, l'usager est donc tenu de ne pas le communiquer lui-même. Lorsque le mot de passe a néanmoins été communiqué à un tiers - par ex. parce que ce tiers a indiqué qu'il offrait des services complémentaires - ce tiers recevra l'accès, par le biais du mot de passe, au compte et aux DCP qu'il contient. Dans ce cas, l'usager assume lui-même la responsabilité des agissements impliqués par l'utilisation qui est faite de son compte.

SISTEC conseille dès lors vivement, lorsqu'il est constaté qu'un tiers a obtenu l'accès au compte, d'en modifier immédiatement le mot de passe.

COOPERATION AVEC LE CLIENT

SISTEC s'engage à communiquer au Client dans les meilleurs délais après réception, toute demande, requête ou plainte qui lui serait adressée par toute personne physique concernée par le traitement de ses Données Personnelles réalisé dans le cadre du Contrat.

En qualité de responsable du traitement, le Client reste responsable de la réponse à apporter aux personnes physiques concernées et SISTEC s'engage à ne pas répondre à de telles demandes. Cependant, compte tenu de la nature du traitement de Données Personnelles, SISTEC s'engage, par des mesures techniques et

organisationnelles appropriées et dans toute la mesure du possible, à aider le Client à s'acquitter de son obligation de donner suite à de telles sollicitations.

Sur demande écrite du Client, SISTEC fournit au Client, aux frais de ce dernier, toute information utile en sa possession afin de l'aider à satisfaire aux exigences de la Règlementation Applicable qui incombent au Client en qualité de responsable du traitement concernant les analyses d'impact relatives à la protection des Données Personnelles menées par et sous la seule responsabilité du Client ainsi que les consultations préalables auprès de la CNIL qui pourraient en découler.

AUDITS

Sous réserve d'un préavis d'un mois envoyé par lettre recommandée avec avis de réception, le Client peut procéder sous sa responsabilité à un audit portant sur le respect par le Sous-Traitant des obligations prévus en matière de sous-traitance au titre des Règlementations Informatique et Libertés. L'audit est réalisé aux frais du Client et pendant les heures habituelles d'ouverture du Sous-Traitant sans que cela ne perturbe les activités et l'organisation quotidienne du Sous-Traitant et que le cabinet d'audit soit approuvé par le Sous-Traitant et reconnu comme auditeur indépendant de l'organisation de chacune des parties.

L'audit ne peut avoir lieu plus d'une fois par année à moins que celui-ci ne soit exigé par une Autorité de Contrôle. Le Client doit communiquer au Sous-Traitant au moins 1 mois avant la date de début de réalisation de l'audit prévu la liste des questions et points devant être audités. Avant de débuter l'audit, le client et le Sous-Traitant devront s'accorder sur l'étendue, le calendrier et la durée de l'audit.

En tout état de cause, le Client s'engage à rembourser le Sous-Traitant pour le temps qu'il a consacré à l'audit.

L'audit doit donner lieu à un rapport d'audit, dont une copie devra est remise au Sous-Traitant pour que ce dernier puisse émettre ses observations et réponses ou pour qu'il puisse discuter avec le Client, si besoin, de l'éventuel plan de correction qui serait décidé d'un commun accord, le cas échéant.

SECURITE ET CONFIDENTIALITE DES DONNEES HEBERGEES PAR LE CLIENT

Les données des logiciels SISTEC dits CLIENT / SERVEUR sont hébergées par le client. Ces logiciels utilisent un système de gestion de bases de données relationnelles dont les accès sont sécurisés.

SISTEC propose des sauvegardes manuelles tous les 7 jours et la mise en place d'une sauvegarde automatisée sur 7 jours.

SISTEC n'est pas responsable de la sécurisation de ces sauvegardes ni des infrastructures mise en place par le client pour les accès à distance aux logiciels.

SECURITE ET CONFIDENTIALITE DES DONNEES HEBERGEES ET DES APPLICATIONS DITES FULLWEB

SISTEC héberge l'ensemble des applications fullweb et des données sur un cloud souverain sécurisé.

La conception, la fourniture, la maintenance, la sécurisation et le maintien en condition opérationnelle de cette plateforme est assurée par SISTEC. Le fournisseur d'infrastructures et hébergeur la Société OVH.

Les rôles et responsabilités de chacun

Le matériel mis à disposition reste la propriété de l'hébergeur.

Les serveurs mis à la disposition peuvent être différents et les configurations hardware et software peuvent évoluer.

Le cloud est constitué de plusieurs serveurs pouvant héberger différents clients. L'accès physique aux serveurs est interdit à toute personne étrangère à l'hébergeur.

Le client ne pourra prétendre à des droits d'administrateur sur le serveur loué. Il n'aura pas la possibilité d'installer par lui-même des applications ou logiciels tiers sur le serveur. Ces installations devront obligatoirement être réalisées par SISTEC ou ses sous-traitants, et donc seront sous son entière responsabilité. Le client ne pourra alors être tenu pour responsable d'un défaut de fonctionnement du serveur consécutif à ces installations.

Le client est responsable des données contenues et accessibles sur les systèmes hébergés.
Le client supportera seul les conséquences du défaut de fonctionnement du serveur consécutif à toute utilisation illicite, par toute personne à laquelle le client aura fourni ses identifiants d'accès, y compris les membres de son personnel. De même, le client supportera seul les conséquences de la perte du ou des mots de passe précités.

Engagements sur la sécurité et la réversibilité

SISTEC s'engage à apporter tout le soin et la diligence nécessaires à la fourniture d'un service de qualité conformément aux usages de la profession et à l'état de l'art.

SISTEC s'engage à restituer les données dans le format et suivant le délai défini dans la clause de réversibilité du contrat Client.

Eléments de sécurité

- Les serveurs CLOUD sont hébergés en France métropolitaine ;
- L'accès des personnes physiques aux serveurs n'est confié qu'aux personnels de l'hébergeur ;
- Le matériel mis à disposition reste la propriété de l'hébergeur ;
- La sécurité du CLOUD est assurée par les éléments suivants :
    - la protection contre tous les types d'attaques de déni de service disponible en standard sur l'offre souscrite auprès de l'hébergeur,
    - les montées de version des différents composants comme les systèmes d'exploitation par exemple,
    - la sauvegarde des données et la reprise d'activité (voir paragraphe suivant),
    - le « load balancing » applicatif permettant un équilibrage de charge en temps réel,
    - le cloisonnement des ressources permettant la bonne isolation des données hébergées,
    - la traçabilité des accès utilisateurs y compris les administrateurs,

Sécurisation de l'Accès au cloud et aux données

Concernant les échanges d'informations entre le poste client et l'application hébergée, il est à noter que toutes les communications sont cryptées, par l'intermédiaire d'un certificat SSL/TLS, et utilisent le protocole standard HTTPS (port 443).

Chaque accès aux logiciels est conditionné par la fourniture d'un compte utilisateur et d'un mot de passe.

Chaque utilisateur déclaré dans la base d'autorisation est soumis à l'application de préférences et de droits librement fixés par le gestionnaire des utilisateurs : Le client.

La sauvegarde des données

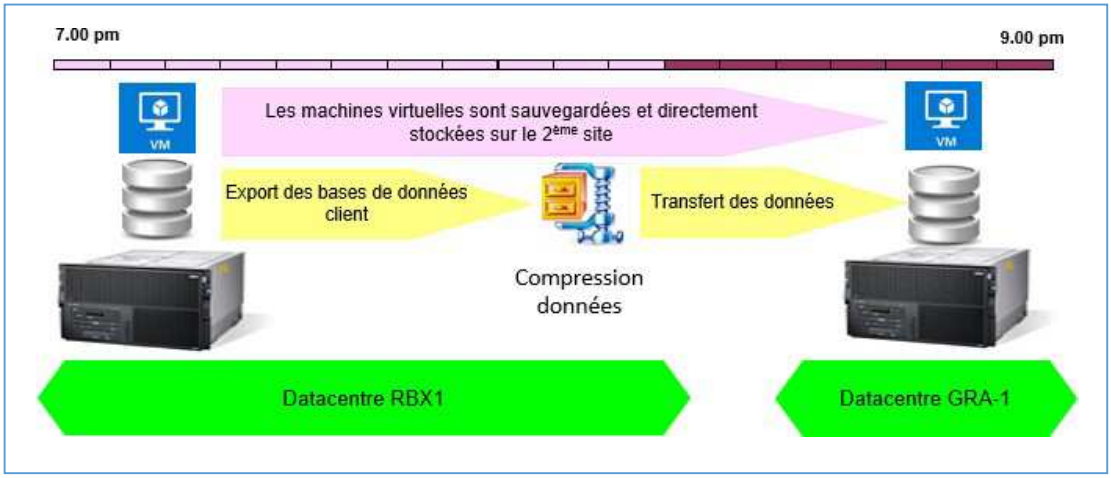
En standard, toutes les données sont sauvegardées quotidiennement vers un site géographiquement différent du site de production. Notre politique de sauvegarde permet de récupérer les données sur une période de 7 jours. SISTEC sous traite l'externalisation de ses données auprès de la société ARXONE.

En cas d'incident, SISTEC s'engage à :

- une perte de données (RPO) maximale de 8 heures ouvrées en fonction de l'apparition d'un incident,
- une période d'indisponibilité de remise en place de l'application (RTO) maximale de 8 heures ouvrées.

Les sauvegardes des données utilisateurs sont sous la responsabilité de SISTEC et se déroulent de la façon suivante :

- Les données contenues dans la base de données sont exportées et sauvegardées chaque soir ;
- Les mécanismes internes de protection des données de la base de données ont été activés afin de garantir la cohérence de celles-ci ;
- Les sauvegardes de données sont enfin externalisées à travers un agent et transférées dans un autre centre de données. Lors du processus de sauvegarde, les données sont compressées puis chiffrées.



PROCESSUS DE SAUVEGARDE

Une politique de rotation des sauvegardes est mise en œuvre. Elle est différente suivant les besoins du client.

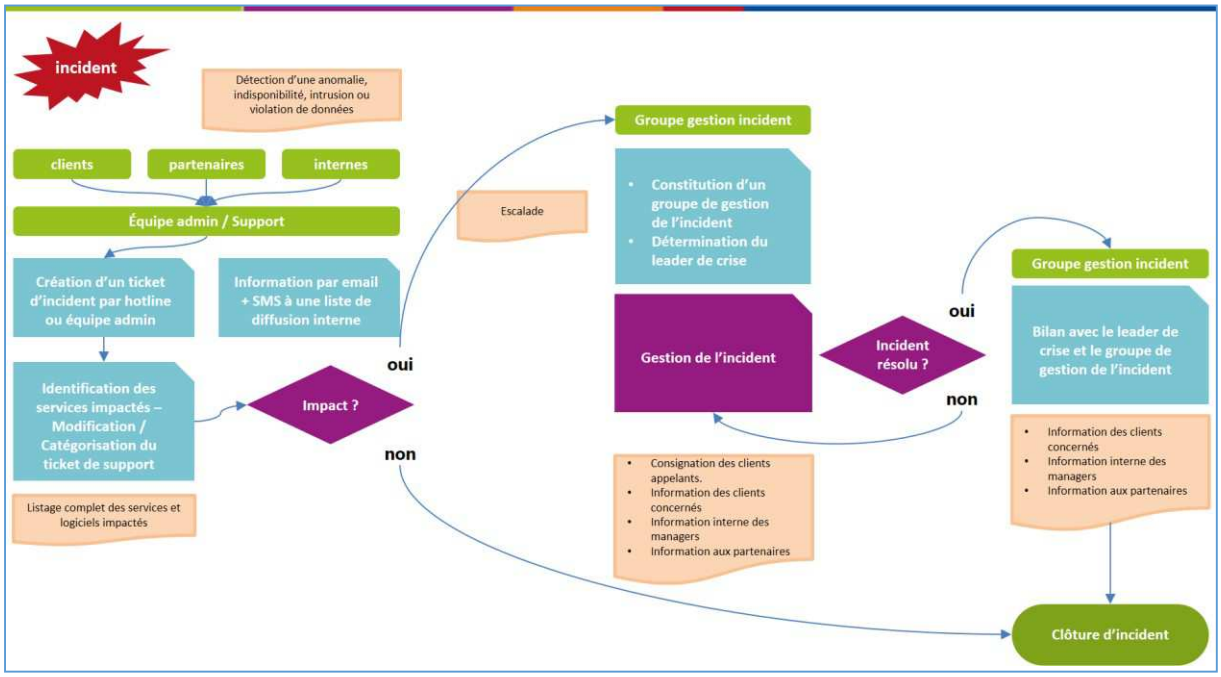
7 versions de sauvegarde sont enregistrées et disponibles. Les sauvegardes sont réalisées quotidiennement et peuvent être de type « complètes » ou « incrémentales ».

Un système d'alerte par email est mis en place et complété par une console de supervision accessible depuis un simple navigateur permettant ainsi la visualisation des anomalies.

Le taux de disponibilité de la plateforme de sauvegarde est de 99,98%.

PROCESSUS DE GESTION DE CRISE

Un Processus de Gestion de crise est appliqué dès qu'un incident est constaté. Ces incidents peuvent être déclarés par chacune des personnes de SISTEC, partenaires, sous-traitants ou toute personne utilisatrices de la plateforme.



Le processus tient compte des éléments suivants :

- détection d'incident ou d'indisponibilité d'un service ou d'une application,
- déclaration des incidents ou violation de données par le biais de l'outil de signalement, téléphone, mail, fax,
- Vous pensez être victime d'une cyber malveillance, envoyez un mail à cybermalveillance@jvs.fr.
- communication auprès des partenaires et managers de SISTEC,
- Analyse de l'incident pouvant aboutir à une violation de données à caractère personnel et dans ce cas à une déclaration de violation de données à l'autorité de contrôle. Dans ce cas le processus suivant est engagé :
    - prise en compte de l'escalade Niveau 1, 2 ou 3 en fonction du temps et des niveaux d'impacts,
    - consignation de la liste des clients impactés,
    - communication régulière de l'évolution auprès des clients consignés jusqu'à la clôture de l'incident.

En fonction des impacts et de la durée de la rupture d'activité, une information générale est faite à l'issue de la clôture auprès des clients consignés, des partenaires et managers de SISTEC.

ACTUALISATION DE LA DECLARATION DE CONFIDENTIALITE

SISTEC peut actualiser la présente Déclaration de Confidentialité en proposant une nouvelle version sur son site internet, site extranet ou au sein des documents fournis avec les applications.

Dans ce cadre, il est particulièrement indiqué de consulter régulièrement ces supports et les pages concernées sur lesquelles la Déclaration de Confidentialité est reproduite.

Autres sites web

Les sites internet édités par SISTEC peuvent éventuellement contenir des hyperliens vers d'autres sites internet. En aucun cas SISTEC n'est responsable de la politique de confidentialité ou des pratiques relatives à la vie privée d'une quelconque tierce partie.

RECLAMATIONS ET QUESTIONS

Si vous avez des réclamations concernant la manière dont SISTEC collecte, utilise et/ou traite les données à caractère personnel, ou si vous avez simplement des questions sur cette Déclaration de Confidentialité, veuillez nous contacter par email à l'adresse : dpo@jvs.fr