NORMES DE CONFORMITE

Madame, Monsieur,

Accenture s'engage depuis toujours à gérer ses relations commerciales de manière responsable. Cet engagement d'agir conformément aux normes éthiques les plus exigeantes s'inscrit dans ses valeurs fondamentales.

L'intégrité et la conformité aux lois constituent des conditions déterminantes pour Accenture dans la conduite de ses affaires. Dans ce contexte, Accenture vous a sélectionné en qualité de fournisseur/prestataire ce qui suppose que vous garantissiez le strict respect de l'éthique et la conformité aux réglementations en vigueur. En acceptant de livrer des biens et/ou de fournir des services (les « **Offres du Prestataire** » à Accenture dans le cadre de la Commande:

- ✓ Vous adhérez aux « Supplier Standards of Conduct » (https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-58/accenture-supplier-standards-of-conduct-final-french.pdf#zoom=50)
- ✓ Vous déclarez être conforme aux garanties listées par l'Annexe Anti-Corruption ;
- ✓ Vous déclarez être conforme aux exigences techniques et opérationnelles propres à la sécurité selon les modalités définies à l'Annexe Exigences en matière de Sécurité des Informations ;
- ✓ Vous déclarez être conforme engagements relatifs aux données personnelles définis à l'Annexe relative à la Protection des Données et aux Clauses Contractuelles Types dans la plus récente version approuvée par le CE, Option 1.

Vous serez identifié ci-dessous comme étant le Prestataire.

1. DETERMINATION DES PARTIES CONTRACTANTES.

Accenture, client, est entendu d'Accenture S.A.S.U., Société par Actions Simplifié à associé Unique (SASU) / RCS Paris 732 075 312 / Capital: 17,250,911.00 EUR, ayant son siège social sis au 118-122 avenue de France, 75013 Paris, France ou de toute entité du groupe Accenture dument identifiée dans le document contractuel.

Vous êtes identifié ci-dessous comme étant le Prestataire, société qui est identifiée dans le Bon de Commande ou « PO ».

2. ETHIQUE.

Chaque Partie respecte les lois, ordonnances et règlements applicables en particulier les réglementations relatives à la lutte contre la corruption, à la concurrence, et à la conformité des exportations. Le Prestataire ne commettra pas et ne mettra jamais Accenture ou l'un de ses clients dans la situation de commettre une infraction auxdites réglementations.

Le Prestataire déclare être conforme avec les garanties, déclarations et engagements définis dans l'Annexe Anti-Corruption.

Registres et Audit : Pendant toute la durée des relations commerciales entretenues avec Accenture et pendant les trente-six (36) mois suivant, le Prestataire conservera et, sous réserve d'un préavis raisonnable, fournira à Accenture ou à un tiers désigné par lui, l'accès nécessaire à l'audit de ses livres, comptes et registres relatifs aux Offres du Prestataire exécutés par le Prestataire et aux paiements associés. Tout tiers désigné par Accenture sera tenu d'accepter un accord de confidentialité/de non-divulgation approprié. Le Prestataire coopérera de bonne foi à toute audit effectué par ou pour le compte d'Accenture ou d'un de ses clients.
Si vous n'agréez pas les garanties, déclarations et engagements de l'Annexe Anti-corruption, merci de l'indiquer avant le début des prestations à procurement.support@accenture.com ou à votre contact Accenture (identifié dans la Commande).

3. SECURITE DE L'INFORMATION.

Dans le cas où vous fournissez à Accenture, une prestation ou des fournitures impliquant :

- ✓ un transfert, le stockage, ou un traitement de données personnelles au sens des lois informatiques et libertés ;
- ✓ un transfert, le stockage, ou un traitement de données sensibles d'Accenture ou de l'un de ses clients ;
- ✓ la fourniture de biens ou d'équipements liés aux nouvelles technologies ;

vous vous engagez à respecter les exigences techniques et opérationnelles propres à la sécurité selon les modalités définies en Annexe Exigences en matière de sécurité des Informations qui sont essentielles et déterminante de l'engagement d'Accenture.

Si vous n'agréez pas les modalités propres à la sécurité définies aux présentes, merci de l'indiquer avant le début des prestations à procurement.support@accenture.com ou à votre contact Accenture (identifie dans la Commande).

4. DONNEES PERSONNELLES

Le Prestataire et Accenture s'engagent à respecter les dispositions de la loi « Informatique et libertés » n° 78-17 du 6 janvier 1978 ainsi que du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (le « **Règlement Général de Protection des Données** »), dès lors qu'ils seront amenés à traiter des « Données à caractère Personnel » au sens desdites normes dans le cadre de l'exécution du Contrat. Le Prestataire s'engage essentiellement sur un traitement des Données Accenture dans le respect d'une finalité déterminée et légitime, d'une collecte loyale et licite, et de données pertinentes et non excessives. Les engagements réciproques des Parties à cet égard sont décrits à l'Annexe relative à la protection des Données.

Le Prestataire est informé qu'Accenture met en œuvre un traitement de données à caractère personnel pour gérer ses relations avec ses prestataires. Les données collectées sont indispensables à cette gestion et seront analysées, traitées et transmises aux services intéressés d'Accenture.
Ces données peuvent faire l'objet, pour communication ou réalisation d'opérations d'un transfert à destination des sociétés du groupe Accenture, leurs sous-traitants ou prestataires établis dans des pays bénéficiant ou pas, selon le cas, d'un niveau de protection adéquat. Des règles internes visant à organiser les flux transfrontières de données à caractère personnel intra-groupe et des conventions visant à encadrer les transferts de telles données vers des sociétés tierces ont été élaborées afin de garantir un niveau de protection adéquat.

Le droit d'information et d'accès des salariés du Prestataire peut s'exercer par courrier postal auprès de l'interlocuteur Procurement 118 avenue de France 75013 Paris, accompagné d'une copie d'un titre d'identité ou par courrier électronique auprès du Data Privacy Officer d'Accenture à l'adresse suivante : dataprivacy@accenture.com.
Il appartient au Prestataire d'en informer ses salariés.

LES DOCUMENTS À FOURNIR PAR LE SERVICE PRESTATAIRE/FOURNISSEUR/CONTRACTANT CONCERNANT LES LOIS RELATIVES AU TRAVAIL ILLÉGAL

L'ensemble de ces documents et déclarations doivent être rédigés en français ou **accompagnés d'une traduction en français.**

Les déclarations sous l'honneur et documents communiqués au moment de la signature du contrat de sous-traitance doivent être renouvelés tous les six mois jusqu'à l'achèvement de l'exécution du contrat.

Merci de lire attentivement les remarques suivantes qui vous rappellent vos obligations légales et contractuelles à l'égard d'Accenture.

Accenture a désigné PROVIGIS pour collecter les documents suivants.
Merci de remplir votre profil fournisseur sur le site :
http://www.provigis.com

Merci de télécharger les documents requis sans oublier les « documents spécifiques » requis.

NORMES DE CONFORMITÉ ET D'ÉTHIQUE DES FOURNISSEURS D'ACCENTURE - France (Revu Janvier 2024)

PRESTATAIRE/FOURNISSEUR/CONTRACTANT ÉTABLI EN FRANCE (ARTICLE D 8222-5 DU CODE DU TRAVAIL ET ARTICLE D 243-15 DU CODE DE SÉCURITÉ SOCIALE)

1. Une attestation de fourniture des déclarations sociales et de paiement des cotisations et contributions sociales fixées en vertu de l'article L243-15 du code de sécurité social émanant de l'URSSAF et datant de moins de six mois.
2. Un extrait de l'inscription au registre du commerce et des sociétés (Kbis).
3. Une attestation d'assurance professionnelle.
4. En cas de recours à des salariés étrangers soumis à une autorisation de travail (Article D8254-2 du Code du Travail) : une liste nominative précisant, pour chaque salarié, sa date d'embauche, sa nationalité et le type et le numéro d'ordre du titre valant autorisation de travail ("Liste nominative des travailleurs étrangers").

PRESTATAIRE /FOURNISSEUR/CONTRACTANT ÉTABLI OU DOMICILIÉ À l'ÉTRANGER (ARTICLE D 8222-7 ET 8254-1 ET SUIV. DU CODE DU TRAVAIL):

1. Un document mentionnant le numéro de TVA intracommunautaire ou, si le pays d'établissement n'appartient pas à l'Union Européenne, un document mentionnant les coordonnées de son représentant fiscal en France.

2. a) Un document attestant de la régularité de la situation sociale au regard du règlement (CE) n° 883/2004 du 29 avril 2004 ou d'une convention internationale de sécurité sociale Il peut s'agir d'attestations de travail temporaire à l'étranger appelés « E101 ou A1 ».
   Et, si les lois du pays de domiciliation le requièrent, un document émanant de l'organisme de protection sociale chargé du recouvrement des cotisations et des contributions sociales et mentionnant que votre entreprise est à jour de ses déclarations sociales et de paiement des cotisations et contributions sociales, ou tout document équivalent.
   b) En l'absence des documents visés au point 2 a) ci-dessus, une attestation de fourniture de déclarations sociales et de paiement des cotisations et contributions sociales fixées en vertu de l'article L243-15 du code de sécurité social émanant de l'URSSAF.

3. Lorsque l'immatriculation du cocontractant à un registre professionnel est obligatoire dans le pays d'établissement ou de domiciliation, un document émanant des autorités tenant le registre professionnel ou un document équivalent certifiant cette inscription.

4. Une attestation d'assurance professionnelle.

5. Lorsque des salariés étrangers sont employés sur le site d'Accenture, et soumis à une autorisation de travail (Article D8254-2 du Code du Travail): une liste nominative précisant, pour chaque salarié, sa date d'embauche, sa nationalité et le type et le numéro d'ordre du titre valant autorisation de travail. Cette liste doit obligatoirement être remplie si, au cours de l'exécution sur site, le sous-traitant décide d'employer du personnel étranger qui n'était pas prévu à l'origine et qui est soumis à une autorisation de travail.

6. Lorsque des salariés étrangers sont employés sur le site d'Accenture (travailleur détaché) : une copie de la déclaration de détachement de travailleurs en France (cerfa 13816-02)
   https://entreprendre.service-public.fr/vosdroits/R42380
   Copie du mandat de représentation du fournisseur en France (cerfa 13816-02)
   Pour plus d'informations :
   https://travail-emploi.gouv.fr/droit-du-travail/detachement-des-salaries-posting-of-employees/detachement-des-salaries/article/donneurs-d-ordre-maitres-d-ouvrage-en-france-vos-obligations
   et le guide rédigé à l'attention des prestataires de services étrangers :
   https://travail-emploi.gouv.fr/droit-du-travail/detachement-des-salaries-posting-of-employees/detachement-des-salaries/article/ressources-utiles

ANNEXE RELATIVE A LA PROTECTION DES DONNEES

La présente Annexe relative à la Protection des Données **(« Annexe relative à la Protection des Données »)** est soumise aux dispositions du Contrat. Les termes qui ne sont pas définis dans la présente Annexe auront le sens qui leur est donné dans le Contrat. En cas de conflit entre les dispositions du Contrat et de la présente Annexe relative à la Protection des Données, les dispositions de la présente Annexe prévaudront. Le non-respect par le Prestataire de toute disposition de la présente Annexe sera réputé constituer une violation substantielle du Contrat.

SECTION 1 – Rôle du Prestataire – Responsable de Traitement

La présente Section 1 de l'Annexe relative à la Protection des Données régit le Traitement par le Prestataire des Donnée à caractère Personnel par Accenture où (a) le Prestataire (ou un Sous-traitant Ultérieur du Prestataire) traite les Données à caractère Personnel d'Accenture à ses propres fins commerciales, et (b) le Prestataire obtient des Données à caractère Personnel principalement de la (des) personne(s) concernée(s) individuelle(s).

1.1. Le Prestataire sera tenu (et s'assurera que ses Sous-traitants Ultérieurs seront tenus) aux obligations suivantes :

1.1.1. Traiter les Données à caractère Personnel d'Accenture aux seules fins définies au Contrat, dans la mesure raisonnablement nécessaire à l'exécution du Contrat, ou tel que requis par la loi applicable. À moins qu'il ne soit autorisé à traiter les Données à caractère Personnel sur la base du consentement collecté de la personne concernée par le Prestataire conformément aux lois applicables, le Prestataire ne doit pas collecter, conserver, utiliser, divulguer ou autrement traiter les Données à caractère Personnel d'Accenture pour toute autre fin. Le Prestataire ne vendra en aucun cas les Données à caractère Personnel d'Accenture. Le Prestataire confirme qu'il comprend et respecte les restrictions de la présente Section 3.1.1 et délivrera cette certification à Accenture et/ou au Client sur demande raisonnable d'Accenture;

1.1.2. respecter les Dispositions Légales en matière de Protection des Données applicables ainsi que toutes les politiques de conformité avec les Dispositions Légales en matière de Protection des Données et toutes les procédures relatives à la protection des données mises en place par le Prestataires et à jour ;

1.1.3. obtenir (le cas échéant) le consentement de la (des) personne(s) concernée(s) et/ou le(les) informer conformément aux Dispositions Légales en matière de Protection des Données applicables afin de permettre l'exécution du Contrat par les Parties et la fourniture des Offres du Prestataire par le Prestataire aux personnes concernées et à Accenture (le cas échéant) ;

1.1.4. Le Prestataire ne conservera pas les Données à caractère Personnel d'Accenture au-delà de la durée nécessaire aux fins de l'exécution des Offres du Prestataire et/ou de ses(leurs) obligations au titre du Contrat, ou de la durée prescrite ou autorisée par la loi applicable ;

1.1.5. respecter (et s'assurer que ses Sous-traitants Ultérieurs respectent) les Clauses Contractuelles Types figurant en Annexe A (pour les Données à caractère Personnel qui proviennent d'un État membre de l'Espace économique européen (EEE)) de la présente Annexe; et s'assurer que les transferts internationaux de Données à caractère Personnel respectent les Dispositions Légales en matière de Protection des Données, et le Prestataire devra conclure tout accord supplémentaire et/ou adhérer à tout mécanisme de transfert de données juridiquement valide prescrit par les Dispositions Légales en matière de Protection des Données ;

1.1.6. assister et coopérer pleinement avec Accenture et ses Clients pour leur permettre de se conformer avec les lois en matière d'Incident

relatif à la Sécurité. Notamment, le Prestataire devra (i) notifier à Accenture sans délai et par écrit (et en tout état de cause dans les quarante-huit (48) heures de l'occurrence de tout Incident relatif à la Sécurité; et(ii) mener une investigation visant l'Incident relatif à la Sécurité, en prenant toutes les mesures nécessaires pour éliminer ou circonscrire le risque auquel il est exposé, y compris en collaborant à l'investigation menée par Accenture et en élaborant toute mesure corrective visant à atténuer tout dommage, et en développant et exécutant un plan, sous réserve de l'approbation d'Accenture, permettant de réduire rapidement les risques de récurrence de l'Incident relatif à la Sécurité ; et

1.1.7. mettre en œuvre et appliquer les mesures physiques, techniques et organisationnelles appropriées qui, a minima et lorsque cela est nécessaire, comprennent, aux fins de la Décision de la Cour de Justice de l'Union Européenne dans l'Affaire C-311/18 (également connue sous le nom de « Schrems II ») du 16 juillet 2020, des mesures qui constituent des mesures supplémentaires notamment de manière à (i) garantir un niveau de sécurité approprié au risque auquel sont exposées les Données à caractère Personnel et (ii) permettre au Prestataire (ou à tout Sous-traitant Ultérieur) de remplir ses obligations, aux frais du Prestataire, de répondre aux demandes émanant des personnes concernées dans l'exercice de leurs droits au titre des Dispositions Légales en matière de Protection des Données applicables

1.2. Si Accenture doit fournir des informations (y compris des détails relatifs aux Offres du Prestataire) à une autorité de contrôle compétente , le Prestataire assistera Accenture dans la fourniture de ces informations s'il est le seul ou si ses Sous-traitants Ultérieurs sont les seuls à détenir ces informations.

1.3. Les Parties fourniront leur pleine assistance et coopération en permettant à la/aux personne(s) concernée(s) par les Données à caractère Personnel d'Accenture (i) d'avoir accès à ces Données à caractère Personnel et aux informations relatives à leur Traitement; et (ii) de s'assurer de la suppression ou de la correction de ces Données à caractère Personnel si ces dernières sont manifestement inexactes. Les Parties s'assureront de la tenue d'un registre de toutes demandes de personnes visant à la correction de ces informations.

1.4. Le Prestataire s'assurera qu'il fera appel, pour le traitement des Données à caractère Personnel d'Accenture, à un Sous-traitant Ultérieur garantissant au moins le même niveau de protection des Données à caractère Personnel et les mesures de sécurité telles que convenues avec Accenture. Le Prestataire devra indemniser Accenture en cas de perte, d'engagement de sa responsabilité, de coûts engendrés par à un dommage et des frais engagés suite à une violation par le Prestataire, ses intermédiaires ou ses Sous-traitants Ultérieurs des dispositions de la présente Annexe relative à la Protection des Données.

1.5. Chacune des Parties devra prendre les mesures raisonnables pour informer son personnel ainsi que toute autre personne agissant sous son contrôle, des responsabilités au titre des Dispositions Légales en matière de Protection des Données résultant de l'accès aux Données à caractère Personnel d'Accenture, et de s'assurer de la fiabilité des personnes susceptibles d'être en contact avec ces Données à caractère Personnel, ou d'y avoir accès ou de les Traiter.

1.6. Les Parties sont tenues de conserver un registre des demandes formulées par les personnes concernées et de toutes autres demandes individuelles d'informations, des décisions prises et de toute information échangée. Ces registres doivent inclurent des copies des demandes formulées par les personnes concernées et des autres demandes d'informations, les détails des données auxquelles il a été accédé et qui ont été partagées et, le cas échéant, toute note de réunion, toute correspondance et tout appel téléphonique en lien avec la demande. La Partie qui a collecté les Données à caractère Personnel directement auprès des personnes concernées est tenue de traiter toute demande formulée par une personne concernée agissant en cette capacité et, le cas échéant, de fournir à la personne concernée les informations demandées. Chaque Partie fournira à l'autre Partie toute assistance raisonnable dans la mesure du nécessaire pour permettre à l'autre Partie de répondre à toute demande d'une personne concernée et de répondre à toute autre demande ou réclamation émanant des personnes concernées. Si le Prestataire reçoit une demande de la part d'une (des) personne concernée(s) concernant les informations qu'Accenture a collecté directement et lorsque le dernier agit en tant que responsable de traitement, le Prestataire doit en informer Accenture sans délai et, dans une telle situation, le Prestataire ne doit pas répondre à de telles demandes mais est obligé de donner à la (aux) personnes concernées les coordonnées de l'entreprise concernée.

SECTION 2 – Rôle du Prestataire – Sous-Traitant

Lorsque le Prestataire (ou son sous-traitant) Traite les Données à caractère Personnel en tant que Sous-traitant pour le compte d'Accenture et sur la base des instructions d'Accenture, les termes suivants s'appliqueront et seront réputées faire partie intégrante des termes et conditions du Contrat. Nonobstant ce qui précède, si le Prestataire agit en tant que Responsable de Traitement des Données à caractère Personnel d'Accenture en déterminant les moyens et finalités du traitement, le traitement du Prestataire ne sera pas assujetti à cette Section II, mais sera fait conformément à la Section I.

1. Définitions.

« **Données à caractère Personnel d'Accenture** » signifie les Données à caractère Personnel dont Accenture ou ses Affiliés disposent, sont propriétaires ou titulaires d'une licence, ou qu'il ou elles contrôle(nt) ou traite(nt) par ailleurs (y compris les Données à caractère personnel traitées par Accenture ou ses filiales pour le compte de ses Clients).

« **Dispositions Légales en matière de Protection des Données** » signifie l'ensemble des dispositions légales, réglementations, orientations et directives réglementaires applicables concernant le Traitement ou la protection des Données à caractère Personnel, ainsi que leurs éventuelles modifications ultérieures, y compris sans toutefois s'y limiter, le Règlement (UE) 2016/79 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 (le « **GDPR** »).

« **Obligations relatives à la Sécurité des Informations** » signifie les mesures physiques, techniques et organisationnelles appropriées et raisonnables d'un point de vue commercial, y compris celles décrites dans le Contrat ainsi que dans ses Annexes et dans l'Annexe II des Clauses Contractuelles Types, qui, a minima et si nécessaire, comprennent, aux fins de l'arrêt de la Cour de justice de l'Union Européenne dans l'affaire C-311/18 (également connue sous le nom de « **Schrems II** ») du 16 juillet 2020, des mesures qui constituent des mesures supplémentaires.

« **Données à caractère Personnel** » signifie toute information concernant une personne physique identifiée ou identifiable (ou bien, si les Dispositions Légales en matière de Protection des Données s'appliquent aux informations concernant les personnes morales, toute information concernant une personne morale identifiée ou identifiable), ou toute autre information telle que définie dans les Dispositions Légales en matière de Protection des Données.

« **Traitement** » signifie toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données à caractère Personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'accès, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, le blocage, l'effacement ou la destruction. Les termes « **Traiter** » et « **Traitant** » seront réputés avoir la même signification. Le Traitement inclut la sous-traitance.

« **Incident relatif à la Sécurité** » signifie toute perte, acquisition, divulgation, accès, utilisation connus ou pouvant être raisonnablement suspecté, survenu de manière accidentelle ou non autorisée, ou tout autre évènement de nature à compromettre les Données à caractère Personnel d'Accenture.

2. Portée et application.

La présente Annexe relative à la Protection des Données régit les conditions d'accès et de Traitement des Données à caractère Personnel d'Accenture par le Prestataire (y compris leur Traitement par tout sous-traitant du Prestataire), lorsque le Prestataire (ou son sous-traitant) accède à et/ou traite les Données à caractère Personnel d'Accenture pour le compte d'Accenture.

3. Dispositions générales.

3.1 Respect des Dispositions Légales en matière de Protection des Données.

Le Prestataire respectera (et s'assurera que ses sous-traitants respecteront) les Dispositions Légales en matière de Protection des Données dans le cadre de son Traitement des Données à caractère Personnel d'Accenture.

3.2 Respect des Dispositions Légales en matière d'Incidents Relatifs à la Sécurité.

Le Prestataire assistera et coopèrera (et s'assurera que ses sous-traitants assisteront et coopèreront) pleinement avec Accenture pour lui permettre de se conformer aux lois en matière d'Incident relatif à la Sécurité. Le Prestataire assistera et coopèrera pleinement avec Accenture et ses Clients pour leur permettre de se conformer aux dispositions légales en matière d'incidents relatifs à la Sécurité, y compris l'article 33 du GDPR. Le Prestataire devra notamment : (i) notifier à Accenture rapidement et par écrit (et en tout état de cause dans les vingt-quatre (24) heures) dès que le Prestataire a connaissance ou peut raisonnablement suspecter l'occurrence d'un Incident relatif à la Sécurité ; et (ii) mener une investigation visant l'Incident relatif à la Sécurité, en prenant toutes les mesures nécessaires pour éliminer ou circonscrire le risque auquel il est exposé, y compris en collaborant avec les équipes d'Accenture en charge de mener des investigations et d'élaborer des solutions, en réduisant tout dommage, et en développant et appliquant un plan permettant de réduire rapidement les risques de récurrence de l'Incident relatif à la Sécurité, sous réserve de l'accord préalable d'Accenture.

3.3 Conservation limitée des Données à caractère Personnel d'Accenture.

Le Prestataire ne conservera pas les Données à caractère Personnel d'Accenture au-delà de la durée nécessaire aux fins de l'exécution des Offres du Prestataire, ou de la durée prescrite ou autorisée par la loi applicable. À l'expiration ou à la résiliation de la fourniture des Offres du Prestataire en lien avec le Traitement des Données à caractère personnel d'Accenture, ou à tout moment en fonction de la demande d'Accenture, le Prestataire procédera sans délai à la suppression sécurisée (ou à leur restitution à Accenture) des Données à caractère Personnel d'Accenture (y compris toute copie existante), et à la suppression de toute copie existante, sauf Dispositions Légales en matière de Protection des Données contraires.

3.4 Transferts Internationaux de Données à caractère Personnel :

Le Prestataire s'engage :

3.4.1 à respecter les Clauses Contractuelles Types.

3.4.2 à s'assurer que les transferts internationaux de Données à caractère Personnel respectent les Dispositions Légales en matière de Protection des Données, et, sur demande raisonnable d'Accenture, conclure tout accord supplémentaire et/ou adhérer à tout mécanisme de transfert de données juridiquement valide régissant l'accès, le Traitement ou le transfert international de Données à caractère Personnel.

3.4.4 à fournir toute assistance raisonnable à Accenture, sur demande de celui-ci, et/ou à ses clients dans le cadre de tout dépôt de dossier, demande d'approbation ou toute autre exigence relative à un accord conclu au titre des Dispositions Légales en matière de Protection des Données.

3.4.5 Le Prestataire, agissant en tant qu'importateur des données, reconnait explicitement que (i) il n'a pas créé intentionnellement des portes dérobées ou des programmes similaires qui pourraient être utilisés pour accéder au système et/ou aux données personnelles ; (ii) il n'a pas délibérément créé ou modifié ses processus d'entreprise d'une manière qui facilite l'accès aux données ou systèmes personnels, et (iii) la législation nationale ou la politique gouvernementale n'exige pas que le Prestataire créé ou maintienne des portes dérobées ou facilite l'accès aux données personnelles ou aux systèmes ou que le Prestataire soit en possession ou remette la clé de cryptage.

4. Le Traitement des Données à caractère Personnel d'Accenture.

4.1 Si, dans le cadre de la fourniture des Offres du Prestataire et/ou de l'exécution de ses obligations au titre du Contrat, le Prestataire (ou un sous-traitant du Prestataire) traite les Données à caractère Personnel d'Accenture, il sera tenu (et s'assurera que ses sous-traitants seront tenus) aux obligations suivantes :

4.1.1 S'assurer qu'il ne causera, par tout acte intentionnel ou omission, aucune violation des Dispositions Légales en matière de Protection des Données qui soit imputable à Accenture ;

4.1.2 Traiter les Données à caractère Personnel d'Accenture uniquement et conformément aux instructions écrites données par Accenture, ou bien dans les conditions raisonnablement nécessaires à l'exécution du Contrat, ou bien conformément aux Dispositions Légales en matière de Protection des Données. Le Prestataire ne doit pas collecter, conserver, utiliser, divulguer ou traiter de toute autre manière les Données à caractère Personnel d'Accenture à d'autres fins. Le Prestataire ne vendra en aucun cas les Données à caractère Personnel d'Accenture. Le Prestataire certifie par la présente qu'il comprend et respecte les restrictions de la présente Section et délivrera cette certification à Accenture/à son Client sur sa/leur simple demande raisonnablement effectuée ;

4.1.3 Prendre les mesures raisonnables pour informer son personnel ainsi que toute autre personne agissant sous son contrôle, des responsabilités au titre des Dispositions Légales en matière de Protection des Données résultant de l'accès aux Données à caractère personnel d'Accenture et s'assurer de la fiabilité de toute personne agissant sous son contrôle susceptible d'être en contact avec les Données à caractère Personnel d'Accenture, ou d'y avoir accès ou de les Traiter ;

4.1.4 Assister et coopérer pleinement avec Accenture en s'assurant que les demandes et les droits légaux des personnes auxquelles se rapportent les Données à caractère Personnel d'Accenture soient traités de manière appropriée et dans les meilleurs délais pour l'accomplissement de l'obligation d'Accenture de répondre à de telles requêtes concernant les Dispositions Légales en matière de Protection des Données, y compris les droits d'accès, de rectification, d'effacement, de portabilité, ainsi que le droit de limiter ou de s'opposer à certains Traitements ;

4.1.5 Notifier Accenture rapidement lorsque le Prestataire est tenu par la loi, par une décision de justice, par un mandat, une assignation, ou tout autre procédure légale, de divulguer les Données à caractère Personnel d'Accenture à tout personne autre qu'Accenture, son Client concerné ou un autre sous-traitant d'Accenture ayant l'autorisation expresse et écrite d'Accenture pour recevoir ces informations, sauf si les dispositions légales applicables lui interdise de procéder à une telle notification. Sauf si la loi applicable l'interdit, le Prestataire devra : (i) notifier rapidement Accenture préalablement à cette divulgation ; (b) coopérer avec Accenture si ce dernier décide de contester juridiquement cette divulgation, d'assurer le Traitement confidentiel de ces informations, ou de tenter d'éviter ou de restreindre cette divulgation ; et (c) restreindre cette divulgation dans la limite de ce qui est permis par la loi ;

4.1.6 Faire tous les efforts raisonnables pour s'assurer que les Données à caractère Personnel d'Accenture sont exactes et maintenues à jour à tout moment pendant toute la durée où le Prestataire en est le dépositaire ou en a le contrôle, dans les limites de ses capacités ;

4.1.7 Fournir à Accenture toutes les informations nécessaires afin de démontrer le respect par le Prestataire (ou son sous-traitant) des dispositions de la présente Annexe relative à la Protection des Données, des Dispositions Légales en matière de Protection de Données et des Obligations relatives à la Sécurité des Informations ;

4.1.8 Autoriser Accenture ou tout représentant habilité à cet effet, sous réserve d'un préavis raisonnable, à diligenter une inspection ou un audit des activités de Traitement du Prestataire (ou des sous-traitants du Prestataire) pertinentes pour le Traitement des Données à caractère

personnel d'Accenture, à vérifier que les activités de Traitement des Données à caractère personnel d'Accenture par le Prestataire (ou les sous-traitants du Prestataire) respectent les dispositions du Contrat (y compris ses Annexes), les instructions écrites d'Accenture et les Dispositions Légales en matière de Protection des Données. Le Prestataire autorise et collabore aux audits, en ce compris les inspections, diligentés par Accenture ou tout auditeur mandaté par Accenture;

4.1.9 notifier Accenture immédiatement et par écrit (i) si le Prestataire considère que les instructions fournies par Accenture ou les dispositions du Contrat constituent une violation des Dispositions Légales en matière de Protection des Données ; et/ou (ii) de toute enquête, contentieux, arbitrage ou autre litige visant les pratiques du Prestataire (ou de ses sous-traitants) en matière de sécurité et de protection des données ;

4.1.10 coopérer de manière raisonnable avec Accenture en vue d'élaborer une solution corrective visant à la mise en œuvre des nouvelles obligations imposées suite à toute évolution des Dispositions légales en matière de Protection des Données applicables aux Données à caractère personnel d'Accenture (y compris toute nouvelle mesure physique, technique, organisationnelle, de sécurité ou de protection des données).

4.2 Sous-traitants ultérieurs.

Le Prestataire ne doit pas engager un Sous-traitant Ultérieur en ce qui concerne le Traitement des Données à caractère Personnel d'Accenture sans l'accord écrit préalable d'Accenture. Le cas échéant, le Prestataire et le(s) Sous-traitant(s) Ultérieur(s) concerné(s) devront être liés par un accord écrit aux termes duquel le(s) Sous-traitant(s) Ultérieur(s) sera(seront) tenu(s) aux mêmes obligations de protection des données que celles décrites dans la présente Annexe relative à la Protection des Données (y compris les Clauses Contractuelles Types en Annexe A) et devront mettre à la disposition d'Accenture, sur demande de ce dernier, une copie de cet(ces) contrat(s). Le Prestataire restera entièrement responsable envers Accenture de tout acte ou omission de tout Sous-traitant Ultérieur. dans l'exécution de ses obligations. Les instructions données par le Prestataire à un Sous-traitant Ultérieur doivent l'être conformément aux instructions données par Accenture au Prestataire. Si le Prestataire (ou un Sous-traitant Ultérieur) n'est pas en mesure de se conformer aux instructions données par Accenture ou aux dispositions de la présente Annexe relative à la Protection des Données, le Prestataire devra en notifier Accenture rapidement et par écrit, auquel cas Accenture sera en droit de suspendre le transfert de Données à caractère personnel.

4.3 Coopération.

Le Prestataire assistera et coopèrera pleinement avec Accenture et ses Clients pour garantir leur respect des articles 32 à 36 du GDPR. Si Accenture doit fournir des informations (y compris des détails relatifs aux Offres du Prestataire fournies par le Prestataire) à une autorité de contrôle (directement ou par le biais d'un client d'Accenture), le Prestataire assistera Accenture dans la fourniture de ces informations s'il est le seul ou si ses sous-traitants sont les seuls à détenir ces informations.

4.4 Recours.

Le Prestataire accepte qu'en cas de violation des dispositions de la présente Annexe relative à la Protection des Données, Accenture ou tout Client concerné d'Accenture ne saurait obtenir de réparation adéquate par le biais d'une action en indemnisation. Par conséquent, Accenture ou tout Client concerné d'Accenture sera fondé à requérir une injonction ou à intenter un recours en équité afin de faire cesser ou d'empêcher tout Traitement, utilisation ou divulgation des Données à caractère Personnel d'Accenture qui ne serait pas prévu dans le Contrat, et/ou afin d'obtenir l'exécution des dispositions du Contrat (y compris de la présente Annexe relative à la Protection des Données), et/ou afin de garantir le respect de toute Disposition Légale en matière de Protection des Données. Le Prestataire devra indemniser Accenture en cas de perte, d'engagement de sa responsabilité, de coûts engendrés par à un dommage et des frais engagés suite à une violation par le Prestataire, ses mandataires ou ses sous-traitants des dispositions de la présente Annexe relative à la Protection des Données.

5. Les Données à caractère Personnel du Prestataire.

Accenture est susceptible de recevoir des Données à caractère Personnel concernant les employés, directeurs et autres membres du personnel du Prestataire dans le cadre habituel de ses relations commerciales avec le Prestataire au titre du Contrat. Accenture peut obtenir ces Données à caractère Personnel indirectement par le biais des systèmes de sécurité internes ou par tout autre moyen. Accenture est autorisé par la présente, et le Prestataire l'autorise par la présente, à Traiter ces Données à caractère Personnel aux fins du Contrat et des objectifs pertinents poursuivis dans le cadre de la Politique de Protection des Données globale d'Accenture (dont Accenture mettra une copie à la disposition du Prestataire sur demande). À cette fin, Accenture pourra transférer ces Données à caractère Personnel vers tout pays dans lequel la structure internationale d'Accenture, ses clients et ses distributeurs exercent leurs activités. Si les Dispositions Légales en matière de Protection des Données le requièrent, Accenture et le Prestataire conviennent de conclure tout accord supplémentaire ou tout avenant nécessaire pour pouvoir procéder au transfert de ces Données à caractère Personnel hors de leur juridiction d'origine en vertu de ces dispositions légales.

EXIGENCES EN MATIERE DE SECURITE DE L'INFORMATION

La présente Annexe relative aux Exigences en matière de sécurité de l'information « **Annexe relative à la Sécurité des Informations** »), est soumise aux dispositions du Contrat. Aux fins des présentes, « **Prestataire** » désigne le Prestataire, qui pour les besoins des présentes, comprend ses tiers fournisseurs/distributeurs/agents et sous-traitants et « **Accenture** » désigne Accenture, tel que défini au Contrat. Les termes qui ne sont pas définis dans la présente Annexe relative à la Sécurité des Informations auront le sens qui leur est donné dans le Contrat. En cas de conflit entre les dispositions du Contrat et de la présente Annexe relative à la Sécurité des Informations, les dispositions de la présente Annexe relative à la Sécurité des Informations prévaudront.

1. EXIGENCES EN MATIÈRE DE SÉCURITÉ DES INFORMATIONS.

1.1. Si le Prestataire a connaissance, ou suspecte de manière raisonnable la perte, ou tout incident comme la destruction, acquisition, divulgation, accès, manipulation, utilisation non-autorisée ou accidentelle, des Données d'Accenture ou qu'elles ont été compromises de toute autre manière, (« **Incident relatif à la Sécurité** »), le Prestataire notifiera immédiatement son interlocuteur Accenture par écrit et en tout état de cause dans un délai de quarante-huit (48) heures, ou dans le délai prescrit par les lois/réglementations en vigueur, suivant la découverte de l'évènement et coopèrera avec Accenture dans toute investigation visant l'atteinte concernée ou à l'élaboration de toute solution corrective. Si Accenture informe le Prestataire d'une vulnérabilité ou d'un Incident relatif à la Sécurité identifié(e) par Accenture ou un tiers, le Prestataire résoudra de bonne foi la vulnérabilité ou l'incident, sans délai, tel que prévu par cette annexe « Exigence en matière de sécurité des informations » et conformément aux exigences d'Accenture en matière de sécurité des Informations (voir https://www.Accenture.com/us-en/about/legal/information-security-supplier-security-requirements). Aux fins de la présente Annexe relative à la Sécurité des Informations : (i) « les Données d'Accenture » signifie les Données de l'acheteur ou a le sens défini dans le Contrat, ou, en l'absence d'une telle définition, « **les Données d'Accenture** » signifie toutes les informations ou données collectées, conservées, traitées, reçues et/ou générées par le Prestataire en lien avec la fourniture des Offres du Prestataire concernées à Accenture, y compris les Données d'Accenture ; et (ii) le terme «**Offres du Prestataire** » signifie la Technologie et les Services Professionnels du Prestataire ou a le sens défini dans le Contrat et comprend également tout autre prestation fournie par le Prestataire au titre du Contrat, et inclut tout logiciel ou équipement fourni par le Prestataire (y compris tout logiciel et équipement de tiers) nécessaire afin d'accéder ou de fournir les Offres du Prestataire .

1.2. Le Prestataire déclare et garantit qu'il mettra en œuvre les mesures techniques et organisationnelles liées à la sécurité issues des normes en vigueur définies par l'industrie. Le terme « **Normes de l'Industrie** » signifie toute mesure de sécurité commercialement raisonnable visant tout équipement, système logiciel et plateforme pertinents que le Prestataire utilise pour accéder, traiter et/ou conserver les Données d'Accenture, destinée à garantir la sécurité, l'intégrité et la confidentialité des Données d'Accenture, et à protéger les Données d'Accenture contre tout Incident relatif à la Sécurité ou toute autre divulgation non autorisée des Données d'Accenture, y compris les garanties, pratiques et procédures décrites dans l'un (au moins) des documents suivants :

(i) Les séries ISO / IEC 27000 – voir https://www.iso.org/isoiec-27001-information-security.html ; et/ou
(ii) COBIT 5 – http://www.isaca.org/cobit/; et/ou
(iii) Le cadre de cybersécurité du NIST (*Cyber Security Framework*) – voir http://www.nist.gov/cyberframework/; et/ou
(iv) Le cadre de développement sécurisé des logiciels – voir https://csrc.nist.gov/publications/detail/sp/800-218/fina l ; et/ou
(v) Centre de Contrôle de la Sécurité sur l'Internet (*Center for Internet Security Controls*) – voir https://www.cisecurity.org/; et/ou
(vi) Lorsque des données de carte de crédit sont conservées, consultées ou traitées, ou que l'on peut y accéder : Les normes de sécurité PCI DSS (*Payment Card Industry Data Security Standards* -"**PCI DSS**") – voir http://www.pcisecuritystandards.org/; et/ou
(vii) Lorsque des "informations de santé protégées" sont conservées, consultées ou traitées, ou que l'on peut y accéder : la loi américaine sur l'assurance maladie *Health Insurance and Portability Accountability Act* ("**HIPAA**") : http://www.hhs.gov/hipaa/.

En outre, le Prestataire déclare et garantit qu'il respectera les exigences légales et règlementaires applicables afin de garantir que les Données d'Accenture ne sont pas détruites (sauf si une telle destruction est expressément autorisée au titre du Contrat), perdues, altérées, corrompues ou affectées de tout autre manière de sorte qu'elles ne sont plus immédiatement utilisables. À la demande d'Accenture, les Données d'Accenture seront immédiatement fournies ou autrement mises à la disposition d'Accenture par le Prestataire, soit, à la discrétion d'Accenture, soit selon les modalités de la Offres du Prestataire convenue, soit dans un format défini par une Norme de l'Industrie précisé par Accenture.

Également, le Prestataire déclare et garantit qu'il possède actuellement et qu'il maintiendra en vigueur, pendant toute la durée du Contrat et de toutes les Commandes, les méthodes, pratiques et autres exigences de sécurité énoncées dans l'Appendice 1 de la présente Annexe de Sécurité de l'Information, telles qu'elles peuvent être raisonnablement modifiées de temps à autre par Accenture après notification au Prestataire.

1.3. **Code illicite.** Hormis les fonctions et caractéristiques figurant expressément dans la documentation fournie ou mise à disposition d'Accenture par le Prestataire, déclare et garantit que ces Offres du Prestataire, Livrables, logiciels ou équipements qui traitent, conservent ou transfèrent les Données d'Accenture sont et seront libres, à sa connaissance, de tout code malveillant y compris, sans toutefois s'y limiter, tout virus, logiciel malveillant, ver informatique, bombe à retardement, porte dérobée malveillant, bombes logiques, , rançongiciel (*ransomware*), logiciel espion (*spyware*), logiciels suspects (*rogue software*), cheval de Troie (*trojan horse*) et tout autre code invalidant.

1.4. **Sécurité de tous les composants logiciels.** Le Prestataire accepte cataloguer de manière appropriée tous les composants logiciels (y compris, sans toutefois s'y limiter, les logiciels *open source*) utilisés dans les Offres du Prestataire, logiciels, équipements et/ou livrables du Prestataire. Le Prestataire déterminera si l'un quelconque de ces composants logiciels présente des défauts et/ou failles de sécurité susceptibles d'entraîner un Incident relatif à la Sécurité. Le Prestataire réalisera cette évaluation avant de livrer ou de donner accès à ces composants logiciels à Accenture puis de manière continue pour toute la durée du Contrat ou de toute Commande ou de tout Document de Mission. En outre, le Prestataire accepte de ne pas divulguer l'existence du présent Contrat, ni aucune des Données d'Accenture ou élément de propriété intellectuelle d'Accenture dans le cadre l'élaboration de toute solution corrective (y compris, par exemple, la fourniture d'un code dans le cadre d'un projet de logiciel *open source*).

1.5. **Protection du Code Source**. Le Prestataire doit protéger le code source contre les différents risques de sécurité, y compris les menaces provenant de l'extérieur et de l'intérieur. Le Prestataire mettra en œuvre une approche de sécurité à plusieurs niveaux, notamment a) en définissant un ensemble de règles, d'exigences et de procédures pour la manipulation et la protection du code, b) en utilisant des outils d'analyse de la sécurité du code source, tels que les tests statiques de sécurité des applications (SAST), pour détecter les failles de sécurité et autres problèmes au cours du développement, c) en définissant les personnes autorisées à accéder au code source, à la base de code et aux référentiels de code source, d) crypter les données confidentielles et sensibles en transit et au repos, e) mettre en œuvre des solutions de sécurité réseau telles que des pare-feu, des réseaux privés virtuels (VPN), des logiciels antivirus et anti logiciels malveillants comme protections de base, f) sécuriser les points d'extrémité ou les points d'entrée des dispositifs des utilisateurs finaux avec des logiciels de sécurité des points d'extrémité, et g) veiller à ce que tous les concepts et inventions liés aux logiciels soient protégés par la loi sur les droits d'auteur et les brevets nécessaires.

1.6. **Résilience.** Pendant la durée du Contrat et de toutes les Commandes et des Documents de Mission, le Prestataire maintiendra en place une solution d'haute disponibilité (*highly availability* – HA) et plan y associé qui soit conforme aux Normes de l'Industrie eu égard aux Offres du Prestataire fournies.
La solution HA devra proposer une architecture technique hautement disponible à l'échelle de toutes les applications tiers (par exemple, Web, application, base de données, etc.) avec des nœuds déployés dans les différents centres de données physiques (par exemple, dans l'ensemble des zones de disponibilité AWS) avec non plus qu'une (1) heure de récupération à compter de toute perte des données. Si une solution HA ne peut pas être déployée, le Prestataire maintiendra en vigueur une solution de continuité des activités (Disaster Recovery – DR) (« **DR** ») et un plan y associé qui soit conforme aux Normes de l'Industrie eu égard aux Offres du Prestataire fournies.
La solution DR devra garantir que les fonctionnalités critiques identifiées seront rétablies dans les vingt-quatre (24) heures et non plus que douze (12) heures en cas de toute perte des données, suivant la survenance déclarée de l'évènement de sinistre ou de panne système majeure.

Le Prestataire testera la solution DR ou HA et le plan associé au moins deux (2) fois chaque année ou plus fréquemment si les résultats font état de l'incapacité de rétablir certains systèmes critiques dans les délais ci-dessus. Le Prestataire fournira une synthèse des résultats des tests pour chaque exercice qui inclura le point de récupération effectif (combien de données perdues, le cas échéant) et les délais de rétablissement (délai pour rétablir les applications et/ou les Offres du Prestataire, en l'absence de basculement automatique) observés lors de chaque exercice. Le Prestataire fournira les plans d'actions convenus pour traiter et résoudre toute carence, préoccupation ou tout problème susceptible de faire obstacle au rétablissement de la fonctionnalité critique de l'application et/ou des Offres du Prestataire dans les vingt-quatre (24) heures suivant la survenance de l'évènement de sinistre déclaré ou de panne système majeure. En outre, le Prestataire notifiera Accenture, dans un délai raisonnable, lorsqu'il lance le plan de continuité.

2. ÉVALUATION DE LA SÉCURITÉ.

2.1. Évaluation de la Sécurité. Si Accenture estime de manière raisonnable ou considère en toute bonne foi que les pratiques et procédures du Prestataire en matière de sécurité ne satisfont pas aux obligations de ce dernier au titre du Contrat ou de la

présente Annexe relative à la Sécurité des Informations, alors Accenture a la possibilité de notifier le Prestataire par rapport à ces manquements. Le Prestataire devra sans délai (i) remédier à ces manquements à ses frais et (ii) autoriser Accenture, ou ses mandataires dûment habilités, sous réserve d'un préavis raisonnable, à évaluer les pratiques relatives à la sécurité du Prestataire et de ses mandataires pertinentes aux fins du Contrat. En outre, (A) le Prestataire remplira, en temps utiles et avec précision, un questionnaire relatif à la sécurité des informations que lui aura fourni Accenture, chaque année ou plus fréquemment si Accenture en fait la demande, afin de vérifier le respect exigences en matière de sécurité présentes dans le Contrat par le Prestataire et ses sous-traitants et (B), si le Prestataire fournit, dans le cadre des Offres du Prestataire, des services d'infrastructure gérée, de cloud (par exemple Iaas), de vulnérabilité ou de sécurité à Accenture ou à son client, le Prestataire accepte de se soumettre à une évaluation de ces Offres du Prestataire et des livrables connexes et le Prestataire fournira la preuve que les Offres du Prestataire convenues répondent aux exigences de sécurité et/ou aux exigences spécifiques des clients d'Accenture pour les Offres du Prestataire («**Évaluation de la Sécurité**»).

2.2. Problèmes de Sécurité et Plan de Rétablissement. Les problèmes de sécurité identifiés par Accenture au cours de l'Évaluation de la Sécurité se verront attribuer un niveau de risque et un délai mutuellement convenu pour y remédier. Le Prestataire devra remédier tous les problèmes de sécurité identifiés dans les délais de rétablissement convenus et en cas de non-respect des obligations ci-dessus, Accenture se réserve le droit de résilier le présent Contrat sans paiement d'aucune indemnité, ni d'aucun frais supplémentaire, tout en ayant le droit au remboursement de tout acompte survenant pendant la période suivante la date effective d'une telle résiliation.

3. DROITS DE CONTROLE D'AUDIT.

Rapports SSAE18 SOC2

Au cours de chaque année calendaire, le Prestataire fournira, à ses frais, le cas échéant, le rapport SSAE18 SOC2 pour les sites identifiés et les Offres du Prestataire qui couvrent la gestion de l'implémentation des exigences en matière de sécurité de l'information et l'effectivité opérationnelle utilisées par le Prestataire lors du développement du logiciel ou la delivrance des Offres du Prestataire et qui sont développées et/ou établies par une société indépendante, experte en matière de comptabilité et reconnue à l'échelle internationale. La portée minimale de ces rapports est fondée sur la base des Principes de Sécurité relatifs au Service de Confiance (i.e Trust Service Principles of Security) (également connus sous la dénomination « **Critères Communs** ») (i.e. Common Criteria) et de Disponibilité. Le Prestataire respectera les directives futures concernant la norme SSAE18 telles que fixées par l'AICPA, l'IAASB, la Securities and Exchange Commission des États-Unis (SEC) ou le Public Company Accounting Oversight Board des États-Unis.

Si le Prestataire demande que les Offres du Prestataire ou le développement de logiciels, qui, en conformité avec l'avis raisonnable d'Accenture, doivent être délivrées à partir d'un emplacement couvert par un rapport SSAE18 SOC 2, tel que décrit ci-dessus, soient fournis à partir d'un emplacement non couvert par un rapport SSAE18 SOC2, les Parties détermineront la manière dont cette exigence peut être satisfaite avant la fourniture des Offres du Prestataire à partir de cet emplacement.

Lorsque le rapport SSAE18 SOC2 type II n'est pas disponible, le Prestataire devra fournir une copie mise à jour et récente de son rapport d'audit annuel reconnu par l'Industrie, couvrant la mise en œuvre de la gestion des exigences en matière de sécurité de l'information et l'efficacité opérationnelle des systèmes, ou la certification sur demande.

Rapports SSAE18 SOC1

Au cours de chaque année calendaire, le Prestataire fournira, à ses frais, le cas échéant, les rapports SSAE18 SOC1 pour les sites identifiés qui couvrent des centres communs du Prestataire (c'est-à-dire des centres de services à partir desquels des services sont fournis à plusieurs clients) réalisés par une société indépendante et de renommée internationale en matière de comptabilité. La portée de ces rapports sera les contrôles communs qui prennent en charge plusieurs clients servis à partir des centres du Prestataire. La période de couverture de ces révisions couvrira au moins neuf (9) mois de l'exercice fiscal du Client et sera mise à la disposition du Client au plus tard le 30 septembre de chaque année, ou avec une période de couverture et une date de livraison différentes convenues d'un commun accord par le Prestataire et le Client. Le Prestataire fournira à Accenture une lettre de déclaration (autrement appelée « **Lettre Relais** ») (eng. Bridge letter) concernant la période qui n'est pas couverte par les rapports. Le Prestataire respectera les directives futures concernant la norme SSAE18 telle que fixée par l'AICPA, l'IAASB, la *Securities and Exchange Commission* ou le *Public Company Accounting Oversight Board*.

Dans toute situation autre que dans le cadre de la fourniture des Offres du Prestataire, au titre d'un plan de continuité des opérations et/ou d'un plan d'aide à la reprise des activités en cas de sinistre tel qu'approuvés par le Client, si l'une ou l'autre des Parties demande et si le Prestataire considère raisonnablement qu'elles doivent être fournies à partir d'un emplacement relevant d'un rapport SSAE18 SOC1 décrit ci-dessus, les Offres du Prestataire soient fournies à partir d'un emplacement non couvert par un rapport SSAE18 SOC1 si les Parties détermineront la manière dont cette exigence peut être satisfaite avant la fourniture des Offres du Prestataire à partir du site en question.

Le Client, à ses propres frais, pourra auditer le Prestataire (soit dans les sites du Prestataire, soit dans le centre du Prestataire à partir duquel les Services sont fournis au Client). Le Prestataire permettra au Client, ou à ses représentants dûment autorisés, moyennant un préavis raisonnable, d'évaluer les activités du Prestataire et de ses agents qui sont pertinentes pour cette section. Si le Client demande un rapport SSAE18 SOC1 spécifique au Client, le Prestataire conclura un contrat avec une société indépendante, experte en matière de comptabilité reconnue au niveau international ou national pour effectuer ledit audit. Le Client sera responsable de tous les coûts associés à l'audit spécifique. Le Client pourra définir la portée de l'audit qui sera raisonnablement liée aux Offres du Prestataire et aux parties des sites du Prestataire à partir desquelles les Offres du Prestataire seront fournies au Client. Le Client pourra établir les objectifs de l'audit, déterminer sa fréquence et la période de rapport.

MESURES SUPPLÉMENTAIRES. En outre, conformément aux directives réglementaires suite à la prononciation et motivation de la décision « **Schrems II** » de la Cour de Justice de l'Union Européenne, le Prestataire s'engage à maintenir les mesures techniques, organisationnelles et juridiques/contractuelles supplémentaires suivantes en ce qui concerne les Données d'Accenture, y compris les données personnelles.

Mesures Techniques Supplémentaires :

Les Données d'Accenture en transit entre les entités du Prestataire seront fortement cryptées avec un cryptage qui :

i. Est conforme à l'état de l'art,
ii. Garantit la confidentialité pendant la période requise,
iii. Est mis en œuvre par un logiciel proprement entretenu,
iv. Est fiable et offre une protection efficace contre les attaques actives et passives des autorités publiques, y compris l'analyse cryptographique et,
v. Ne contient pas de portes dérobées (ang. *back doors*) dans le matériel informatique ou le logiciel, sauf accord contraire avec le Client.

Les Données d'Accenture au repos et stockées par toutes les entités du Prestataire seront fortement cryptées avec un cryptage qui :

i. Est conforme à l'état de l'art,
ii. Garantit la confidentialité pendant la période requise,
iii. Est mis en œuvre par un logiciel proprement entretenu,
iv. Est fiable et offre une protection efficace contre les attaques actives et passives des autorités publiques, y compris l'analyse cryptographique et,
v. Ne contient pas de portes dérobées (ang. *back doors*) dans le matériel informatique ou le logiciel, sauf accord contraire avec le Client.

EXIGENCES EN MATIERE DE SECURITE DE L'INFORMATION

Le Prestataire déclare qu'il a mise en œuvre et maintiendra, pour toute la durée du Contrat, de toutes les Commandes et de tous les Documents de Mission, les mesures techniques et organisationnelles, mécanismes de contrôle et pratiques relatives à la sécurité des informations suivantes :

1. Politiques relatives à la Sécurité des Informations.

i. **Politiques relatives à la Sécurité des Informations.** Les politiques relatives à la Sécurité des Informations du Prestataire doivent être documentées par le Prestataire, approuvées par la direction de ce dernier, publiées et communiquées au personnel, co-contractants, mandataires et tiers pertinents du Prestataire.

ii. **Réexamen des Politiques relatives à la Sécurité des Informations.** Les politiques du Prestataire relatives à la Sécurité des Informations doivent faire l'objet d'un réexamen par le Prestataire au moins une fois par an, ou immédiatement suivant toute modification essentielle apportée à ces politiques, afin de confirmer leur applicabilité et efficacité.

iii. **Évaluations de la Sécurité des Informations.** L'approche du Prestataire en matière de gestion de la sécurité des informations et de sa mise en œuvre (c'est-à-dire les finalités du contrôle, les mécanismes de contrôle, les politiques, les processus et procédures relatives à la sécurité des informations) fera l'objet d'évaluations indépendantes à intervalles programmées ou en cas de modification majeure.

2. Organisation de la Sécurité des Informations.

i. **Responsabilité en matière de Sécurité.** Le Prestataire nommera un ou plusieurs responsable(s) sécurité en charge de la coordination et du suivi de la fonction Sécurité des Informations du Prestataire ainsi que des politiques et procédures y associées.

ii. **Rôles et Devoirs en matière de Sécurité**. Le personnel, les co-contractants et mandataires du Prestataire impliqués dans la fourniture des Offres du Prestataire seront soumis à des accords de confidentialité avec le Prestataire.

iii. **Gestion des risques.** Des évaluations adaptées des risques en matière de sécurité des informations seront réalisées par le Prestataire dans le cadre d'un programme permanent sur la gouvernance du risque établi aux fins d'identification des risques ; d'évaluation des risques ; de gestion des risques ; et lorsque des stratégies de réduction ou d'atténuation des risques sont identifiées et mises en œuvre, une gestion effective des risques en tenant compte de l'évolution constante des menaces.

3. Sécurité en matière de Ressources Humaines.

i. **Formation en matière de Sécurité.** Tout le personnel et tous les co-contractants du Prestataire bénéficieront d'une sensibilisation, éducation et formation à la sécurité appropriées.

4. Gestion des actifs.

a. Inventaire des actifs. Le Prestataire tiendra à jour un inventaire de tous ses actifs supports et équipements dans lesquels sont conservées les Données d'Accenture. L'accès à ces supports et équipements sera restreint au seul personnel autorisé du Prestataire. Le Prestataire garantit qu'aucun logiciel ou matériel de toute nature ayant dépassé sa fin de vie (ang. « End of Life » - EOL) ne sera utilisé dans le cadre des Offres du Prestataire sans l'accomplissement d'une évaluation préalable de gestion des risques sur ces équipements, tel qu'agréé par les Parties.

b. Gestion des Actifs.

i. Le Prestataire catégorisera les Données d'Accenture de manière à en assurer une identification appropriée et l'accès aux Données d'Accenture sera restreint de manière adéquate.

ii. Le Prestataire maintiendra une politique d'utilisation acceptable prévoyant des restrictions de l'impression des Données d'Accenture et des procédures de destruction adaptée des documents imprimés contenant des Données d'Accenture lorsque ces données ne sont plus nécessaires au Prestataire aux fins de la fourniture des Offres du Prestataire au titre du Contrat.

iii. Le Prestataire maintiendra une procédure d'autorisation adéquate visant le personnel, les co-contractant et mandataires avant toute conservation des données d'Accenture sur des terminaux portables ; tout accès à distance aux Données d'Accenture ; tout traitement de ces données en dehors des installations du Prestataire. En cas d'autorisation et d'octroi d'une conservation des Données d'Accenture sur des portables, le Prestataire doit procéder en conformité avec les Normes de l'Industrie applicables et en vigueur au moment de l'autorisation et de la conservation et pendant toute la période de l'usage, relatives au cryptage standard de l'industrie sur le portable (ang. Industry Standard encryption on the portable device). Si des portables sont utilisés pour accéder ou conserver les Données d'Accenture, le Prestataire devra s'assurer que tous les membres de son personnel qui ont accès à ces Données, y compris ses sous-traitants et/ou mandataires, utilisent une solution de Gestion des appareils mobiles (eng. « *Mobile Device Management Solution* » - MDM/mobile application management - MAM) qui applique les paramétrages de cryptage, de codes d'accès *et* d'effacement à distance pour sécuriser les Données d'Accenture. Le Prestataire interdira l'inscription des dispositifs qui ont été « débridés » (*i.e.* « jail broken »).

5. Contrôle de l'accès.

Le Prestataire maintiendra une politique adaptée de contrôle de l'accès visant à restreindre l'accès aux Données d'Accenture et aux actifs du Prestataire à son personnel, ses mandataires et ses co-contractants autorisés.

a. Autorisation

i. Le Prestataire maintiendra des procédures de création et de suppression de compte utilisateur visant à octroyer ou retirer l'accès à tous les actifs, Données d'Accenture et toutes les applications internes au cours de la fourniture des Offres du Prestataire au titre du Contrat. Le Prestataire attribuera des droits d'administrateur à une personne autorisée pour la création des comptes utilisateurs ou bien des niveaux élevés d'accès pour les comptes existants.

ii. Le Prestataire maintiendra et mettra à jour des dossiers sur le personnel autorisé à accéder aux systèmes du Prestataire utilisés dans le cadre de la fourniture des Offres du Prestataire et réexaminera ces dossiers au moins une fois par trimestre.

iii. Le Prestataire s'assurera que chaque personne possède un compte utilisateur et un mot de passe uniques et spécifiques. Les comptes utilisateurs individuels ne peuvent être partagés.

iv. Le Prestataire retirera les droits d'accès aux actifs où sont conservées les Données Accenture aux membres du personnel et co-contractants au terme de leur contrat de travail, ou accord ou contrat, dans un délai de deux (2) jours ouvrables, ou bien les droits d'accès seront adaptés de façon pertinente en cas de changement de situation (par exemple changement de poste d'un membre du personnel)

v. Le Prestataire procèdera à des réexamens périodiques des utilisateurs système au moins une fois par trimestre pour l'ensemble des systèmes de support dont l'accès est contrôlé.

b. Accès le moins privilégié

i. Le Prestataire restreindra l'accès aux systèmes du Prestataire utilisés aux fins de la fourniture des Offres du Prestataire aux seules personnes ayant besoin d'y avoir accès pour exécuter leurs tâches sur la base du principe de l'accès le moins privilégié.

ii. Le personnel de soutien, les mandataires ou les co-contractants agissant dans les domaines administratifs et techniques ne pourront accéder aux données que lorsque les circonstances l'exigent.

iii. Le Prestataire doit prendre en charge la séparation des responsabilités entre ses environnements afin qu'aucune personne physique n'ait à effectuer des activités qui créeraient un conflit d'intérêts en matière de sécurité (par exemple, des activités de programmation/de gestion, de développement/en matière d'opérations).

c. Authentification

i. Le Prestataire aura à minima recours aux fonctionnalités définies par les Normes de l'Industrie applicables aux fins de l'identification et de l'authentification du personnel, des mandataires et des co-contractants qui tentent d'accéder aux systèmes d'information et aux actifs.

ii. Le Prestataire mettra en œuvre les pratiques définies par les Normes de l'Industrie applicables aux fins de désactivation des mots de passe corrompus ou divulgués.

iii. Le Prestataire assurera une surveillance des tentatives d'accès répétées aux systèmes d'information et aux actifs.

iv. Le Prestataire appliquera les pratiques de protection des mots de passe définies par les Normes de l'Industrie applicables dont la conception et le maintien en vigueur visent à préserver la confidentialité et l'intégrité des mots de passe générés, attribués, distribués et conservés sous toute forme.

v. Le Prestataire fournira à Accenture une fonctionnalité (SAML, Autorisation Ouverte (Oauth v2) etc.) d'identification unique (*Single Sign-On* – SSO) issue des Normes de l'Industrie, qui prendra en charge l'intégration avec les solutions SSO d'Accenture pour permettre une authentification pour accéder à toute application internet du Prestataire fournie dans le cadre des Offres du Prestataire, sauf accord contraire express d'Accenture. Les détails sur la manière dont l'intégration de la solution SSO devra être mise en œuvre seront transmis à Accenture sur demande. Si la solution SSO n'est pas mise en œuvre en raison de limitations techniques ou d'exigences d'Accenture, l'authentification multi-facteurs sera nécessaire pour accéder à toute application internet du Prestataire fournie dans le cadre des Offres du Prestataire.

vi. Le Prestataire doit implémenter et appliquer une politique par rapport aux mots de passe qui soit conforme avec les Normes de l'Industrie en vigueur, y compris de NIST, PCI DSS (norme de sécurité de l'industrie des cartes de paiement), Centre de Contrôle de la Sécurité sur l'Internet. En outre, le Prestataire veillera que les mots de passe générés par défaut seront modifiés avant de déployer tout nouveau dispositif. Dans le cas où les Offres du Prestataire comprennent la gestion de toute infrastructure et/ou de tout environnement d'Accenture et/ou de ses Clients, les seuils de verrouillage de compte doivent être conformes avec les normes de verrouillage implémentées soit par Accenture, soit par son Client, selon la politique la plus stricte de ces deux.

vii. Le personnel, mandataires et co-contractants autorisés du Prestataire utiliseront une authentification multi-facteur et des sessions chiffrées pour tous les accès aux systèmes du Prestataire. Si les Offres du Prestataire exigent des connexions externes à des environnements d'Accenture et/ou de son Client, Accenture doit autoriser en préalable ces connexions.

6. Cryptographie.

a. Le Prestataire maintiendra des politiques et normes relatives à l'utilisation de mécanismes de contrôle par cryptographie mis en œuvre pour protéger les Données d'Accenture. Le Prestataire mettra en œuvre les politiques et pratiques de gestion clés définies par les Normes de l'Industrie visant à protéger et à générer les clés de chiffrement pour toute leur durée de vie.

7. Sécurité matérielle et environnementale.

a) **Accès physique aux Installations.** Le Prestataire restreindra l'accès aux installations (où sont situés les systèmes utilisés dans le cadre de la fourniture des Offres du Prestataire) au personnel, mandataires et co-contractants identifiés.

b) **Accès physique aux Composants.** Le Prestataire tiendra à jour un registre des supports entrants et sortants contenant des Données Accenture, comprenant le type de support, les expéditeurs/destinataires autorisés, la date et l'heure, le nombre de support et le type de données contenues dans le support. Le Prestataire s'assurera que toutes les sauvegardes (y compris les sauvegardes à distance, sur Cloud) soient protégées par toute mesure de sécurité mise en œuvre sur le site ou par des services de cryptage lorsqu'elles sont hébergées, ainsi que lorsqu'elles sont déplacées sur le réseau. Dans le cas où des supports de sauvegarde qui contiennent des Données d'Accenture et/ou de ses clients, sont expédiés hors site, le Prestataire doit obtenir de la part d'Accenture l'approbation préalable de l'emplacement de stockage.

c) **Protection contre les Perturbations**. Le Prestataire devra protéger les équipements contre les pannes de courant ou toute autre perturbation causée par toute panne des sources d'énergie. Les télécommunications et le câblage réseau doivent être protégés de toute interception, interférence et/ou dommage.

d) **Élimination ou réutilisation sécurisée des équipements.** Le Prestataire vérifiera les équipements contenant des supports de stockage afin de confirmer que toutes les Données d'Accenture ont été supprimées ou écrasées de manière sécurisée via des processus conformes aux Normes de l'Industrie, avant toute élimination ou réutilisation.

e) **Politique de bureau rangé et d'écran vide**. Le Prestataire adoptera une politique de bureau rangé s'agissant des papiers et supports de conservation transportable, et une politique d'écran vide.

8. Sécurité des opérations.

a) **Politique relative aux opérations.**
Le
Prestataire maintiendra des procédures opérationnelles d'exploitation et sécurité adéquates, et ces procédures devront être mises à disposition de tout membre du personnel qui en justifie un besoin**.**

b) **Enregistrement et Suivi des Évènements.**
   i. Le Prestataire doit permettre l'enregistrement et le suivi de tous les systèmes d'exploitation, bases de données, applications, équipements de sécurité et de réseaux utilisés dans le cadre de la fourniture des Offres du Prestataire. Les données de connexion (eng. Logs) doivent être conservées pendant au moins 6 mois ou aussi longtemps que la loi l'exige, selon la période la plus longue. Les données de connexion doivent saisir l'ID d'accès, l'autorisation accordée ou refusée, la date et l'heure, l'activité pertinente et être régulièrement révisées. Tous les systèmes pertinents de traitement de l'information vont synchroniser l'heure sur une seule source de temps de référence.
   ii. Les fonctionnalités d'enregistrement devront être protégées de toute dégradation ou accès non autorisé.

c) **Protections contre les logiciels malveillants (*Malware*).** Le Prestataire doit maintenir des mécanismes de contrôle anti-malware destinés à protéger les systèmes contre tout logiciel malveillant, y compris ceux provenant de réseaux publics. Le Prestataire devra maintenir les logiciels dans leurs dernières versions à date s'agissant des logiciels anti-malware dont le Prestataire est propriétaire, et devra maintenir les services de maintenance et d'assistance appropriés pour les nouvelles versions de ces logiciels.

d) **Sauvegarde cryptée**. Le Prestataire maintiendra une politique de sauvegarde cryptée et de rétablissement protégeant également les Données d'Accenture de toute exposition à des attaques de *ransomware* (rançongiciel), et sauvegardera les Données d'Accenture, logiciels et images systèmes conformément à la politique du Prestataire, sauf exigences contraires requises par Accenture et convenues entre les Parties. Le Prestataire testera régulièrement les procédures de rétablissement.

e) **Contrôle des logiciels et des utilitaires.** Le Prestataire aura en place des politiques et procédures régissant l'installation des logiciels et commodités par le personnel.

f) **Gestion des évolutions.** Le Prestataire maintiendra et mettra en œuvre des procédures pour garantir que seules les versions approuvées et sécurisées des codes, configurations, systèmes, utilitaires et applications qui seront déployées pour usage.

g) **Cryptage des Données Inactives**. Le Prestataire procèdera au chiffrement des données inactives, y compris les données inactives stockées dans les instances cloud et dans les compartiments de stockage (ang. « storage buckets ») par une solution de chiffrement conforme avec les Normes de l'Industrie en vigueur, ou transmettra à Accenture la technologie et le savoir-faire correspondant, avec ses instructions, afin de permettre à Accenture d'effectuer tout cryptage supplémentaire, au choix d'Accenture.

9. Sécurité des communications.

a) **Transfert des informations.**
   i. Le Prestataire procèdera au chiffrement, selon les Normes de l'Industrie en vigueur, TLS (Transport Layer Security) version minimale admise 1.2, des Données d'Accenture en transit.
   ii. Le Prestataire devra utiliser le TLS, version minimale admise 1.2, sur SMTP (Simple Mail Transfer Protocol) lors de l'échange de courriels en tant que pratique standard pour crypter les courriels en transit.
   iii. Le Prestataire doit mettre en œuvre une politique DMARC (« Domain-based Message Authentication, Reporting and Conformance ») afin de prévenir et réduire le risque de piratage ou de modification des courriels provenant de domaines valides. Ces dispositions s'appliquent aux courriels provenant des applications du Prestataire.

iv. Lorsque les Offres du Prestataire comprennent la gestion des systèmes de courriel d'Accenture ou de ses Clients, ces systèmes doivent être configurés et mis en œuvre selon les normes convenues.

v. Le Prestataire doit utiliser une plate-forme de collaboration sécurisée permettant de restreindre l'accès et de crypter les communications et les Données d'Accenture.

vi. Le Prestataire restreindra l'accès par le biais du chiffrement des Données d'Accenture conservées sur des supports transportés physiquement depuis les installations du Prestataire.

b) **Sécurité des Offres du** Prestataire **relatifs aux Réseaux**. Le Prestataire s'assurera de la mise en œuvre des mécanismes de contrôle et de procédures en matière de sécurité issus des Normes de l'Industrie pour toutes les Offres du Prestataire et tous les composants réseaux, que ces Offres du Prestataire soient fournies en interne ou externalisées. Si les Offres du Prestataire incluent aussi la gestion de services et de composants réseau appartenant à Accenture ou à son client, ces services et composants doivent être configurés et mis en œuvre selon les normes convenues.

c) **Détection des intrusions**. Le Prestataire déploiera des systèmes de détection et de prévention des intrusions afin d'assurer une surveillance permanente permettant d'intercepter et de répondre aux évènements de sécurité dès qu'ils sont identifiés, et mettra jour la base de données de signatures dès que de nouvelles versions deviennent disponibles à la distribution commerciale.

d) **Pare-feu.** Le Prestataire mettra en place les pare-feu adaptés n'autorisant que les ports et services documentés et autorisés en vue de leur utilisation. Tous les autres ports seront paramétrés en mode refus d'accès (en mode « *deny all* »).

e) **Filtrage Web.** Le Prestataire aura mis en place une politique de filtrage Web pour contrôler le contenu auxquels les utilisateurs peuvent accéder sur Internet. Cela inclut la restriction de l'utilisation des courriels personnels et des sites de partage de fichiers.

f) **Prévention de la perte de données**. Le Prestataire doit mettre en place une politique de prévention des pertes de données pour contrôler ou restreindre tout déplacement non autorisé des Données d'Accenture.

10. Acquisition, développement et maintenance du système.

a) **Chiffrement du poste de travail.** Le Prestataire exigera le chiffrement entier du disque en relation avec le standard de l'Industrie pour tous les postes de travail et/ou ordinateurs portables utilisés par le personnel, les co-contractants ou les mandataires lorsqu'ils ont accès aux Données d'Accenture ou procèdent à leur traitement.

b) **Renforcement de la sécurité des applications.**

i. Le Prestataire maintiendra et mettra en œuvre des politiques, procédures et normes de développement d'application sécurisées conformes aux pratiques issues des Normes de l'Industrie telles que les premières 25 Erreurs de Logiciels établis par le SANS, l'OWASP *Top Ten* des failles de sécurité et le NIST Secure Software Development Framework (SSDF). Ceci s'applique aux applications internet, mobiles, aux logiciels embarqués et au développement de *firmware,* selon le cas.

ii. Tout membre du personnel responsable de la conception, du développement, de la configuration, des essais et du déploiement d'applications sécurisées sera compétent aux fins de l'exécution des Offres du Prestataire et recevra la formation appropriée dans le domaine des pratiques de développement d'application sécurisées du Prestataire.

c) **Renforcement de la sécurité des systèmes et des configurations.**

i. Le Prestataire établira et garantira l'utilisation de Normes de l'Industrie sécurisées pour les infrastructures des technologies. Les images devront représenter des versions renforcées des systèmes d'exploitation sous-jacents et des applications installées sur le système. Ces images devront être validées régulièrement afin de mettre à jour leur configuration de sécurité en tant que de besoin.

ii. Le Prestataire procèdera à des réexamens périodiques des administrateurs systèmes au moins une fois par trimestre pour l'ensemble des systèmes support dont l'accès est contrôlé.

iii. Le Prestataire mettra en œuvre des outils et processus de correction des logiciels des applications installées dans les systèmes et des systèmes opérationnels. Le Prestataire doit avoir mis en œuvre un processus défini pour corriger les constatations et s'assurer que les vulnérabilités urgentes/critiques sont traitées sans délai dès que possible, dans un délai de quatorze (14) jours ; les vulnérabilités à haut risque sont traitées dans les trente (30) jours ; et les vulnérabilités présentant un risque moyen doivent être traitées dans un délai de quatre-vingt-dix (90) jours. Lorsque des systèmes obsolètes ne peuvent plus être corrigés, le Prestataire mettra à jour la dernière version compatible avec le système opérationnel et des applications installées dans les systèmes. Si cela s'avère impossible, le Prestataire devra faire appel à une assistance supplémentaire et notifiera Accenture de manière à ce qu'il soit procédé à une évaluation des risques appropriée. Le Prestataire supprimera du système les logiciels obsolètes, anciens et non utilisés. Lorsque les Offres du Prestataire incluent la gestion des correctifs (eng. « Patch Management ») pour les systèmes d'exploitation et les applications appartenant à Accenture ou à son Client, le Prestataire doit documenter et mettre en œuvre un plan de mise à jour corrective approprié qui inclut les obligations agréées par les Parties par rapport au(x) Niveau(x) de Service(s)

iv. Le Prestataire restreindra les privilèges administratifs aux seuls membres du personnel ayant à la fois les connaissances nécessaires pour administrer le système d'exploitation et un besoin, à titre commercial, de modifier la configuration du système d'exploitation sous-jacent.

d) **Analyse de la Vulnérabilité des Infrastructures** : le Prestataire analysera, en utilisant des produits conformes aux Normes de l'Industrie en vigueur, son environnement interne et externe (par exemple les serveurs, les équipements réseaux, etc.) lié aux Offres du Prestataire une fois par trimestre. Le Prestataire aura en place un processus défini de remédiation des conclusions et s'assurera que les vulnérabilités présentant un risque urgent/critique sont traitées urgemment, dès que possible, dans un délai de quatorze (14) jours ; les vulnérabilités à haut risque soient remédiées dans un délai de trente (30) jours et les vulnérabilités à risque moyen doivent être traitées dans un délai de quatre-vingt-dix (90) jours. Lorsque les Offres du Prestataire incluent la gestion des vulnérabilités de l'infrastructure pour l'infrastructure appartenant à Accenture ou à son client, le Prestataire doit documenter et mettre en œuvre un plan d'analyse de l'infrastructure et de correction des vulnérabilités qui doit être approuvé par Accenture.

e) **Évaluation de la Vulnérabilité des Applications**. Le Prestataire procédera à une évaluation de la vulnérabilité des applications en matière de sécurité avant toute actualisation et d'une manière régulière. L'évaluation devra porter sur toutes les vulnérabilités des applications internet, des applications mobiles, des applications autonomes, des logiciels intégrés et des micrologiciels définies par l'OWASP (*Open Web Application Security Project*) ou énumérées dans les Top 25 Software Errors, établis par le SANS ou son successeur au moment où le test est effectué. D'une manière régulière, le Prestataire s'assurera de la résolution des vulnérabilités présentant un risque important avant toute actualisation. D'une manière régulière, le Prestataire s'assurera que les urgences/vulnérabilités présentant un risque critique et important soient traitées sans délai, dès que possible dans un délai de quatorze (14) jours ; les vulnérabilités à haut risque soient traitées dans un délai de trente (30) jours et les défauts ou failles de sécurité présentant un risque moyen dans un délai de quatre-vingt-dix (90) jours. Cela s'applique aux applications Web, aux applications mobile, aux applications autonomes, aux logiciels intégrés et au développement de micrologiciels, selon le cas. Lorsque les Offres du Prestataire incluent la gestion des vulnérabilités des applications appartenant à Accenture ou à son client, le Prestataire doit documenter et mettre en œuvre un plan d'évaluation et de remédiation des vulnérabilités constatés au sein des applications qui doit être approuvé par Accenture.

f) **Essais d'Intrusion et Évaluation de la Sécurité des Sites Internet**. Le Prestataire réalisera, à travers un programme qui réponde aux critères imposés par les Normes de l'Industrie en vigueur, des essais d'intrusion exhaustifs et une évaluation de la sécurité de tous les systèmes et sites internet utilisés dans le cadre de la fourniture des Offres du Prestataire avant toute utilisation et de façon récurrente à une fréquence d'au moins une fois tous les douze

(12) mois par un tiers indépendant reconnu par l'Industrie. Le Prestataire aura en place un processus défini de remédiation des conclusions et s'assurera que les vulnérabilités présentant un risque urgent/critique et important soient traitées sans délais, dès que possible dans un délai de quatorze (14) jours ; les vulnérabilités à haut risque soient traitées dans un délai de trente (30) jours et les défauts ou failles de sécurité présentant un risque moyen dans un délai de quatre-vingt-dix (90) jours.

g) **Documentation d'Analyse.** Le Prestataire fournira à Accenture, sur demande, une synthèse des résultats de l'analyse des vulnérabilités, des essais d'intrusion et/ou de toute évaluation de la sécurité, comprenant les actions ouvertes de remédiation à mettre en œuvre. En l'absence d'une telle synthèse, une documentation suffisante pour prouver que ces analyses ont été effectuées doit être fournie.

h) **Séparation des environnements.** Le Prestataire maintiendra des environnements distincts pour les systèmes de production et ceux hors production et il s'assurera que le développeurs n'auront pas un accès non surveillé aux environnements de production.

11. Relations du Prestataire.

a) Lorsque le Prestataire a recours à des applications ou services tiers, le contrat conclu entre le Prestataire et le tiers concerné doit mentionner clairement les obligations appropriées en matière de sécurité, substantiellement similaires aux obligations en matière de sécurité figurant dans la présente Annexe relative à la Sécurité des Informations. En outre, les engagements de niveau de service convenus avec le tiers doivent être définis de façon claire.

b) Tout tiers ou ressource extérieur(e) ayant accès aux systèmes doit être tenu par un engagement contractuel faisant état de la confidentialité conforme aux obligations en matière de confidentialité de et de sécurité figurant dans le Contrat.

c) Le Prestataire procèdera à des évaluations régulières de ses fournisseurs tiers afin de gérer les obligations de sécurité physiques et logiques, la protection de droits personnels et de la confidentialité, le signalement des violations et les obligations contractuelles. Le Prestataire s'assurera que toutes les conclusions relevées à travers ces évaluations de sécurité seront remédiées sans délai.

d) Le Prestataire procèdera à des contrôles de qualité et à une surveillance de la gestion de la sécurité lorsque le développement de logiciels est externalisé.

12. Gestion des Incidents relatifs à la Sécurité des Informations.

a) **Processus de réponse aux Incidents**

i. Le Prestataire tiendra un registre des Incidents relatifs à la Sécurité comprenant une description de l'Incident relatif à la Sécurité, les délais applicables, les effets, la personne en faisant le signalement et la personne à qui l'Incident relatif à la Sécurité est signalé, ainsi que les procédures visant à sa résolution.

ii. En cas d'Incident relatif à la Sécurité identifié soit par le Prestataire, soit par Accenture, soit par un tiers, le Prestataire : (a) diligentera immédiatement une investigation visant l'Incident relatif à la Sécurité ; (b) fournira immédiatement à Accenture toutes les informations détaillées pertinentes, telles que demandées d'une manière raisonnable par Accenture, concernant l'Incident relatif à la Sécurité ; et (c) prendra toutes les mesures raisonnables pour réduire les effets ou minimiser tout dommage résultant de l'Incident relatif à la Sécurité.

iii. Le Prestataire assurera un suivi de toutes les divulgations de Données d'Accenture, y compris le type de données divulguées, le destinataire et à quel moment a lieu la divulgation.

13. Conformité.

a) **Exigences légales et contractuelles.**

i. Les dispositions relatives à la conformité aux dispositions légales, dispositions en matière de propriété intellectuelle et de protection des données figurent dans le corps du Contrat et des annexes applicables.

DECLARATION ET CERTIFICAT DE CONFORMITE AU U.S. FOREIGN CORRUPT PRACTICES ACT ET AUX LOIS ANTICORRUPTION

En relation avec les Offres du Prestataire délivrées en vertu du Contrat, le Prestataire, qui pour les besoins de ce certificat, comprend ses propriétaires, directeurs, officiers, employés, représentants, partenaires et agents (le « **Cocontractant** »)

1. N'a pas enfreint (à l'exception de ceux qui ont été divulgués à Accenture par écrit dans le cadre de l'Annexe Anti-corruption) et n'enfreindra pas le U.S. Foreign Corrupt Practices Act, le U.K. Bribery Act, ou les autres lois applicables en matière d'anti-corruption et de lutte contre le blanchiment d'argent (collectivement les « **Lois Anti-corruption** »), ou par ailleurs n'offrira pas ou ne fournira pas d'argent ou toute chose de valeur à toute personne, en vue d'obtenir et/ou de conserver des activités au profit d'Accenture et/ou du Cocontractant, et/ou d'obtenir tout autre avantage inapproprié pour le compte d'Accenture et/ou du Cocontractant;
2. Ne soumettra pas de factures fausses ou inexactes à Accenture et par ailleurs ne falsifiera pas les documents liés aux Offres du Prestataire exécutées pour Accenture, et soumettra une documentation fidèle et adéquate avec toutes les factures, incluant: a) une explication des Offres du Prestataire exécutées au cours de la période couverte par la facture ; et b) les frais précis et détaillés engagés, accompagnés des reçus (ou d'autres documents dans l' indisponibilité d'un reçu) identifiant la date de paiement, le montant et l'objet de la dépense;
3. N'offrira pas de cadeaux, de repas ou de divertissements, ou ne paiera pas les frais de voyage, de tout tierce partie, sans l'approbation écrite et préalable d' Accenture, toutes ces dépenses devant être conformes aux lois applicables ainsi qu'aux politiques internes de l'employeur du bénéficiaire;
4. Devra aviser par écrit et sans délais Accenture dans le cas où le Cocontractant ne se conforme pas aux dispositions de ce l'Annexe Anti-corruption;
5. A sa connaissance, n'est pas et n'entrera dans aucune situation de conflit d'intérêt réel ou potentiel avec Accenture ou avec les Offres du Prestataire qui : (i) affecterait la performance du Cocontractant dans l'exécution des Offres du Prestataire; (ii) affecterait tout autre aspect du Contrat ; (iii) violerait toute loi ou règlement ; ou (iv) créerait l'apparence d'une irrégularité; et,
6. Convient que, dans le cas où Accenture croit de bonne foi qu'il y a eu violation des déclarations et engagements pris dans l'Annexe Anti-corruption, Accenture peut mettre fin au Contrat avec le Cocontractant immédiatement par avis écrit et sans pénalité.
7. Dans le cas où il est soumis à l'obligation, en application de la loi n°2016-1691 du 9 décembre 2016 dite « loi Sapin II », de mettre en place un programme de conformité de lutte contre la corruption, garantit qu'il a mis en place un programme conforme à ladite réglementation et s'engage à en fournir les justificatifs nécessaires à première demande d' Accenture.
8. Pour signaler une grave préoccupation, veuillez appeler la Ligne Ethique Accenture au 0800-91-2270, disponible 24h/24, 7jours/7 (les frais peuvent être pris en charge par Accenture) ou en visitant le site sécurisé https://businessethicsline.com/accenture.