NORMES DE CONFORMITE ET ETHIQUE DES FOURNISSEURS D'ACCENTURE – France
(Revu Novembre 2019)

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 à Accenture dans le cadre de la Commande:

- Vous adhérez aux « standard code of conduct » ((https://www.accenture.com/t20170816T083116Z__w__/us-en/_acnmedia/PDF-58/Accenture-Supplier-Standards-of-Conduct-Final-2-French.pdf);
- Vous déclarez être conforme aux garanties listées par le Certificat de conformité (Annexe 1) relatif à la lutte contre la corruption ;
- Vous déclarez être conforme aux exigences techniques et opérationnelles propres à la sécurité selon les modalités définies au présent document (Annexe 2) ;
- Vous déclarez être conforme engagements relatifs aux données personnelles définis au présent document (Annexe 3).

Ces termes et conditions s'appliqueront pourvu qu'aucun contrat particulier n'a été négocié avec vous.

Vous serez identifié ci-dessous comme étant le prestataire.

1 - DETERMINATION DES PARTIES CONTRACTANTES

Accenture, client, est entendu d'Accenture SAS, société par actions simplifiée, au capital de 17 250 000 euros, ayant son siège social à Paris (75013) 118 avenue de France, immatriculée au RCS de Paris sous le numéro B 732 075 312 ou de toute entité du groupe Accenture dument identifiée dans le document contractuel.

Le groupe Accenture est entendu ici de toute société immatriculée en France qui est contrôlée au sens de l'article L233-3 du code de commerce par Accenture Holdings France SAS, société par actions simplifiée au capital de 407 037 000,00€ dont le siège social est à Paris (75013) 118 avenue de France, RCS PARIS 477 832 612.

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

2 – DOCUMENTS A FOURNIR PAR LE PRESTATAIRE CONCERNANT LES LOIS SUR LE TRAVAIL DISSIMULE

Veuillez examiner avec attention les informations suivantes rappelant vos obligations légales envers Accenture. Accenture vous rappelle que votre non-conformité à cette obligation légale autorise Accenture à mettre fin à la relation contractuelle (Contrat) immédiatement par avis écrit et sans pénalité.

Accenture a désigné PROVIGIS en tant que collecteur des documents suivants.
*Veuillez compléter votre profil de fournisseur dans Provigis :*http://www.provigis.com
Veuillez insérer les documents demandés sans oublier les "documents spécifiques".
Tous les documents doivent être rédigés en français et fournis tous les six mois jusqu'à la fin de l'exécution du Contrat.

Prestataire établi ou domicilié en France (article d.8222-5 du code de travail et d 243-15 du code de la sécurité sociale)
1. Une attestation de fourniture de déclarations sociales et de paiement des allocations et des cotisations de sécurité sociale prévues par l'article L243-15 du code de la sécurité sociale fournie par l'URSSAF, datant de moins de 6 mois.
2. Une copie de l'extrait de l'inscription au Registre du Commerce et des Sociétés (KBIS).
3. L'attestation d'assurance professionnelle.
4. Dans le cas des employés étrangers soumis à autorisation de travail (article D8254-2 du Code du travail): une liste nominative spécifiant, pour chaque employé, la date du recrutement, la nationalité et le type et le numéro d'ordre du titre valant autorisation de travail («Liste nominative des Travailleurs Étrangers»).

Prestataire établi ou domicilié à l'étranger (article d 8222-7 et 8254-1 et suivants du code de travail):

1. Un document mentionnant le numéro de TVA intracommunautaire ou, si vous n'êtes pas établis dans un pays de l'Union européenne, un document mentionnant l'identité et l'adresse de votre représentant auprès de l'administration fiscale française.

2.a) Un document attestant la régularité de votre situation sociale au regard du règlement (CE) No.883 / 2004 du 29 Avril 2004 ou d'une convention internationale de sécurité sociale. Il peut s'agir des certificats de détachement dits "E101 ou A1".
Et, lorsque la législation du pays de domiciliation le prévoit, un document émanant de l'organisme gérant le régime social obligatoire et mentionnant que votre entreprise a été à jour de vos déclarations sociales et du paiement des cotisations afférentes, ou un document équivalent.
b) A défaut des documents mentionnés au 2 a) ci-dessus, une attestation de fourniture des déclarations sociales et le paiement des cotisations et contributions de sécurité sociale prévue à l'article L243-15 du code de la sécurité sociale émanant de l'URSSAF.

3. Lorsque votre immatriculation 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. En cas d'emploi sur le site d'Accenture des travailleurs étrangers, soumis à autorisation de travail (article D8254-2 du Code du travail): une liste nominative précisant, pour chaque employé, la date de recrutement, la nationalité ainsi que le type et le numéro d'ordre du titre valant autorisation de travail. Cette liste doit impérativement être complétée, si le sous-traitant décide, en cours d'exécution sur le site, d'employer sur celui-ci du personnel étranger, non prévu à l'origine, soumis à l'autorisation de travail.

6. En cas d'emploi sur le site d'Accenture des travailleurs étrangers (travailleur détaché): copie de la déclaration de détachement des travailleurs en France (Cerfa 13816-02)
http://travail-emploi.gouv.fr/IMG/pdf/IT_300-2.pdf
Copie du mandat de représentation du fournisseur en France (Cerfa 13816-02)
Pour des informations complémentaires:
http://travail-emploi.gouv.fr/europe-et-international/detachement-des-salaries/article/temporary-posting-of-workers-in-france
et le guide créé à l'attention des prestataires étrangers de services:
http://travail-emploi.gouv.fr/IMG/pdf/Guide_employeur_en_Anglais.pdf

3- 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 le certificat «Certificat de conformité » (Annexe 1 « Certificat de conformité »).

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 services 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 DU CERTIFICAT, MERCI DE L'INDIQUER AVANT LE DÉBUT DES PRESTATIONS À PROCUREMENT.SUPPORT@ACCENTURE.COM OU À VOTRE CONTACT ACCENTURE (IDENTIFIE DANS LE PO).

4 – 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 2 « sécurité de l'information » 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 LE PO).

5 – 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 Données Personnelles »), dès lors qu'ils seront amenés à traiter des « données personnelles » 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 en Annexe 3.

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.

ANNEXE 1: CERTIFICAT DE CONFORMITE

En relation avec les prestations effectuées en vertu du Contrat, le Prestataire, qui implique, pour les besoins de ce certificat, ses actionnaires, associés, directeurs, mandataires, employés, représentants, partenaires et agents :

1. Reconnait qu'il n'a pas enfreint (à l'exception des faits qui ont été divulgués à Accenture par écrit dans le cadre du Certificat) et qu'il s'engage à ne pas enfreindre 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 ("les Lois Anti-corruption") et d'autre part, à ne pas offrir ou fournir d'argent ou toute chose de valeur à toute personne, en vue d'obtenir et/ou de conserver des activités à son profit ou au profit d'Accenture et/ou d'un intermédiaire commercial, et/ou d'obtenir tout autre avantage inapproprié pour son compte ou pour le compte d'Accenture et/ou d'un intermédiaire commercial;
2. S'engage à ne pas soumettre de factures fausses ou inexactes à Accenture et par ailleurs à ne pas falsifier les documents liés aux prestations exécutées pour Accenture, ainsi qu'à soumettre une documentation fidèle et adéquate de toutes les factures, incluant: a) une explication des prestations exécutées au cours de la période couverte par la facture ; b) les frais précis et détaillés engagés, accompagnés des reçus (ou de tout autre document dans l' indisponibilité d'un reçu) identifiant la date de paiement, le montant et l'objet de la dépense;
3. S'engage à ne pas offrir de cadeaux, de repas, de divertissements, ou à supporter les frais de voyage, de toute tierce partie, sans l'approbation écrite et préalable d'Accenture. Toutes ces dépenses doivent être conformes aux lois applicables ainsi qu'aux politiques internes de l'employeur du bénéficiaire ;
4. S'engage à aviser par écrit et sans délais Accenture dans le cas où le Prestataire ne se conformerait pas aux dispositions de ce Certificat ;
5. Reconnait qu'il n'est pas entré et s'engage à ne pas entrer dans une situation de conflit d'intérêt réel ou potentiel avec Accenture ou en relation avec les prestations délivrées à ou pour Accenture qui : (i) affecterait la performance du Prestataire dans l'exécution de la prestation des services ; (ii) affecterait tout autre aspect de la lettre de mission ; (iii) violerait toute loi ou règlement ; ou (iv) créerait l'apparence d'une irrégularité;
6. Convient que, dans le cas où Accenture croit de bonne foi qu'il y a eu violation des déclarations et engagements pris dans ce Certificat, Accenture peut mettre fin au Contrat avec le Prestataire immédiatement par avis écrit et sans pénalité.

Pour signaler une grave préoccupation, le Prestataire appellera la Ligne Ethique Accenture au +1 312 737 8262, disponible 24h/24, 7jours/7 (les frais peuvent être pris en charge par Accenture) ou en visitant le site sécurisé https://businessethicsline.com/accenture.

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.

ANNEXE 2: SECURITE DE L'INFORMATION

1. EXIGENCES EN MATIERE DE SECURITE DE L'INFORMATION

1.1 Si le Prestataire a connaissance, ou suspecte de manière raisonnable la perte, l'acquisition non autorisée, la divulgation, l'utilisation des Données à caractère personnel d'Accenture ou qu'elles ont été compromises de toute autre manière, le Prestataire notifiera immédiatement son interlocuteur Accenture par écrit et en tout état de cause dans un délai de quarante-huit (48) heures 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. Aux fins de la présente Annexe relative à la Sécurité des Informations : (i) « **les Données d'Accenture** » a le sens défini dans le Contrat, ou, en l'absence d'une telle définition, « les Données d'Accenture » signifie toutes les informations et données collectées, conservées, traitées, reçues et/ou générées par le Prestataire en lien avec la fourniture des Prestations concernés à Accenture, y compris les Données à caractère personnel d'Accenture telles que définies dans le Contrat ; et (ii) le terme « **Prestations** » a le sens défini dans le Contrat et comprend également tout autre service fourni 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 Prestation.
1.2 Le Prestataire déclare et garantit qu'il mettra en œuvre les mesures techniques et organisationnelles liées à la sécurité issues des normes 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 une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, y compris les garanties, pratiques et procédures décrites dans l'un au moins des documents suivants :

- Les séries ISO / IEC 27000 – voir http://www.iso27001security.com/; et/ou
- COBIT 5 – http://www.isaca.org/cobit/; et/ou
- Le cadre de cyber-sécurité du NIST (*Cyber Security Framework*) – voir http://www.nist.gov/cyberframework/; et/ou
- 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
- 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 par Accenture dans le cadre de ses activités commerciales. À la demande d'Accenture, les Données d'Accenture seront immédiatement rendues à Accenture par le Prestataire, soit, à la discrétion d'Accenture, soit selon les modalités de la Prestation convenue, soit dans un format défini par une Norme ou un Standard de l'Industrie précisé par Accenture.

Le Prestataire déclare et garantit qu'il dispose actuellement et qu'il maintiendra en vigueur, pour toute la durée du Contrat et de toute les Commandes, les méthodes, pratiques, procédure ainsi que toute autre obligation relative à la sécurité mentionnées en appendice 1 de la présente Annexe relative à la Sécurité des Informations, susceptible d'être modifiée ultérieurement par Accenture après notification préalable adressée 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, au moment de la livraison ou de la transmission à Accenture, à une filiale d'Accenture ou à un Client, de toute Prestation, logiciel, équipement ou livrable, ou au moment où le Prestataire met ses éléments à la disposition d'Accenture, d'une filiale d'Accenture ou d'un Client, selon le cas, ces Prestations, logiciels, équipements et/ou livrables seront libres de tout programme, sous-programme, code, instruction, données ou fonctions (y compris, sans toutefois s'y limiter, tout virus, logiciel malveillant, ver informatique, bombe à retardement, bombes logiques, dispositifs d'arrêt, clés, codes d'autorisation, porte dérobée ou mots de passe donnant accès au Prestataire), susceptible d'entraîner : (a) une impossibilité d'exploiter les Prestations, logiciels, équipements ou livrables ; ou (b) un dommage, une interruption, une interférence dans l'exploitation des Prestations, logiciels, équipements ou livrables, configuration des équipements où se situent les Prestations, logiciels, équipements ou livrables, tout autre logiciel ou donnée couvert par cette configuration matérielle, ou tout autre équipement ou système susceptible de communiquer avec la configuration matérielle, les Prestations, logiciels, équipements ou livrables.

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 Prestations, logiciels, équipements et/ou livrables du Prestataire, et de fournir cet inventaire à Accenture sur demande de ce dernier. Le Prestataire déterminera si un quelconque de ces composants logiciels présente des défauts et/ou failles de sécurité susceptibles d'entraîner une divulgation non autorisée des Données d'Accenture ou de la propriété intellectuelle d'Accenture ou de ses clients. 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. Le Prestataire accepte de notifier Accenture de tout défaut ou faille de sécurité identifiée et d'y remédier en temps utiles. Le Prestataire notifiera immédiatement Accenture de son plan de rétablissement. S'il ne peut être remédié à ce défaut ou cette faille de sécurité en temps utiles, le Prestataire accepte de remplacer le composant logiciel concerné par un composant qui n'est pas affecté par ce défaut ou cette faille de sécurité et qui ne réduit pas la fonctionnalité globale des Prestations, logiciels, équipements ou livrables fournis au titre du présent Contrat. 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*).

5. **Continuité des activités.** Pendant la durée du Contrat et de toutes les Commandes, le Prestataire maintiendra en place une solution de continuité des activités (*Disaster Recovery* – DR) ou de haute disponibilité (*highly availability* – HA) et plan y associé qui soit conforme aux Normes de l'Industrie eu égard aux Prestations 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) de telle sorte que si un tiers et/ou un centre de données physique était affecté, l'application pourrait continuer de fonctionner sans interruption sur les nœuds situés dans les sites non affectés.
- La solution DR devra garantir que les fonctionnalités critiques identifiées seront rétablies dans les 24 heures suivant la survenance déclarée de l'évènement de sinistre ou de panne système majeure. Un plan DR garantira le basculement automatique ou manuel des fonctionnalités critiques dans les 60 minutes suivant la survenance de l'évènement de sinistre déclaré ou de panne système majeure affectant un site.

Le Prestataire testera la solution DR ou HA et le plan associé au moins tous les six (6) mois 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 Prestations, 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 dans les 24 heures suivant la survenance de l'évènement de sinistre déclaré ou de panne système majeure

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 (y compris son appendice 1), alors Accenture notifiera au Prestataire ces manquements. En outre, 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. De plus, 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 des dispositions du Contrat par le Prestataire et ses sous-traitants. (« 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 convenu pour y remédier. Le Prestataire devra remédier à tous les problèmes de sécurité identifiés dans les délais de

rétablissement convenus. Si le Prestataire ne parvient pas à résoudre les problèmes de niveau moyen ou élevé dans les délais de rétablissement mentionnés, Accenture se réserve le droit de résilier le présent Contrat pour violation substantielle immédiatement après notification préalable adressée au Prestataire.

3. DROITS DE CONTROLE D'AUDIT

Rapports SSAE18 SOC2

Au cours de chaque année calendaire, le Prestataire fournira, à ses frais, le cas échéant, les rapports SSAE18 SOC2 pour les sites identifiés i) qui sont des installations partagées du Prestataire (par exemple, les centres de service à partir desquels des Prestations sont fournies à de multiples clients) ou ii) où les logiciels sont développés, établis par un cabinet d'experts-comptables indépendant reconnu à l'échelle internationale. Ces rapports porteront sur les mécanismes de contrôle communs auxquels sont soumis les multiples clients fournis par le Prestataire à partir des centres de ce dernier ou qui portent sur le développement de logiciels, selon le cas. Ces évaluations couvriront une période d'au moins huit mois au cours de l'exercice fiscal d'Accenture, et seront mises à la disposition d'Accenture au plus tard le 30 septembre de chaque année, sauf accord mutuel du Prestataire et d'Accenture sur une autre période et une autre date de remise. Le Prestataire fournira à Accenture une lettre de déclaration (également appelée « lettre relais ») pour la période non couverte par les rapports. Le Prestataire respectera les orientations 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 l'une quelconque des parties demande, dans toute situation autre que la fourniture des Prestations 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'approuvé par Accenture, que l'une quelconque de ces Prestations soit fournie à partir d'un site non couvert par un rapport SSAE18 SOC2, et alors que le Prestataire considère raisonnablement qu'elles doivent être fournies à partir d'un site relevant d'un rapport SSAE18 SOC2, alors les parties détermineront la manière dont cette exigence peut être satisfaite avant la fourniture des Prestations à partir du site en question.

Outre le rapport SSAE18 SOC2, Accenture peut diligenter un audit du Prestataire, à ses frais et pour son propre compte ou pour le compte d'un Client (dans les installations du Prestataires ou la partie de ces installations à partir desquelles les Prestations sont fournies à Accenture ou dans lesquelles les logiciels sont développés). Sous réserve d'un préavis raisonnable, le Prestataire autorisera Accenture, ou ses mandataires dûment habilités, à procéder à l'évaluation des activités du Prestataires et des mandataires de ce dernier en matière de sécurité pertinentes aux fins de la présente section. Si Accenture demande l'établissement d'un rapport SSAE18 SOC2 spécifique à Accenture, le Prestataire contactera un cabinet d'experts-comptables indépendant reconnu à l'échelle internationale afin d'effectuer cet audit spécifique à Accenture. Accenture aura la charge de tous les frais associés à l'audit spécifique à Accenture. Accenture pourra définir la portée d'un tel audit spécifique qui devra être raisonnablement liée aux Prestations fournis par le Prestataire ou aux activités de développement de logiciels ainsi qu'aux parties des sites du Prestataires à partir desquelles les Prestations sont fournis à Accenture ou dans lesquelles les logiciels sont développés, établir les finalités du contrôle, définir la fréquence d'un tel audit et la période couverte par le rapport.

APPENDICE 1 A L'ANNEXE 2- OBLIGATIONS RELATIVES À LA SÉCURITÉ

Le Prestataire déclare qu'il a mise en œuvre et maintiendra, pour toute la durée du Contrat et de toutes les Commandes, 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. Le Prestataire n'apportera aucune modification à ces politiques susceptible d'altérer de manière significative les obligations relatives à la sécurité sans en notifier Accenture au préalable.

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 Prestations 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. Sur demande, le Prestataire se réunira avec Accenture au moins une fois par an pour discuter de la sécurité des informations en lien avec les Prestations et fournira à Accenture des synthèses des évaluations des risques pertinentes.

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.

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 Prestations 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'un accès à distance, le personnel, les mandataires et co-contractants du Prestataire seront soumis à une authentification multi-facteurs. L'authentification multi-facteurs peut inclure des techniques telles que l'utilisation de cartes SIM avec certificats, mot de passe à usage unique (OTP), et biométrie.

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 Prestations 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 Prestations 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 Prestations 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.

c. Authentification

i. Le Prestataire aura recours aux fonctionnalités définies par les Normes de l'Industrie 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 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 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, etc.) d'identification unique (*Single Sign-On* – SSO) issue des Normes de l'Industrie, nécessitant une authentification pour accéder à toute application internet du Prestataire fournie dans le cadre des Prestations, 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. S'il a été renoncé à la solution SSO, l'authentification multi-facteurs restera nécessaire pour accéder à toute application internet du Prestataire fournie dans le cadre des Prestations.
vi. Le Prestataire exigera que l'ensemble des comptes soient sécurisés par des mots de passe complexes d'au moins 8 caractères contenant des lettres, des chiffres et des caractères spéciaux et devant être modifiés au moins tous les 90 jours.
vii. Le Prestataire utilisera une authentification multi-facteur pour tous les accès administratifs, y compris l'accès administratif aux domaines réseaux et au *cloud*. L'authentification multi-facteurs peut inclure des techniques telles que l'utilisation de cartes SIM avec certificats, mot de passe à usage unique (OTP), et biométrie

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 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 Prestations) 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.
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.**
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 Prestations.
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 fournir maintenance et assistance pour les nouvelles versions de ces logiciels.
d) **Sauvegarde**. Le Prestataire maintiendra une politique de sauvegarde et de rétablissement protégeant également les Données d'Accenture de toute exposition à des attaques de *ranswomware* (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) **Gestion de la vulnérabilité**. Le Prestataire aura en place des politiques 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/applications seront déployées dans l'(les) environnement(s) de production.
g) **Cryptage des Données Inactives**. Le Prestataire procèdera au chiffrement des données inactives par une solution commerciale de chiffrement bénéficiant d'un support d'un éditeur par le système ou transmettra à Accenture la technologie et le savoir-faire correspondant, avec ses instructions, afin de permettre à Accenture d'effectuer tout chiffrement supplémentaire, au choix d'Accenture. Les solutions de cryptage seront déployées à au moins 256 bits ou AES (*Advanced Encryption Standard*).

9. Sécurité des communications

a) **Transfert des informations.**
i. Le Prestataire procèdera au chiffrement, selon les Normes de l'Industrie, des Données d'Accenture en transit.
ii. 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 Prestations 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 Prestations et tous les composants réseaux, que ces Prestations soient fournies en interne ou externalisées.

c) **Détection des intrusions**. Le Prestataire déploiera des systèmes de détection ou 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 (en mode « *deny all* »).

10. Acquisition, développement et maintenance du système.

a) **Chiffrement du poste de travail.** Le Prestataire exigera le chiffrement du disque dur à au moins 256 bits ou AES (*Advanced Encryption Standard*) 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 mettre en œuvre des politiques, procédures et normes de développement d'application sécurisées conformes aux pratiques issues des Normes de l'Industrie telles que Les 35 Meilleures Techniques de Développement en matière de Sécurité (*Top 35 Security Development Techniques*), les Erreurs de Programmation Fréquentes en matière de Sécurité *(Common Security Errors in Programming*) établis par le SANS et l'OWASP *Top Ten* des failles de sécurité. 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 Prestations et recevra la formation appropriée dans le domaine des pratiques de développement d'application sécurisées du Prestataire.

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

i. Le Prestataire établira et garantira l'utilisation de configurations standards sécurisées pour les systèmes d'exploitation. Les images devront représenter des versions renforcées des systèmes d'exploitation sous-jacents et des applications installées sur le système. Le renforcement inclut : la suppression des comptes inutiles (y compris les comptes de service), la désactivation ou la suppression des services inutiles, l'application de correctifs, la fermeture des ports réseaux ouverts non utilisés, la mise en œuvre de systèmes de détection et/ou de prévention des intrusions, et l'utilisation de pare-feu hôtes 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 et des systèmes d'exploitation. Lorsque des systèmes obsolètes ne peuvent plus être corrigés, le Prestataire mettra à jour la dernière version du logiciel d'application. Si cela s'avère impossible, le Prestataire 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.

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 son environnement interne (par exemple les serveurs, les équipements réseaux, etc.) lié aux Prestations une fois par mois et son environnement externe lié aux Prestations une fois par semaine. Le Prestataire aura en place un processus défini de gestion des conclusions mais s'assurera que les vulnérabilités présentant un risque important soient traitées dans un délai de 30 jours.

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. Le test devra porter sur toutes les vulnérabilités des applications internet définies par l'OWASP (*Open Web Application Security Project*) ou énumérées dans les Risques Principaux en matière de Cyber Sécurité (*Top Cyber Security Risks*) établis par le SANS ou son successeur au moment où le test est effectué. Le Prestataire s'assurera de la résolution des vulnérabilités présentant un risque important avant toute actualisation. Le Prestataire fournira sur demande une synthèse des résultats d'évaluation de la vulnérabilité, y compris les actions ouvertes de remédiation à mettre en œuvre. Le Prestataire aura en place un processus défini de gestion des conclusions mais s'assurera que les vulnérabilités présentant un risque important soient traitées dans un délai de 30 jours.

f) **Essais d'Intrusion et Évaluation de la Sécurité des Sites Internet**. Le Prestataire réalisera 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 Prestations avant toute utilisation et de façon récurrente à une fréquence d'au moins une fois tous les trois mois. De plus, le Prestataire mandatera un tiers indépendant reconnu par l'Industrie pour réaliser l'un des essais trimestriels. Le Prestataire aura en place un processus défini de gestion des conclusions mais s'assurera que les vulnérabilités présentant un risque important soient traitées dans un délai de 30 jours. Le Prestataire fournira à Accenture, sur demande, une synthèse des résultats des essais d'intrusion et de l'évaluation de la sécurité, comprenant les actions ouvertes de remédiation à mettre en œuvre.

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 en matière de sécurité conformes aux obligations en matière de sécurité figurant dans la présente Annexe relative à la Sécurité des Informations, qui seront appliquées par le tiers. En outre, les engagements de qualité 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.

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. Un « **Incident relatif à la Sécurité** » signifie toute destruction, perte, acquisition, altération, divulgation ou accès non autorisé, survenu de manière accidentelle ou non autorisée, à toute Donnée d'Accenture conservée dans les équipements ou les installations du Prestataire, ou tout accès non autorisé à ces équipements ou installations entrainant la perte, divulgation ou altération des Données d'Accenture.

ii. 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.

iii. En cas d'Incident relatif à la Sécurité, le Prestataire : (a) notifiera Accenture de l'Incident de Sécurité en contactant son interlocuteur Accenture par écrit immédiatement et en tout état de cause dans un délai de quarante-huit (48) heures suivant la découverte de l'évènement ; (b) diligentera immédiatement une investigation visant l'Incident relatif à la Sécurité ; (c) fournira immédiatement à Accenture toutes les informations détaillées pertinentes concernant l'Incident

relatif à la Sécurité ; et (d) prendra toutes les mesures raisonnables pour réduire les effets ou minimiser tout dommage résultant de l'Incident relatif à la Sécurité.

iv. 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.

SCHEDULE 3 –DATA PRIVACY SCHEDULE

La présente Annexe relative à la Protection des Données (« **Annexe relative à la Protection des Données** ») est soumise aux dispositions du contrat liant Accenture et le Fournisseur (« **Contrat** »). La présente Annexe relative à la Protection des Données sera considérée comme une Annexe du Contrat et réputée en faire partie intégrante. 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 un manquement à une condition essentielle du contrat.

1. DEFINITIONS

« **Données à caractère personnel d'Accenture** » signifie les Données à caractère personnel dont Accenture ou ses filiales dispose, est propriétaire ou titulaire d'une licence, ou qu'il(s) ou elle(s) 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 client).

« **Données relatives aux Contacts Professionnels** » signifie toute Donnée à caractère personnel utilisée pour communiquer ou pour faciliter la communication avec une personne dans le cadre de son emploi, son activité ou sa profession, tel que son nom, le titre de son poste, son adresse professionnelle, son numéro de téléphone professionnel, son numéro de fax professionnel ou son adresse électronique professionnelle.

« **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** »).

« **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 « Traitements » et « Traitant » seront réputés avoir la même signification. Le Traitement inclut la sous-traitance du Traitement

2. ACCÈS DU PRESTATAIRE AUX DONNÉES À CARACTÈRE PERSONNEL D'ACCENTURE

2.1 Le Prestataire n'accèdera pas ni ne cherchera à avoir accès (y compris à obtenir les moyens d'accéder) aux Données à caractère personnel d'Accenture. Le Prestataire s'assurera que l'ensemble de ses sous-traitants et/ou de ses sous-traitants de données personnelles sont contractuellement tenus au respect de cette obligation.

2.2 Si le Prestataire (ou ses sous-traitants et/ou ses sous-traitants de données personnelles) accède ou a accès ou obtient les moyens d'accéder aux Données à caractère personnel d'Accenture, il sera tenu (et s'assurera que ses sous-traitants et/ou ses sous-traitants de données personnelles seront tenus) :

2.2.1 d'en notifier rapidement Accenture; et

2.2.2 d'empêcher tout traitement ultérieur ou velléité de traitement ultérieur de ces Données à caractère personnel d'Accenture; et

2.2.3 de restituer à Accenture rapidement et de manière sécurisée les Données à caractère personnel d'Accenture.

2.3 Le Prestataire ne fera pas appel à un sous-traitant pour le traitement des Données à caractère personnel d'Accenture sans l'accord préalable de ce dernier obtenu par écrit. Le cas échéant, le Prestataire et son(ses) sous-traitant(s) concerné(s) devront être liés par un contrat écrit aux termes duquel le(s) sous-traitant(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. Le Prestataire demeurera pleinement responsable à l'égard d'Accenture pour tout acte ou omission du sous-traitant dans l'exécution de ses obligations.

3. DONNÉES RELATIVES AUX CONTACTS PROFESSIONNELS

Chacune des Parties est susceptible de recevoir des Données relatives aux Contacts Professionnels de l'autre Partie dans le cadre habituel de leurs relations commerciales au titre du Contrat. Le Prestataire traitera les Données relatives aux Contacts Professionnels d'Accenture conformément aux Dispositions Légales en matière de Protection des Données. Accenture peut également obtenir les Données à caractère personnel indirectement par le biais des systèmes de sécurité internes ou par tout autre moyen. Accenture traitera les Données à caractère personnel du Prestataire 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 le groupe 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.

.

4. MODIFICATIONS DES DISPOSITIONS LÉGALES EN MATIÈRE DE PROTECTION DES DONNÉES

En cas de modification des Dispositions Légales en matière de Protection des Données applicables aux Données à caractère personnel d'Accenture dont résulteraient de nouvelles obligations (y compris de nouvelles mesures physiques, techniques, organisationnelles, de sécurité ou de protection des données), le Prestataire coopérera de manière raisonnable avec Accenture en vue de l'élaboration d'une solution visant à la mise en œuvre de ces nouvelles obligations.