Mesures Techniques et Organisationnelles Accenture

pour la protection des Données Client

Les termes ci-après décrivent les mesures techniques et organisationnelles, les contrôles internes et procédures de sécurité de l'information qu'Accenture implémente pour la protection des données transmises par les clients ou pour leur compte dans le cadre des contrats conclus avec les clients (« **Données Client** »). Lesdites mesures de sécurité visent à protéger les Données Client sur les environnements Accenture (systèmes, réseaux, installations) contre tout accès accidentel, non autorisé ou illégal, divulgation, altération, perte ou destruction.

Lorsque les Données Client comprennent des Données à caractère Personnel, la mise en place des présentes mesures de sécurité, ainsi que les mesures additionnelles prévues dans le contrat applicable conclu avec le Client concerné sont destinées à fournir un niveau de sécurité approprié pour le traitement des Données à caractère Personnel.

Accenture peut modifier à tout moment et sans préavis les présentes mesures sous réserve que ces modifications ne réduisent, ni ne dégradent substantiellement le niveau de protection accordé aux Données Client.

1. Organisation de la Sécurité de l'Information

a) Responsable Sécurité. Accenture nommera un ou plusieurs responsables de la sécurité chargé(s) de la coordination et du suivi des règles et des procédures de sécurité.

b) Rôles et Obligations en matière de Sécurité. Les membres du personnel Accenture ayant accès aux Données Client seront tenus à une obligation de confidentialité.

c) Programme de Gestion des Risques. Accenture mettra en place un programme de gestion des risques afin d'identifier, évaluer et prendre les mesures appropriées contre les risques liés au traitement par Accenture des Données Client dans le cadre du contrat conclu entre les Parties.

2. Gestion des Actifs

a) Inventaire des actifs. Accenture tiendra un inventaire des actifs de son infrastructure, de ses réseaux, ses applications et ses environnements Cloud. Accenture tiendra également un inventaire des supports sur lesquels elle stocke les Données Client. L'accès à ces inventaires sera limité aux seuls membres de son personnel ayant une autorisation d'accès écrite.

b) Traitement des Données. Accenture :

- **i.** classera les Données Client par catégories afin de faciliter leur identification et de restreindre leur accès de manière appropriée.
- **ii.** limitera au strict nécessaire l'impression sur support papier des Données Client depuis ses systèmes aux fins d'exécution des Prestations et mettra en place des procédures concernant la destruction des documents imprimés comportant les Données Client.
- **iii.** exigera de son personnel les autorisations requises préalablement au stockage des Données Client en dehors des localisations ou systèmes autorisés contractuellement, pour tout accès à distance ou pour tout traitement des Données Client en dehors des installations des Parties.

3. Sécurité en matière de Ressources Humaines

a) Formation à la Sécurité.

i. Accenture informera son personnel au sujet des procédures de sécurité qu'elle met en place, ainsi que de leurs fonctions respectives,

ii. Accenture informera son personnel des conséquences potentielles des manquements aux règles et procédures de sécurité,

iii. Accenture utilisera exclusivement des données anonymisées lors des formations.

4. Sécurité Physique et des Environnements

a) Accès Physique aux installations. Accenture implémentera ou maintiendra des procédures aux fins de limiter, aux seules personnes autorisées, l'accès à ses installations hébergeant des systèmes d'information traitant des Données Client.

b) Accès Physique aux composants. Accenture tiendra des registres de tout support entrant ou sortant contenant des Données Client, en ce inclus le type de support, l'expéditeur/ les destinataires autorisés, la date et l'heure, le nombre de supports et les types de Données Client qu'ils contiennent.

c) Destruction des composants. Accenture appliquera les normes de l'industrie applicables (notamment en fonction des cas ISO 27001, CIS Sans 20, NIST Cyber-Security Framework) pour la destruction des Données Client lorsqu'elles ne sont plus nécessaires.

5. Gestion des Communications et des Opérations

a) Politique Opérationnelle. Accenture établira des politiques de sécurité détaillant les mesures de sécurité mises en place par Accenture, ainsi que les procédures et responsabilités applicables à tout membre de son personnel ayant accès aux Données Client.

b) Gestion des Appareils Mobiles (« MDM ») / Management des Applications Mobiles (« MAM »). Accenture maintiendra une politique de gestion de ses appareils mobiles afin de :

i. mettre en œuvre un dispositif de chiffrement pour ses appareils mobiles,

ii. interdire l'usage des applications blacklistées,

iii. faire obstacle à l'enregistrement d'appareils mobiles « débridés » (« jail broken »).

c) Procédures de Récupération de Données.

i. Accenture mettra en place des procédures spécifiques de récupération de données afin de permettre la récupération des Données Client conservées dans ses systèmes.

ii. Accenture reverra lesdites procédures de récupération de données au moins une fois par an.

iii. Accenture consignera dans un journal les différentes mesures de restauration de données qu'elle a engagées sur ses systèmes, en ce compris : la personne responsable, la description des données restaurées et, le cas échéant, la personne responsable et/ou les données pour lesquelles une saisie manuelle dans le processus de récupération des données a été nécessaire (le cas échéant).

d) Logiciels Malveillants (« malware »). Accenture réalisera des contrôles contre les logiciels malveillants en vue de bloquer les accès non-autorisés aux Données Client via des logiciels malveillants et ce, y compris ceux provenant de réseaux publics.

e) Données hors Environnement.

i. Accenture procèdera au chiffrement des Données Client qu'elle transmet via les réseaux publics.

ii. Accenture protègera les Données Client figurant sur les supports quittant ses installations (notamment au moyen du chiffrement).

iii. Accenture implémentera, dans la mesure du possible, des outils automatisés visant à réduire le risque d'erreurs d'envois pour les mails, courriers ou télécopies envoyés depuis ces systèmes.

f) Journal (« Logs ») d'Événements.

i. Accenture consignera dans un journal les évènements intervenant sur ses systèmes lorsque des Données Client sont en jeu conformément à ses politiques et normes de sécurité.

6. Contrôle des Accès

a) Politique en matière d'Accès.

Accenture tiendra un registre des privilèges de sécurité accordés aux membres de son personnel ayant accès aux Données Client via ses systèmes.

b) Autorisation d'Accès.

i. Accenture tiendra à jour un registre des membres de son personnel autorisé à accéder aux Données Client via ses systèmes.

ii. Lorsqu'elle est responsable de fournir les accès, Accenture fournira rapidement les identifiants d'authentification.

iii. Accenture désactivera les identifiants d'authentification lorsque ceux-ci n'auront pas été utilisés pendant une certaine période (une telle période de non-usage ne pouvant excéder 90 jours).

iv. Accenture désactivera les identifiants d'authentification en cas de notification que l'accès n'est plus nécessaire (par exemple en cas de licenciement d'un salarié, réaffectation sur d'autres projets, etc.) dans un délai de deux jours ouvrables.

v. Accenture identifiera les membres de son personnel susceptibles d'accorder, de modifier ou d'annuler des autorisations d'accès aux données et ressources.

vi. Lorsque plusieurs personnes ont accès à ses systèmes contenant des Données Client, Accenture veillera à ce que ces personnes disposent d'identifiants/log-in personnels (et non des identifiants partagés).

c) Privilège Minimum (« least privilege »).

i. Accenture autorisera l'accès aux Données Client par son service de support technique uniquement lorsque cela est nécessaire.

ii. Accenture maintiendra des contrôles permettant un accès en cas d'urgence aux systèmes de production via des identifiants spécifiques (« firefighter ID »,) des identifiants temporaires ou des identifiants managés par une solution de gestion des accès privilégiés (« *Privileged Access Management* » « PAM »).

iii. Accenture limitera l'accès aux Données Client aux seules personnes qui en ont besoin pour exercer leur fonction.

iv. Accenture limitera l'accès aux Données Client aux seules données nécessaires pour la réalisation des prestations.

v. Accenture mettra en œuvre le principe de la ségrégation des tâches (« *segregation of duty* ») entre ses environnements afin qu'aucune personne n'y ait accès pour réaliser des tâches susceptible de poser un risque de conflit d'intérêts en termes de sécurité (par exemple : développeur/personne faisant la revue ou développeur/ testeur).

e) Intégrité et Confidentialité. Accenture donnera instruction à tous les membres de son personnel de déconnecter leurs sessions administratives lorsqu'ils quittent les locaux ou que les ordinateurs sont laissés sans surveillance.

f) Authentification.

i. Accenture appliquera les normes de l'industrie (normes ISO 27001, CIS Sans 20 et/ou NIST Cyber-Security Framework, selon les cas) pour l'identification et l'authentification des utilisateurs qui tentent d'accéder à ses systèmes d'information.

ii. Lorsque les mécanismes d'authentification reposent sur des mots de passe, Accenture exigera **(a)** que ces mots de passe soient renouvelés régulièrement et **(b)** que ces mots de passe comprennent au moins huit caractères dont trois parmi les quatre types de caractères suivants : chiffres (0-9), lettres minuscules (a-z), lettres majuscules (A-Z) ou caractères spéciaux (!, &,*…).

iii. Accenture veillera à ce que les identifiants désactivés ou expirés ne soient pas attribués à d'autres personnes.

iv. Accenture surveillera les tentatives répétées d'accès à ses systèmes d'information via des mots de passe invalides.

v. Accenture appliquera les normes de l'industrie pour les procédures de désactivation des mots de passe corrompus ou divulgués par inadvertance (notamment ISO 27001, CIS Sans 20 et /ou NIST Cyber-Security Framework, selon les cas).

vi. Accenture appliquera les normes de l'industrie applicables en matière de protection des mots de passe (notamment suivant les cas : normes ISO 27001, CIS Sans 20 et/ou NIST Cyber-Security Framework), y compris les procédures visant à protéger la confidentialité et l'intégrité des mots de passe lorsqu'ils sont attribués et distribués, et pendant leur stockage.

g) Authentification multi-facteurs. Accenture mettra en œuvre l'authentification multi-facteurs pour l'accès interne et l'accès à distance via un réseau privé virtuel (VPN) à ses systèmes.

7. Test de pénétration et de vulnérabilité des systèmes Accenture.

1. Au moins une fois par an, Accenture effectuera des tests de pénétration et de vulnérabilité sur ses environnements informatiques conformément aux politiques de sécurité internes d'Accenture et aux pratiques standards.

2. Accenture accepte de communiquer au Client un résumé des tests réalisés à ce titre par Accenture dans la mesure où ils sont en lien avec les prestations qu'elle réalise pour le Client concerné.

3. Il est précisé qu'en ce qui concerne les tests de pénétration et de vulnérabilité, le Client ne sera pas autorisé à (i) accéder aux données ou informations appartenant à d'autres clients d'Accenture, (ii) tester des environnements informatiques tiers sauf dans le cas où Accenture a le droit d'autoriser de tels tests; (iii) accéder ou tester les infrastructures ou environnements de services partagés, ni (iv) à accéder à toute autres Informations Confidentielles d'Accenture qui ne sont pas directement pertinentes pour lesdits tests, ou pour les prestations réalisées pour le client concerné.

4. Pour les systèmes d'information d'Accenture physiquement dédiés au Client, les Parties peuvent convenir de plans de tests séparés par écrit. Ce type de tests sont limités à deux tests par an au maximum.

8. Conception et gestion des réseaux et des applications.

a) Accenture mettra en place des contrôles afin d'éviter des accès non autorisés aux Données Client par des individus sur ses systèmes.
b) Accenture aura un plan de prévention contre les pertes de données via e-mail pour surveiller ou restreindre les mouvements des données sensibles.
c) Accenture utilisera un filtrage sur le réseau Web pour empêcher l'accès à des sites non autorisés.
d) Accenture utilisera des identifiants spécifiques (« *firefighters ID* ») ou des identifiants d'utilisateurs temporaires pour accéder à la production.
e) Accenture mettra en place la détection et/ou la prévention des intrusions sur le réseau dans ses systèmes.
f) Accenture utilisera des normes de codage sécurisées.
g) Accenture recherchera et corrigera les vulnérabilités « OWASP » (« Open Web Application Security Project ») dans ses systèmes.
h) Lorsque cela est techniquement possible, il est attendu que les Parties travaillent ensemble pour limiter la possibilité pour le personnel d'Accenture d'accéder depuis les systèmes du Client à d'autres environnements que ceux du Client ou d'Accenture.
i) Accenture maintiendra à jour les normes de configuration de sécurité de ses serveurs, de ses réseaux, infrastructures, applications et cloud.
j) Accenture scannera ses environnements pour vérifier la correction des vulnérabilités identifiées.

9. Gestion des correctifs (patchs)

Accenture disposera d'une procédure de gestion des correctifs de sécurité, permettant de déployer ces correctifs de sécurité sur ses systèmes utilisés pour le traitement des Données Client et comprenant :

i. Un délai de mise en œuvre des correctifs (étant précisé que ce délai ne pourra excéder 90 jours pour les correctifs de sécurité élevés ou medium tels que définis suivant les standards Accenture); et
ii. Un process défini pour le traitement des correctifs urgents ou critiques qui interviendra aussi vite que possible.

10. Postes de Travail

Pour tous les postes de travail mis à disposition par Accenture et utilisés dans le cadre de la fourniture des Prestations, Accenture implémentera les mécanismes de contrôle suivants :

i. Agent logiciel de gestion de la conformité de l'ensemble des postes de travail avec transmission des informations au moins une fois par mois à un serveur central,
ii. Disque dur crypté,
iii. Processus de patchs permettant de s'assurer que les postes de travail disposent d'une version à jour de tous les correctifs requis,
iv. Possibilité de bloquer l'installation de certains types de logiciels blacklistés,
v. Antivirus avec un scan hebdomadaire minimum,
vi. Pares-feux installés.

11. Gestion des Failles de Sécurité

a) Procédure applicable en cas de Failles de Sécurité. Accenture maintiendra un registre de ses failles de sécurité intervenant sur ses systèmes qui comprendra le cas échéant une description de la faille de sécurité, de la période concernée, des conséquences de la faille, le nom de la personne l'ayant signalée et celui de la personne à qui elle a été signalée, ainsi que le processus de récupération des données.

b) Surveillance. L'équipe de sécurité d'Accenture examinera ses propres registres et logs dans le cadre de sa procédure applicable en cas de failles de sécurité afin de proposer, si nécessaire, des mesures correctives.

12. Gestion du Plan de Continuité

Accenture disposera de processus et de programmes alignés sur la norme ISO 22301 visant à permettre la restauration des activités à la suite d'événements affectant sa capacité à exécuter conformément au contrat conclu avec le Client.

MESURES SUPPLEMENTAIRES.

En outre, conformément aux orientations réglementaires intervenues à la suite à la décision « Schrems II » émise par la Cour Européenne de Justice, Accenture s'engage à mettre en œuvre les mesures techniques, organisationnelles et juridiques/contractuelles supplémentaires, telles que décrites ci-après, pour la protection des Données Client (y compris des Données à caractère Personnel).

Mesures Techniques Complémentaires :

1. Les Données Client en transit entre les entités d'Accenture seront fortement cryptées suivant un mécanisme de cryptage qui :
- **a)** est à l'état de l'art,
- **b)** permet de maintenir la confidentialité des données pour la durée requise,
- **c)** est mis en œuvre avec des logiciels régulièrement mis à jour,
- **d)** est robuste et offre une protection contre les attaques actives et passives émanant des autorités publiques y compris par voie de crypto-analyse,
- **e)** ne contient pas de « back doors » au niveau des matériels ou des logiciels, sauf accord contraire avec le Client concerné.

2. Les Données Client au repos et stockées par toute entité Accenture seront fortement cryptées avec un mécanisme de cryptage qui :
- **a)** est à l'état de l'art,
- **b)** permet de maintenir la confidentialité des données pour la durée requise,
- **c)** est mis en œuvre avec des logiciels régulièrement mis à jour,
- **d)** est robuste et offre une protection contre les attaques actives et passives d'autorités publiques y compris par voie de crypto-analyse, et
- **e)** ne contient pas de « back doors » au niveau des matériels ou des logiciels, sauf accord contraire avec le Client concerné.

Mesures supplémentaires organisationnelles :

1. Tout transfert de Données Client entre les entités Accenture, ainsi que tout traitement de ces Données par toute entité Accenture devra se conformer :
- **a)** aux politiques et procédures internes d'Accenture applicables en matière de gestion des demandes d'accès aux Données à caractère Personnel émises par des autorités publiques,
- **b)** aux politiques et procédures internes d'Accenture applicables pour l'accès aux données et la protection de la confidentialité des données,
- **c)** aux politiques et procédures internes d'Accenture relatives au principe de minimisation des données, et
- **d)** aux politiques et procédures internes d'Accenture pour la sécurité des données et pour la protection des Données à caractère Personnel.

2. Accenture documentera dans un registre toute demande d'accès à des Données à caractère Personnel qu'elle reçoit de la part d'autorités publiques, ainsi que de la réponse qu'elle y a apporté, du raisonnement juridique utilisé et des parties concernées.

3. Accenture rapportera, le cas échéant, régulièrement auprès de son Directeur de la Conformité des demandes d'accès à des Données à caractère Personnel qu'elle a reçues de la part d'autorités publiques.

Mesures complémentaires légales/contractuelles :

1. Accenture établira des rapports d'évaluation, régulièrement mis à jour, sur les lois locales de surveillance et sur les politiques applicables en matière de protection de la vie privée dans les pays dans lesquels Accenture traite les Données Client lorsque ces pays ne sont pas officiellement reconnus comme offrant un niveau de protection adéquat essentiellement équivalent à celui assuré au sein de l'Union Européenne. Accenture fournira au Client, sur demande, des copies de ces rapports d'évaluation.

2. Toute entité d'Accenture traitant les Données Client certifie, sauf accord contraire avec le Client concerné, (a) qu'elle n'a pas délibérément créé de « back doors » ou de programmes similaires pouvant être utilisés en vue d'accéder aux systèmes et/ou aux Données à caractère Personnel, (b) qu'elle n'a pas délibérément créé ou modifié ses process commerciaux pour faciliter l'accès aux systèmes et/ou aux Données à caractère Personnel et (c) qu'à sa connaissance, la réglementation locale applicable ou la politique des autorités locales n'exigent pas que l'entité d'Accenture concernée crée ou mette en place des « back doors », ni qu'elle facilite l'accès aux systèmes ou aux Données à caractère Personnel, ni qu'elle soit en possession de clés de cryptage ou qu'elle remette des clefs de cryptage alors que cela n'a pas été requis par une décision d'un juge ou d'un tribunal légalement valide à la suite d'un examen juridique approprié.

3. Sous réserve que cela soit autorisé par la loi applicable, toute entité d'Accenture traitant les Données Client informera le Client concerné de toute demande dont elle est saisie par toute autorité gouvernementale concernant des Données à caractère Personnel qu'Accenture traite pour le compte de ce Client. Si, en vertu de la loi applicable, Accenture n'est pas autorisée à informer le Client d'une telle demande émise par une autorité gouvernementale, Accenture prendra des mesures raisonnables afin (i) d'obtenir une autorisation administrative ou judiciaire pour informer le Client dans les meilleurs délais ou (ii) de demander à l'autorité gouvernementale concernée d'informer directement le Client. En tout état de cause, Accenture prendra des mesures raisonnables devant les tribunaux ou suivant les procédures administratives applicables pour contester les demandes du gouvernement concerné qu'elle considère comme illicite.

4. Accenture informera le Client concerné de tout changement de loi applicable qui affecterait la capacité d'Accenture à se conformer au mécanisme de transfert sur lequel elle s'est basée pour réaliser le transfert de données.

5. Toute entité Accenture traitant les Données Client permettra au Client concerné de vérifier si des Données à caractère Personnel de ce Client ont été divulguées à des autorités publiques, le cas échéant via des procédures d'audit telles que convenues dans le contrat conclu avec le Client concerné.

6. L'entité Accenture traitant les Données Client n'effectuera aucun transfert ultérieur des Données Client, ni ne suspendra les transferts en cours, sans obtenir l'approbation du Client tel que requis le cas échéant dans le cadre du contrat conclu avec le Client ou par la loi applicable.

7. Rien dans les présentes ne portera atteinte aux droits des personnes concernées d'obtenir des dommages-intérêts à l'encontre d'Accenture dans la mesure permise par la loi applicable dans l'hypothèse où Accenture divulgue les Données Client transférées en violation des engagements mis à sa charge en application du mécanisme de transfert choisi.