Code d'ADP relatif à la protection des Données pour le traitement des Données Client

Code d'ADP relatif à la protection des Données pour le traitement des Données Client

Introduction

ADP offre une vaste gamme de services de gestion de capital humain à ses Clients. ADP s'est engagée à protéger les Données à Caractère Personnel dans le cadre de son **Code Ethique et Déontologique des affaires.**

Le présent Code d'ADP relatif à la protection des Données pour le Traitement des Données Client indique comment cet engagement est mis en œuvre pour le Traitement par ADP des Données à Caractère Personnel relatives aux Employés de ses Clients, dans le cadre de la prestation de Services et des Activités de support fournis aux Clients. Dans ce cadre, les Données Client sont Traitées par ADP en tant que Sous-traitant du Traitement de Données pour le compte de ses Clients.

Pour les règles applicables au Traitement par ADP, en qualité de Responsable du Traitement de Données, des Données à Caractère Personnel relatives aux Individus avec lesquels ADP entretient une relation d'affaires (par exemple, les Individus qui représentent des Clients, Fournisseurs et Partenaires commerciaux d'ADP, d'autres Professionnels et des Consommateurs), ainsi qu'à d'autres Individus dont les Données à Caractère Personnel sont traitées par ADP, dans le cadre de ses activités commerciales en tant que Responsable du Traitement de Données, veuillez-vous reporter au ***Code d'ADP relatif à la protection des Données commerciales***.

Article 1. – Champ d'application, applicabilité et mise en œuvre

Champ d'application – Applicabilité aux Données de l'EEE

1.1 Le présent Code porte sur le Traitement des Données à Caractère Personnel des Employés du Client par ADP en sa qualité de Sous-traitant du Traitement de Données pour le compte de ses Clients dans le cadre de la prestation de Services client. Ces Données à Caractère Personnel sont (a) soumises à la Loi Applicable pour l'EEE (ou qui étaient soumises à la Loi Applicable pour l'EEE avant le transfert de ces Données à Caractère Personnel à une société du Groupe en dehors de l'EEE, dans un pays qui n'a pas été jugé comme fournissant un niveau de protection adéquat des Données par les institutions compétentes de l'EEE) ; et (b) traitées dans le cadre d'un Contrat de service spécifiant explicitement que le présent Code s'applique auxdites Données à Caractère Personnel .

En cas de question quant à l'applicabilité du présent Code, le Privacy Steward concerné demandera l'avis de l'Équipe Global Data Privacy & Governance avant la réalisation du Traitement.

Traitement de supports électroniques et papier

1.2 Le présent Code vise le Traitement des Données Client par ADP par tous moyens électroniques ainsi que par tous systèmes de classement de supports papier accessibles systématiquement.

Applicabilité de la

1.3 Aucune partie du présent Code ne pourra être interprétée de manière à se

loi locale		soustraire à un quelconque droit ou recours dont les Individus disposeraient en vertu de la Loi Applicable. Lorsque la Loi Applicable prévoit des dispositions plus protectrices que le présent Code, celles-ci s'appliqueront. Lorsque le présent Code apporte plus de protection que la Loi Applicable, ou qu'il prévoit des garanties, droits ou recours supplémentaires pour les Individus, le présent Code s'appliquera.
Politiques et lignes directrices	**1.4**	ADP pourra compléter le présent Code au moyen de politiques, de normes, de lignes directrices et d'instructions compatibles avec le présent Code.
Responsabilité	**1.5**	Le présent Code est contraignant pour ADP. Les Cadres Responsables seront tenus responsables du respect du présent Code par leurs organisations commerciales. Le Personnel d'ADP doit respecter le présent Code.
Date d'Entrée en vigueur	**1.6**	Le présent Code a été approuvé par le General Counsel, sur présentation par le Global Chief Privacy Officer, et a été adopté par le Comité Exécutif d'ADP. Le présent Code entrera en vigueur le 11 avril 2018 (**Date d'entrée en vigueur**). Ce Code (qui comprend une liste des sociétés du Groupe impliquées dans le Traitement des Données Client) sera publié sur le site Web www.adp.com. Il sera également mis à la disposition des Individus sur demande. Le présent Code doit être mis en œuvre par le Groupe ADP selon les délais prévus à l'Article 16.
Politiques antérieures	**1.7**	Le présent Code complète les politiques d'ADP en matière de respect de la protection des Données et remplace toutes déclarations antérieures en contradiction avec le présent Code.
Rôle de l'Entité Déléguée d'ADP	**1.8**	Automatic Data Processing, Inc. a désigné ADP Nederland B.V., ayant son siège social Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Pays-Bas, en qualité d'Entité Déléguée d'ADP, chargée de faire respecter le présent Code au sein du Groupe ADP, et ADP Nederland B.V. a accepté cette désignation.

Article 2. – Contrat de service

Contrat de Service, Sous-traitants de second rang	**2.1**	ADP ne traitera les Données Client que sur la base d'un Contrat de Service, qui comprendra les prescriptions contractuelles en matière de traitement obligatoire des données aux termes de la Loi Applicable au Sous-traitant du Traitement de Données et aux finalités légitimes énoncées à l'article 4. L'Entité Signataire d'ADP recourt à des Sous-traitants de second rang, à la fois

des Sous-traitants de second rang d'ADP et des Tiers Sous-traitants de second rang, dans le cadre de l'exécution de la prestation des Services au Client. Les Contrats de Service d'ADP autoriseront le recours à de tels Sous-traitants de second rang, à condition que l'Entité Signataire d'ADP demeure responsable envers le Client de la conformité des prestations des Sous-traitants de second rang avec les termes du Contrat de Service. Les dispositions de l'Article 7 régiront ultérieurement le recours à des Tiers Sous-traitants de second rang.

Cessation du Contrat de Service **2.2** En cas de résiliation des Services Client, ADP doit se conformer à ses obligations envers le Client en application du Contrat de Service en ce qui concerne la restitution des Données Client en lui fournissant les Données Client nécessaires à la continuité des activités commerciales du Client (si les Données n'ont pas été précédemment fournies ou rendues accessibles au Client via la fonctionnalité du produit concerné, comme la possibilité de télécharger les Données Client).

Lorsque les obligations d'ADP dans le cadre du Contrat de Service ont été remplies, ADP détruira, de manière sécurisée, les copies restantes des Données Client et (sur demande du Client) certifiera au Client qu'elle s'est exécutée. ADP peut conserver une copie des Données Client dans la mesure où cela est autorisé par la Loi Applicable, par le Client ou pour des besoins de résolution de litiges. ADP ne Traitera plus ces Données Client, sauf dans la mesure où cela serait nécessaire aux fins précitées. Les obligations de confidentialité d'ADP dans le cadre du Contrat de Service subsisteront aussi longtemps qu'ADP conservera une copie de ces Données Client.

Audit des mesures faisant suite à la cessation des Services **2.3** Dans les 30 jours suivant la cessation du Contrat de Service (sauf indication contraire prescrite par une Autorité de Protection des Données compétente), ADP rendra possible, à la demande du Client ou de l'Autorité de Protection des Données, l'audit de ses installations de Traitement conformément à l'Article 11.2 ou 11.3 (selon le cas) pour vérifier qu'ADP respecte ses obligations faisant suite à la cessation des Services conformément à l'Article 2.2.

Article 3. – Obligations de conformité

Instructions du Client **3.1** ADP Traitera les Données Client pour le compte du Client, uniquement dans le cadre du Contrat de service, conformément à toutes instructions documentées reçues du Client ou autant que de besoin pour se conformer à la Loi Applicable.

Respect de la Loi Applicable **3.2** ADP Traitera les Données Client dans le respect de la Loi Applicable au Sous-traitant du Traitement de Données.

ADP répondra dans les plus brefs délais et de manière appropriée aux demandes d'assistance émanant du Client, comme l'exige la loi, afin de permettre

au Client de respecter ses obligations légales en sa qualité de Responsable du Traitement de Données, conformément au Contrat de Service.

Non-conformité, effet négatif substantiel **3.3** Si une société du Groupe apprend que dans un pays hors EEE la Loi Applicable au Sous-traitant du Traitement de Données, toute modification de la Loi Applicable au Sous-traitant du Traitement de Données ou toute instruction du Client est susceptible d'avoir pour effet d'affecter de façon substantielle la capacité d'ADP à répondre à ses obligations en vertu de l'Article 3.1, 3.2 ou 11.3, ladite société du Groupe en informera dans les plus brefs délais l'Entité Déléguée d'ADP et le Client, auquel cas celui-ci aura le droit, en vertu du présent Code, de suspendre temporairement le transfert concerné de Données Client à ADP, jusqu'à ce que le Traitement soit ajusté pour remédier à la non-conformité. Dans le cas où un ajustement ne serait pas possible, le Client aura le droit de mettre fin à la partie concernée du Traitement par ADP, conformément aux termes du Contrat de Service. Ces droits et obligations ne sont pas applicables lorsque les circonstances ou la modification de la Loi Applicable au Sous-traitant du Traitement de Données résultent de Prescriptions Obligatoires.

Demande de divulgation de Données Client **3.4** Si ADP reçoit une demande de divulgation de Données Client d'une autorité chargée de l'application de la loi ou d'un organe de sécurité d'un pays hors EEE (Autorité), elle évaluera d'abord, au cas par cas, si cette demande est légalement valable et contraignante pour ADP. Toute demande qui n'est pas légalement valable et contraignante pour ADP sera rejetée conformément à la Loi Applicable.

Sous réserve du paragraphe suivant, ADP informera dans les plus brefs délais le Client, le DPA Chef de file et le DPA compétent pour le Client aux termes de l'article 11.3, de toute demande légalement valable et contraignante pour ADP émanant d'une telle Autorité, et demandera à l'Autorité de mettre cette demande en suspend pendant une période raisonnable afin de permettre au DPA Chef de file d'émettre un avis sur la validité de la divulgation demandée.

Si la suspension du traitement et/ou de la notification au DPA Chef de file d'une demande de divulgation légalement valable et contraignante est interdite, par exemple si cela constitue une violation du secret de l'instruction, ADP demandera à l'Autorité de lever cette interdiction et justifiera cette demande. ADP fournira chaque année au DPA Chef de file des informations générales sur le nombre et le type de demandes de divulgation qu'elle a reçues ces 12 derniers mois de la part d'Autorités.

Cet article ne concerne pas les demandes reçues par ADP de la part d'autorités dans le cadre de ses activités de fournisseur de services de gestion de capital humain (par exemple, ordonnances du tribunal pour la saisie de salaires), qu'ADP peut continuer à traiter, conformément à la Loi applicable, au Contrat de Service et aux instructions des Clients.

Demandes de Clients **3.5** ADP répondra dans les plus brefs délais et de manière appropriée aux demandes de renseignements émanant de Clients en rapport avec le Traitement des Données Client, conformément aux termes du Contrat de Service.

Article 4. – Finalités du Traitement des Données

Finalités Commerciales légitimes **4.1** ADP Traite les Données à Caractère Personnel (y compris les Catégories Particulières de Données) relatives aux Employés du Client, en fonction des besoins, afin de fournir des Services Client, mener des Activités de support clients, ainsi que pour les finalités supplémentaires suivantes :

(a) L'hébergement, le stockage et tous autres Traitements nécessaires à la continuité et à la reprise des activités après un sinistre, notamment les sauvegardes et l'archivage de copies de Données à Caractère Personnel;

(b) L'administration et la sécurisation des systèmes et des réseaux, y compris la surveillance des infrastructures, la gestion, vérification et authentification des identités et des identifiants, ainsi que le contrôle d'accès ;

(c) La surveillance et tous autres contrôles nécessaires pour garantir la sécurité et l'intégrité des transactions (comme les transactions financières et des activités de mouvements de fonds), y compris pour procéder à une vérification préalable comme, par exemple, la vérification de l'identité de l'Individu et l'admissibilité de l'Individu à recevoir des produits ou des services (par exemple, la vérification de la situation d'emploi ou du statut du compte) ;

(d) L'application des contrats et la protection d'ADP, de ses Collaborateurs, de ses Clients, des Employés de ses Clients et du grand public contre la fraude, le vol, la responsabilité juridique ou des abus, y compris : (i) détecter, enquêter, prévenir et atténuer les dommages causés par les (tentatives de) fraudes financières, les usurpations d'identité et les autres menaces visant les actifs financiers et matériels, les identifiants d'accès et les systèmes d'information ; (ii) participer à des initiatives externes en matière de cybersécurité, de lutte contre la fraude et le blanchiment d'argent ; et (iii) si nécessaire, protéger les intérêts vitaux des Individus, par exemple en alertant les Individus d'une menace de sécurité observée ;

(e) L'exécution et la gestion de processus commerciaux internes d'ADP entraînant un Traitement accessoire de Données Client pour :

(1) L'audit interne et le reporting consolidé ;

(2) Le respect de la législation, y compris les dépôts obligatoires et les utilisations et divulgations de renseignements exigées par la Loi Applicable ;

(3) L'anonymisation de données et l'agrégation de données anonymisées pour la minimisation de données et les analyses de services ;

(4) L'utilisation de données anonymisées et agrégées, autorisée par les Clients, pour faciliter l'analyse, la continuité et l'amélioration des produits et services d'ADP ; et

(5) La facilitation de la gouvernance d'entreprise, y compris les fusions, acquisitions, cessions et co-entreprises.

Article 5. – Exigences de sécurité

Sécurité des Données **5.1** ADP utilisera des mesures techniques physiques et organisationnelles commercialement raisonnables et appropriées afin de protéger les Données Client de tout(e) abus ou destruction, perte, altération, divulgation, acquisition ou accès accidentel(le), illicite ou non autorisé(e) durant le Traitement, qui répondront aux exigences de la Loi applicable pour l'EEE ou d'autres contraintes plus strictes imposées en vertu du Contrat de service. ADP doit, en tout état de cause, prendre les mesures prévues à l'Annexe 2 du présent Code, mesures qui peuvent être modifiées par ADP, à condition que ces modifications ne diminuent pas, de façon significative, le niveau de sécurité fourni pour les Données Client en vertu de l'Annexe 2.

Accès aux Données et confidentialité des Données **5.2** Le Personnel sera autorisé à accéder aux Données Client uniquement dans la mesure où cela est nécessaire pour répondre aux finalités de Traitement applicables en vertu de l'Article 4. ADP imposera des obligations de confidentialité au Personnel ayant accès aux Données Client.

Notification d'une Violation de la Sécurité des Données **5.3** ADP notifiera le Client de toute Violation de la Sécurité des Données, dans les meilleurs délais dès qu'elle aura eu connaissance qu'une telle violation s'est produite, à moins qu'un agent chargé de l'application de la loi ou qu'une autorité de surveillance décide que la notification contreviendrait à une enquête criminelle, causerait des dommages à la sécurité nationale ou nuirait à la confiance dans le secteur industriel concerné. Dans ce cas, la notification sera retardée selon les instructions de l'agent chargé de l'application de la loi ou de l'autorité de surveillance. ADP devra répondre dans les plus brefs délais aux demandes de renseignements de Clients relatives à ladite Violation de la Sécurité des Données.

Article 6. – Transparence à l'égard des Employés du Client

Autres demandes des Employés du Client

6.1 ADP notifiera dans les plus brefs délais au Client toutes demandes ou plaintes liées au Traitement de Données à Caractère Personnel par ADP, reçues directement d'Employés du Client, sans répondre à ces demandes ou plaintes, sauf dispositions contraires prévues au Contrat de Service ou dictées par le Client.

Si le Client lui donne instruction, au sein du Contrat de Service, de répondre aux demandes et aux plaintes de ses Employés, ADP veillera à ce que les Employés du Client reçoivent toutes les informations raisonnablement nécessaires (par exemple, la personne de contact et la procédure) afin que l'Employé du Client puisse efficacement introduire sa demande ou sa plainte.

Les dispositions du présent Article 6.1 ne seront pas applicables aux demandes gérées par ADP dans le cours normal de ses prestations de Services client et de ses Activités de support clients.

Article 7. – Sous-traitants de second rang

Contrats avec des Sous-traitants de second rang **7.1** Les Tiers Sous-traitants de second rang ne peuvent traiter des Données Client qu'en vertu d'un Contrat de sous-traitance de second rang. Le Contrat de sous-traitance de second rang imposera au Tiers Sous-traitant de second rang des conditions de Traitement en matière de protection des Données similaires que celles imposées par le Contrat de Service et le présent Code à l'Entité Signataire d'ADP.

Publication de l'aperçu des Sous-traitants de second rang **7.2** ADP publiera, sur le site Web approprié d'ADP, un aperçu des catégories de Tiers Sous-traitants de second rang concernés par la prestation des Services client concernés. Cet aperçu devra être mis à jour dans les plus brefs délais en cas de modifications.

Notification de nouveaux Tiers Sous-traitants de second rang et droit d'objection **7.3** ADP notifiera au Client tout nouveau Tiers Sous-traitant de second rang engagé par ADP pour la prestation des Services client. Dans les 30 jours suivant la réception de cette notification, le Client pourra s'opposer à ce Tiers Sous-traitant de second rang par notification écrite faite à ADP, énonçant des motifs valables et objectifs relatifs à l'incapacité de ce Tiers Sous-traitant de second rang de protéger les Données Client conformément aux obligations du Contrat de Sous-traitance de second rang, comme visé à l'Article 7.1. Dans le cas où les parties ne peuvent parvenir à une solution mutuellement acceptable, ADP devra soit ne pas autoriser le Tiers Sous-traitant de second rang à accéder aux Données client, soit permettre au Client de résilier les Services Client concernés conformément aux termes du Contrat de Service.

Exception **7.4** Les dispositions du présent Article 7 ne seront pas applicables lorsque le Client donne instruction à ADP d'autoriser un Tiers à Traiter des Données Client en vertu d'un contrat que le Client a directement conclu avec le Tiers (par exemple, un Tiers fournisseur d'avantages sociaux).

Article 8. – Surveillance et conformité

Global Chief Privacy Officer **8.1** Le groupe ADP disposera d'un Global Chief Privacy Officer, responsable des tâches suivantes :

(a) Présider le Privacy Leadership Council ;
(b) Surveiller le respect du présent Code ;
(c) Superviser, coordonner, communiquer avec, et consulter, les membres concernés du Privacy Network sur les questions de respect de la vie privée et de protection des Données ;
(d) Fournir au Comité Exécutif d'ADP des rapports annuels sur le respect de la protection des Données au regard des questions liées aux risques et à la conformité en matière de protection des Données ;
(e) Coordonner les enquêtes ou demandes officielles relatives au Traitement des Données Client par une autorité gouvernementale, en collaboration avec les membres concernés du Privacy Network et du département juridique d'ADP ;
(f) Gérer les conflits entre le présent Code et la Loi Applicable ;

(g) Surveiller le processus de conduite des Analyses d'Impact Relatives à la Protection des Données (PIA) et examiner les PIA, si nécessaire ;
(h) Surveiller la documentation, la notification et la communication des Violations de la Sécurité des Données ;
(i) Fournir des conseils sur les processus, systèmes et outils de gestion des Données mise en œuvre dans le cadre de la gestion de la protection de la vie privée et des Données, établi par le Privacy Leadership Council, y compris :
    (1) Entretenir, mettre à jour et publier le présent Code, ainsi que les politiques et normes y afférent ;
    (2) Fournir des conseils sur les outils permettant de collecter, gérer et mettre à jour les inventaires contenant des informations sur la structure et le fonctionnement de tous les systèmes qui traitent des Données Client ;
    (3) Dispenser des formations au Personnel sur le respect de la protection des Données, apporter une assistance ou donner des conseils en la matière, afin que le Personnel comprenne et exerce ses responsabilités en vertu du présent Code ;
    (4) Assurer une coordination avec le département d'audit interne et d'autres départements d'ADP afin de développer et gérer un programme approprié en vue de surveiller, d'auditer et d'établir un rapport relatif au respect du présent Code, et afin de permettre à ADP de vérifier et de garantir ce respect, le cas échéant ;
    (5) Mettre en œuvre les procédures pour répondre aux questions, préoccupations et plaintes relatives à la protection de la vie privée et des Données ; et
    (6) Communiquer sur les sanctions appropriées à appliquer en cas de violation du présent Code (par exemple, normes disciplinaires).

Privacy Network **8.2** ADP mettra en place un Privacy Network, suffisant pour faire respecter le présent Code à l'échelon mondial au sein de la structure d'ADP.

Ce Privacy Network créera et gérera un cadre organisationnel pour soutenir le Global Chief Privacy Officer et pour assurer la surveillance régionale et locale des tâches énoncées à l'Article 8.1 ainsi que toutes autres tâches qui puissent être appropriées pour gérer et mettre à jour le présent Code. Les membres du Privacy Network, selon leur propre rôle dans la région ou l'organisation concernée, exécuteront les tâches supplémentaires suivantes :

(a) Superviser la mise en œuvre des processus, systèmes et outils de gestion des données qui permettent le respect du Code par les Sociétés du Groupe dans leurs régions ou organisations respectives ;
(b) Soutenir et évaluer la gestion de la protection de la vie privée et des Données par les Sociétés du Groupe, dans leurs régions ;
(c) Conseiller régulièrement leurs Privacy Stewards et le Global Chief Privacy Officer sur les questions liées aux risques et au respect en matière de protection des Données aux niveaux local ou régional ;

(d) S’assurer de la gestion appropriée des inventaires des systèmes qui traitent les Données Client ;
(e) Se rendre disponible afin de répondre aux demandes d’approbation ou de conseil en matière de protection des Données ;
(f) Fournir les informations nécessaires au Global Chief Privacy Officer pour compléter le rapport annuel sur le respect de la protection des Données ;
(g) Aider le Global Chief Privacy Officer en cas d’enquêtes ou demandes officielles émanant d’autorités gouvernementales ;
(h) Élaborer et publier des politiques et des normes régionales appropriées en fonction de leurs régions ou organisations respectives ;
(i) Conseiller les Sociétés du Groupe sur la conservation et la destruction des données ;
(j) Informer le Global Chief Privacy Officer des plaintes et aider à la résolution de ces plaintes ; et
(k) Fournir une assistance au Global Chief Privacy Officer, aux autres membres du Privacy Network, aux Privacy Stewards et à d’autres intervenants, selon les besoins, afin de :
    (1) Permettre aux Sociétés ou Organisations du Groupe de respecter le Code à l’aide des instructions, outils et formations mis au point ;
    (2) Partager les bonnes pratiques en matière de protection de la vie privée et des Données dans la région ;
    (3) Confirmer que les exigences en matière de respect de la vie privée et de protection des Données sont prises en compte chaque fois que de nouveaux produits et services sont mis en œuvre dans les Sociétés ou organisations du Groupe ; et
    (4) Aider les Privacy Stewards, les Sociétés du Groupe, les unités opérationnelles et les domaines fonctionnels, ainsi que le personnel du service Achats en matière de recours à des Sous-traitants.

Privacy Stewards **8.3** Les Privacy Stewards sont des cadres d’ADP qui ont été nommés par un Cadre Responsable et/ou la Haute Direction d’ADP pour mettre en œuvre et faire respecter le Code au sein d’une unité opérationnelle ou d’un domaine fonctionnel d’ADP. Les Privacy Stewards sont responsables de la mise en œuvre effective du Code au sein de l’unité opérationnelle ou du domaine fonctionnel concerné(e). En particulier, les Privacy Stewards doivent s’assurer que des contrôles efficaces de la gestion de la protection de la vie privée et des Données soient intégrés dans toutes les pratiques commerciales ayant un impact sur les Données Client et que des ressources et un budget suffisants soient disponibles pour satisfaire aux obligations du présent Code. Les Privacy Stewards peuvent déléguer des tâches et doivent affecter des ressources appropriées, au besoin, pour exercer leurs responsabilités et atteindre les

objectifs en matière de conformité.

Les responsabilités des Privacy Stewards comprennent les tâches suivantes :

(a) Surveiller la gestion de la protection de la vie privée et des Données, ainsi que son respect au sein de leur Société du Groupe, unité opérationnelle ou domaine fonctionnel, et s'assurer que tous les processus, systèmes et outils mis au point par l'Équipe Global Data Privacy & Governance ont été effectivement mis en œuvre ;

(b) Confirmer que les tâches en matière de gestion et de respect de la protection de la vie privée et des Données sont déléguées de manière appropriée dans le cours normal des activités, ainsi que pendant et après les restructurations organisationnelles, les externalisations, les fusions et acquisitions, ainsi que les cessions ;

(c) Collaborer avec le Global Chief Privacy Officer et les membres concernés du Privacy Network pour comprendre les nouvelles obligations juridiques et y satisfaire, et vérifier que les processus de gestion de la protection de la vie privée et des Données sont mis à jour pour tenir compte des changements de circonstances et des obligations juridiques et réglementaires ;

(d) Consulter le Global Chief Privacy Officer et les membres concernés du Privacy Network dans tous les cas où il y a un conflit réel ou potentiel entre la Loi Applicable et le présent Code ;

(e) Surveiller les Sous-traitants employés par la Société du Groupe, l'unité opérationnelle ou le domaine fonctionnel afin de garantir le respect permanent du présent Code et des contrats de sous-traitance conclus avec ces Sous-traitants ;

(f) Confirmer que l'ensemble du Personnel de la Société du Groupe, de l'unité opérationnelle ou du domaine fonctionnel a suivi les cours de formation requis en matière de respect de la protection des Données ; et

(g) Ordonner que les Données Client stockées soient supprimées, détruites, anonymisées ou transférées conformément à l'Article 2.2.

Cadres Responsables

8.4 Les Cadres Responsables, en tant que responsables d'unités opérationnelles ou de domaines fonctionnels, sont chargés de s'assurer de la mise en œuvre d'une gestion efficace de la protection de la vie privée et des Données dans leurs organisations. Chaque Cadre Responsable (a) nommera des Privacy Stewards, (b) veillera à ce que des ressources et un budget suffisants soient disponibles pour assurer la conformité, et (c) apportera un soutien au Privacy Stewards en cas de nécessité pour combler les lacunes en matière de conformité et de gestion des risques.

Privacy Leadership Council **8.5** Le Global Chief Privacy Officer présidera un Privacy Leadership Council, composé des Privacy Stewards, des membres du Privacy Network sélectionnés par le Global Chief Privacy Officer et d'autres personnes pouvant contribuer à la mission du Council. Le Privacy Leadership Council créera et gérera un cadre opérationnel pour soutenir, le cas échéant, les tâches visant à permettre aux Sociétés du Groupes, unités opérationnelles et domaines fonctionnels de respecter le présent Code, pour entreprendre les tâches énoncées dans les présentes, et pour soutenir le Global Chief Privacy Officer.

Absence de membres du Privacy Network et de Privacy Stewards **8.6** Si, à un moment quelconque, il n'y a pas de Global Chief Privacy Officer nommé ou en mesure d'assurer les tâches attribuées à cette fonction, le General Counsel nommera une personne pour agir en qualité de Global Chief Privacy Officer intérimaire. Si, à un moment quelconque, il n'y a aucun membre du Privacy Network nommé pour une région ou une organisation donnée, le Global Chief Privacy Officer prendra à sa charge les tâches dudit membre du Privacy Network énoncées à l'Article 8.2.

Si, à un moment quelconque, il n'y a pas de Privacy Steward nommé pour une Société du Groupe, une unité opérationnelle ou un domaine fonctionnel, le Cadre Responsable nommera une personne appropriée pour exercer les tâches énoncées à l'Article 8.3.

Fonctions règlementaires **8.7** Lorsque des membres du Privacy Network, comme par exemple des responsables de la protection des données en vertu de la Loi Applicable pour l'EEE, sont nommés aux termes de la loi, ils exercent leurs responsabilités dans la mesure où elles n'entrent pas en conflit avec leurs fonctions règlementaires.

Article 9. – Politiques et procédures

Politiques et procédures **9.1** ADP élaborera et mettra en œuvre des politiques, des normes, des lignes directrices et des procédures pour être en conformité avec le présent Code.

Système d'information **9.2** ADP maintiendra à disposition les informations relatives à la structure et au fonctionnement de tous les systèmes et processus Traitant des Données Client, comme les inventaires des systèmes et des processus impactant les Données Client, ainsi que des informations générées dans le cadre des Analyses d'impact sur la protection des données (DPIA). Une copie de ces informations sera fournie sur demande au DPA Chef de file ou au DPA compétente pour le Client aux termes de l'Article 11.3.

Article 10. – Formation

Formation **10.1** ADP dispensera une formation sur les obligations et principes énoncés dans le présent Code, et sur toutes autres obligations en matière de respect de protection des Données et de sécurité des Données à tout le Personnel ayant accès aux Données Client ou exerçant des responsabilités liées au Traitement de Données Client.

Article 11. – Suivi et audits de conformité

Audits internes **11.1** ADP auditera les processus et procédures de nature commerciale qui impliquent le Traitement de Données des Clients afin de vérifier régulièrement leur conformité au présent Code. En particulier :

(a) Les audits pourront être effectués dans le cadre des activités régulières du département d'audit interne d'ADP (y compris par le recours à des Tiers indépendants), par d'autres équipes internes engagées dans des fonctions de contrôle et, sur demande *ad hoc* du Global Chief Privacy Officer ;

(b) Le Global Chief Privacy Officer peut également demander qu'un audit soit effectué par un auditeur externe et, selon le cas, il informera le Cadre responsable de l'unité métier concernée et/ou le Comité exécutif d'ADP ;

(c) Les normes professionnelles applicables en matière d'indépendance, d'intégrité et de confidentialité doivent être observées au cours du processus d'audit ;

(d) Le Global Chief Privacy Officer et le membre concerné du Privacy Network seront informés des résultats des audits ;

(e) Dans la mesure où l'audit révèle une violation du présent Code, ces résultats seront communiqués aux Privacy Stewards et aux Cadres Responsables concernés. Les Privacy Stewards coopéreront avec l'Équipe Global Data Privacy & Governance pour élaborer et mettre en œuvre un plan de remédiation approprié ;

(f) Une copie des résultats de l'audit lié au respect du présent Code sera remise sur demande au DPA Chef de file ou au DPA compétent, aux termes de l'Article 11.3.

Audit du Client **11.2** ADP traitera les demandes d'audit du Client comme décrit dans le présent Article 11.2. ADP répondra à toutes questions posées par le Client relatives au Traitement des Données Client par ADP. Dans le cas où le Client estime raisonnablement que les réponses fournies par ADP justifient une analyse plus approfondie, ADP devra, en accord avec le Client, soit :

(a) Rendre les installations qu'elle utilise pour le Traitement des Données Client disponibles pour un audit par un tiers évaluateur indépendant qualifié engagé par le Client, qu'ADP juge raisonnablement acceptable et couvert par des obligations de confidentialité satisfaisantes pour ADP. Le Client fournira une copie du rapport d'audit au Global Chief Privacy Officer, qui sera traité au même titre que les informations confidentielles d'ADP. Les audits auront lieu au maximum une fois par an, par Client, pendant la durée du Contrat de Service, pendant les heures de travail

normales, et seront soumis (i) à une demande écrite introduite auprès d'ADP au moins 45 jours avant la date proposée pour l'audit ; (ii) à un plan d'audit écrit et détaillé, examiné et approuvé par l'organisation de la sécurité d'ADP ; et (iii) aux politiques de sécurité sur site d'ADP. Ces audits n'auront lieu qu'en présence d'un représentant du bureau mondial de la Sécurité d'ADP, de l'Équipe Global Data Privacy & Governance d'ADP ou d'une personne désignée par le représentant approprié. Les audits ne pourront pas perturber les activités de Traitement d'ADP ni compromettre la sécurité et la confidentialité des Données à Caractère Personnel relatives à d'autres Clients d'ADP ; soit

(b) fournir au Client une déclaration émise par un Tiers évaluateur indépendant qualifié, certifiant que les processus et procédures commerciaux d'ADP impliquant le Traitement de Données Client sont conformes au présent Code.

ADP peut facturer aux Clients un prix raisonnable pour cet audit.

Le présent Article 11.2 s'ajoute ou clarifie les droits d'audit dont les Clients peuvent bénéficier en vertu de la Loi Applicable et des Contrats de Service. En cas de contradiction, les dispositions de la Loi Applicable et des Contrats de Service prévaudront.

Audits réalisés par les DPA

11.3 Tout DPA d'un pays de l'EEE compétente pour auditer un Client d'ADP sera autorisée à auditer le Transfert de Données concerné pour vérifier le respect du présent Code, aux mêmes conditions que celles applicables à un audit du Client réalisé par ce DPA dans le cadre de la Loi Applicable au Responsable du Traitement de Données.

En vue de faciliter cet audit :

(a) ADP et le Client collaboreront de bonne foi pour tenter de résoudre la demande en fournissant des informations au DPA, comme les rapports d'audit d'ADP, et faciliteront les discussions entre le DPA et les experts du Client et d'ADP en la matière, qui peuvent examiner les contrôles de sécurité, de confidentialité et des aspects opérationnels qui sont en place. Le Client aura accès à ses Données client conformément au Contrat de Service et pourra déléguer cet accès aux représentants du DPA ;

(b) Si les informations disponibles par le biais de ces mécanismes sont insuffisantes pour répondre aux objectifs de DPA, ADP fournira au DPA la possibilité de communiquer avec l'auditeur d'ADP ;

(c) Si cela s'avère encore insuffisant, ADP donnera au DPA un droit d'examiner directement les installations de Traitement de Données d'ADP utilisées pour Traiter les Données Client en respectant un préavis raisonnable, pendant les heures ouvrables, et dans le respect total de la confidentialité des informations obtenues et du secret des affaires. Le DPA ne peut accéder qu'aux Données Client appartenant au Client.

Le présent Article 11.3 s'ajoute ou clarifie les droits d'audit que pourraient avoir les DPA en vertu de la Loi Applicable et des Contrats de Service. En cas de divergence, les dispositions de la Loi Applicable prévaudront.

Rapport annuel **11.4** Le Global Chief Privacy Officer doit rédiger un rapport annuel relatif au respect du présent Code, au respect de la protection des Données, aux risques pour la protection des Données et à tous autres problématiques pertinentes, à destination du Comité Exécutif d'ADP. Ce rapport tiendra compte des informations fournies par le Privacy Network et d'autres personnes en rapport avec les évolutions régionales et des sujets spécifiques au sein des Sociétés du Groupe.

Atténuation des risques **11.5** ADP prendra des mesures appropriées pour remédier à tout cas de non-respect du présent Code identifié lors des audits.

Article 12. – Questions juridiques

Droits des Employés du Client **12.1** Si ADP enfreint les dispositions du présent Code en matière de Données à Caractère Personnel d'un Employé du Client, celui-ci peut, en tant que tiers bénéficiaire, se prévaloir des Articles 1.5, 1.6, 2.1, 2.2, 3, 5, 6, 7.1, 7.3, 7.4, 11.2, 11.3, 12.1, 12.2, 12.3, 12.5, 12.7, 12.8 et 14.3 du présent Code du Sous-traitant de Données, contre l'Entité Signataire d'ADP.

Dans la mesure où l'Employé du Client peut faire valoir l'un de ces droits contre l'Entité Signataire d'ADP, l'Entité Signataire d'ADP ne peut invoquer une violation de ses obligations par un Sous-traitant de second rang pour échapper à sa responsabilité juridique, sauf dans la mesure où la défense d'un Sous-traitant de second rang constituerait également une défense pour ADP. ADP peut toutefois invoquer toutes les exceptions ou droits qui auraient été à la disposition du Client. ADP peut également invoquer toutes les exceptions qu'ADP aurait pu opposer au Client (comme la négligence contributive), dans le cadre de la défense développée à l'encontre de la réclamation de l'Individu.

Procédure en cas de plainte **12.2** Les Employés du Client peuvent déposer une plainte écrite relative à toute réclamation au titre des dispositions de l'Article 12.1, auprès de l'équipe Global Data Privacy & Governance, par courrier ou par courriel expédié aux adresses respectives indiquées à la fin du présent Code. L'Employé du Client peut également déposer une plainte ou une réclamation auprès des autorités ou des tribunaux, conformément à l'Article 12.3 du présent Code.

L'équipe Global Data Privacy & Governance prendra en charge l'intégralité du traitement des plaintes/réclamations. Chaque plainte sera attribuée à un membre approprié du Personnel (soit au sein de l'équipe Global Data Privacy & Governance soit

au sein de l'unité opérationnelle ou du domaine fonctionnel). Ce membre du Personnel :

(a) Accusera réception de la plainte dans les plus brefs délais ;

(b) Analysera la plainte et, le cas échéant, ouvrira une enquête ;

(c) Si la plainte est fondée, il en informera le Privacy Steward concerné et le membre compétent du Privacy Network afin qu'un plan de remédiation puisse être élaboré et exécuté ; et

(d) Conservera une copie des dossiers de toutes les plaintes reçues, des réponses apportées et des mesures de remédiation prises par ADP.

ADP déploiera des efforts raisonnables pour résoudre les plaintes dans les meilleurs délais afin qu'une réponse soit donnée à l'Employé du Client dans un délai de quatre semaines suivant la date à laquelle la plainte a été déposée. La réponse sera apportée par écrit et envoyée à l'Employé du Client par la même voie de communication que celle initialement utilisée par l'Employé du Client pour prendre contact avec ADP (par exemple, par courrier ou par e-mail). La réponse décrira les mesures qu'ADP a prises pour enquêter sur la plainte et indiquera la décision d'ADP concernant les mesures (le cas échéant) qu'elle prendra à la suite de la plainte.

Dans le cas où ADP ne pourrait raisonnablement clore son enquête et apporter une réponse dans un délai de quatre semaines, elle informera l'Employé du Client dans le même délai que l'enquête est en cours et qu'une réponse sera apportée sous un délai supplémentaire de huit semaines.

Si l'Employé du Client juge insatisfaisante la réponse d'ADP à sa plainte (par exemple, si sa demande est rejetée), ou si ADP ne respecte pas les conditions de la procédure de plainte prévues au présent Article 12.2, l'Employé du Client pourra déposer une plainte ou une réclamation auprès des autorités ou des tribunaux, conformément aux dispositions de l'Article 12.3.

Compétence en matière de réclamations d'Employés du Client

12.3 Il est recommandé aux Employés du Client de suivre en premier lieu la procédure de plainte visée à l'Article 12.2 du présent Code, avant de déposer une plainte ou réclamation auprès des autorités ou des tribunaux.

Les Employés du Client peuvent, à leur discrétion, soumettre leurs réclamations aux termes de l'Article 12.1 en déposant une plainte auprès
(i) du DPA du pays où l'Employé a sa résidence habituelle, son lieu de travail ou du lieu où s'est produite l'infraction, à l'encontre soit de l'Entité Signataire d'ADP soit de l'Entité Déléguée d'ADP ; ou
(ii) du DPA Chef de file ou des tribunaux des Pays-Bas, mais, dans ce dernier cas, uniquement à l'encontre de l'Entité Déléguée d'ADP.

Les Employés du Client peuvent, à leur discrétion, soumettre leurs réclamations aux termes de l'Article 12.1 en déposant une plainte auprès

(i) des tribunaux du pays où ils ont leur résidence habituelle, ou encore du pays d'origine du transfert des Données en vertu du présent Code, à l'encontre soit de l'Entité Signataire d'ADP soit de l'Entité Déléguée d'ADP ; ou
(ii) du DPA Chef de file ou des tribunaux des Pays-Bas, mais, dans ce dernier cas, uniquement à l'encontre de l'Entité Déléguée d'ADP.

Les DPA et les tribunaux doivent appliquer aux litiges leurs droits matériels et procéduraux. Le choix effectué par l'Employé du Client ne portera pas atteinte aux droits matériels ou procéduraux dont les parties peuvent bénéficier en vertu de la Loi Applicable.

Droits des Clients

12.4 Le Client peut faire valoir le présent Code contre (i) l'Entité Signataire d'ADP ou (ii) l'Entité Déléguée d'ADP devant le DPA Chef de file ou les tribunaux des Pays-Bas, mais seulement si l'Entité Signataire d'ADP n'est pas établie dans un pays de l'EEE. L'Entité Déléguée d'ADP veillera à ce que des mesures adéquates soient prises pour remédier aux violations du présent Code par l'Entité Signataire d'ADP ou toute autre Société du Groupe concernée.

L'Entité Signataire d'ADP et l'Entité Déléguée d'ADP ne peuvent invoquer une violation de leurs obligations par une autre Société du Groupe ou par un Sous-traitant pour échapper à leur responsabilité juridique, sauf dans la mesure où la défense de cette Société du Groupe ou de ce Sous-traitant constituerait également un moyen de défense pour ADP.

Recours disponibles, limitations des dommages, charge de la preuve pour les Employés du Client

12.5 Dans le cas où un Employé du Client introduirait une demande de dommages-intérêts en vertu de l'Article 12.1, l'Employé du Client aura droit à une réparation des dommages dans les conditions prévues par la loi en vigueur dans l'EEE.

Si des Employés d'un Client introduisent une demande de dommages-intérêts en vertu de l'Article 12.1, il incombera aux Employés du Client d'établir la preuve qu'ils ont subi des dommages et que ces dommages sont survenus en raison d'une violation du présent Code. Par la suite, l'Entité Signataire d'ADP (ou l'Entité Déléguée d'ADP, selon le cas) aura la charge de prouver que les dommages subis par les Employés du Client en raison d'une violation du présent Code ne sont pas imputables à la Société du Groupe concernée ou à un Sous-traitant, ou de faire valoir tous autres moyens de défense applicables.

Réparation pour le Client

12.6 En cas de violation du présent Code, et sous réserve des dispositions applicables du Contrat de Service, les Clients auront droit à une réparation des dommages directs, conformément aux dispositions du Contrat de Service.

Assistance mutuelle

12.7 Toutes les Sociétés du Groupe coopéreront et s'entraideront, au besoin et dans la mesure du possible, pour (a) répondre à la gestion d'une demande, d'une plainte ou d'une réclamation introduite par un Client ou un Employé du Client, ou (b) se conformer à une enquête licite ou une demande de renseignements conduite ou introduite par une autorité gouvernementale

compétente.

La Société du Groupe qui reçoit une demande d'informations conformément à l'Article 6.1 ou une demande au titre de plainte ou de réclamation en vertu de l'Article 12.2 ou 12.3, est responsable de la gestion des communications avec le Client ou avec l'Employé du Client relatives à la demande ou à la réclamation, sauf si les circonstances l'exigent autrement, ou selon les directives de l'Équipe Global Data Privacy & Governance.

Avis et décisions contraignantes du DPA

12.8 ADP collaborera de bonne foi et déploiera tous les efforts raisonnables pour suivre les avis émis par le DPA Chef de file et le DPA compétent, aux termes de l'Article 12.3, sur l'interprétation et l'application du présent Code. ADP se conformera aux décisions contraignantes prises par les DPA compétentes.

Droit applicable au présent Code

12.9 Le présent Code sera régi et interprété conformément au droit néerlandais.

Article 13. – Sanctions en cas de non-respect

Non-respect

13.1 Le non-respect du présent Code par le Personnel pourra entraîner toutes mesures disciplinaires ou contractuelles appropriées conformément à la Loi Applicable et aux politiques d'ADP, pouvant aller jusqu'à la cessation de la relation ou du contrat de travail.

Article 14. – Conflits entre le présent Code et la Loi Applicable au Sous-traitant du Traitement de

Données

Conflit entre le présent Code et la loi

14.1 En cas de conflit entre la Loi Applicable au Sous-traitant du Traitement de Données et le présent Code, le Cadre Responsable ou le Privacy Steward consultera le Global Chief Privacy Officer, le ou les membre(s) concerné(s) du Privacy Network (le cas échéant), et le département juridique de l'unité opérationnelle pour déterminer la façon de respecter le présent Code et de résoudre le conflit dans la mesure du possible, compte tenu des obligations légales pesant sur ADP.

Nouvelles obligations juridiques contradictoires

14.2 Les membres du département juridique, les directeurs de la sécurité commerciale d'ADP et les Privacy Stewards informeront dans les plus brefs délais l'Équipe Global Data Privacy & Governance de toutes nouvelles obligations juridiques dont ils ont connaissance et qui peuvent interférer avec la capacité d'ADP d'être en conformité avec le présent Code.

Les Privacy Stewards concernés, en concertation avec le département juridique, informeront dans les plus brefs délais les Cadres Responsables de toute nouvelle obligation juridique susceptible d'interférer avec la capacité d'ADP d'être en conformité avec le présent Code.

Reporting au DPA Chef de file

14.3 Si ADP apprend que la Loi Applicable au Sous-traitant du Traitement de Données ou que toute modification de la Loi Applicable au Sous-traitant du Traitement de Données est susceptible d'affecter de façon substantielle la capacité d'ADP à répondre à ses obligations en vertu des Articles 3.1, 3.2 ou 11.3, ADP en informera le DPA Chef de file.

Article 15. – Modifications apportées au présent Code

Approbation des modifications **15.1** Toute modification substantielle apportée au présent Code nécessite l'approbation préalable du Global Chief Privacy Officer et du General Counsel, et son adoption par le Comité Exécutif d'ADP ; elle sera communiquée ensuite aux différentes sociétés du Groupe. Des modifications non substantielles peuvent être apportées au présent Code avec l'approbation préalable du Global Chief Privacy Officer. L'Entité Déléguée d'ADP informera chaque année le DPA Chef de file des modifications apportées au présent Code.
Si une modification apportée au présent Code a un impact significatif sur les conditions de traitement des Services Client, ADP en informera dans les plus brefs délais le DPA Chef de file, en incluant une brève explication des raisons de cette modification, et informera aussi le Client de la modification apportée. Dans les 30 jours suivant la réception de cette information, le Client pourra s'opposer à cette modification en communiquant un avis écrit à ADP. Si les parties ne parviennent pas à s'entendre sur une solution mutuellement acceptable, ADP déploiera une solution alternative de transfert de données. Si aucune solution alternative de transfert de données ne peut être déployée, le Client aura le droit, aux termes du présent Code, de suspendre le transfert correspondant des Données Client à ADP. Si la suspension des transferts de données n'est pas possible, ADP devra permettre au Client de résilier les Services Client pertinents, aux termes du Contrat de Service.

Date d'entrée en vigueur des modifications **15.2** Toute modification entrera en vigueur avec effet immédiat après son approbation conformément à l'Article 15.1, sa publication sur le site Web www.adp.com et sa communication aux Clients.

Versions antérieures **15.3** Toute demande, plainte ou réclamation d'un Employé du Client au sujet du présent Code sera examinée au regard de la version du présent Code en vigueur au moment de l'introduction de la demande, plainte ou réclamation.

Article 16. – Mise en œuvre et périodes transitoires

Mise en œuvre **16.1** La mise en œuvre du présent Code sera supervisée par les Privacy Stewards, avec l'aide de l'Équipe Global Data Privacy & Governance. Sauf indication figurant ci-dessous, une période transitoire de dix-huit mois à partir de la Date d'Entrée en vigueur (indiquée à l'Article 1.6) s'appliquera au respect du présent Code.

Par conséquent, sauf indication contraire, dans un délai de dix-huit mois à compter de la Date d'Entrée en vigueur, tout Traitement de Données Client devra s'effectuer dans le respect du présent Code, et le Code sera pleinement en vigueur. Au cours de la période transitoire, le Code entrera en vigueur pour une Société du Groupe dès que celle-ci aura mené à bien les tâches nécessaires à sa mise en œuvre complète et qu'elle en aura expressément informé le Global Chief Privacy Officer.

Nouvelles Sociétés du Groupe **16.2** Toute entité qui devient une Société du Groupe après la Date d'Entrée en vigueur doit se conformer au présent Code dans les deux ans suivant son entrée dans le Groupe.

Entités Cédées **16.3** Une Entité Cédée restera couverte par le présent Code après sa cession pendant la période imposée par ADP pour distinguer le Traitement des Données Client relatif à une telle Entité Cédée.

Période transitoire pour les contrats existants **16.4** Lorsqu'il existe des contrats avec des Sous-traitants de second rang ou d'autres Tiers concernés par le présent Code, les dispositions des contrats prévaudront jusqu'à ce que les contrats soient renouvelés selon le cours normal des activités, à condition, toutefois, que tous ces contrats existants soient conformes au présent Code dans les 18 mois suivant la Date d'Entrée en vigueur.

Coordonnées

Équipe Global Data Privacy & Governance d'ADP : privacy@adp.com

Entité Déléguée d'ADP
ADP Nederland B.V.
Lylantse Baan 1, 2908
LG CAPELLE AAN DEN IJSSEL
PAYS-BAS

Interprétations

INTERPRÉTATION DU PRÉSENT CODE :

i. Sauf exigence contraire dictée par le contexte, toutes les références à un article ou une annexe en particulier sont des références à cet article ou annexe figurant au présent document, qui peuvent être modifié(e)s de temps à autre ;
ii. Les titres ne sont inclus que pour des raisons de commodité et ne doivent pas être utilisés pour interpréter une disposition quelconque du présent Code ;
iii. Si un mot ou une expression a été défini(e), ses autres formes grammaticales ont une signification correspondante ;
iv. La forme masculine comprendra la forme féminine ;
v. Les mots « comprendre », « comprend », « comprenant » et tout mot qui les suit, devront être interprétés sans limitation de la généralité de tout mot ou concept qui les précède et vice versa ;
vi. Le mot « écrit » comprendra tout(e) communication documentée, écrit, contrat, dossier électronique, signature électronique, télécopie ou tout autre instrument légalement valable et exécutoire sans égard pour son format ;
vii. Une référence à un document (y compris, notamment, une référence au présent Code) est une référence au document tel que modifié, complété ou remplacé, sauf dans la mesure où c'est interdit par le présent Code ou le document référencé ; et
viii. Une référence à la loi comprend toute exigence réglementaire,

recommandation sectorielle et bonne pratique publiée par les autorités de surveillance nationales et internationales compétentes ou d'autres organismes.

ANNEXE 1 – Définitions des Règles d'entreprise contraignantes (BCR)

Terme	Définition
Activités de Support aux Clients	ACTIVITÉS DE SUPPORT AUX CLIENTS signifie les activités de Traitement entreprises par ADP pour soutenir la fourniture de ses produits et services. Les Activités de support aux Clients peuvent consister, par exemple, à former des Professionnels, à répondre à des questions sur les services, à ouvrir et résoudre des tickets de support, à fournir des informations sur les produits et services (y compris des mises à jour et des alertes en matière de conformité), à contrôler et surveiller la qualité, et à mener toutes activités connexes qui facilitent l'utilisation efficace des produits et services d'ADP.
ADP (Groupe ADP)	ADP (le GROUPE ADP) signifie, collectivement, Automatic Data Processing, Inc. (la société mère) et les Sociétés du Groupe, y compris ADP, Inc.
Analyse d'impact relative à la protection des données (DPIA)	ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (DPIA) signifie une procédure pour mener et documenter une analyse préalable de l'impact qu'un Traitement donné peut avoir sur la protection des Données à Caractère Personnel , lorsque ledit Traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des Individus, notamment lorsque de nouvelles technologies sont utilisées. Un DPIA comprend : 1. une description : a. de la portée et du contexte du Traitement ; b. des Finalités commerciales pour lesquelles les Données à caractère personnel font l'objet d'un Traitement ; c. des finalités spécifiques pour lesquelles des Catégories Particulières de Données font l'objet du Traitement ; d. des catégories de destinataires des Données à Caractère Personnel, y compris les destinataires non couverts par une Décision d'adéquation ; e. des durées de conservation des Données à Caractère Personnel ; 2. une évaluation : a. de la nécessité et de la proportionnalité du Traitement ; b. des risques pour les droits et libertés des personnes concernées ; et les mesures pour atténuer ces risques, y compris les garanties, mesures de sécurité et autres mécanismes (tels que la protection dès la conception) visant à assurer la protection des Données à Caractère Personnel.
Archives	ARCHIVES désigné un ensemble Données à Caractère Personnel lorsqu'elles ne sont plus nécessaires pour atteindre les finalités pour lesquelles les Données ont été initialement recueillies ou qui ne sont plus utilisées pour des activités commerciales, mais qui pourraient potentiellement être utilisées à des fins historiques, scientifiques ou statistiques, de règlement de litiges, d'enquêtes ou à des fins générales d'archivage. L'accès aux Archives est limité aux administrateurs système et à d'autres personnes dont la fonction nécessite expressément un accès aux Archives.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. est la société mère du Groupe ADP. Il s'agit d'une société du Delaware (États-Unis), ayant son principal siège d'exploitation One ADP Boulevard, Roseland, New Jersey, 07068-1728, États-Unis.

Autorité de Protection des Données ou DPA	AUTORITÉ DE PROTECTION DES DONNÉES, ou DPA, signifie toute autorité réglementaire ou de surveillance qui supervise la protection des données ou le respect de la vie privée dans un pays dans lequel une Société du Groupe est établie.
Cadre Responsable	CADRE RESPONSABLE désigne le Directeur général d'une Société du Groupe ou le responsable d'une unité opérationnelle ou d'un domaine fonctionnel, qui est responsable du budget pour la Société du Groupe, l'unité opérationnelle ou le domaine fonctionnel.
Candidat	CANDIDAT signifie tout Individu qui fournit des Données à Caractère Personnel à ADP dans le cadre d'une candidature pour un poste chez ADP en qualité de Collaborateur.
Catégories Particulières de Données	CATÉGORIES PARTICULIÈRES DE DONNÉES signifie les Données à Caractère Personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques ou l'appartenance à des partis politiques ou à des organisations similaires, les convictions religieuses ou philosophiques, l'appartenance à une organisation professionnelle, commerciale ou syndicale, la santé physique ou mentale, y compris toute opinion à ce sujet, des handicaps, le code génétique, les addictions, la vie sexuelle, les infractions pénales, le casier judiciaire ou les procédures relatives à un comportement criminel ou illicite d'un Individu.
Client	CLIENT signifie tout Tiers qui utilise un ou plusieurs produits ou services d'ADP dans le cadre de ses propres activités.
Code	CODE signifie (selon le cas) le Code d'ADP relatif à la protection des Données commerciales, le Code d'ADP relatif à la protection des Données sur le lieu de travail (interne à ADP) et le Code d'ADP relatif à la protection des Données pour le Traitement des Données Client – collectivement dénommés les Codes.
Collaborateur	COLLABORATEUR signifie un Candidat, un employé actuel d'ADP ou un ancien employé d'ADP, à l'exception d'un Individu Co-employé. REMARQUE : Le Code d'ADP relatif à la protection des Données sur le lieu de travail ne s'applique par conséquent pas au Traitement de Données à Caractère Personnel des Individus Co-employés.
Comité Exécutif d'ADP	COMITÉ EXÉCUTIF D'ADP signifie le comité de direction comprenant (i) le président-directeur général (CEO) d'Automatic Data Processing, Inc., et (ii) les autres dirigeants qui relèvent directement du CEO et qui sont, collectivement, responsables des activités du Groupe ADP.
Consommateur	CONSOMMATEUR signifie un Individu qui interagit directement avec ADP à titre personnel. Par exemple, les Consommateurs comprennent des individus qui participent à des programmes de développement de talents ou qui utilisent des produits et services d'ADP pour leur usage personnel (c.-à-d. en dehors d'une relation d'emploi avec ADP ou un Client d'ADP).
Contrat de Services	CONTRAT DE SERVICES signifie tout contrat, accord ou conditions en vertu desquels ADP fournit des Services client à un Client.
Contrat de Sous-traitance	CONTRAT DE SOUS-TRAITANCE signifie tout contrat de Traitement de Données à Caractère Personnel conclu par ADP et un Tiers Sous-traitant.

Contrat de Sous-traitance de second rang	CONTRAT DE SOUS-TRAITANCE DE SECOND RANG signifie un accord écrit ou électronique entre ADP et un Tiers Sous-traitant conformément à l'article 7.1 du Code relatif à la protection des Données pour le traitement des Données Client.
Coordonnées Commerciales	COORDONNÉES COMMERCIALES signifie toutes données relatives à un Professionnel que l'on trouve généralement sur une carte de visite professionnelle ou dans une signature d'e-mail.
Date d'entrée en vigueur	DATE D'ENTRÉE EN VIGUEUR signifie la date à laquelle les Codes entrent en vigueur tel qu'énoncé à l'article 1 des Codes.
Décision d'Adéquation	DÉCISION D'ADÉQUATION signifie toute décision prise par une Autorité de protection des données ou tout autre organe compétent, indiquant qu'un pays, une région ou un destinataire d'un transfert de données est réputé fournir un niveau de protection adéquat pour les Données à Caractère Personnel. Les entités visées par une Décision d'adéquation comprennent les destinataires situés dans des pays qui, en vertu de la Loi applicable, sont réputés fournir un niveau de protection adéquat des données, ainsi que les destinataires qui sont liés par un autre instrument (par exemple, un ensemble de Règles d'entreprise contraignantes) qui ont été approuvés par l'Autorité de protection des données compétente ou tout autre organisme compétent. En ce qui concerne les États-Unis, les entreprises qui sont certifiées dans le cadre d'un accord sur la protection des données US/EEE et/ou US/Suisse seraient couvertes par une Décision d'adéquation.
Données à Caractère Personnel ou Données	DONNÉES À CARACTÈRE PERSONNEL ou DONNÉES signifie toute information relative à un Individu identifié ou identifiable. Les Données à Caractère Personnel peuvent aussi être dénommées, informations personnelles dans les politiques et les normes que mettent en œuvre les Codes.
Données Client	DONNÉES CLIENT signifie les Données à Caractère Personnel relatives aux Employés du Client (y compris les employés potentiels, les anciens employés et les personnes à charge des employés) faisant l'objet d'un Traitement par ADP dans le cadre de la prestation de Services client.
DPA Chef de file	Le DPA CHEF DE FILE signifie l'autorité néerlandaise de protection des données.
Droit applicable de l'EEE	DROIT APPLICABLE de l'EEE signifie les exigences des Lois Applicables de l'EEE, qui s'appliquent à toutes les Données à Caractère Personnel qui sont collectées initialement dans le contexte des activités d'une Société du Groupe établie dans l'EEE (également après avoir été transférées à une autre Société du Groupe établie en dehors de l'EEE).
EEE	Les termes EEE ou ESPACE ÉCONOMIQUE EUROPÉEN se définissent comme tous les états membres de l'Union européenne, auxquels d'ajoutent la Norvège, l'Islande, le Liechtenstein et, aux fins des présents codes, la Suisse et le Royaume-Unis après sa sortie de l'Union Européenne. Conformément à la décision de l'avocat général, qui sera publiée sur le site Web www.adp.com, ces termes peuvent englober d'autres pays dont les lois sur la protection des données comportent des restrictions de transfert de données semblables à celles de l'EEE.

Employé du Client	EMPLOYÉ DU CLIENT signifie tout Individu dont les Données à Caractère Personnel font l'objet d'un Traitement par ADP en tant que Sous-traitant du Traitement de données pour le compte d'un Client en vertu d'un Contrat de services. Par souci de clarté, EMPLOYÉ DU CLIENT renvoie à tous les Individus dont les Données à Caractère Personnel font l'objet d'un Traitement par ADP pour la fourniture de Services client (quelle que soit la nature juridique de la relation entre l'Individu et le Client). Cette notion ne comprend pas les Professionnels dont les Données à Caractère Personnel font l'objet d'un Traitement par ADP dans le cadre de la relation directe d'ADP avec le Client. Par exemple, ADP peut procéder au Traitement des Données à Caractère Personnel d'un Professionnel des ressources humaines afin de conclure un contrat avec le Client ; ces données sont soumises au Code d'ADP relatif à la protection des Données commerciales. Toutefois, lorsqu'ADP fournit des services de Traitement de données de rémunération au Client (par exemple, émet des bulletins de paie ou fournit une assistance pour l'utilisation d'un système d'ADP), les données de l'Individu font l'objet d'un Traitement comme s'il s'agissait de Données client.
Enfants	Aux fins de collecte de données et de prospection d'ADP, ENFANTS signifie des Individus dont l'âge est inférieur à celui défini par la Loi applicable pour donner leur consentement à cette collecte de données et/ou toute opération marketing.
Entité Cédée	ENTITÉ CÉDÉE signifie une Société du Groupe qui n'est plus détenue par ADP à la suite de la vente d'actions et/ou d'actifs de la société, ou autre cession, de sorte que la société ne répond plus aux critères correspondant à ceux d'une Société du Groupe.
Entité Déléguée d'ADP	ENTITÉ DÉLÉGUÉE D'ADP signifie ADP Nederland B.V., ayant son siège social à Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Pays-Bas.
Entité Signataire d'ADP	ENTITÉ SIGNATAIRE D'ADP signifie la Société du Groupe qui a conclu un contrat, tel qu'exigé par les Codes, comme un Contrat de services, un Contrat de Sous-traitance de second rang ou un accord de transfert de données.
Équipe Global Data Privacy & Governance	L'équipe GLOBAL DATA PRIVACY & GOVERNANCE signifie l'Office of Privacy and Data Governance d'ADP. L'Office of Privacy and Data Governance est dirigé par le Global Chief Privacy Officer et comprend des privacy officers, des privacy managers et d'autres Personnels qui dépendent du Global Chief Privacy Officer ou des privacy officers ou des privacy managers.
Finalité Commerciale	FINALITÉ COMMERCIALE signifie une finalité légitime pour le Traitement de Données à Caractère Personnel conformément aux articles 2, 3 ou 4 de tout Code d'ADP, ou pour le Traitement de Catégories particulières de données visées à l'article 4 de tout code d'ADP.
Finalité Secondaire	FINALITÉ SECONDAIRE signifie toute finalité autre que la finalité initiale pour laquelle les Données à Caractère Personnel font l'objet d'un Traitement.
Fournisseur	FOURNISSEUR signifie tout Tiers qui fournit des biens ou des services à ADP (par exemple, en tant que fournisseur de services, agent, Sous-traitant du Traitement de données, consultant ou fournisseur).
General Counsel	GENERAL COUNSEL signifie le General Counsel d'Automatic Data Processing, Inc.

Global Chief Privacy Officer	GLOBAL CHIEF PRIVACY OFFICER signifie le Collaborateur d'ADP qui porte ce titre chez Automatic Data Processing, Inc.
Individu	INDIVIDU signifie toute personne physique identifiée ou identifiable dont les Données à Caractère Personnel font l'objet d'un Traitement par ADP, à titre soit de Sous-traitant du Traitement de Données, soit de Responsable du Traitement de Données, à l'exception des Individus Co-employés. REMARQUE : Le Code d'ADP relatif à la protection des Données commerciales et le Code d'ADP relatif à la protection des Données sur le lieu de travail ne s'appliquent par conséquent pas au Traitement des Données à Caractère Personnel des Personnes Co-employées.
Individu Co-employé	INDIVIDU CO-EMPLOYÉ signifie un employé d'un Client aux États-Unis qui est co-employé par une société affiliée américaine indirecte d'Automatic Data Processing, Inc. dans le cadre de l'offre de services d'organisation employeur aux États-Unis.
Intérêt Prépondérant	INTÉRÊT PRÉPONDÉRANT signifie les intérêts impérieux énoncés à l'article 13.1 du Code d'ADP relatif à la protection des Données sur le lieu de travail et du Code d'ADP relatif à la protection des Données commerciales, sur la base desquels les obligations d'ADP ou les droits d'Individus visés aux articles 13.2 et 13.3 des Codes peuvent, dans des circonstances spécifiques, être supplantés si cet intérêt impérieux l'emporte sur l'intérêt de l'Individu.
Limitation au transfert de Données de l'EEE	LIMITATION AU TRANSFERT DE DONNÉES DE L'EEE signifie toute limitation concernant les transferts transfrontaliers de Données à Caractère Personnel en vertu des lois de protection des données d'un pays de l'EEE.
Loi Applicable	LOI APPLICABLE signifie toute loi sur la protection de la vie privée ou des données qui est applicable à toute activité de Traitement de données.
Loi Applicable au Responsable du Traitement de Données	Aux fins du Code d'ADP relatif à la protection des Données pour le traitement des Données Client, LOI APPLICABLE AU RESPONSABLE DU TRAITEMENT DE DONNÉES signifie toute loi sur la protection de la vie privée ou des données qui est applicable à un Client d'ADP en tant que Responsable du Traitement de ces Données client.
Loi applicable au Sous-traitant du Traitement de Données	Aux fins du Code d'ADP relatif à la protection des Données pour le traitement des Données Client, LOI APPLICABLE AU SOUS-TRAITANT DE DONNÉES signifie toute loi sur la protection de la vie privée ou des données qui est applicable à ADP en tant que Sous-traitant du Traitement de données, pour le compte d'un Client qui est Responsable du Traitement de données.
Partenaire Commercial	PARTENAIRE COMMERCIAL signifie tout Tiers, autre qu'un Client ou un Fournisseur, qui a ou avait une relation d'affaires ou une alliance stratégique avec ADP (par exemple, partenaire commercial conjoint, co-entreprise ou partenaire de développement conjoint).
Personne à charge	PERSONNE À CHARGE signifie le conjoint, le partenaire, l'enfant ou toute autre personne à charge, ou la personne à contacter en cas d'urgence d'un Collaborateur ou d'un Travailleur Externe.
Personnel	PERSONNEL signifie, collectivement, les Collaborateurs actuellement employés par ADP et les Employés externes qui travaillent actuellement pour ADP.

Prescriptions Obligatoires	PRESCRIPTIONS OBLIGATOIRES signifie les obligations résultant de toute Loi applicable au Sous-traitant du Traitement de Données, qui nécessitent le Traitement de Données à Caractère Personnel pour (i) la sécurité ou défense nationale ; (ii) la sûreté publique ; (iii) la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou de violations de la déontologie des professions réglementées ; ou (iv) la protection de tout Individu ou des droits et libertés des Individus.
Privacy Leadership Council	PRIVACY LEADERSHIP COUNCIL signifie le conseil dirigé par le Global Chief Privacy Officer et comprenant des Privacy Stewards, des membres du Privacy Network choisis par le Global Chief Privacy Officer, et d'autres personnes qui pourraient s'avérer nécessaires pour aider à la mission du conseil.
Privacy Network	PRIVACY NETWORK signifie les membres de l'Équipe Global Data Privacy and Governance et d'autres membres du service Legal, y compris les professionnels responsables de la conformité et les délégués à la protection des données chargés de la conformité en matière de protection des données au sein de leur région, pays, unité opérationnelle ou domaine fonctionnel respectif.
Privacy Steward	PRIVACY STEWARD signifie un cadre d'ADP qui a été nommé par un Cadre Responsable et/ou la Haute Direction d'ADP pour mettre en œuvre et faire respecter les codes relatifs à la protection des données au sein d'une Unité opérationnelle d'ADP.
Professionnel	PROFESSIONNEL signifie tout Individu (autre qu'un employé) qui interagit directement avec ADP à titre professionnel ou commercial. Par exemple, les Professionnels comprennent le personnel des RH des Clients en relation avec ADP en tant qu'utilisateurs de produits ou services d'ADP. Les Professionnels comprennent également les représentants de comptes de Clients, de Fournisseurs et de Partenaires commerciaux, les contacts commerciaux, les contacts d'associations commerciales, les régulateurs, les contacts dans les médias et d'autres Individus qui interagissent avec ADP à titre commercial.
Règles d'Entreprise Contraignantes	RÈGLES D'ENTREPRISE CONTRAIGNANTES signifie une politique en matière de protection des données d'un groupe de sociétés affiliées visant à fournir un niveau de protection adéquat pour le transfert de Données à Caractère Personnel au sein de ce groupe de sociétés en vertu de la Loi applicable.
Responsable du Traitement de Données	RESPONSABLE DU TRAITEMENT DE DONNÉES signifie l'entité ou la personne physique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement des Données à Caractère Personnel.
Services Client	SERVICES CLIENT signifie les services de gestion du capital humain fournis par ADP aux Clients, comme le recrutement, les services de paie, les avantages sociaux des employés, la gestion des talents, l'administration des ressources humaines, le conseil et l'analyse, et les services de retraite.
Société du Groupe	SOCIÉTÉ DU GROUPE signifie toute entité juridique qui est une filiale d'Automatic Data Processing, Inc. et/ou d'ADP, Inc., si Automatic Data Processing, Inc., ou ADP, Inc. détient, directement ou indirectement, plus de 50 % du capital social émis, détient 50 % ou plus des droits de vote aux assemblées générales des actionnaires, détient le pouvoir de nommer la majorité des administrateurs ou dirige autrement les activités d'une telle entité juridique.

Sous-traitant de second rang d'ADP	Aux fins du Code d'ADP relatif à la protection des Données pour le traitement des Données Client, un SOUS-TRAITANT DE SECOND RANG D'ADP signifie toute Société du Groupe engagée par une autre Société du Groupe en tant que Sous-traitant de second rang des Données client.
Sous-traitant du Traitement de Données	SOUS-TRAITANT DU TRAITEMENT DE DONNÉES signifie l'entité ou la personne physique qui procède au Traitement des Données à Caractère Personnel pour le compte d'un Responsable du Traitement de données.
Sous-traitant Interne	SOUS-TRAITANT INTERNE désigne toute Société du Groupe qui procède au Traitement de Données à Caractère Personnel pour le compte d'une autre Société du Groupe qui est le Responsable du Traitement de Données.
Sous-traitants de second rang	SOUS-TRAITANTS DE SECOND RANG signifie, collectivement, les Sous-traitants de second rang d'ADP et les Tiers Sous-traitants de second rang.
Tiers	TIERS signifie toute personne, organisation privée ou organisme gouvernemental qui n'est pas une Société du Groupe.
Tiers Responsable du Traitement	TIERS RESPONSABLE DU TRAITEMENT signifie un Tiers qui procède au Traitement de Données à Caractère Personnel et détermine les finalités et les moyens du Traitement.
Tiers Sous-traitant de second rang	TIERS SOUS-TRAITANT DE SECOND RANG signifie tout Tiers engagé par ADP en tant que Sous-traitant de second rang.
Tiers Sous-traitant du Traitement	TIERS SOUS-TRAITANT DU TRAITEMENT signifie un Tiers qui procède au Traitement de Données à Caractère Personnel pour le compte d'ADP et qui ne se trouve pas sous l'autorité directe d'ADP.
Traitement	TRAITEMENT signifie toute opération effectuée sur des Données à Caractère Personnel, que ce soit ou non par des moyens automatiques, comme la collecte, l'enregistrement, le stockage, l'organisation, la modification, l'utilisation, la divulgation (y compris l'octroi d'un accès à distance), la transmission ou la suppression de Données à Caractère Personnel.
Travailleur externe	TRAVAILLEUR EXTERNE signifie un Individu qui fournit des services à ADP (qui est soumis à la surveillance directe d'ADP) à titre provisoire ou non permanent, tels que des employés temporaires, des employés contractuels, des entrepreneurs indépendants ou des consultants.
Violation de la Sécurité des Données	VIOLATION DE LA SÉCURITÉ DES DONNÉES signifie tout incident ayant un impact sur la confidentialité, l'intégrité ou la disponibilité des Données à Caractère Personnel, comme la divulgation ou une utilisation non autorisée de Données à Caractère Personnel, ou l'accès non autorisé à des Données à Caractère Personnel, qui compromet la confidentialité ou la sécurité des Données à Caractère Personnel.

ANNEXE 2 – Mesures de sécurité

Présentation :	**ADP - Global Security Organization**
Version :	**2.0**
Publication :	**Septembre 2019**

Table des matières

Termes et définitions

Les termes suivants peuvent apparaître à la lecture du document :

Terme ou acronyme utilisé	Définition
GETS	**Global Enterprise Technology & Solutions**
GSO	**« Global Security Organization » (Organisation Mondiale de la Sécurité)**
CCC	**Comité consultatif sur les changements**
PRAS	**Plan de reprise après sinistre**
CIRC	**« Critical Incident Response Center » (Centre d'intervention en cas d'incident critique) de GSO**
SIEM	**« Security Information and Event Management » (Sécurité des informations et gestion des événements)**
SDI	**Système de détection des intrusions**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**« Service Organization Controls » (Contrôles de l'organisation des services)**
TPSI	**« Trusted Platform Security Infrastructure » (Infrastructure de sécurité des plateformes de confiance)**

Vue d’ensemble

ADP dispose d'un programme officiel de sécurité de l'information contenant des mesures de protection administratives, techniques et physiques, destinées à préserver la sécurité, la confidentialité et l'intégrité des informations de ses clients. Ce programme est conçu pour (i) protéger la sécurité et la confidentialité des informations des clients (ii) protéger et se protéger contre les risques ou les menaces pesant sur la sécurité ou l'intégrité des informations, et (iii) protéger et se protéger contre l’accès non-autorisé aux informations ou une utilisation de celles-ci non autorisée.

Ce document contient une vue d'ensemble des mesures et des pratiques destinées à assurer la sécurité des informations d'ADP à la date de publication de ce document. Ces mesures et pratiques sont susceptibles d'être modifiées par ADP et sont conçues pour être conformes aux normes de sécurité de l'information ISO/IEC 27001 :2013. ADP évalue régulièrement ses politiques et normes relatives à la sécurité. Notre objectif est d'aider à garantir que le programme de sécurité fonctionne de manière efficace et efficiente afin de protéger toutes les informations que nos clients et leurs employés nous confient.

Section 1 - Politique de Sécurité de l'Information

Indépendance de la fonction de sécurité de l'information

Le chef de la sécurité (Chief Security Officer) d'ADP supervise la Global Security Organization, l'Organisation mondiale de la sécurité (GSO) d'ADP et rend compte au Directeur Juridique (General Counsel) plutôt qu'au chef des services de l'information, ce qui confère à l'GSO l'indépendance nécessaire par rapport au service informatique. GSO est une équipe de sécurité centralisée qui a une approche multidisciplinaire en matière de conformité aux normes de sécurité de l'information et cybernétique, gestion du risque opérationnel, gestion de la sécurité des clients, protection de la main d'œuvre et résilience de l'entreprise. Les responsables GSO, sous la direction de notre chef de la sécurité, sont chargés de la gestion des politiques, procédures et directives relatives à la sécurité.

Définition officielle d'une politique de sécurité de l'information

ADP a élaboré et documenté des politiques de sécurité de l'information officielles qui définissent l'approche d'ADP en matière de gestion de la sécurité de l'information. Les domaines spécifiques couverts par cette politique comprennent, sans s'y limiter :

- **Politique de gestion de la sécurité** - présente les responsabilités de l'Organisation Mondiale de la sécurité (GSO) et du chef de la sécurité (CSO), y compris les responsabilités en matière de sécurité de l'information et les contrôles sur le processus d'embauche d'un point de vue sécurité.
- **Politique de confidentialité mondiale** - décrit la collecte de données personnelles, l'accès à ces dernières, leur exactitude, leur divulgation et les politiques de confidentialité relatives aux clients.
- **Politique des employés sur l'utilisation acceptable des communications électroniques et la protection des données** - décrit l'utilisation acceptable des différentes communications électroniques, du cryptage et de la gestion des clés.
- **Politique sur le traitement de l'information** - présente les exigences relatives à la classification des informations d'ADP et établit des contrôles permettant la protection de ces dernières.
- **Politique relative à la sécurité physique** - définit les exigences de sécurité des installations d'ADP et donc celles applicables aux visiteurs et aux employés qui y travaillent.
- **Politique de gestion des opérations de sécurité** - indique les contrôles minimaux pour maintenir les correctifs du système, traiter efficacement la menace des logiciels malveillants et contrôler la sécurité des sauvegardes et des bases de données.
- **Politique de surveillance de la sécurité** - fournit des contrôles pour les systèmes de détection d'intrusion, les journaux et la prévention des pertes de données.
- **Politique sur les enquêtes et la gestion des incidents** - définit des normes pour la réponse aux incidents, la découverte électronique, la protection de la main-d'œuvre, et l'accès aux données électroniques stockées des employés.
- **Politique sur l'accès et l'authentification** - présente les exigences en matière d'authentification (par exemple, nom d'utilisateur et mot de passe), d'accès à distance et d'accès sans fil.
- **Politique de sécurité réseau** - architecture de sécurité des routeurs, pare-feu, AD, DNS, serveurs de messagerie, DMZ, services infonuagiques, périphériques réseau, proxy Web et technologie de réseau commuté.
- **Politique d'assurance des vendeurs** - définit les contrôles minimaux de sécurité pour qu'une tierce partie puisse aider ADP à atteindre ses objectifs commerciaux.
- **Politique de gestion des applications** - établit des contrôles de sécurité appropriés à chaque étape du cycle de vie de développement du système.
- **Politique de résilience des activités** - régit la protection, l'intégrité et la préservation d'ADP en établissant les exigences minimales pour documenter, mettre en œuvre, maintenir et améliorer continuellement les programmes de résilience des activités.

- **Politique de gestion des risques centralisés** - identification, surveillance, réponse, analyse, gouvernance et nouvelles initiatives commerciales.

Ces politiques sont publiées sur le site intranet d'ADP et sont accessibles par tous les employés et prestataires au sein du réseau d'ADP.

Examen de la Politique de sécurité de l'information

ADP examine ses politiques de sécurité de l'information au moins une fois par an ou lors de tout changement majeur ayant un impact sur le fonctionnement des systèmes d'information d'ADP.

Section 2 - Organisation de la sécurité de l’information

GSO est une équipe de sécurité centralisée s'appuyant sur une approche multidisciplinaire en matière conformité aux normes de sécurité de l'information et cybernétique, gestion du risque opérationnel, gestion de la sécurité des clients, protection de la main d'œuvre, résilience de l’entreprise. Ses rôles et responsabilités ont été officiellement définis par tous les membres de GSO. GSO est chargé de la conception, de la mise en œuvre et de la surveillance de son programme de sécurité de l’information fondé sur les politiques de l'entreprise. Les activités de GSO sont supervisées par le Comité de direction sécurité, composé des chefs de la sécurité, du directeur général, du directeur financier, du directeur de la stratégie, du directeur des ressources humaines et du directeur juridique d'ADP.

Informatique mobile et politique de télétravail

ADP exige le cryptage de toutes les informations confidentielles sur les appareils mobiles pour éviter les fuites de données qui pourraient résulter du vol ou de la perte d'un ordinateur ou d'un appareil. Une protection avancée des terminaux et l'authentification à deux facteurs sur VPN sont également nécessaires pour accéder à distance aux réseaux de l'entreprise. Tous les appareils à distance doivent être protégés par un mot de passe. Les employés d'ADP doivent signaler toute perte ou tout vol d'appareil informatique distant à l'aide d'un processus de déclaration d'incident de sécurité.

Tous les employés et prestataires doivent se conformer à la politique sur l'utilisation acceptable des communications électroniques et la protection des données et d'autres politiques pertinentes. Il s’agit d’une condition de leur emploi.

Section 3 - Sécurité des Ressources Humaines

Vérifications des antécédents

Conformément aux exigences légales applicables dans le pays de l'employé, ADP réalise des vérifications des antécédents correspondant aux fonctions et aux responsabilités de ses employés, prestataires et tierces parties. Ces vérifications confirment l'aptitude du candidat à traiter les informations des clients avant son embauche.

Ces vérifications d'antécédents peuvent comprendre les éléments suivants :

- Vérification de l'identité/de l'employabilité
- Expérience professionnelle
- Antécédents de formation et de qualifications professionnelles
- Casier judiciaire (lorsque c'est autorisé légalement et en fonction des réglementations locales)

Accords de confidentialité avec les employés et entrepreneurs

Les contrats de travail d'ADP et les contrats avec des prestataires contiennent des conditions qui indiquent les obligations et les responsabilités liées aux données des clients auxquelles ils ont accès. Tous les employés et les entrepreneurs d'ADP sont liés par des obligations de confidentialité.

Formations à la sécurité des données

Tous les employés doivent participer à une formation à la sécurité des données dans le cadre de leur plan d'intégration. De plus, ADP dispense une formation à la sécurité annuelle pour rappeler aux employés leurs responsabilités dans l'exercice de leurs fonctions.

Responsabilités des employés et procédures disciplinaires

ADP a publié une politique de sécurité que tous les employés doivent respecter. Les infractions aux politiques de sécurité peuvent conduire à une révocation des privilèges d'accès et/ou des mesures disciplinaires pouvant aller jusqu'à la résiliation des contrats de conseil ou le licenciement.

Responsabilités lors d'une cessation d'emploi

Les responsabilités lors d'une cessation d'emploi ont été officiellement documentées et incluent, au minimum:

- Le retour de tous les actifs et toutes les données d'ADP en possession de l'employé concerné, quel que soit le support de stockage
- La résiliation des droits d'accès aux installations, aux données et aux systèmes d'ADP
- Le changement des mots de passe pour les comptes partagés actifs restants, le cas échéant
- Le transfert des connaissances, le cas échéant.

Section 4 - Gestion d’actifs

Utilisation acceptable des actifs

L'utilisation acceptable des actifs est expliquée dans plusieurs politiques applicables aux employés d'ADP et aux prestataires, afin d’assurer que les données d'ADP et des clients ne sont pas exposées à des risques liés à l'utilisation de ces actifs. Des exemples des domaines décrits dans ces politiques sont : l'utilisation de communications électroniques, l'utilisation des équipements électroniques et l'utilisation des actifs informationnels.

Classification des données

Les données acquises, créées ou conservées par ou pour le compte d'ADP se voient attribuer, selon le cas, les classifications de sécurité suivantes :

- Publique - Exemple : brochures commerciales, publications de rapports annuels
- À usage interne d’ADP uniquement - Exemple : communications entre bureaux, procédures opérationnelles
- Confidentielles ADP - Exemple : données personnelles et données personnelles de nature sensible
- Restreintes ADP - Exemple : prévisions financières, informations de planification stratégique

Les exigences en matière de traitement des données sont directement corrélées à la classification de sécurité des données. Les données personnelles et les données personnelles de nature délicate sont toujours considérées comme confidentielles pour ADP. Toutes les données des clients sont classifiées comme confidentielles.

Les employés d'ADP sont responsables de la protection et du traitement des actifs informationnels conformément à leur niveau de classification de sécurité, qui prévoit les exigences de protection de l'information et de traitement applicables pour chaque niveau de classification. La classification de confidentialité d'ADP est appliquée à toutes les données stockées, transmises et traitées par des tiers.

Élimination des équipements et des supports

Lorsque des équipements, documents, fichiers et supports sont éliminés ou réutilisés, des mesures appropriées sont prises pour éviter une récupération future des données des clients qui y étaient initialement stockées. Toutes les données sur des ordinateurs ou des supports de stockage électroniques, quelle que soit leur classification, sont éliminées de manière sécurisée, sauf lorsque le support est détruit physiquement avant de quitter les installations d'ADP ou d'être recyclé. Les procédures de destruction sécurisée/d'effacement des données d'ADP contenues dans des équipements, documents, fichiers et supports sont documentées officiellement.

Supports physiques en transit

Des protections organisationnelles ont été mises en œuvre pour protéger les supports écrits contenant des données des clients contre le vol, la perte, l’accès, ou une modification non-autorisée (i) lors de leur transport (par exemple dans des enveloppes scellées, des contenants et lors de livraisons en mains propres aux utilisateurs autorisés) et (ii) au cours de l'examen, de la révision ou d'autres traitements hors du lieu de stockage sécurisé

Section 5 - Contrôle d’accès

Exigences commerciales de contrôle des accès

La politique de contrôle de l'accès d’ADP est basée sur des exigences définies par l'entreprise. Les politiques et les normes de contrôle sont organisées autour de contrôles d'accès qui sont appliqués obligatoirement dans tous les composants du service fourni et sont fondés sur des principes du « moindre privilège » et du « besoin de savoir ».

Accès aux infrastructures - Gestion du contrôle des accès

Les demandes d'accès pour déplacer, ajouter, créer et effacer des données sont enregistrées, approuvées et revues régulièrement.

Un examen officiel est effectué au moins une fois par an pour confirmer que chaque utilisateur a accès à l'activité opérationnelle pertinente et n'a plus le même accès après un changement d'activité. Ce processus est vérifié et documenté dans un rapport de type II SOC1[1]. Au sein du système de gestion des identités, une équipe ADP dédiée est responsable de l'octroi, du refus, de l'annulation, de la résiliation et du démantèlement/de la désactivation des accès aux installations et aux systèmes d'information d'ADP. ADP utilise un outil de gestion des identités et des accès (GIA) centralisé qui est géré centralement par une équipe de GETS dédiée. Selon la demande de droit d'accès effectuée par l'intermédiaire de l'outil de GIA, un flux de travail de validation est déclenché pouvant impliquer le responsable de l'utilisateur. Les accès sont accordés temporairement et il existe des flux de travail pour éviter que de tels accès restent permanents. L'accès d'un employé à une installation est annulé immédiatement après son dernier jour d'emploi en désactivant sa carte d'accès (le badge de l'employé). Les identifiants d'utilisateur des employés sont désactivés immédiatement. Tous les actifs des employés sont retournés et vérifiés par le responsable hiérarchique compétent et sont comparés par rapport à la liste d'actifs dans la base de données de gestion des configurations. Suite à un changement de poste ou organisationnel, les profils ou les droits d'accès des utilisateurs doivent être modifiés par les équipes de gestion de l'unité fonctionnelle et de GIA. De plus, un examen officiel des droits d'accès a lieu chaque année pour vérifier que les droits de chaque utilisateur correspondent bien à leur activité et qu'il ne reste pas de droits d'accès non pertinent après un changement de poste.

Politique des mots de passe

Les politiques de mot de passe des employés d'ADP sont appliquées obligatoirement dans les appareils et applications des serveurs, les bases de données et réseaux, dans la mesure permise par l'appareil ou l'application. La complexité du mot de passe est fonction d'une analyse fondée sur les risques des données et du contenu protégés. Les politiques respectent les normes du secteur en matière de robustesse et de complexité, y compris sans s'y limiter, l'utilisation d'une authentification progressive, à deux facteurs ou biométrique le cas échéant.

Les exigences d'authentification d'une application client varient par produit, et des services fédérés (SAML 2.0) sont disponibles sur des applications ADP spécifiques utilisant un réseau unifié et une couche de sécurité gérée par GETS.

Délais d’expiration des sessions

ADP applique une expiration automatique des connexions de tous les serveurs, postes de travail, applications et VPN selon une approche fondée sur les risques conforme aux normes du secteur. Le rétablissement de la connexion ne peut avoir lieu qu'après la saisie d'un mot de passe valide par l'utilisateur.

---

[1] Dans le cas de certains services américains offerts par ADP, cela fait l'objet d'une vérification dans un rapport de type 2 SOC2.

Section 6 - Cryptographie

Contrôles cryptographiques

ADP exige que les informations sensibles échangées entre ADP et des tiers soient cryptées (ou que le canal de transmission soit lui-même crypté) selon une robustesse et à l'aide de techniques de cryptage acceptées par le secteur. Alternativement, une ligne louée privée peut être utilisée.

Gestion des clés

ADP a mis en place une norme de sécurité du cryptage interne qui inclut des procédures de gestion et de récupération des clés, notamment une gestion des clés à la fois symétrique et asymétrique.

Les clés de cryptage utilisées pour les données d'ADP sont toujours classées comme des informations confidentielles. L'accès à ces clés est strictement limité à ceux qui « ont besoin de savoir » et si une approbation d'exception est accordée. Les clés de cryptage et la gestion du cycle de vie des clés respectent les pratiques standard du secteur.

Section 7 - Sécurité Physique et Environnementale

L'approche d'ADP en matière de sécurité physique a deux objectifs : créer un environnement de travail sûr pour les collaborateurs d'ADP et protéger les données personnelles détenues dans les centres de données d'ADP et les autres emplacements stratégiques d'ADP.

La politique de sécurité d'ADP oblige ses responsables à identifier les zones nécessitant un niveau spécifique de sécurité physique. L'accès à ces zones n'est accordé qu'aux collaborateurs habilités à des fins autorisées. Les zones sécurisées d'ADP utilisent divers dispositifs de sécurité physique, notamment des systèmes de vidéosurveillance, l'utilisation de badges de sécurité (accès contrôlés en fonction de l'identité) et des agents de sécurité postés aux points d'entrée et de sortie. Les visiteurs ne peuvent se voir accorder l'accès que sur autorisation et sont surveillés en permanence.

Section 8 - Sécurité des opérations

Formalisation des procédures opérationnelles du service informatique.

GETS est l'unité d'ADP responsable du fonctionnement et de la maintenance de l'infrastructure informatique. GETS documente et met à jour officiellement les politiques et procédures informatiques. Ces procédures comprennent, sans s'y limiter :

- La gestion du changement
- La gestion des sauvegardes
- Le traitement des erreurs système
- Le redémarrage et la restauration des systèmes
- La surveillance des systèmes
- La planification et la surveillance des tâches

Gestion du changement des infrastructures

Un comité consultatif sur le changement (CCC) périodique, qui inclut des représentants de nombreuses équipes d'ADP, est réuni par GETS. Les réunions du CCC discutent de l'impact des fenêtres de déploiement et des mises en production, et permettent de coordonner tout autre changement de l'infrastructure de production.

Planification et acceptation des capacités des systèmes

Les exigences de capacité sont surveillées en permanences et revues régulièrement. Après ces revues, les tailles des systèmes et des réseaux sont augmentées et réduites en conséquence. Lorsque des changements importants doivent être effectués en raison d'un changement de capacité ou de l'évolution d'une technologie, l'équipe d'étalonnage de GETS peut réaliser des tests de résistance sur les applications et/ou systèmes concernés. À la fin des tests de résistance, l'équipe fournit un rapport détaillé de l’évaluation de la performance en évaluant les changements dans (i) les composants (ii) la configuration ou la version du système ou (iii) la configuration ou la version du logiciel.

Protection contre les programmes malveillants

Des technologies de protection des terminaux aux normes du secteur sont utilisées pour protéger les actifs d'ADP conformément aux meilleures pratiques du secteur.

Politique de gestion des sauvegardes

ADP a mis en place des politiques qui exigent de toutes les opérations d'hébergement de la production de sauvegarder les données de production. La portée et la fréquence des sauvegardes correspondent aux exigences commerciales des services d'ADP concernés, aux exigences de sécurité des données en question et au caractère critique des données dans le cadre d'une reprise après sinistre. La surveillance des sauvegardes programmées est effectuée par GETS, afin d'identifier les problèmes de sauvegarde ou les exceptions y relatives.

Connexion de sécurité et surveillance

ADP a mis en place une infrastructure de connexion centrale et en lecture seule (SIEM) et un système de corrélation des connexions et d'alerte (TPSI). Les alertes de connexion sont surveillées et traitées rapidement par le CIRC.

Tous ces systèmes sont synchronisés à l'aide d'un Network Time Protocol (NTP) unique à référence d'horloge.

Chaque connexion contient au minimum :

- L'horodatage

- L'identité (de l'opérateur ou de l'administrateur)
- L'objet (information concernant l'événement)

Les pistes de vérification et les connexions au système pour les applications d'ADP sont conçues et établies pour enregistrer les informations suivantes :

- Les accès autorisés
- Les opérations privilégiées
- Les tentatives d'accès non autorisés
- Les alertes ou défaillances du système
- Les modifications des paramètres de sécurité du système, lorsque celui-ci permet un tel enregistrement

Seul le personnel autorisé d'ADP a accès à ces enregistrements, qui sont envoyés en direct pour éviter que les données soient falsifiées avant d'être stockées dans les dispositifs d'enregistrement sécurisés.

Systèmes et surveillance des infrastructures

ADP prend les mesures appropriées pour surveiller les infrastructures 24 heures sur 24 et 7 jours sur 7. Les alertes de perturbation sont gérées par différentes équipes en fonction de leur sévérité et des compétences requises pour résoudre le problème.

Les installations de centre d'hébergement d'ADP utilisent des applications de surveillance qui fonctionnent en permanence sur tous les systèmes de traitement connexes et sur les composants du réseau pour fournir au personnel d'ADP des avis proactifs sur les problèmes et des avertissements avant des problèmes éventuels.

Gestion de la vulnérabilité technique

Un système d'exploitation à la sécurité renforcée (ou un processus sécurisé) doit être installé sur tous les ordinateurs faisant partie de l'infrastructure d'hébergement. Les opérations hébergées emploient une version renforcée, approuvée et standardisée pour tous les types de serveurs utilisés au sein de nos infrastructures. Les installations standard des systèmes d'exploitation sont interdites, puisque de telles installations pourraient créer des vulnérabilités, comme des mots de passe de compte système génériques, qui introduiraient un risque d'infrastructure. Ces configurations réduisent le risque que des ordinateurs hébergés fassent tourner des services inutiles qui pourraient créer des vulnérabilités.

ADP a documenté une méthodologie pour les mises à jour, des évaluations de vulnérabilité régulières et des examens de la conformité des applications connectées à Internet et de leurs composants matériels correspondants, qui incluent au moins 15 catégories de tests principales. La méthode d'évaluation est fondée sur les meilleures pratiques internes et du secteur, notamment celles de l'Open Web Application Security Project (OWASP), du SANS Institute et du Web Application Security Consortium (WASC).

Section 9 - Sécurité des communications

Gestion de la sécurité du réseau

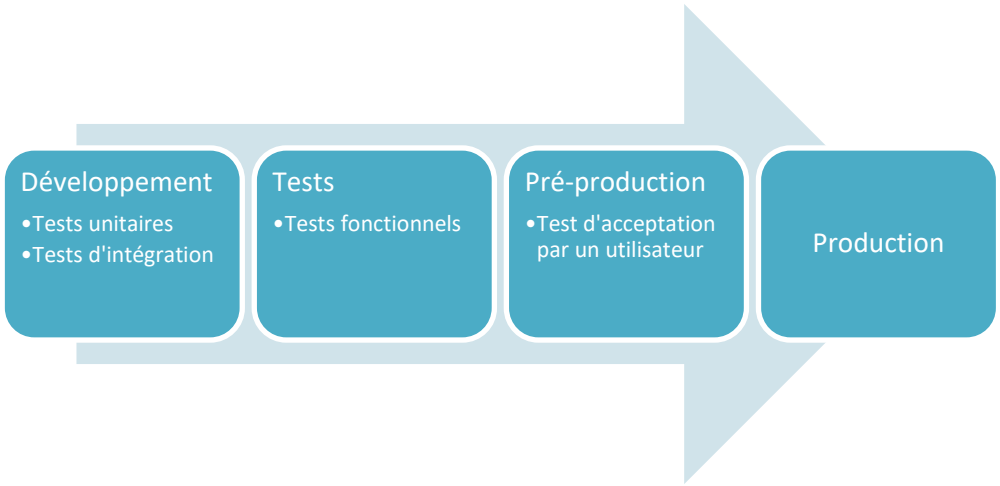
ADP emploie un système de détection des intrusions fondé sur le réseau qui surveille le trafic au niveau de l'infrastructure réseau (24 heures sur 27, 7 jours sur 7) et identifie les activités suspectes ou les attaques potentielles.

Échange d'informations

ADP met en œuvre des contrôles appropriés de sorte que les données des clients d'ADP envoyées à des tiers soient transférées entre des systèmes et ressources informatiques autorisés seulement, et soient échangées uniquement à l'aide des mécanismes de transfert autorisés et sécurisés d'ADP.

Sécurité lors du développement et processus de soutien

Au cours du cycle de développement, la documentation appropriée est produite, et des plans de test sont élaborés pour la phase de tests. Différentes étapes sont définies pour chaque environnement, chacune d'elle devant recevoir l'approbation appropriée :



- Pour passer de l'environnement de test à celui de pré-production, il faut l'approbation de l'équipe qualité d'ADP.
- Pour passer de l'environnement de pré-production à celui de production, il faut l'approbation des opérations informatiques.

Les équipes de développement doivent utiliser des méthodes de programmation sécurisées. Les changements d'application sont testés dans des environnements de développement et de régression avant d'atteindre les systèmes de production. Des tests sont réalisés et documentés. Une fois approuvés, les changements sont déployés dans l'environnement de production. Des tests de pénétration sont réalisés après tout changement important.

Un CCC périodique, qui inclut des représentants de nombreuses équipes d'ADP, est réuni par GETS. Les réunions du CCC se tiennent régulièrement et permettent de discuter des impacts, de convenir des fenêtres de déploiement et d'approuver la promotion des logiciels dans l'environnement de production, ainsi que de communiquer tout changement de l'infrastructure de production.

L'équipe Opérations informatiques d'ADP fournit l'approbation définitive avant la promotion des logiciels vers l'environnement de production.

Sécurité de l'environnement de développement

Les environnements de développement et de production sont séparés et indépendants l'un de l'autre. Des contrôles d'accès appropriés sont employés pour garantir une séparation correcte des responsabilités. Les logiciels sont accessibles à chaque étape du processus de développement et uniquement par les équipes impliquées dans l'étape en question.

Données de test

La politique de gestion des applications d'ADP interdit l'utilisation de données réelles ou non nettoyées dans l'environnement de développement, et les tests sont interdits sauf en cas de demande et d'autorisation expresses du client.

Section 11 - Relations avec les fournisseurs

Identification des risques liés aux parties externes

Les évaluations des risques des tiers qui ont besoin d'accéder aux données d'ADP et/ou de clients sont effectuées régulièrement pour déterminer leur conformité aux exigences de sécurité d'ADP pour les tiers, et pour identifier toute lacune dans les contrôles appliqués. Si une lacune de sécurité est identifiée, de nouveaux contrôles sont convenus avec ces parties externes.

Accords de sécurité des données avec les parties externes

ADP conclut des accords avec tous les tiers qui incluent des engagements en matière de sécurité appropriés pour répondre aux exigences de sécurité d'ADP.

Section 12 - Gestion des incidents affectant la sécurité de l'information

Gestion et des incidents affectant la sécurité de l'information et améliorations

ADP a documenté une méthodologie pour répondre aux incidents de sécurité de manière rapide, cohérente et efficace.

En cas d'incident, une équipe prédéfinie d'employés d'ADP met en œuvre un plan de réponse aux incidents officiel qui couvre des domaines tels que :

- L'escalade fondée sur la classification de l'incident ou sa sévérité
- Les coordonnées pour la déclaration/l'escalade des incidents
- Des directives pour les réponses initiales et le suivi avec les clients concernés
- La conformité aux lois relatives à la déclaration des infractions à la sécurité applicables
- Un journal d'enquête
- La restauration des systèmes
- La résolution, la déclaration et l'examen des problèmes
- L'identification des causes profondes et les mesures correctives
- Les leçons apprises

Les politiques d'ADP définissent un incident de sécurité, la gestion d'incident et les responsabilités de tous les employés concernant la déclaration des incidents de sécurité. ADP organise également des formations régulières pour ses employés et entrepreneurs pour les sensibiliser aux exigences de déclaration. Ces formations font l'objet d'une surveillance pour s'assurer qu'elles sont effectivement suivies.

Section 13 - Aspects de sécurité de l’information liés à la gestion de la résilience des activités

Programme de résilience des activités d'ADP

ADP s'est engagé à assurer le bon fonctionnement de ses services et opérations, pour fournir à ses clients le meilleur service possible. Notre priorité est d'identifier - et d'atténuer - les risques technologiques, environnementaux, liés aux processus et sanitaires qui pourraient être un obstacle à la prestation de nos services commerciaux. ADP a créé un cadre intégré qui présente nos processus d'atténuation, de préparation, de réponse et de récupération et comprend :

- Évaluation des risques
- Analyse des risques
- Analyse de l'impact sur l'activité
- Élaboration de plans
- Planification de la continuité des activités
- Planification de reprise après sinistre
- Planification de la santé et sécurité
- Réponse pratique
- Gestion de crise
- Réponse d'urgence
- Tests et validation
- Revue
- Révision
- Exercise

Section 14 - Conformité

Conformité avec les politiques de sécurité et les normes

ADP emploie un processus visant à réaliser des examens de la conformité internes régulièrement. De plus, ADP réalise une vérification de type II SOC1[2] régulièrement. Ces vérifications sont effectuées par un cabinet de vérification tiers bien connu, et des rapports de vérification sont disponibles chaque année pour les clients sur demande, le cas échéant.

Conformité technique

Pour garantir la conformité technique avec les meilleures pratiques, ADP réalise régulièrement des examens planifiés de la vulnérabilité du réseau. Les résultats de cet examen sont ensuite classés par ordre de priorité et des plans de mesures correctives sont développés avec les équipes d'hébergement et leurs responsables.

Des examens de vulnérabilité sont effectués régulièrement sur les environnements internes et externes. De plus, des examens du code source et des tests de pénétration sont effectués pour chaque produit. À l'aide d'outils d'examen d'application spécialisés, les vulnérabilités au niveau des applications sont identifiées le cas échéant, communiquées aux équipes de direction du développement de produit, et incorporées dans les processus de contrôle de qualité pour que des mesures correctives soient prises. Les résultats sont analysés, et des plans de mesures correctives sont élaborés et priorisés.

Conservation des données

La politique de conservation des données d'ADP relative aux données des clients est conçue pour être conforme aux lois applicables. À la fin du contrat d'un client, ADP remplit ses obligations contractuelles associées aux données du client. ADP retourne ou permet au client de récupérer (par téléchargement des données) toutes les informations du client nécessaires à la continuité des activités commerciales du client (si elles n'ont pas été fournies précédemment). Ensuite, ADP détruit de manière sécurisée les informations du client restantes, sauf dans la mesure exigée par la loi en vigueur, autorisée par le client ou nécessaire aux fins d'une résolution de litige.

[2] Dans le cas de certains services américains offerts par ADP, des rapports exécutifs de type II SOC2 sont également disponibles.

ANNEXE 3 – Liste des sociétés du Groupe liées par le Code du Sous-traitant de Données

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Philippines, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Suisse
ADP Brazil Ltda.	João Tibiriçá, 1112 - Vila Anastácio, São Paulo - SP, 05077-000, Brésil
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canada
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Brussels, Belgique
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praha 8, République tchèque
ADP Employer Services GmbH	Frankfurter Str. 227, 63263 Neu-Isenburg, Allemagne
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcelone, Espagne
ADP Employer Services Italia SPA	Viale G. Richard 5/A – 20143 Milan, Italie
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord – 1003 Tunis, Tunisie
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, France
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, France
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Pays-Bas
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, France
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai – 600 032 Inde
ADP International Services B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Pays-Bas
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Rotterdam
ADP Outsourcing Italia SRL	Viale G. Richard 5/A – 20143 Milan, Italie
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Polska Sp. zo.o.	Prosta 70, 00-838 Warsaw, Pologne

ADP Private Limited	6-3-1091/C/1, Fortune 9, Raj Bhavan Road, Somajiguda, Hyderabad, Telangana, Inde – 500082
ADP RPO UK Limited	22 Chancery Lane, London, Angleterre, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Findlay, OH, USA 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Slovaquie
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Turin, Italie
ADP Sverige AB	Östermalmstorg 1, 114 42 Stockholm, Suède
ADP, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st – 6th floor, District 2, Bucharest, Roumanie 020334
Automatic Data Processing Limited (Australie)	6 Nexus Court, Mulgrave, VIC 3170, Australie
Automatic Data Processing Limited (Royaume-Uni)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT, England
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ, England
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Celergo PTE. LTD.	62, Ubi Road 1, #11-07, Oxley Bizhub 2, Singapour 408734
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portugal
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068