Code d'ADP relatif à la confidentialité des services de traitement des données de clients

Code d'ADP relatif à la confidentialité des services de traitement des données de clients

Introduction

ADP offre un vaste éventail de services de gestion du capital humain à ses clients. ADP s'est engagée à protéger les données personnelles dans le **Code d'ADP d'éthique et de déontologie des affaires**.

Le présent Code d'ADP relatif à la confidentialité des services de traitement des données de clients énonce la façon dont ADP a mis en œuvre son engagement envers le traitement des données personnelles relatives aux employés des clients, relativement à ses activités de prestation de services à la clientèle et d'activités de soutien au client. Dans le cadre de cette structure, les données des clients sont traitées par ADP à titre de responsable du traitement de données au nom de ses clients.

Pour connaître les règlements s'appliquant au traitement des données personnelles par ADP à titre de contrôleur des données relatives aux personnes avec qui ADP entretient une relation d'affaires (p. ex., les personnes qui représentent les clients d'ADP, les fournisseurs, les partenaires commerciaux, les autres professionnels et les consommateurs) et aux autres personnes dont ADP traite les données personnelles dans le cadre de ses activités commerciales à titre de contrôleur des données, veuillez consulter le ***Code d'ADP relatif à la confidentialité des données commerciales***.

Article 1 – Portée, applicabilité et mise en œuvre

Portée – Applicabilité relative aux données de l'EEE

1.1 Le présent code aborde le traitement des données personnelles des employés des clients d'ADP dans le cadre de son rôle de responsable du traitement de données pour les clients et de la prestation de ses services à la clientèle, où ces données personnelles sont (a) sujettes aux lois applicables de l'EEE (ou étaient sujettes aux lois applicables de l'EEE avant le transfert de ces données personnelles à une société du groupe à l'extérieur de l'EEE, dans un pays qui n'est pas réputé assurer un niveau adéquat de protection des données par des institutions compétentes de l'EEE), et (b) traitées en vertu d'un contrat de services stipulant expressément que le présent code s'appliquera à ces données personnelles.

Lorsqu'on s'interroge sur l'applicabilité du présent code, le responsable de la confidentialité concerné demandera conseil auprès de l'équipe mondiale de protection des données personnelles et de la gouvernance avant le traitement des données.

Traitement électronique et papier

1.2 Le présent code s'applique au traitement des données des clients par ADP par voie électronique et à l'aide de systèmes de classement papier systématiquement accessibles.

Applicabilité des

1.3 Aucune disposition du présent code ne sera interprétée comme retirant les

lois locales

droits ou les recours dont peuvent jouir les employés des clients en vertu des lois applicables. Lorsque les lois applicables fournissent une protection supérieure à celle du présent code, les dispositions des lois applicables en question s'appliqueront. Lorsque le présent code fournit une protection supérieure à celle des lois applicables, ou offre aux personnes des mesures de protection, des droits ou des recours supplémentaires, le présent code s'appliquera.

Politiques et lignes directrices **1.4** ADP peut compléter le présent code à l'aide de politiques, de normes, de lignes directrices et de directives cohérentes en vertu de ce code.

Responsabilité **1.5** Le présent code est contraignant pour ADP. Les cadres responsables seront tenus responsables de la conformité de leur organisation commerciale avec le présent code. Le personnel d'ADP doit respecter le présent code.

Date d'entrée en vigueur **1.6** Le présent code a été approuvé par l'avocat général, à la suite de sa présentation par le chef mondial de la confidentialité, et adopté par le comité de direction d'ADP. Le présent code entrera en vigueur le 11 avril 2018 (la **date d'entrée en vigueur**). Le code (y compris une liste des sociétés du groupe participant au traitement de données des clients) sera publié sur le site Web www.adp.com. Il sera également remis aux personnes qui en font la demande.

Le présent code sera mis en œuvre par le groupe ADP selon le calendrier précisé à l'article 16.

Politiques précédentes **1.7** Le présent code complète les politiques de confidentialité d'ADP et remplace tous les énoncés précédents, dans la mesure où ils sont en contradiction avec le présent code.

Rôle de l'entité déléguée d'ADP **1.8** Automatic Data Processing, Inc. a nommé ADP Nederland B.V., dont le siège social est enregistré à Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Pays-Bas, comme entité déléguée d'ADP responsable de faire respecter le présent code au sein du groupe ADP, et ADP Nederland B.V. a accepté ce mandat.

Article 2 – Contrat de services

Contrat de services, sous-traitants de données

2.1 ADP traitera les données des clients uniquement dans le cadre d'un contrat de services intégrant les exigences obligatoires de conclusion de contrat avec des responsables du traitement de données en vertu des lois régissant les responsables du traitement de données et aux fins légitimes décrites à l'article 4.

L'entité contractante d'ADP fait appel à des sous-traitants de données, à la fois des sous-traitants de données d'ADP et des tiers sous-traitants de données, dans le cadre de la prestation ordinaire de services à la clientèle. Les contrats de service d'ADP autoriseront l'utilisation de tels sous-traitants de données, pourvu que l'entité contractante d'ADP soit toujours tenue responsable envers le client du rendement des sous-traitants de données, conformément aux modalités du contrat de services. Les dispositions de l'article 7 régiront l'utilisation de sous-traitants de données.

Résiliation du contrat de services

2.2 En cas de suspension des services offerts au client, ADP respectera ses obligations décrites dans le contrat de services en ce qui concerne le retour des données du client, en lui fournissant les données requises pour assurer la continuité de ses activités commerciales (si les données n'ont pas déjà été fournies ou rendues accessibles à l'aide d'une fonctionnalité de produit, dont la capacité de télécharger les données du client).

Lorsque les obligations d'ADP en vertu du contrat de services ont été remplies, ADP détruira de façon sécuritaire les copies restantes des données du client, et (à la demande du client) attestera auprès du client que les données ont été détruites. ADP pourra conserver une copie des données du client dans les limites permises par les lois applicables, comme autorisé par le client, ou aux fins de résolution de différends, au besoin. ADP cessera de traiter les données du client, sauf dans la mesure requise pour les fins indiquées ci-dessus. Les obligations de confidentialité d'ADP en vertu du contrat de services en question persisteront tant qu'ADP conserve une copie de ces données du client.

Audit des mesures de résiliation

2.3 Dans les 30 jours suivant la résiliation du contrat de services (sauf si autrement requis par une autorité de la protection des données), ADP permettra, à la demande du client ou de l'autorité de la protection des données compétente, l'audit de ses établissements de traitement conformément aux articles 11.2 ou 11.3 (selon le cas) afin d'assurer qu'ADP respecte ses obligations en matière de résiliation en vertu de l'article 2.2.

Article 3 – Obligations de conformité

Directives du client **3.1** ADP doit traiter les données du client au nom du client, uniquement dans le cadre du contrat de services, conformément à toutes les directives consignées reçues de la part du client, ou aux fins du respect de la loi applicable.

Respect des lois applicables **3.2** ADP traitera les données du client conformément aux lois régissant les responsables du traitement de données.

ADP répondra rapidement et convenablement aux demandes d'assistance du client, comme requis par la loi, afin de lui permettre de respecter ses obligations en vertu des lois applicables au contrôleur des données, conformément au contrat de services.

Non-conformité, effet préjudiciable considérable **3.3** Si une société du groupe apprend qu'une loi régissant les responsables du traitement de données d'un pays non membre de l'EEE, ou toute modification d'une loi régissant les responsables du traitement de données d'un pays non membre de l'EEE, ou une directive du client aura vraisemblablement un effet préjudiciable considérable sur la capacité d'ADP de respecter ses obligations en vertu des articles 3.1, 3.2 ou 11.3, elle devra rapidement en aviser l'entité déléguée d'ADP et le client, et celui-ci aura le droit, en vertu du présent code, de temporairement suspendre le transfert des données en question à ADP jusqu'à ce qu'on ait modifié le processus de traitement afin d'en corriger la non-conformité. Lorsqu'il est impossible de modifier le processus de traitement, le client aura le droit de mettre fin à la partie du traitement en question effectuée par ADP, conformément aux modalités du contrat de services. Ces droits et obligations ne s'appliquent pas lorsque les circonstances ou la modification des lois régissant les responsables du traitement de données découlent d'exigences obligatoires.

Demande de divulgation de données de clients **3.4** Si ADP reçoit une demande de divulgation de données de clients de la part d'un organisme chargé de l'application de la loi ou d'un organisme chargé de la sécurité d'État (un organisme) d'un pays non membre de l'EEE, elle déterminera si la demande est légalement valide et contraignante pour ADP, au cas par cas. Toute demande non légalement valide et contraignante pour ADP sera refusée, conformément aux lois applicables.

Sous réserve du paragraphe suivant, ADP informera rapidement le client, la principale autorité chargée de la protection des données (principale APD) et l'APD compétente pour le client en vertu de l'article 11.3, de cette demande légalement valide et contraignante pour ADP de la part d'un organisme, et demandera à l'organisme de la suspendre pendant une période raisonnable afin de permettre à la principale APD d'émettre une opinion au sujet de la validité de la demande de divulgation.

Si la suspension de l'application ou le signalement à la principale APD d'une demande de divulgation légalement valide et contraignante sont interdits, comme c'est le cas en vertu du droit criminel afin d'assurer la confidentialité d'une enquête policière, ADP demandera à l'organisme de renoncer à cette interdiction et documentera le dépôt de cette demande. ADP fournira annuellement à la principale APD des renseignements généraux sur le nombre et le type de demandes de divulgation reçues au cours des 12 derniers mois de la part d'organismes.

Le présent article ne s'applique pas aux demandes reçues par ADP de la part d'organismes dans le cadre de ses activités ordinaires à titre de fournisseur de services de GCH (telle une ordonnance de la cour pour saisir un salaire), qu'ADP peut continuer à offrir conformément aux lois applicables, au contrat de services et aux directives du client.

Demandes des clients

3.5 ADP répondra rapidement et convenablement aux demandes des clients relativement au traitement de leurs données en vertu des modalités du contrat de services.

Article 4 – Objectifs du traitement de données

Fins commerciales légitimes

4.1 ADP traite des données personnelles (incluant des catégories spéciales de données) relatives aux employés de ses clients lorsque nécessaire dans le cadre de la prestation de ses services à la clientèle, de ses activités de soutien au client et pour les fins additionnelles suivantes :

(a) L'hébergement, le stockage et toute autre forme de traitement requise pour la continuité des activités et la reprise d'activité après un sinistre, y compris la création de copies de sauvegarde et d'archivage de données personnelles;

(b) L'administration et la sécurité des réseaux et des systèmes, incluant la surveillance des infrastructures, la gestion, la vérification et l'authentification

des identités et des authentifiants, ainsi que le contrôle des accès;

(c) La surveillance et les autres formes de contrôle nécessaires à la préservation de la sécurité et de l'intégrité des transactions (p. ex., les transactions financières et les transferts de fonds), y compris aux fins de contrôle diligent (dont la vérification de l'identité d'une personne et de son admissibilité à recevoir des produits et services, en vérifiant par exemple sa situation d'emploi ou l'état de son compte);

(d) L'exécution de contrats et la protection d'ADP, de ses collaborateurs, de ses clients, des employés de ses clients et du public contre le vol, la responsabilité civile, la fraude ou les abus, y compris; (i) la détection, l'étude, la prévention et l'atténuation de préjudices découlant d'une fraude financière réelle ou d'une tentative de fraude, d'un vol d'identité et d'autres menaces envers les actifs financiers et physiques, les données d'accès et les systèmes d'information, (ii) la participation à des initiatives externes de cybersécurité et contre la fraude et le blanchiment d'argent et (iii) au besoin, pour protéger les intérêts vitaux de personnes, par exemple, en les avertissant d'une menace à la sécurité observée;

(e) L'exécution et la gestion des processus commerciaux internes d'ADP menant au traitement de données de clients connexe pour :

(1) les audits internes et la production de rapports consolidés;

(2) la conformité légale, y compris le classement, l'utilisation et la divulgation obligatoires d'information requis en vertu des lois applicables;

(3) la dépersonnalisation des données et le cumul de données dépersonnalisées aux fins de minimisation des données et d'analyse des services;

(4) l'utilisation de données dépersonnalisées et cumulatives, comme permis par les clients, afin de faciliter l'analyse, la continuité et l'amélioration des produits et services d'ADP;

(5) la facilitation des activités de gouvernance d'entreprise, dont les fusions, les acquisitions, les désinvestissements et les coentreprises.

Article 5 – Exigences de sécurité

Sécurité des données

5.1 ADP mettra en œuvre des mesures techniques, physiques et organisationnelles appropriées et raisonnables d'un point de vue commercial pour protéger les données des clients contre toute mauvaise utilisation ou contre toute destruction, perte, altération, divulgation, acquisition ou tout accès accidentels, illégaux ou non autorisés, lesquelles mesures respecteront les exigences des lois applicables de l'EEE, ou toutes autres exigences plus strictes, conformément au contrat de services. Dans tous les cas, ADP prendra les mesures précisées à l'annexe 2 du présent code, qu'ADP peut modifier pourvu que les modifications ne réduisent pas substantiellement le degré de sécurité fourni aux données des clients en vertu de l'annexe 2.

Accès aux données et confidentialité

5.2 Le personnel sera autorisé à accéder aux données des clients uniquement pour remplir les objectifs de traitement de données applicables en vertu de l'article 4. ADP imposera des obligations de confidentialité au personnel ayant accès aux données des clients.

Avis de brèche de sécurité des données

5.3 En cas de brèche de sécurité des données, ADP informera le client sans retard excessif une fois qu'elle aura pris connaissance de ladite brèche, sauf si un responsable de l'application de la loi ou une autorité de surveillance déterminent que cela entraverait une enquête criminelle, porterait atteinte à la sécurité nationale ou donnerait lieu à un abus de confiance dans le secteur de marché concerné. Dans ce cas, l'avis sera reporté selon les directives du responsable de l'application de la loi ou de l'autorité de surveillance. ADP répondra rapidement aux questions du client au sujet de ladite brèche de sécurité des données.

Article 6 – Transparence envers les employés du client

Autres demandes des employés du client

6.1 ADP informera sans tarder le client de toute demande ou plainte concernant le traitement des données personnelles par ADP qui sera transmise directement par un employé du client, et elle ne répondra pas à ladite demande ou plainte, sauf disposition contraire prévue dans le contrat de services ou énoncée par le client.

Si le client demande à ADP de répondre aux demandes et plaintes de ses employés dans le contrat de services, ADP s'assurera de fournir aux employés du client tous les renseignements raisonnablement requis (dont la personne-ressource et la procédure) pour leur permettre de déposer efficacement leur demande ou leur plainte.

Les dispositions du présent article 6.1 ne s'appliqueront pas aux demandes gérées par ADP dans le cadre de la prestation ordinaire de services à la clientèle et d'activités de soutien au client.

Article 7 – Sous-traitants de données

Contrats de sous-traitance des données avec des tiers

7.1 Des tiers sous-traitant des données peuvent traiter des données du client uniquement en conformité avec un contrat de sous-traitance des données. Le contrat de sous-traitance des données devra imposer au tiers sous-traitant des données des conditions similaires en matière de protection des données traitées, conditions qui ne s'avéreront pas moins sécuritaires que celles imposées à l'entité contractante d'ADP par le contrat de services et le présent code.

Publication d'un aperçu des sous-traitants de données **7.2** ADP publiera un aperçu des catégories de sous-traitants de données participant à la prestation des services à la clientèle en question sur le site d'ADP convenable. Cet aperçu sera rapidement mis à jour en cas de modification.

Avis concernant les nouveaux sous-traitants de données et droit d'objection **7.3** ADP avisera le client de tout nouveau sous-traitant de données embauché par ADP pour participer à la prestation de services à la clientèle. Dans les 30 jours suivant la réception d'un tel avis, le client peut s'opposer au sous-traitant de données en fournissant un avis écrit à ADP décrivant les motifs objectifs valables quant à l'incapacité de ce sous-traitant de données à protéger les données du client conformément aux obligations connexes dans le contrat de sous-traitance des données, comme mentionné à l'article 7.1. Dans le cas où les parties ne peuvent trouver une solution mutuellement acceptable, ADP ne permettra pas, à sa discrétion, au sous-traitant de données d'accéder aux données du client ou permettra au client de résilier les services à la clientèle en question conformément aux modalités du contrat de services.

Exception **7.4** Les dispositions de la présente section 7 ne s'appliqueront pas dans la mesure où le client demande à ADP de permettre à un tiers de traiter ses données en vertu d'un contrat que le client a conclu directement avec ce tiers (p. ex., un tiers fournisseur d'avantages sociaux).

Article 8 – Supervision et conformité

Directeur principal de la confidentialité à l'échelle mondiale **8.1** Le groupe ADP comptera un chef mondial de la confidentialité responsable des tâches suivantes :

(a) présider le conseil de direction en matière de confidentialité;

(b) superviser la conformité avec le présent code;

(c) superviser, coordonner, communiquer et consulter les membres concernés du réseau de protection de la confidentialité au sujet de questions de confidentialité et de protection des données;

(d) présenter des rapports annuels sur les risques relatifs à la confidentialité et la protection des données et les problèmes de conformité au comité de direction d'ADP;

(e) coordonner les enquêtes officielles sur le traitement des données des clients par un organisme gouvernemental, en conjonction avec les membres concernés du réseau de protection de la confidentialité et du service juridique d'ADP;

(f) gérer les conflits entre le présent code et les lois applicables;

(g) surveiller le processus d'exécution des évaluations de l'incidence sur la confidentialité et les passer en revue, au besoin;

(h) surveiller les documents, les avis et les communications relatifs aux brèches de sécurité des données;

(i) offrir des conseils relatifs aux processus, systèmes et outils de gestion des données afin de mettre en œuvre la structure de gestion de la confidentialité et de la protection des données, comme établie par le conseil de direction en matière de confidentialité, notamment :

(1) entretenir, mettre à jour et publier le présent code ainsi que les politiques et normes connexes;

(2) offrir des conseils sur les outils requis pour recueillir, entretenir et mettre à jour les registres contenant l'information sur la structure et le fonctionnement de tous les systèmes traitant des données des clients;

(3) fournir de l'assistance ou des conseils relativement à la formation sur la confidentialité destinée aux employés afin qu'ils comprennent et assument leurs responsabilités en vertu du présent code;

(4) coordonner les activités avec le service d'audit interne d'ADP et d'autres services afin de créer et d'entretenir un programme d'assurance convenable visant à surveiller, auditer et produire des rapports sur la conformité au présent code, et permettre à ADP de vérifier et d'attester cette conformité, au besoin;

(5) mettre en œuvre des procédures, au besoin, afin de gérer les demandes, les inquiétudes et les plaintes relatives à la confidentialité et à la protection des données;

(6) offrir des conseils au sujet des sanctions appropriées pour les infractions au présent code (p. ex., des mesures disciplinaires).

Réseau de protection de la confidentialité

8.2 ADP établira un réseau de protection de la confidentialité suffisant pour assurer la conformité avec le présent code au sein de l'entreprise mondiale d'ADP.

Le réseau de protection de la confidentialité créera et entretiendra une structure visant à soutenir le chef mondial de la confidentialité et à entreprendre la coordination des tâches décrites à l'article 8.1 et des autres tâches nécessaires pour entretenir et mettre à jour le présent code. Les membres du réseau de protection de la confidentialité, selon leur rôle dans la région ou au sein de l'entreprise, effectueront les tâches supplémentaires suivantes :

(a) coordonner la mise en œuvre des processus, systèmes et outils de gestion des données permettant aux sociétés du groupe de respecter le code dans leur région ou au sein de leur organisation respectives;

(b) soutenir et évaluer la gestion de la confidentialité et de la protection des données ainsi que la conformité des sociétés du groupe dans leur région;

(c) offrir régulièrement des conseils aux responsables de la confidentialité et au chef mondial de la confidentialité sur les risques régionaux et locaux liés à la confidentialité et les problèmes de conformité;

(d) s'assurer qu'on tient des registres convenables des systèmes traitant des données des clients;

(e) être disponibles pour répondre aux demandes d'approbation ou de conseils;

(f) fournir les renseignements requis par le chef mondial de la confidentialité pour achever le rapport annuel sur la confidentialité;

(g) offrir de l'assistance au chef mondial de la confidentialité en cas d'enquêtes ou de demandes officielles de la part d'organismes gouvernementaux;

(h) créer et publier des politiques et normes sur la confidentialité pour leurs régions ou entreprises;

(i) offrir des conseils aux sociétés du groupe sur la conservation et la destruction de données;

(j) informer le chef mondial de la confidentialité des plaintes reçues et participer à leur résolution;

(k) offrir de l'assistance au chef mondial de la confidentialité, aux autres membres du réseau de protection de la confidentialité, aux responsables de la confidentialité et à d'autres intervenants, au besoin, afin de :

    (1) permettre aux sociétés du groupe de se conformer au code à l'aide des directives, outils et formations qui ont été mis au point;

    (2) communiquer les pratiques exemplaires pour la gestion confidentialité et de la protection des données dans la région;

    (3) confirmer qu'on tient compte des exigences en matière de confidentialité et de protection des données lorsqu'on met en œuvre de nouveaux produits et services au sein des sociétés du groupe;

    (4) offrir de l'assistance aux responsables de la confidentialité, aux sociétés du groupe, aux unités d'affaires, aux domaines fonctionnels et au personnel d'approvisionnement relativement au recours à des sous-traitants de données.

Responsables de la confidentialité **8.3** Les responsables de la confidentialité d'ADP sont des cadres nommés par un cadre responsable ou la haute direction d'ADP afin de mettre en œuvre et de faire respecter le code au sein d'une unité d'affaires ou d'un domaine fonctionnel d'ADP. Ils sont responsables de la mise en œuvre efficace du code au sein de l'unité d'affaires ou des domaines fonctionnels en question. Ils doivent notamment s'assurer que des contrôles efficaces de gestion de la confidentialité et de la protection des données sont intégrés à toutes les pratiques commerciales touchant les données des clients et que des ressources et un budget adéquats sont fournis afin de respecter les obligations du présent code. Ils peuvent déléguer des tâches et attribueront les ressources nécessaires, au besoin, afin de s'acquitter de leurs responsabilités et d'atteindre les objectifs de conformité.

Les responsabilités des responsables de la confidentialité comprennent :

(a) surveiller la gestion et la conformité globales de la confidentialité et de la protection des données au sein de leur société du groupe, unité d'affaires ou domaine fonctionnel et s'assurer que tous les processus, systèmes et outils créés par l'équipe mondiale de protection des données personnelles et de la gouvernance ont été efficacement mis en œuvre;

(b) confirmer que les tâches liées à la gestion et la conformité de la confidentialité et de la protection des données sont convenablement déléguées dans le cadre des activités ordinaires, ainsi que pendant et à la suite des activités de restructuration organisationnelle, d'externalisation, de fusion et d'acquisition et de désinvestissement;

(c) collaborer avec le chef mondial de la confidentialité et les membres pertinents du réseau de protection de la confidentialité afin de comprendre et de traiter toute nouvelle exigence légale et de s'assurer que les processus de gestion de la confidentialité et de la protection des données sont mis à jour afin de refléter les circonstances et les exigences réglementaires et légales changeantes;

(d) consulter le chef mondial de la confidentialité et les membres pertinents du réseau de protection de la confidentialité dans tous les cas de conflit réel ou potentiel entre les lois applicables et le présent code;

(e) surveiller les sous-traitants de données utilisés par la société du groupe, l'unité d'affaires ou le domaine fonctionnel afin de confirmer leur respect continu du présent code et des contrats de sous-traitance des données;

(f) confirmer que tout le personnel de la société du groupe, de l'unité d'affaires ou du domaine fonctionnel a suivi les formations requises relatives à la confidentialité;

(g) demander que les données des clients enregistrées soient supprimées, dépersonnalisées ou transférées, conformément à l'article 2.2.

Cadres responsables

8.4 À titre de chefs d'unité d'affaires ou de domaine fonctionnel, il incombe aux cadres responsables de s'assurer que leur organisation adopte des pratiques de gestion de la confidentialité et de la protection des données efficaces. Chaque cadre responsable (a) nommera des responsables de la confidentialité convenables, (b) veillera à ce que des ressources et un budget adéquats soient prévus pour assurer la conformité et (c) offriront du soutien, au besoin, au responsable de la confidentialité pour traiter toute lacune en matière de conformité et gérer les risques.

Conseil de direction en matière de confidentialité

8.5 Le chef mondial de la confidentialité présidera un conseil de direction en matière de confidentialité composé des responsables de la confidentialité, de membres du réseau de protection de la confidentialité choisis par chef mondial de la confidentialité et d'autres personnes qui pourraient s'avérer nécessaires à la réalisation de la mission du conseil. Le conseil de direction en matière de confidentialité créera et maintiendra une structure soutenant les activités qui permettent aux sociétés du groupe, unités d'affaires et domaines fonctionnels de respecter le présent code, réaliser les tâches qui y sont décrites et soutenir le chef mondial de la confidentialité.

Membres du réseau de protection de la confidentialité et responsables de la confidentialité par défaut

8.6 Si, à tout moment, aucun chef mondial de la confidentialité n'est nommé ou habilité pour remplir les fonctions attribuées à ce poste, l'avocat général nommera quelqu'un pour agir à titre de chef mondial de la confidentialité. Si, à tout moment, aucun membre du réseau de protection de la confidentialité n'est désigné pour une région ou une organisation particulière, le chef mondial de la confidentialité effectuera les tâches du membre du réseau de protection de la confidentialité décrites à l'article 8.2.

Si, à tout moment, aucun responsable de la confidentialité n'est désigné pour une société du groupe, une unité d'affaires ou un domaine fonctionnel, le cadre responsable nommera une personne convenable pour effectuer les tâches décrites à l'article 8.3.

Poste statutaire

8.7 Lorsque les membres du réseau de protection de la confidentialité, p. ex., les directeurs de la protection des données en vertu des lois applicables de l'EEE, occupent leur poste en vertu de la loi, ils s'acquitteront de leurs responsabilités dans la mesure où elles n'entrent pas en conflit avec leur poste statutaire.

Article 9 – Politiques et procédures

Politiques et procédures **9.1** ADP créera et mettra en œuvre des politiques, des normes, des lignes directrices et des procédures en conformité avec le présent code.

Information sur les systèmes **9.2** ADP conservera de l'information facilement accessible sur la structure et le fonctionnement de tous les systèmes et processus qui traitent des données de clients, dont des registres de systèmes et de processus qui influencent les données des clients ainsi que l'information générée dans le cadre des évaluations de l'incidence sur la protection des données. Une copie de cette information sera fournie sur demande à la principale APD ou à une APD compétente pour le client en vertu de l'article 11.3.

Article 10 – Formation

Formation **10.1** ADP fournira de la formation sur les obligations et les principes décrits dans le présent code ainsi que toute autre obligation en matière de confidentialité et de sécurité des données à tous les employés ayant accès à des données de clients ou ayant des responsabilités associées au traitement de données de clients.

Article 11 – Surveillance et audit de la conformité

Audits internes **11.1** ADP auditera régulièrement les processus et procédures commerciaux nécessitant le traitement de données de clients pour en assurer la conformité avec le présent code. Notamment :

(a) Les audits peuvent être effectués dans le cadre des activités ordinaires du service d'audit interne d'ADP (y compris en faisant appel à des tiers indépendants) et des autres équipes internes participant à des activités d'assurance, et de façon ponctuelle à la demande du chef mondial de la confidentialité;

(b) Le chef mondial de la confidentialité peut aussi demander qu'un audit soit effectué par un auditeur externe et en informera le cadre responsable de l'unité d'affaires en question ou le comité de direction d'ADP, au besoin;

(c) Les normes professionnelles applicables en matière d'indépendance, d'intégrité et de confidentialité seront respectées durant le processus d'audit;

(d) Le chef mondial de la confidentialité et le membre convenable du réseau de protection de la confidentialité seront informés des résultats de l'audit;

(e) Dans la mesure où l'audit révèle des cas de non-conformité avec le présent code, ces résultats seront communiqués aux responsables de la confidentialité et aux cadres responsables applicables. Les responsables de

la confidentialité collaboreront avec l'équipe mondiale de protection des données personnelles et de la gouvernance afin de créer et d'exécuter un plan de mesures correctives convenable;

(f) Une copie des résultats de l'audit lié à la conformité avec le présent code sera fournie sur demande à la principale APD ou à une APD compétente en vertu de l'article 11.3.

Demande d'audit du client

11.2 ADP traitera les demandes d'audit du client comme décrit dans le présent article 11.2. ADP répondra aux questions posées par le client relativement au traitement de ses données par ADP. Dans le cas où le client juge raisonnablement que les réponses fournies par ADP justifient une analyse plus approfondie, ADP prendra l'une des mesures suivantes, avec l'accord du client :

(a) ADP rendra accessibles les installations qu'elle utilise pour traiter les données des clients pour un audit effectué par un tiers évaluateur indépendant qualifié raisonnablement acceptable pour ADP, lié par des obligations de confidentialité satisfaisantes pour ADP et embauché par le client. Le client fournira une copie du rapport d'audit au chef mondial de la confidentialité, qui sera traitée comme des renseignements confidentiels d'ADP. Pas plus d'un audit ne sera effectué par année, par client, durant la période du contrat de services et pendant les heures d'ouverture ordinaires. Les vérifications seront sujettes (i) à une demande écrite remise à ADP au moins 45 jours avant la date d'audit proposée, (ii) à un plan d'audit écrit détaillé examiné et approuvé par l'organisation de sécurité d'ADP et (iii) aux politiques d'ADP sur la sécurité sur place. De tels audits auront lieu uniquement en la présence d'un représentant de l'organisation mondiale de la sécurité d'ADP, de l'équipe mondiale de protection des données personnelles et de la gouvernance d'ADP ou de la personne désignée par le représentant approprié. On ne permettra pas aux audits d'interrompre les activités de traitement d'ADP ou de compromettre la sécurité et la confidentialité des données personnelles d'autres clients d'ADP;

(b) ADP fournira une déclaration au client rédigée par un tiers évaluateur indépendant qualifié attestant que les processus et procédures commerciaux d'ADP nécessitant le traitement de données de clients respectent le présent code.

ADP peut exiger des frais raisonnables au client pour un tel audit.

Le présent article 11.2 constitue un ajout ou une précision aux droits d'audit potentiellement accordés au client en vertu des lois applicables et des contrats de service. En cas de contradiction, les dispositions des lois applicables et des contrats de service auront préséance.

Audits par les APD **11.3** Toute APD ou tout pays de l'EEE dont les compétences lui permettent d'auditer un client d'ADP obtiendra l'autorisation d'auditer les transferts de données concernés pour évaluer la conformité au présent code, selon les mêmes conditions qui s'appliqueraient si cette APD auditait le client lui-même en vertu des lois applicables au contrôleur des données.

Afin de faciliter lesdits audits :

(a) ADP et le client collaboreront de bonne foi pour tenter de répondre à la demande en fournissant à l'APD les renseignements requis, tels que les rapports d'audit d'ADP, et faciliteront la discussion entre l'APD et les experts en la matière du client et d'ADP, qui peuvent examiner les mécanismes de contrôle en place en matière de sécurité, de confidentialité des données et d'opérations. Le client aura accès à ses propres données conformément au contrat de services et peut déléguer cet accès aux représentants de l'APD;

(b) Si les renseignements rendus disponibles grâce à ces mécanismes ne suffisaient pas à répondre aux objectifs avoués de l'APD, ADP lui donnera l'occasion de communiquer avec son auditeur;

(c) Si cela s'avérait insuffisant, ADP donnera à l'APD le droit d'examiner directement les installations de traitement qui servent à traiter les données du client, moyennant un préavis raisonnable, durant les heures d'ouverture et dans le plus grand respect de la confidentialité des renseignements obtenus et des secrets commerciaux d'ADP. L'APD aura accès uniquement aux données qui appartiennent à ce client.

Le présent article 11.3 constitue un ajout ou une précision aux droits d'audit potentiellement accordés à l'APD en vertu des lois applicables et du contrat de services. En cas de contradiction, les dispositions des lois applicables auront préséance.

Rapport annuel **11.4** Le chef mondial de la confidentialité devra produire un rapport annuel destiné au comité de direction d'ADP qui traitera de la conformité au présent code, de la confidentialité, des risques en matière de protection des données ainsi que d'autres questions pertinentes. Ledit rapport présentera les renseignements fournis par le réseau de protection de la confidentialité et d'autres instances concernant les avancées locales et les enjeux particuliers des sociétés du groupe.

Mesures d'atténua-tion **11.5** ADP s'engage à prendre les mesures nécessaires pour remédier à toute violation du présent code relevée lors d'audits portant sur la conformité.

Droits des employés du client

12.1 En cas de violation, de la part d'ADP, du présent code en ce qui a trait aux données personnelles d'un employé d'un client régies par le présent code, ledit employé du client peut, en tant que tiers bénéficiaire, exiger l'application 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 traitement des données à l'encontre de l'entité contractante d'ADP.

Dans la mesure où l'employé du client peut faire valoir tous ces droits à l'encontre de l'entité contractante d'ADP, celle-ci ne peut pas plaider le manquement d'un sous-traitant de données à ses obligations pour se dégager de ses responsabilités, sauf dans la mesure où le sous-traitant de données constituerait aussi une défense pour ADP. ADP peut toutefois se pourvoir de toute défense ou tout droit auquel le client aurait pu avoir recours. ADP peut se pourvoir de toute défense dont elle aurait pu se pourvoir contre le client (comme la négligence contributive de la victime) dans le cadre de sa défense relative à la réclamation de la personne touchée.

Procédure relative aux plaintes

12.2 Les employés du client peuvent déposer une plainte par écrit concernant toute réclamation en vertu de l'article 12.1 auprès de l'équipe mondiale de protection des données personnelles et de la gouvernance par la poste ou par courriel à l'adresse indiquée à la fin du présent code. L'employé du client peut aussi déposer une plainte ou une réclamation auprès des autorités ou des tribunaux en conformité avec l'article 12.3 du présent code.

L'équipe mondiale de protection des données personnelles et de la gouvernance sera responsable de traiter la plainte. Chaque plainte sera assignée à un membre du personnel compétent (soit au sein de l'équipe mondiale de protection des données personnelles et de la gouvernance, soit au sein de l'unité d'affaires ou du domaine fonctionnel concerné). Ce membre du personnel aura la responsabilité :

(a) d'accuser rapidement réception de la plainte;

(b) de l'analyser et, s'il y a lieu, d'entreprendre une enquête;

(c) d'en informer, si la plainte s'avère fondée, le responsable de la confidentialité et les membres du réseau de protection de la confidentialité concernés de sorte qu'un plan de mesures correctives soit élaboré et exécuté;

(d) de tenir à jour un registre de toutes les plaintes reçues, de toutes les réponses fournies et de toutes les mesures correctives prises par ADP.

ADP déploiera des efforts raisonnables pour traiter les plaintes sans retard injustifié, de sorte que l'employé du client reçoive une réponse dans les

quatre semaines suivant le dépôt de la plainte. La réponse sera envoyée par écrit et transmise de la manière utilisée au départ par l'employé du client pour communiquer avec ADP (*p. ex.*, par la poste ou par courriel). La réponse exposera les mesures prises par ADP pour enquêter sur la plainte et indiquera la décision d'ADP quant aux mesures à prendre (le cas échéant) à la suite de la plainte.

Advenant le cas où ADP n'arriverait pas à terminer raisonnablement son enquête et à répondre en moins de quatre semaines, l'entreprise informera l'employé du client dans les quatre semaines qu'une enquête est en cours et qu'une réponse lui sera communiquée dans les huit semaines suivantes.

Si l'employé du client n'est pas satisfait de la réponse donnée à sa plainte par ADP (p. ex., la demande est refusée) ou si ADP ne respecte pas les conditions des procédures relatives aux plaintes énoncées dans le présent article 12.2, l'employé du client peut déposer une plainte ou une réclamation auprès des autorités ou des tribunaux conformément aux dispositions de l'article 12.3.

Autorité compétente pour les réclamations des employés du client

12.3 Les employés du client sont encouragés à suivre d'abord la procédure relative aux plaintes énoncée à l'article 12.2 du présent code avant de déposer une plainte ou une réclamation auprès des autorités ou des tribunaux.

Les employés du client peuvent, à leur discrétion, soumettre une réclamation en vertu de l'article 12.1 en transmettant une plainte :
(i) à l'APD de son pays de résidence habituel, de son lieu de travail ou de l'endroit où la violation a eu lieu à l'encontre de l'entité contractante ou déléguée d'ADP;
(ii) à l'APD en chef ou aux tribunaux des Pays-Bas, mais, dans ce cas, uniquement à l'encontre de l'entité déléguée d'ADP.

Les employés du client peuvent, à leur discrétion, soumettre une réclamation en vertu de l'article 12.1 en transmettant une plainte :
(i) aux tribunaux de son pays de résidence habituel ou du pays d'origine du transfert de données en vertu du présent code à l'encontre de l'entité contractante ou déléguée d'ADP;
(ii) à l'APD en chef ou aux tribunaux des Pays-Bas, mais, dans ce cas, uniquement à l'encontre de l'entité déléguée d'ADP.

Les APD et les tribunaux appliqueront aux différends leurs propres droits substantiel et procédural. Le choix de l'employé du client n'influencera pas les droits fondamentaux ou procéduraux octroyés aux parties en vertu des lois applicables.

Droits des clients **12.4** Le client peut faire valoir ses droits en vertu du présent code à l'encontre de (i) l'entité contractante d'ADP ou de (ii) l'entité déléguée d'ADP devant l'APD en chef ou les tribunaux des Pays-Bas, mais uniquement si l'entité contractante d'ADP n'est pas établie dans un pays de l'EEE. L'entité déléguée d'ADP veillera à ce que des mesures appropriées soient prises pour remédier aux violations du présent code par l'entité contractante d'ADP ou toute autre société du groupe concernée.

Ni l'entité contractante ni l'entité déléguée d'ADP ne peuvent plaider le manquement d'une autre société du groupe ou d'un sous-traitant de données à ses obligations pour se dégager de ses responsabilités, sauf dans la mesure où la défense de ladite société du groupe ou dudit sous-traitant de données constituerait aussi une défense pour ADP.

Recours possibles et fardeau de la preuve pour les employés du client **12.5** Advenant le cas où l'employé d'un client dépose une réclamation en vertu de l'article 12.1, l'employé du client aura droit à une compensation pour les dommages subis dans la mesure prévue par les lois applicables de l'EEE.

Si l'employé du client dépose une réclamation pour dommages en vertu de l'article 12.1, le fardeau incombera à l'employé du client de prouver qu'il a subi des dommages et de présenter les faits qui démontrent qu'il est plausible que les dommages aient été subis en raison d'une violation du présent code. Par la suite, il incombera à l'entité contractante d'ADP (ou à son entité déléguée, selon le cas) de prouver que les dommages subis par l'employé du client en raison d'une violation du présent code ne sont pas attribuables à la société du groupe concernée ou à un sous-traitant de données ou de se pourvoir de toute autre défense applicable.

Dédommagement du client **12.6** En cas de violation du présent code, et sous réserve des modalités du contrat de services, les clients ont droit à un dédommagement pour les dommages directs subis conformément aux dispositions du contrat de services.

Assistance mutuelle **12.7** Toutes les sociétés du groupe doivent, s'il y a lieu, collaborer et aider, dans la mesure de ce qui est raisonnablement possible, (a) à traiter une demande, une plainte ou une réclamation déposée par un client ou par l'employé d'un client ou (b) à se soumettre à une enquête ou investigation licite menée par une autorité gouvernementale compétente.

La société du groupe qui reçoit une demande de renseignements conformément à l'article 6.1, ou une plainte ou une réclamation conformément aux articles 12.2 ou 12.3, a la responsabilité de gérer les communications avec le client ou l'em-

ployé du client concernant la demande ou la réclamation, sauf si les circonstances exigent qu'il en soit autrement ou conformément aux directives de l'équipe mondiale de protection des données personnelles et de la gouvernance.

Recommandations et décisions contraignantes de l'APD **12.8** ADP collaborera de bonne foi avec l'APD en chef et fournira tous les efforts nécessaires pour suivre les recommandations formulées par celle-ci et l'APD compétente en vertu de l'article 12.3 sur l'interprétation et l'application du présent code. ADP respectera les décisions contraignantes des APD compétentes.

Lois applicables en vertu du présent code **12.9** Le présent code est régi et interprété en fonction des lois des Pays-Bas.

Article 13 – Sanctions pour non-conformité

Non-conformité **13.1** Pour le personnel, le fait de ne pas se conformer au présent code peut entraîner des mesures disciplinaires ou contractuelles appropriées, conformément aux lois applicables et aux politiques d'ADP, pouvant mener à la fin de la relation employeur-employé ou à la résiliation du contrat.

Article 14 – Conflits entre le présent code et les lois applicables au responsable du traitement de données

Conflits entre le présent code et les lois **14.1** En cas de conflit entre les lois applicables au responsable du traitement de données et le présent code, le cadre responsable ou le responsable de la confidentialité consultera le chef mondial de la confidentialité, les membres concernés du réseau de protection de la confidentialité (selon le cas), ainsi que les Services juridiques de l'unité d'affaires afin de déterminer la manière de se conformer au présent code et de résoudre le conflit dans la mesure de ce qui est raisonnablement possible en fonction des exigences prévues par la loi régissant ADP.

Conflits liés aux nouvelles exigences prévues par la loi **14.2** Le personnel des Services juridiques, les directeurs de la sécurité d'entreprise d'ADP et les responsables de la confidentialité se doivent d'informer rapidement l'équipe mondiale de protection des données personnelles et de la gouvernance de toute nouvelle exigence prévue par la loi dont ils pourraient être mis au courant et qui pourrait interférer avec la capacité d'ADP de se conformer au présent code.

Le responsable de la confidentialité concerné, de concert avec les Services juridiques, se doit d'informer rapidement les cadres responsables de toute nouvelle exigence prévue par la loi qui pourrait interférer avec la capacité d'ADP de se conformer au présent code.

Signalement à l'APD en chef **14.3** Si ADP se rend compte que les lois applicables au responsable du traitement de données ou qu'une modification apportée à ces lois risque d'entraîner des conséquences négatives considérables sur la capacité d'ADP de remplir ses obligations en vertu des articles 3.1, 3.2 ou 11.3, ADP le signalera à l'APD en chef.

Article 15 – Modifications du présent code

Approbation des modifications **15.1** Toute modification importante du présent code doit être préalablement approuvée par le chef mondial de la confidentialité ainsi que par l'avocat général et adoptée par le comité de direction d'ADP avant d'être communiquée aux sociétés du groupe. Des modifications mineures peuvent être apportées au présent Code avec l'approbation du chef mondial de la confidentialité. L'entité déléguée d'ADP se doit d'informer l'APD en chef des modifications apportées au présent code sur une base annuelle.

Dans le cas où une modification du présent code aurait d'importantes répercussions sur les conditions de traitement des services à la clientèle, ADP en informera rapidement l'APD en chef, en plus de lui fournir une brève explication des raisons qui ont motivé cette modification, et préviendra le client desdites modifications. Le client bénéficie de 30 jours suivant la réception du préavis pour notifier ADP par écrit en cas de désaccord avec ladite modification. Advenant le cas où les parties n'arriveraient pas à s'entendre sur une solution acceptable, ADP devra mettre en œuvre une autre solution de transfert de données. Advenant le cas où aucune autre solution de transfert de données ne pourrait être mise en œuvre, le client aura le droit, en vertu du présent code, de suspendre le transfert de données concerné à ADP. Advenant le cas où il serait impossible de suspendre le transfert de données, ADP se doit de permettre au client de résilier les services à la clientèle concernés conformément aux modalités du contrat de services.

Date d'entrée en vigueur des modifications **15.2** Toute modification entrera en vigueur dès qu'elle aura été approuvée conformément à l'article 15.1, publiée sur le site Web www.adp.com et communiquée aux clients.

Versions précédentes

15.3 Toute demande, plainte ou réclamation provenant de l'employé d'un client concernant le présent code sera examinée en fonction de la version du présent code en vigueur au moment où la demande, plainte ou réclamation est déposée.

Article 16 – Mise en œuvre et périodes de transition

Mise en œuvre

16.1 La mise en œuvre du présent code sera supervisée par les responsables de la confidentialité, avec l'aide de l'équipe mondiale de protection des données personnelles et de la gouvernance. À l'exception du cas prévu ci-dessous, une période de transition de 18 mois à compter de la date de prise d'effet (telle qu'elle a été établie à l'article 1.6) afin de permettre de se conformer au présent code.

Par conséquent, sauf indication contraire, tout le traitement des données de client devra être effectué conformément aux dispositions du présent code dans les 18 mois suivant la date de prise d'effet du code, lequel devra être pleinement en vigueur d'ici là. Pendant la période de transition, le présent Code prendra effet pour une société du groupe aussitôt que ladite société du groupe aura terminé les tâches nécessaires à la mise en œuvre complète et en aura informé le chef mondial de la confidentialité de manière appropriée.

Nouvelles sociétés du groupe

16.2 Toute entité qui devient une société du groupe après la date d'entrée en vigueur aura deux ans, à partir du moment où elle devient une société du groupe, pour se conformer au présent code.

Entités cédées

16.3 Une entité cédée restera soumise au présent code après sa cession durant la période nécessaire à ADP pour démêler le traitement des données des clients lié à ladite entité cédée.

Période de transition relative aux conventions existantes

16.4 Dans le cas où le présent code affecterait des conventions existantes avec des sous-traitants de données ou d'autres tiers, les modalités de la convention prévaudront jusqu'à ce que ladite convention soit renouvelée dans le cours normal des activités à condition, toutefois, que toutes lesdites conventions existantes se conforment au présent code dans les 18 mois suivant la date de prise d'effet.

Coordonnées

Équipe mondiale de protection des données personnelles et de la gouvernance d'ADP :
privacy@adp.com

Entité déléguée d'ADP

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

Interprétation

INTERPRÉTATION DU PRÉSENT CODE :

(i) À moins que le contexte ne dicte autrement, toute référence à un article ou une annexe en particulier fait référence à cet article ou à cette annexe du présent document, avec toutes leurs modifications successives;

(ii) Les titres ont été ajoutés uniquement à des fins pratiques et ne doivent pas être utilisés pour interpréter quelque modalité du présent code;

(iii) Si la définition d'un mot ou d'une phrase est fournie, ses autres formes grammaticales prennent une signification équivalente;

(iv) La forme masculine comprend la forme féminine;

(v) Les termes « comprendre », « comprend », « y compris » et tous les mots qui les suivent ne doivent pas être interprétés de manière à limiter la généralité des mots ou des concepts qui les précèdent et inversement;

(vi) Le terme « écrit » comprend toutes les communications documentées, les écrits, les contrats, les dossiers et signatures électroniques, les télécopies ou les autres instruments ayant une valeur légale et exécutoire sans égard au format;

(vii) Une référence à un document (y compris, sans s'y limiter, au présent code) fait référence au document amendé, modifié, avec supplément ou remplacé, sauf dans la mesure où cela serait interdit par le présent code ou le document de référence lui-même;

(viii) Une référence à une loi comprend toutes les exigences réglementaires, les recommandations sectorielles et les meilleures pratiques publiées par les autorités de surveillance ou autres entités nationales ou internationales.

ANNEXE 1 – Définitions relatives aux REC

Activités de soutien aux clients	Le terme ACTIVITÉS DE SOUTIEN AUX CLIENTS se définit comme les activités de traitement entreprises par ADP dans un objectif de prestation de ses produits et services. Les activités de soutien au client peuvent comprendre, par exemple, la formation de professionnels, la réponse à des questions sur les services, l'ouverture et la résolution de tickets de soutien technique, la fourniture d'information sur les produits et services (y compris des mises à jour et des alertes relatives à la conformité), le contrôle et le suivi de la qualité ainsi que d'autres activités connexes qui facilitent l'utilisation efficace des produits et services d'ADP.
ADP (Groupe ADP)	Le terme ADP (GROUPE ADP) fait référence, collectivement, à Automatic Data Processing, Inc. (la société mère) et aux sociétés du groupe, y compris ADP, Inc.
Analyse d'impact sur la protection des données (AIPD)	Le terme ANALYSE D'IMPACT SUR LA PROTECTION DES DONNÉES (AIPD) devrait se définir comme une procédure visant à mener et à documenter une analyse préalable de l'impact que pourrait avoir un traitement particulier sur la protection des données personnelles lorsque les probabilités qu'un tel traitement comporte un risque important pour les droits et libertés individuels sont élevées, particulièrement lors de l'utilisation de nouvelles technologies. Une AIPD devrait comprendre : (i) une description : (a) de la portée et du contexte du traitement; (b) des fins commerciales pour lesquelles les données personnelles sont traitées; (c) des raisons précises pour lesquelles les catégories spéciales de données sont traitées; (d) des catégories de destinataires des données personnelles, y compris les destinataires non régis par une décision d'adéquation; (e) des périodes de stockage des données personnelles; (ii) une évaluation : (a) de la nécessité et de la proportionnalité du traitement; (b) des risques pour les droits individuels relatifs à la confidentialité des données; et des moyens pris pour réduire ces risques, y compris les dispositifs et les mesures de sécurité ainsi que les autres mécanismes (comme la confidentialité

	des données dès la conception) visant à assurer la protection des données personnelles.
Archive	Le terme ARCHIVE se définit comme une collection de données personnelles qui ne sont plus nécessaires pour atteindre l'objectif pour lequel les données ont été recueillies à l'origine ou qui ne sont plus utilisées dans le cadre des activités générales, mais qui peuvent être utilisées uniquement à des fins historiques, scientifiques ou statistiques, ou encore à des fins de résolution de conflits, d'enquêtes ou d'archivage général. L'accès aux archives est limité aux administrateurs de systèmes et aux autres employés dont les fonctions en exigent expressément l'accès.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC., la société mère du Groupe ADP, est une société par actions du Delaware (É.-U.) dont le principal lieu d'affaires est situé au : 1, ADP Boulevard, Roseland, New Jersey, 07068-1728, États-Unis.
Autorité de protection des données ou APD	Les termes AUTORITÉ DE PROTECTION DES DONNÉES OU APD se définissent comme toute autorité de réglementation ou de surveillance qui supervise la protection ou la confidentialité des données dans un pays où est établie une société du groupe.
Avocat général	Le terme AVOCAT GÉNÉRAL se définit comme l'avocat général d'Automatic Data Processing, Inc.
Brèche de sécurité des données	Le terme BRÈCHE DE SÉCURITÉ DES DONNÉES se définit comme tout incident qui a des conséquences sur la confidentialité, l'intégrité ou la disponibilité des données personnelles, tel que l'usage non autorisé ou la divulgation des données personnelles ou un accès non autorisé qui compromet la confidentialité ou la sécurité des données personnelles.
Cadre responsable	Le terme CADRE RESPONSABLE se définit comme le directeur général d'une société du groupe ou le chef d'une unité d'affaires ou d'un domaine fonctionnel qui est le principal responsable du budget de la société du groupe, de l'unité d'affaires ou du domaine fonctionnel.
Candidat	Le terme CANDIDAT se définit comme toute personne qui fournit des données personnelles à ADP dans un contexte de soumission de candidature pour un poste de collaborateur à ADP.
Catégories spéciales de données	Le terme CATÉGORIES SPÉCIALES DE DONNÉES se définit comme des données personnelles qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, son appartenance à des partis politiques ou à d'autres organisations similaires, ses croyances religieuses ou philosophiques, son appartenance à une organisation professionnelle ou à un syndicat, son état de santé physique ou psychologique y compris toute opinion sur

	celui-ci, ses handicaps, son code génétique, ses dépendances, sa vie sexuelle, les infractions criminelles qu'elle a commises, son casier judiciaire ou les procédures relatives à des activités criminelles ou illégales.
Chef mondial de la confidentialité	Le terme CHEF MONDIAL DE LA CONFIDENTIALITÉ se définit comme le collaborateur d'ADP qui porte ce titre au sein d'Automatic Data Processing, Inc.
Client	Le terme CLIENT se définit comme tout tiers qui utilise un ou plusieurs produits ou services d'ADP dans le cadre de ses propres activités.
Code	Le terme CODE fait référence (selon le cas) au Code d'ADP relatif à la confidentialité des données commerciales, au Code d'ADP relatif à la confidentialité en milieu de travail (à l'interne) et au Code d'ADP relatif à la confidentialité des services de traitement des données de clients, collectivement appelés les codes.
Collaborateur	Le terme COLLABORATEUR se définit comme 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 confidentialité en milieu de travail ne régit donc pas le traitement des données personnelles des individus coemployés.
Comité de direction d'ADP	Le terme COMITÉ DE DIRECTION D'ADP se définit comme le comité de directeurs constitué (i) du chef de la direction d'Automatic Data Processing, Inc. et (ii) des autres directeurs qui sont directement sous ses ordres et qui, collectivement, sont responsables des activités du Groupe ADP.
Conseil de direction en matière de confidentialité	Le terme CONSEIL DE DIRECTION EN MATIÈRE DE CONFIDENTIALITÉ se définit comme le conseil dirigé par le chef mondial de la confidentialité et composé des responsables de la confidentialité, des membres du réseau de protection de la confidentialité sélectionnés par le chef mondial de la confidentialité et d'autres personnes dont la participation peut s'avérer essentielle à la mission du Conseil.
Consommateur	Le terme CONSOMMATEUR se définit comme une personne qui interagit directement avec ADP à titre personnel. Par exemple, sont comprises dans les consommateurs les personnes qui participent aux programmes de développement de talents ou font un usage personnel des produits et services d'ADP (c.-à-d. en l'absence d'une relation employeur-employé entre eux et ADP ou un client d'ADP).
Contrat de service	Le terme CONTRAT DE SERVICE se définit comme tout contrat, toute convention ou toutes modalités en vertu desquels ADP fournit des services à la clientèle à un client.
Contrat de sous-	Le terme CONTRAT DE SOUS-TRAITANCE DES DONNÉES se définit

traitance des données	comme une entente écrite ou électronique conclue entre ADP et un tiers sous-traitant des données en vertu de l'article 7.1 du Code d'ADP relatif à la confidentialité des services de traitement des données de clients.
Contrat de traitement des données	Le terme CONTRAT DE TRAITEMENT DES DONNÉES doit se définir comme tout contrat relatif au traitement de données personnelles conclu entre ADP et un tiers responsable du traitement des données.
Contrôleur des données	Le terme CONTRÔLEUR DES DONNÉES se définit comme l'entité ou la personne physique qui, seule ou avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.
Coordonnées d'affaires	Le terme COORDONNÉES D'AFFAIRES se définit comme toute donnée appartenant à un professionnel qui figure normalement sur une carte de visite ou dans une signature de courriel.
Date de prise d'effet	Le terme DATE DE PRISE D'EFFET se définit comme la date à laquelle les codes entrent en vigueur, tel que cela est énoncé à l'article 1 des codes.
Décision d'adéquation	Le terme DÉCISION D'ADÉQUATION se définit comme toute résolution prise par une autorité de protection des données ou une autre entité compétente reconnaissant qu'un pays, une région ou le destinataire d'un transfert de données fournit une protection adéquate des données personnelles. Les entités régies par une décision d'adéquation comprennent les destinataires situés dans des pays qui, en vertu des lois applicables, sont reconnus pour fournir une protection adéquate des données et les destinataires tenus par un autre instrument (comme un ensemble de Règles d'entreprise contraignantes) qui sont approuvés par l'autorité de protection des données concernée ou une autre entité compétente. En ce qui concerne les États-Unis, les entreprises qui obtiennent une certification dans le cadre d'une structure de confidentialité des données É.-U./EEE ou É.-U./Suisse, comme le bouclier de protection des données, seraient régies par une décision d'adéquation.
Données du client	Le terme DONNÉES DU CLIENT se définit comme les données personnelles appartenant aux employés du client (y compris les employés éventuels, les anciens employés et les personnes à charge des employés) qui sont traitées par ADP dans le cadre de la prestation de services à la clientèle.
Données personnelles ou données	Les termes DONNÉES PERSONNELLES ou DONNÉES se définissent comme toute information concernant une personne identifiée ou identifiable. Les données personnelles peuvent aussi être appelées renseignements personnels dans le cadre de politiques ou de normes visant à mettre en œuvre les codes.
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. 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	Le terme EMPLOYÉ DU CLIENT se définit comme toute personne dont les données personnelles sont traitées par ADP à titre de responsable du traitement de données pour un client conformément à une convention de services. Par souci de clarté, le terme EMPLOYÉ DU CLIENT se définit comme toutes les personnes dont les données personnelles sont traitées par ADP dans le cadre de l'exécution des services à la clientèle (sans égard à la nature juridique de la relation entre la personne et le client). Ne sont pas compris dans ce terme les professionnels dont les données personnelles sont traitées par ADP dans le cadre de la relation directe entre ADP et le client. Par exemple, ADP pourrait traiter les données personnelles d'un professionnel des RH afin de signer un contrat avec le client; ces données sont régies par le Code d'ADP relatif à la confidentialité des données commerciales. Toutefois, si ADP fournit des services de traitement de la paie au client (p. ex., émission de fiches de paie ou assistance pour l'utilisation d'un système ADP), les données de la personne seront traitées comme des données du client.
Enfants	Aux fins de collecte de données et de marketing d'ADP, le terme ENFANTS se définit comme toute personne qui, selon les lois applicables, n'a pas atteint l'âge nécessaire pour pouvoir consentir à ladite collecte de données ou audit marketing.
Entité cédée	Le terme ENTITÉ CÉDÉE se définit comme une société du groupe dont ADP n'est plus propriétaire à la suite de la vente d'actions ou d'actifs de l'entreprise ou de tout autre désinvestissement, de sorte que l'entreprise ne se qualifie plus en tant que société du groupe.
Entité contractante d'ADP	Le terme ENTITÉ CONTRACTANTE D'ADP se définit comme la société du groupe qui a conclu un contrat exigé par les codes, tels qu'un contrat de service, un contrat de sous-traitance des données ou une convention de transfert de données.
Entité déléguée d'ADP	Le terme ENTITÉ DÉLÉGUÉE D'ADP se définit comme ADP Nederland, B.V., dont le siège social est enregistré au Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Pays-Bas.
Équipe mondiale de protection des données personnelles et de la gouvernance	Le terme ÉQUIPE RESPONSABLE DE LA GOUVERNANCE ET DE LA CONFIDENTIALITÉ DES DONNÉES À L'ÉCHELLE MONDIALE se définit comme le bureau de la confidentialité et de la gouvernance des données d'ADP. Le bureau de la confidentialité et de la gouvernance des données d'ADP est dirigé par le chef mondial de la confidentialité et est composé des chefs et des gestionnaires de la confidentialité des données ainsi que des

	autres membres du personnel qui ont un lien hiérarchique avec le chef mondial de la confidentialité ou avec les chefs et les gestionnaires de la confidentialité des données.
Exigences obligatoires	Le terme EXIGENCES OBLIGATOIRES doit se définir comme les obligations en vertu de toute loi régissant les responsables du traitement de données qui nécessitent le traitement de données personnelles dans un objectif (i) de sécurité ou de défense nationale; (ii) de sécurité publique; (iii) de prévention, d'enquête, de détection ou de poursuite liée à des infractions criminelles ou à des violations des codes d'éthique des professions réglementées; ou (iv) de protection de toute personne ou des droits et libertés individuels.
Fins commerciales	Le terme FINS COMMERCIALES se définit comme des fins légitimes de traitement de données personnelles conformément aux articles 2, 3 ou 4 de tout code d'ADP ou de catégories spéciales de données conformément à l'article 4 de tout code d'ADP.
Fournisseur	Le terme FOURNISSEUR se définit comme tout tiers qui fournit des biens ou des services à ADP (p. ex., à titre de fournisseur de services, d'agent, de responsable du traitement de données, de consultant ou de vendeur).
Individus coemployé	Le terme INDIVIDU COEMPLOYÉ se définit comme un employé d'un client états-unien qui est coemployé par une société états-unienne indirectement affiliée à Automatic Data Processing, Inc. dans le cadre de l'offre de services de l'organisation employeur professionnelle d'ADP aux É.-U.
Intérêt prédominant	Le terme INTÉRÊT PRÉDOMINANT se définit comme les intérêts urgents, énoncés dans l'article 13.1 du Code d'ADP relatif à la confidentialité en milieu de travail et du Code d'ADP relatif à la confidentialité des données commerciales, selon lesquels les obligations d'ADP ou les droits individuels énoncés dans les articles 13.2 et 13.3 desdits codes peuvent, dans certaines circonstances particulières, être transgressés si l'intérêt urgent surpasse l'intérêt individuel.
Loi applicable	Le terme LOI APPLICABLE se définit comme toute loi sur la confidentialité ou la protection des données à laquelle est soumise toute activité particulière de traitement des données.
Loi applicable de l'EEE	Le terme LOI APPLICABLE DE L'EEE se définit comme les exigences en vertu des lois applicables de l'EEE qui régissent toutes les données personnelles recueillies à l'origine dans le cadre des activités d'une société du groupe établie dans l'EEE (même si elles ont été transférées à une autre société du groupe établie hors de l'EEE).
Loi applicables au contrôleur des	Aux fins du Code d'ADP relatif à la confidentialité des services de traitement des données de clients, le terme LOIS APPLICABLES AU CONTRÔLEUR DES

données	DONNÉES se définit comme toute loi sur la confidentialité ou la protection des données à laquelle est soumis un client d'ADP à titre de contrôleur desdites données.
Loi régissant les responsables du traitement de données	Aux fins du Code d'ADP relatif à la confidentialité des services de traitement des données de clients, le terme LOI RÉGISSANT LES RESPONSABLES DU TRAITEMENT DE DONNÉES se définit comme toute loi sur la confidentialité ou la protection des données à laquelle est soumise ADP à titre de responsable du traitement de données pour le compte d'un client contrôleur des données.
Objectif secondaire	Le terme OBJECTIF SECONDAIRE se définit comme tout objectif autre que l'objectif original en raison duquel les données personnelles sont traitées dans une plus large mesure.
Partenaire commercial	Le terme PARTENAIRE COMMERCIAL se définit comme tout tiers, outre un client ou un fournisseur, qui a ou a eu une relation d'affaires ou une alliance stratégique avec ADP (*p. ex.*, un partenaire dans le cadre d'une commercialisation en commun, une coentreprise ou un partenaire de développement commun).
Personne	Le terme PERSONNE se définit comme toute personne physique identifiée ou identifiable, à l'exception des individus coemployés, dont les données personnelles sont traitées par ADP soit à titre de responsable du traitement de données ou de contrôleur des données. REMARQUE : le Code d'ADP relatif à la confidentialité des données commerciales et le Code d'ADP relatif à la confidentialité en milieu de travail ne régissent donc pas le traitement des données personnelles des individus coemployés.
Personne à charge	Le terme PERSONNE À CHARGE se définit comme l'époux, le conjoint, l'enfant ou le bénéficiaire d'un collaborateur ou la personne à contacter en cas d'urgence d'un collaborateur ou d'un travailleur intérimaire.
Personnel	Le terme PERSONNEL se définit collectivement comme les collaborateurs actuellement employés par ADP et les travailleurs intérimaires qui travaillent actuellement pour ADP.
Principale autorité chargée de la protection des données (principale APD)	Le terme PRINCIPALE APD doit se définir comme l'autorité néerlandaise de protection des données.
Professionnel	Le terme PROFESSIONNEL se définit comme toute personne (autre qu'un employé) qui interagit directement avec ADP à des fins professionnelles ou commerciales. Par exemple, les professionnels comprennent les membres du personnel des RH des clients qui collaborent avec ADP en tant qu'utilisateurs de ses produits ou services. Les professionnels comprennent également les

	représentants spéciaux des clients, des fournisseurs et des partenaires commerciaux, les relations d'affaires, les organismes de réglementation, les relations dans les médias et toute autre personne qui interagit avec ADP à des fins commerciales.
Règles d'entreprise contraignantes	Le terme RÈGLES D'ENTREPRISE CONTRAIGNANTES se définit comme une politique de confidentialité des données d'un groupe d'entreprises affiliées reconnues comme fournissant une protection adéquate pour le transfert de données personnelles au sein de ce groupe d'entreprises en vertu des lois applicables.
Réseau de protection de la confidentialité	Le terme RÉSEAU DE PROTECTION DE LA CONFIDENTIALITÉ se définit comme les membres de l'équipe mondiale de protection des données personnelles et de la gouvernance ainsi que les membres des Services juridiques, y compris les professionnels en matière de conformité et les directeurs de la protection des données qui sont chargés de la conformité de la confidentialité dans leurs régions, pays, unités d'affaires ou domaines fonctionnels.
Responsable de la confidentialité	Le terme RESPONSABLES DE LA CONFIDENTIALITÉ se définit comme un cadre d'ADP qui a été nommé par un cadre responsable ou par la haute direction d'ADP afin de mettre en œuvre et de faire respecter les Codes relatifs à la confidentialité par une unité d'affaires d'ADP.
Responsable du traitement de données	Le terme RESPONSABLE DU TRAITEMENT DE DONNÉES se définit comme l'entité ou la personne physique qui traite les données personnelles pour le compte du contrôleur des données.
Restrictions de transfert de données de l'EEE	Le terme RESTRICTIONS DE TRANSFERT DE DONNÉES DE L'EEE se définit comme toute restriction concernant le transfert transfrontalier de données personnelles en vertu des lois sur la protection des données d'un pays de l'EEE.
Service à la clientèle	Le terme SERVICES À LA CLIENTÈLE se définit comme les services de gestion du capital humain fournis par ADP à ses clients, tels que le recrutement, les services liés à la paie et à la rémunération, les avantages sociaux des employés, la gestion des talents, l'administration des RH, les services de conseil et d'analyse, ainsi que le service des régimes de retraite.
Société du groupe	Le terme SOCIÉTÉ DU GROUPE se définit comme toute entité juridique affiliée à Automatic Data Processing, Inc. ou à ADP, Inc. si Automatic Data Processing, Inc. ou ADP, Inc. possède directement ou indirectement plus de 50 % du capital-actions émis, détient au moins 50 % des droits de vote lors de l'assemblée générale des actionnaires, a le pouvoir de nommer la majorité des directeurs ou dirige autrement les activités de ladite entité juridique.
Sous-traitant de	Aux fins du Code d'ADP relatif à la confidentialité des services de traitement des

données d'ADP	données de clients, le terme SOUS-TRAITANT DE DONNÉES D'ADP se définit comme toute société du groupe engagée par une autre société du groupe à titre de sous-traitant de données du client.
Sous-traitant interne	Le terme SOUS-TRAITANT INTERNE doit se définir comme toute société du groupe qui traite des données personnelles pour le compte d'une autre société du groupe qui en est le contrôleur.
Sous-traitants de données	Le terme SOUS-TRAITANT DE DONNÉES se définit, collectivement, comme les sous-traitants de données d'ADP et les tiers sous-traitants des données.
Tiers	Le terme TIERS se définit comme toute personne, toute entreprise privée ou tout organisme gouvernemental qui n'est pas une société du groupe.
Tiers responsable du contrôle des données	Le terme TIERS RESPONSABLE DU CONTRÔLE DES DONNÉES se définit comme un tiers qui traite les données personnelles et détermine les finalités et les moyens du traitement.
Tiers responsable du traitement des données	Le terme TIERS RESPONSABLE DU TRAITEMENT DES DONNÉES se définit comme un tiers qui traite les données personnelles pour le compte d'ADP sans être directement sous son autorité.
Tiers sous-traitant des données	Le terme TIERS SOUS-TRAITANT DES DONNÉES se définit comme tout tiers engagé par ADP à titre de sous-traitant de données.
Traitement	Le terme TRAITEMENT se définit comme toute opération effectuée sur les données personnelles, par des moyens automatisés ou non, telle que 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 personnelles.
Travailleur intérimaire	Le terme TRAVAILLEUR INTÉRIMAIRE se définit comme une personne qui fournit des services à ADP (et qui est sous la supervision directe d'ADP) sur une base provisoire ou temporaire, comme les employés temporaires ou contractuels, les entrepreneurs indépendants ou les experts-conseils.

ANNEXE 2 – Mesures de sécurité

Présentées par :	**ADP - Organisation de la sécurité mondiale**
Version :	**2.0**
Publication :	**Septembre 2019**

Table des matières

Termes et définitions

Les termes suivants apparaissent tout au long du document :

Terme ou acronyme utilisé	Définition
GETS	« Global Enterprise Technology & Solutions » (Technologie et Solutions de l'Organisation Mondiale)
GSO	« Global Security Organization » (Organisation de la sécurité mondiale)
CAB	« Change Advisory Board » (Comité consultatif sur les changements)
DRP	« Disaster Recovery Plan » (Plan de reprise après sinistre)
CIRC	« GSO's Critical Incident Response Center » (Centre d'intervention en cas d'incident critique) du « GSO »
SIEM	« Security Information and Event Management » (Sécurité des informations et gestion des événements)
IDS	« Intrusion Detection System » (Système de détection des intrusions)
DNS	« Domain Name System » (Systèmes de noms de domaines)
NTP	« Network Time Protocol » (Protocole de temps réseau)
SOC	« Service Organization Controls » (Contrôles de l'organisation des services)
TPSI	« Trusted Platform Security Infrastructure » (Infrastructure de sécurité des plateformes de confiance)

Terme ou acronyme utilisé	Définition
GETS	« Global Enterprise Technology & Solutions » (Technologie et Solutions de l'Organisation Mondiale)

Vue d'ensemble

ADP dispose d'un programme de sécurité de l'information officiel qui contient des mesures de protection physiques, techniques et administratives destinées à préserver la sécurité, la confidentialité et l'intégrité des informations des clients. Ce programme est raisonnablement destiné à (i) protéger la sécurité et la confidentialité des informations des clients (ii) protéger contre les risques ou les menaces pesant sur la sécurité ou l'intégrité des informations, et (iii) protéger contre des accès aux informations ou une utilisation de celles-ci non autorisés.

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 et susceptibles d'être modifiées par ADP. Ces exigences et pratiques 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 but est d'aider à garantir que le programme de sécurité fonctionne de manière efficace et économique pour 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 d'ADP supervise l'Organisation de la sécurité mondiale (GSO) d'ADP et rend compte à l'Avocat général plutôt qu'au chef des services de l'information, ce qui confère à GSO l'indépendance nécessaire par rapport au service informatique. GSO est une équipe de sécurité centralisée inter-divisions qui adopte une approche multidisciplinaire en matière de conformité aux normes de sécurité de l'information et cybernétique, et de gestion du risque opérationnel, gestion de la sécurité des clients, protection de la main d'œuvre et résilience d'entreprise. Les responsables du 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 de la sécurité mondiale (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 du point de vue de la 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 entrepreneurs 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

Rôles et responsabilités dans le domaine de la sécurité de l'information

Le GSO regroupe des équipes de sécurité inter-divisions s'appuyant sur une approche multidisciplinaire en matière de conformité aux normes de sécurité de l'information et cybernétique, et de gestion du risque opérationnel, gestion de la sécurité des clients, protection de la main d'œuvre et résilience d'entreprise. Ses rôles et responsabilités ont été officiellement définis par tous les membres du GSO. Le GSO est chargé de la conception, de la mise en œuvre et de la surveillance de notre programme de sécurité de l'information fondé sur les politiques de l'entreprise. Les activités du GSO sont supervisées par le Comité de direction sécurité, composé du chef de la sécurité, le directeur général, le directeur financier, le directeur de la stratégie, le directeur des ressources humaines et le 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 entrepreneurs, doivent respecter, et c'est une condition de leur emploi par ADP, la politique sur l'utilisation acceptable des communications électroniques et la protection des données et d'autres politiques pertinentes.

Section 3 - Sécurité des ressources humaines

Vérifications des antécédents

Conformément aux exigences légales applicables dans le pays de la personne, ADP réalise des vérifications des antécédents correspondant aux fonctions et aux responsabilités de ses employés, entrepreneurs et des tierces parties. Ces vérifications visent à confirmer qu'un candidat devant traiter des données de clients convient avant son engagement ou 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 qualification professionnelle
- Casier judiciaire (lorsque c'est légal et en fonction des réglementations nationales locales)

Accords de confidentialité avec les employés et entrepreneurs

Les contrats de travail d'ADP et les contrats avec des entrepreneurs 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 doivent respecter des obligations de confidentialité.

Programme de formation 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 offre 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 entrepreneurs, afin de s'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, rapports annuels publiés
- À usage interne d'ADP uniquement - Exemple : communications interbureaux, procédures opérationnelles
- Confidentielles ADP - Exemple : données personnelles et données personnelles de nature délicate
- 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 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 ou un accès ou une modification non autorisés (i) lors de leur transport, par exemple des enveloppes scellées, des contenants et des livraisons en main propre 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 des accès

Exigences commerciales de contrôle des accès

La politique de contrôle de l'accès d'ADP est fondée 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 de mot de passe

Les politiques de mot de passe des employés d'ADP sont appliquées obligatoirement dans les appareils et applications des serveurs, bases de données et réseaux, dans la mesure permise par l'appareil/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.

[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.

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.

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. Sinon, une ligne louée privée doit 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 courantes 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 vidéo surveillance, 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 de l'intergiciel.

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

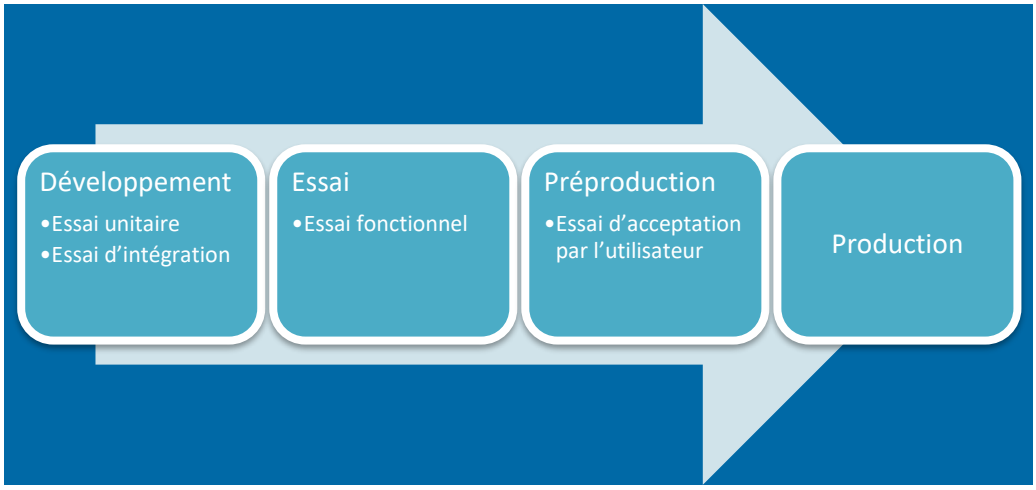
ADP emploie un système de détection des intrusions fondé sur le réseau qui surveille le trafic au niveau de l'infrastructure réseau (24 heures sur 27, 7 jours sur 7) et identifie les activités suspectes ou les attaques potentielles.

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 indidents 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 régies par le code du responsable du traitement

ADP (Philippines), Inc.	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati, Philippines, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Suisse
Compagnie ADP Canada	3250, rue Bloor Ouest, 16e étage, Etobicoke (Ontario) M8X 2X9
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Bruxelles, Belgique
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Prague 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, SAS	31, avenue Jules Quentin, 92000 Nanterre, France
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, France
ADP Gestion des Paiements SAS	31, avenue Jules Quentin, 92000 Nanterre, France
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle-sur-l'Yssel, Pays-Bas
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, France
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-sur-l'Yssel, 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, New Jersey, États-Unis 07068
ADP Polska Sp. zo.o.	Prosta 70, 00-838 Varsovie, 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, Londres, Angleterre, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Findlay, Ohio, États-Unis 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, New Jersey, États-Unis 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Slovaquie
ADP Software Solutions Italia SRL	Via Oropa 28, 10153 Turin, Italie
ADP, Inc.	One ADP Boulevard, Roseland, New Jersey, États-Unis 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st to 6th floor, District 2, Bucarest, Roumanie 020334
Automatic Data Processing Limited (Australia)	6 Nexus Court, Mulgrave, VIC 3170, Australie
Automatic Data Processing Limited (UK)	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, Californie, États-Unis 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, New Jersey, États-Unis 07068