Annexe sur la protection des traitements de données personnelles

Cette Annexe sur la protection des traitements de données personnelles (« **Annexe** ») s'applique dès lors que la fourniture de Services par DELL (au sens de l'entité DELL SA ou de l'entité EMC Computer Systems France, filiales du groupe DELL Technologies, ci-après collectivement 'DELL') au Client implique le traitement de Données à caractère personnel qui sont soumises aux Lois sur la protection des données personnelles quand DELL agit en tant que Sous-traitant des données pour le compte du Client (et non quand DELL est Responsable de traitement). En cas de contradiction entre les clauses de la présente Annexe et le Contrat, la présente Annexe régira les dispositions relatives à l'objet des présentes.

1. **Définitions :** Les termes non définis ci-après auront la signification qui leur est donnée dans le Contrat :

1.1. Le **« Contrat »** correspond à l'accord écrit existant entre le Client et DELL pour la fourniture des services audit Client

1.2. Le « **Responsable du traitement** » désigne l'entité qui, seule ou en groupe, détermine les objectifs et moyens utilisés pour le traitement des Données à caractère personnel.

1.3. Le « **RGPD »** se réfère au Règlement Général (EU) n° 2016/679 sur la Protection des Données à caractère personnel

1.4. Les « **Clauses contractuelles types** » désignent les Clauses contractuelles standard (pour le transfert de Données à caractère personnel vers des Sous-traitants de données (selon le modèle de la Décision 2010/87/EU) susceptibles d'être amendées ou remplacées

1.5. Les « **Données à caractère personnel** » désignent les informations relatives à une personne physique identifiée ou identifiable qui sont traitées par DELL, agissant en tant que Sous-traitant des données dans le cadre de l'exécution du Contrat.

1.6. La **« Violation de la protection des données personnelles »** désigne une faille de sécurité menant à la destruction, perte, altération, divulgation ou accès non autorisé, de manière accidentelle ou illégale, des Données à caractère personnel traitées, transmises ou stockées dans les conditions prévues à cette Annexe.

1.7. Les « **Lois sur la protection des données personnelles** » désignent les lois, décrets, ordonnances, directives ou autres normes relatives à la protection des données personnelles et/ou la protection de la vie privée (y compris le RGPD quand il est applicable) auxquels une partie de ce Contrat est soumise et qui sont applicables aux services fournis.

1.8. Le « **Traitement** » désigne toute opération ou ensemble d'opérations effectuées sur les Données à caractère personnel ou sur des ensembles de Données à caractère personnel, que ce soit de manière automatisée ou non, comme la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la révélation par transmission, la diffusion ou mise à disposition, l'harmonisation ou le regroupement, l'effacement ou la destruction.

1.9. Le « **Sous-traitant des données** » désigne l'entité qui traite les Données à caractère personnel pour le compte du Responsable du traitement.

1.10. Le « **Sous-traitant ultérieur des données** » désigne une tierce partie engagée par DELL (y compris, mais sans s'y limiter, une filiale et/ou un sous-traitant externe de Dell) concernant le traitement des Données à caractère personnel dans le cadre de la fourniture des Services.

2. Traitement des Données à caractère personnel

2.1 Rôles des Parties. DELL peut être amené à traiter des Données à caractère personnel au titre du Contrat en tant que Sous-traitant de données agissant pour le compte du Client en sa qualité de Responsable de traitement

2.2. Instructions. DELL traitera les Données à caractère personnel du Client conformément à ses instructions expresses et documentées. Le Client reconnait que cette annexe, le Contrat auquel celle-ci s'applique et les énoncés de travaux ou commandes de services ultérieurs, et les configurations réalisées par le Client ou ses utilisateurs autorisés, comprennent les instructions complètes du Client à DELL au sujet du Traitement des Données à caractère personnel. Toute instruction supplémentaire ou alternative doit être acceptée par les parties par écrit, notamment les coûts (le cas échéant) afférents à l'application de telles instructions. DELL n'est pas responsable de déterminer si les instructions du Client sont conformes à la loi applicable. Toutefois, si DELL pense que l'instruction du Client enfreint les Lois sur la protection des données personnelles applicables, DELL devra notifier le Client dans les meilleurs délais et celui-ci ne pourra exiger qu'une telle instruction transgressive soit appliquée.

2.3. Détails du Traitement Les détails sur le thème du Traitement, sa durée, sa nature et son objectif, et le type de Données à caractère personnel et les personnes concernées sont tels que spécifiés dans le Contrat.

2.4. Conformité: Le Client et DELL acceptent de respecter leurs obligations respectives dans le cadre des Lois sur la protection des données personnelles applicables aux Traitement de Données à caractère personnel dans le cadre des services. Le Client a seul la responsabilité de la licéité du Traitement des Données à caractère personnel avec les Lois sur la protection des données personnelles avant de divulguer, transférer ou mettre à la disposition de toutes Données à caractère personnel.

3 Sous-Traitants ultérieurs de données

3.1 Utilisation de Sous-Traitants ultérieurs de données. Dell peu avoir recours à des Sous-Traitants ultérieurs de données avec l'autorisation expresse, générale ou spécifique, du Client. Le Client reconnait et accepte que Dell puisse nommer et utiliser des Sous-Traitants ultérieurs de données pour traiter des Données à caractère personnel dans le cadre des Services fournis, sous réserve que Dell mette en place un contrat écrit avec chaque Sous-traitant ultérieur qui impose des obligations à la fois (i) pertinentes par rapport aux services à fournir par les Sous-traitants ultérieurs et (ii) matériellement similaires aux droits et/ou obligations accordés ou imposés à Dell dans cette Annexe. Un Sous-Traitant ultérieur de données peut inclure un prestataire tiers ou toute entité membre du groupe Dell. Lorsqu'un Sous-traitant ultérieur manque à ses obligations de protection des données décrites ci-dessus, Dell sera tenu pour responsable auprès du Client du respect des obligations du Sous-traitant ultérieur des données.

3.2 Liste des Sous-Traitants ultérieurs de données. Sur demande exprès et préalable du Client, Dell fournira une liste de ses Sous-Traitants ultérieurs de données impliqués dans la fourniture des Services ou mettra celle-ci à sa disposition sur son site. Dell informera le Client de toute modification dans sa liste de Sous-Traitants ultérieurs de données. Si le client a une raison légitime à l'ajout ou au retrait d'un des Sous-Traitants ultérieurs de données pour de smotifs liés à la protection des Données à caractère personnel et que dell en peut raisonnablement pas proposer de solution aux objections du Client, les parties conviennent de négocier de bonne foi afin de résoudre ce sujet.

4. Sécurité :

4.1. Mesures techniques et organisationnelles de sécurité ('TOMs') Compte tenu des normes de l'industrie, des coûts d'implémentation, de la nature, de la portée, du contexte et des objectifs du Traitement, et de toute autre circonstance liée au traitement des Données à caractère personnel sur les systèmes Dell, DELL devra mettre en place les mesures techniques et organisationnelles adéquates afin de garantir que la sécurité, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services impliqués dans le Traitement des Données à caractère personnel sont proportionnelles au risque lié à ces Données à caractère personnel. Les parties acceptent que les mesures de sécurité décrites dans la Pièce jointe n° 1 (Mesures de sécurité des informations) fournissent un niveau de sécurité adéquat pour la protection des Données à caractère personnel afin de répondre aux exigences de cette clause. Régulièrement, DELL (i) testera et surveillera l'efficacité de ses protections, contrôles, systèmes et procédures, et (ii) identifiera des risques raisonnablement prévisibles, à la fois internes et externes, qui pèsent sur la sécurité, la confidentialité et l'intégrité des Données à caractère personnel, et s'assurera que ces risques sont traités.

4.2. Progrès techniques. Ces Mesures de sécurité des informations sont soumises à modification par DELL en fonction des progrès et développements techniques sous réserve que ces modifications ne dégradent pas le niveau général de sécurité des Services fournis au titre du Contrat.

4.3. Accès. DELL s'assure que seules les personnes autorisées ont accès aux Données à caractère personnel et (i) se sont engagées à en respecter la confidentialité et (ii) n'y ont accès que sur instruction expresse et documentée de la part de DELL, sauf dans les cas requis par la loi applicable.

5. Violation de la protection des Données personnelles. DELL s'engage à notifier le Client sans retard dès qu'il a connaissance et établi la survenance d'une Violation de la protection des Données personnelles en relation avec les Services fournis par DELL au titre du Contrat et fournira tous les efforts raisonnables pour assister le Client à la limitation, quand possible des effets néfastes de cette Violation de la protection des Données personnelles.

6. Transferts internationaux : La société DELL est autorisée, en lien avec la fourniture des Services ou lors de ses activités normales, à réaliser des transferts internationaux de Données à caractère personnel à ses filiales et/ou Sous-traitants ultérieurs des données. Lors de tels transferts, DELL devra garantir qu'une protection appropriée a été mise en place pour protéger les Données à caractère personnel transférées dans le cadre de ce Contrat. Lorsque la fourniture de Services implique le transfert de Données à caractère personnel depuis l'Espace économique européen vers des pays qui n'en font pas partie (qui ne sont pas soumis à une décision d'adéquation du niveau de protection en vertu des Lois sur la protection des données personnelles), un tel transfert doit être soumis aux exigences suivantes : (a) DELL a mis en place des accords internes avec ses filiales qui peuvent avoir accès aux Données à caractère personnel, accords qui intègrent les Clauses contractuelles types ; et, (b) DELL a mis en place des accords avec ses Sous-traitants ultérieurs des données qui intègrent les Clauses contractuelles types s'il y a lieu.

7. Suppression de Données personnelles : À la fin des Services (quelle qu'en soit la cause) et sur demande écrite du Client, DELL devra, dans les meilleurs délais et en vertu de la loi applicable, restituer ou supprimer les Données à caractère personnel de ses systèmes, sauf si la loi applicable requiert la rétention desdites Données personnelles. DELL est autorisé à différer la suppression des Données à caractère personnel dans la mesure et pendant la période

où les Données à caractère personnel ou leur copie ne peuvent raisonnablement et techniquement pas être expurgées des systèmes Dell. Dans ce cas, les dispositions de cette Annexe continueront de s'appliquer à ces Données à caractère personnel. DELL se réserve le droit de facturer au Client des coûts et dépenses raisonnables engagés par DELL pour supprimer les Données à caractère personnel qui découlent de cette clause.

8. Coopération et assistance

8.1 Demandes de Personnes Concernées. DELL s'engage à informer sans délai le Client de toute demande émanant d'une personne souhaitant exercer ses droits selon les Lois sur la protection des données personnelles. Le Client est responsable de la réponse à apporter à ces demandes. DELL fournira une assistance raisonnable au Client pour apporter une réponse aux requêtes de Personnes Concernées dans la mesure où le Client est dans l'incapacité d'accéder aux Données à caractère personnel dans le cadre de son utilisation des Services. DELL se réserve néanmoins la possibilité de facturer le coût d'une telle assistance si celle-ci dépasse un coût nominal.

8.2 Demande de tiers. Si DELL reçoit une demande d'un tiers ou émanant d'une juridiction, autorité de contrôle, ou agence gouvernementale compétente et à laquelle DELL est soumis et concernant le Traitement de Données à caractère personnel au titre du Contrat, DELL en informera rapidement le Client. DELL redirigera sans délai une telle demande vers le Client. DELL ne répondra pas à une telle demande sans l'autorisation préalable du Client, excepté si DELLy est légalement contraint. DELL informera le Client avant de divulguer dans ce contexte toutes Données à caractère personnel (si la loi applicable le lui permet) et coopérera avec le Client pour limiter le périmètre d'une telle divulgation à ce qui est légalement requis.

8.3 Analyse d'Impact sur la Protection des Données Personnelles (« AIPD ») **et consultation préalable**. Dans le mesure où les Lois sur la protection des Données personnelles l'exigent, DELL fournira une assistance raisonnable au Client pour l'aider à mener une AIPD (aussi appelé ' Privacy Impact Assessment ou 'PIA') afférente au Traitement de Données Personnelles assumé par DELL au titre du Contrat et/ou participera à toute consultation préalable à cet égard tel qu'exigé légalement par les autorités de contrôles compétentes. DELL se réserve la possibilité de facturer un coût nominal au Client pour la fourniture d'une telle assistance.

9. Démonstration de la conformité : DELL devra, sur demande écrite préalable et raisonnable de la part du Client (conformément au Contrat), fournir au Client toute information que serait raisonnablement nécessaire pour démontrer la conformité de DELL avec ses obligations dans le cadre de cette Annexe.

Pièce Jointe n°1 : Mesures Techniques et Organisationnelles de Sécurité (« TOMs ») de DELL

Dell Technologies (y compris ses sociétés affiliées, ci-après « Dell ») prend la sécurité des informations au sérieux. Cet aperçu de nos règles de sécurité des informations s'applique aux contrôles que Dell met en place au niveau de son groupe pour protéger les données à caractère personnel qui sont traitées et transférées parmi les sociétés du groupe Dell Technologies. Le programme de sécurité des informations de Dell permet au personnel de comprendre ses responsabilités. Il se peut que certaines solutions client fassent l'objet de protections différentes, décrites dans l'énoncé des travaux, selon les dispositions acceptées par chaque client.

Pratiques de sécurité

Dell a mis en œuvre des bonnes pratiques et des normes en matière de sécurité des informations à l'échelle de son groupe afin de protéger l'environnement des systèmes d'entreprise de Dell, à savoir (1) la sécurité des informations, (2) la gestion des systèmes et des ressources, (3) le développement, et (4) la gouvernance. Ces pratiques et normes sont approuvées par le DSI de Dell et font l'objet d'une révision formelle chaque année.

Sécurité organisationnelle

Il est de la responsabilité des personnes de chaque organisation de respecter ces pratiques et normes. Pour faciliter l'adhésion à ces pratiques et normes dans l'entreprise, la fonction de sécurité des informations fournit les éléments suivants :

1. Stratégie et conformité aux politiques/normes et réglementations, sensibilisation et formation, évaluations et gestion des risques, gestion des exigences contractuelles en matière de sécurité, consulting des applications et de l'infrastructure, test de l'assurance et orientation de l'entreprise en matière de sécurité.
2. Test de sécurité, conception et implémentation de solutions de sécurité conçues pour permettre l'adoption des contrôles de sécurité dans l'environnement.
3. Opérations de sécurité des solutions de sécurité implémentées, de l'environnement et des ressources, et gestion de la réponse aux incidents.
4. Procédures d'enquête approfondies avec l'organisation opérationnelle de sécurité, le département juridique, le service de protection des données et les ressources humaines pour les procédures d'enquête, notamment eDiscovery et eForensics.

Classification des ressources et contrôle

Dell a pour bonne pratique de répertorier et de gérer toutes les ressources physiques et logiques. Voici des exemples de ressources que Dell IT peut répertorier :

- Les ressources d'informations, comme les bases de données identifiées, les plans de reprise après sinistre, les plans de continuité d'activité, la classification des données, les informations archivées.
- Les ressources logicielles, comme les applications identifiées et les logiciels système.
- Les ressources physiques comme les serveurs identifiés, les ordinateurs de bureau/portables, les bandes de sauvegarde/archive, les imprimantes et les équipements de communication.

Les ressources sont classées en fonction de la criticité de leurs activités afin de déterminer les exigences de confidentialité appropriées. Les recommandations de l'industrie informatique pour la gestion des données à caractère personnel fournissent la base des mesures de protection techniques, organisationnelles et physiques. Elles peuvent comprendre des contrôles comme la gestion de l'accès, le chiffrement, la consignation et la surveillance, et la destruction des données.

Sécurité du personnel

Dans le cadre du processus d'embauche, les employés du groupe Dell sont soumis à un processus de vérification des antécédents selon les réglementations locales applicables. La formation annuelle sur la conformité aux normes de Dell exige des employés qu'ils suivent un cours en ligne et qu'ils se soumettent à une évaluation de leurs connaissances concernant la sécurité des informations et la protection des Données à caractère personnel. Le programme de sensibilisation à la sécurité peut également fournir des documents spécifiques à certaines fonctions.

Sécurité physique et environnementale

Dell utilise plusieurs approches technologiques et opérationnelles dans son programme de sécurité physique en vue de la diminution des risques. L'équipe de sécurité travaille en étroite collaboration avec chaque site pour déterminer si les mesures appropriées sont en place et surveillent de manière continue les changements apportés à l'infrastructure, à l'activité et aux menaces connues. Elle surveille également les mesures de bonnes pratiques utilisées par d'autres acteurs du secteur et sélectionne attentivement des approches qui illustrent la singularité des pratiques et attentes de Dell dans son ensemble. Dell équilibre son approche de la sécurité en tenant compte d'éléments de contrôle qui comprennent l'architecture, les opérations et les systèmes.

Gestion des communications et des opérations

L'organisation IT gère des changements dans l'infrastructure, les systèmes et les applications de l'entreprise par le biais d'un programme centralisé de gestion du changement. Celui-ci peut inclure le test, l'analyse des résultats pour l'entreprise et l'approbation de la gestion, le cas échéant.

Il existe des procédures de réponse aux incidents de sécurité et de protection des données, comme les opérations d'analyse de l'incident, de maîtrise, de réponse, de mesures correctives, de reporting et de retour à la normale.

Comme protection contre l'utilisation malveillante des ressources et les logiciels malveillants, des contrôles supplémentaires peuvent être implémentés en fonction du risque. De tels contrôles peuvent inclure, notamment les pratiques et normes de sécurité des informations, la restriction de l'accès, des environnements dédiés consacrés

au développement et au test, la détection des virus sur les serveurs, ordinateurs de bureau et ordinateurs portables, l'analyse antivirus des pièces jointes aux e-mails, les analyses de conformité des systèmes, la surveillance et la réponse à la prévention des intrusions, la consignation et l'alerte lors d'événements clés, les procédures de gestion des informations basées sur le type de données, les applications d'e-commerce et de sécurité des réseaux, et enfin l'analyse des vulnérabilités du système et des applications.

Contrôles d'accès

L'accès aux systèmes de l'entreprise est restreint en fonction des procédures pour garantir les approbations adéquates. Pour réduire le risque de mauvaise utilisation, qu'elle soit intentionnelle ou non, l'accès est fourni en fonction d'une séparation des tâches et l'octroi du minimum de droits possible.

Les fonctions d'accès distant et de technologie sans fil sont restreintes et requièrent la mise en place de protections à la fois au niveau de l'utilisateur et du système.

Les journaux d'événements spécifiques provenant de périphériques et systèmes clés sont collectés de manière centralisée et signalés sur la base d'exceptions afin de permettre la réponse aux incidents et les procédures d'enquête.

Développement et maintenance du système

Les vulnérabilités tierces qui sont rendues publiques sont passées en revue afin de vérifier leur pertinence dans l'environnement Dell. En fonction du risque pour l'activité et les clients de Dell, il existe des temps de mise en œuvre prédéterminés pour les mesures correctives. En outre, l'analyse des vulnérabilités et les évaluations sont réalisées sur les nouvelles applications clés et l'infrastructure basée sur le risque. Les révisions de code et scanners sont utilisés dans l'environnement de développement avant la production afin de détecter de manière proactive les vulnérabilités de code en fonction du risque. Ces processus permettent l'identification proactive des vulnérabilités ainsi que la conformité.

Conformité

Les départements en charge de la sécurité des informations, des affaires juridiques, de la protection des données personnelles et de la conformité des informations identifient les lois et réglementations locales applicables à Dell. Ces exigences couvrent des domaines tels que la propriété intellectuelle de l'entreprise et de nos clients, les licences logicielles, la protection des données personnelles de nos employés et celles des clients, les procédures de protection et de manipulation des données, la transmission de données en dehors des frontières, les procédures financières et opérationnelles, les contrôles réglementaires en matière d'exportation de technologie et les exigences pour les procédures d'enquêtes.

Des mécanismes tels que le programme de sécurité informatique, le conseil exécutif de protection des données personnelles, les audits et évaluations internes et externes, le recours à des conseillers juridiques internes et externes, l'évaluation des contrôles internes, les tests d'intrusion et les évaluations de vulnérabilité effectués en interne, la gestion des contrats, les opérations de sensibilisation à la sécurité, les conseils liés à la sécurité, l'analyse des exceptions aux règles, et la gestion des risques permettent d'assurer la conformité à ces exigences.