CONDITIONS GÉNÉRALES RELATIVES AU TRAITEMENT DES DONNÉES

Les présentes conditions générales relatives au traitement des données ((dénommées par la suite comme les « DPA », acronyme de *Data Processing General Terms and Conditions*) font partie des conditions générales du Programme Ecolab3D (« Conditions générales ») et sont signées par Ecolab Inc. et une ou plusieurs de ses Filiales et Client (dénommés séparément une « Partie » et collectivement les « Parties »). Les termes utilisés dans ces DPA auront la signification qui leur est donnée ci-dessous. Les termes qui ne sont pas définis dans les présentes auront la signification qui leur est donnée dans les Conditions Générales, sauf si ledit terme a une signification spéciale en vertu de la loi relative à la protection des données (telle que définie ci-dessous), auquel cas la définition de la Loi relative à la protection des données prévaudra. À l'exception des modifications des présentes, les Conditions Générales resteront pleinement en vigueur et de plein effet.

1. Définitions. Dans ces DPA, les termes suivants auront la signification définie ci-dessous et les termes proches en vertu de la Loi relative à la protection des données s'entendront comme suit :

1.1. « **Controller** » aura la signification qui lui est donnée dans la Loi relative à la protection des données ou, si cette définition ne se trouve pas dans la Loi relative à la protection des données, signifiera toute personne physique ou morale, autorité publique ou autre organisme qui, seul ou conjointement avec d'autres, détermines les objectifs et moyens du traitement des informations à caractère personnel.

1.2. « **Loi relative à la protection des données** » signifie toutes les lois complètes étatiques et internationales relatives à la protection des données en vigueur, incluant, mais sans s'y limiter (a), le règlement général sur la protection des données (« RGPD ») de l'Union européenne (« UE »), les lois de l'Espace économique européen (« EEE ») et le RGPD, tel que transposé dans la législation nationale du Royaume-Uni par le biais de la section 3 de la European Union Act (Withdrawal) de 2018 telle que modifiée par le règlement de 2019 (UE Exit) sur la protection des données, la vie privée et les communications électroniques (Amendements, etc.) (« RGPD UK ») avec la loi de 2018 du Royaume-Uni sur la protection des données (collectivement « Loi sur la protection des données du Royaume-Uni »), (b) la California Consumer Privacy Act Cal. Civ. Code § 1798.100 et consécutifs (« CCPA ») et les lois relatives à la protection des données similaires ou d'autres états, (c), la loi générale brésilienne sur la protection des données à caractère personnel (« LGPD ») et (d) les autres lois complètes de protection des données en vigueur qui ont trait au traitement des informations à caractère personnel en vertu des Conditions générales.

1.3. « **Sujet des données** » signifie toute personne physique identifiée ou identifiable, telle que définie par la Loi relative à la protection des données.

1.4. « **Informations à caractère personnel** » signifient toutes les informations à caractère personnel, telles que définies par la loi relative à la protection des données en vigueur (également connues comme Données personnelles ou Informations personnelles identifiables [« IPI »]), et incluent toutes les catégories de données sensibles ou spéciales qui sont traitées en vertu de ou en rapport avec les Conditions générales.

1.5. « **Traitement** » (y compris (« traiter » et les termes associés) signifie toute opération ou ensemble d'opérations réalisées sur les Informations à caractère personnel.

1.6. « **Responsable du traitement** » aura la signification qui lui est donnée dans la Loi relative à la protection des données ou, si cette définition ne se trouve pas dans la Loi relative à la protection des données, signifiera toute personne physique ou morale, autorité publique, agence ou autre organisme qui traite les Informations à caractère personnel au nom du Controller.

1.7. « **Incident de sécurité** » signifie une faille de sécurité entraînant la destruction, perte, altération, divulgation non autorisée ou accès involontaire ou illégal à des Informations à caractère personnel.

1.8. « **Sous-traitant ultérieur** » signifie toute personne (notamment tout tiers, à l'exception du personnel d'Ecolab) nommée par ou au nom d'Ecolab pour traiter les Informations à caractère personnel en rapport avec les Conditions générales.

1.9. Les autres termes en lettres capitales ou non utilisés dans les DPA auront la même signification que dans la Loi relative à la protection des données et les termes proches s'entendront de la même façon.

2. Rôles des Parties

2.1. Les Parties conviennent que, pour les besoins de la Loi relative à la protection des données, le Client est le Controller et Ecolab est le Responsable du traitement en ce qui concerne le traitement des Informations à caractère personnel et que ces termes auront la signification qui leur est donnée conformément à la Loi relative à la protection des données.

2.2. Si la Loi relative à la protection des données n'utilise pas spécifiquement les termes « Controller » et « Responsable du traitement des données », les Parties seront définies par les rôles correspondant aux termes proches pour le Controller et le Responsable du traitement des données en vertu de la Loi relative à la protection des données particulière et en vigueur.

3. Assurance mutuelle de conformité

3.1. Chaque Partie accepte et confirme qu'elle se conformera à toutes les exigences applicables de la Loi relative à la protection des données et aux termes de ces DPA en rapport avec le traitement des Informations à caractère personnel.

3.2. Le Client et Ecolab seront séparément responsables de la conformité à ces dispositions statutaires relatives à la protection des données telles qu'applicables à chacun et rien dans les DPA ne libérera une Partie de ses propres obligations statutaires.

4. Obligations d'Ecolab

4.1. Ecolab devra :

4.1.1 retenir, utiliser, divulguer, transférer ou de quelque façon que ce soit traiter les Informations à caractère personnel uniquement aux fins de performance spécifiées dans les Conditions générales définies à la Section 8 ci-dessous;

4.1.2. traiter les Informations à caractère personnel uniquement en fonction d'instructions documentées provenant du Client (comme indiqué dans les Conditions générales ou toute autre communication écrite ou orale),

4.1.3. ne pas vendre ou « partager » les Informations à caractère personnel, selon la définition de la Loi relative à la protection des données spécifique (par exemple, CCPA), notamment dans un contexte transversal ou pour de la publicité ciblée (toute limitation du « partage » ne s'appliquera pas à l'utilisation par Ecolab du sous-traitant ultérieur ou de tout tiers pour le traitement des données dans la mesure nécessaire pour remplir ses obligations en vertu du Programme et des conditions),

4.1.4. ne pas retenir, utiliser ou divulguer les Informations à caractère personnel du Client (i) à quelque fin que ce soit autre que les fins professionnelles spécifiées dans les Conditions générales (notamment la retenue, l'utilisation ou la divulgation des Informations à caractère personnel du Client à des fins commerciales autres que les fins professionnelles spécifiées dans le Programme) ou de quelque autre façon permise par les Lois relatives à la protection des données en vigueur ou (ii) en dehors de la relation commerciale directe entre le Client et Ecolab,

4.1.5. ne pas associer les Informations à caractère personnel du Client concernant une personne qu'Ecolab reçoit de ou au nom du Client avec les Informations à caractère personnel qu'Ecolab reçoit de ou au nom d'une autre personne ou collecte des interactions d'Ecolab avec cette personne, à condition qu'Ecolab puisse associer les Informations à caractère personnel du Client pour atteindre un but professionnel tel que défini et permis en vertu de la Loi relative à la protection des données en vigueur.

4.1.6. s'assurer que les personnes qui ont l'autorisation de traiter les Informations à caractère personnel se sont engagées à respecter leur confidentialité ou sont soumises à une obligation statutaire adéquate de confidentialité,

4.1.7. vérifier et mettre en œuvre les mises à jour ou les guides réglementaires contraignants relatifs à la nouvelle Loi relative à la protection des données qui sont applicables aux Conditions générales,

4.1.8. rendre disponibles toutes les informations du Client nécessaires pour prouver la conformité d'Ecolab à ses obligations en vertu des Conditions générales. Le Client peut, sur avis écrit raisonnable à Ecolab, prendre des mesures raisonnables et adaptées pour arrêter et corriger toute utilisation non autorisée des Informations à caractère personnel par Ecolab et

4.1.9. rapidement, et sans retard indu, avertir le Client si Ecolab détermine qu'il ne peut plus respecter ses obligations en vertu des Lois relatives à la protection des données en vigueur.

4.2. Si Ecolab reçoit directement une demande du Sujet des données concernant le Sujet des données du Client, il doit avertir le Client de cette demande. Ecolab devra transférer cette demande au Client et ne répondra pas au sujet des données sauf s'il y est légalement obligé. Sur demande écrite raisonnable du Client, et dans la mesure où le Client n'est pas en mesure de répondre à une demande sans l'assistance d'Ecolab par le biais du libre-service ou d'autres options, Ecolab offrira au Client une coopération et une assistance raisonnables pour permettre une réponse à la demande du Sujet des données.

4.3. Si Ecolab reçoit une demande ou une requête contraignante d'une autorité publique ou d'un régulateur de divulgation d'Informations à caractère personnel, il doit en informer le Client, sauf si cela est interdit par la loi. Ecolab accepte de fournir au Client une assistance raisonnable relative à ladite demande, en tenant compte de la nature du traitement et des informations disponibles, notamment assister le Client à récuser ladite demande et tirer parti de toute procédure d'appel disponible.

4.4. Dans le cas où elles seraient reliées au traitement des Informations à caractère personnel, Ecolab devra avertir le Client de toute autre demande ou plainte relative à ce traitement en vertu du Programme ou des Conditions, incluant, mais sans s'y limiter a) toute demande ou plainte reçue des collaborateurs ou filiales du Client ou b) toute demande de divulgation des Informations à caractère personnel qui n'est pas encore définie dans les présentes et qui est reliée au au Programme.

4.5. Ecolab doit fournir une assistance raisonnable si le Client est obligé, en vertu de la Loi relative à la protection des données en vigueur, de procéder à des évaluations de l'incidence des Conditions générales ou du Programme sur la protection des Informations à caractère personnel. En outre, Ecolab doit fournir une assistance raisonnable si le Client est obligé, en vertu de la Loi relative à la protection des données en vigueur, de consulter un régulateur concernant des affaires liées au traitement des Informations à caractère personnel en vertu des Conditions générales.

4.6. Le Client accepte qu'Ecolab engage des sous-traitants ultérieurs pour le traitement des Informations à caractère personnel aux fins des performances en vertu des Conditions générales. Si Ecolab engage un sous-traitant ultérieur pour procéder à des activités spécifiques de traitement des Informations à caractère personnel dans le cadre des performances en vertu des Conditions générales, Ecolab devra exiger des obligations de protection des données conformes à la législation et aux normes du secteur en fonction des services fournis et des Informations à caractère personnel traitées par le sous-traitant ultérieur. Une liste à jour des sous-traitants ultérieurs d'Ecolab qui participent au traitement des Informations à caractère personnel au nom du Client est fournie à l'Annexe II. Ecolab donnera un avis de 30 jours au Client avant d'engager un nouveau Sous-traitant ultérieur. Si le Client ne s'oppose pas dans un délai de 30 jours au nouveau Sous-traitant ultérieur, le Client est considéré comme ayant approuvé l'engagement d'Ecolab.

5. Obligations du Client.

5.1. Le Client devra informer Ecolab sans retard indu et complètement de toute erreur ou irrégularité liée aux dispositions statutaires relatives au traitement des Informations à caractère personnel détectée pendant ledit traitement. Le client sera le seul responsable de la précision, de la qualité et de la légalité des informations à caractère personnel traitées en vertu des présentes et des moyens grâce auxquels le Client ou toute Filiale concernée du Client collecte, stocke, traite et transmet lesdites Informations à caractère personnel.

5.2. Si cela est requis par la Loi relative à la protection des données, le Client est le seul responsable de ses propres responsabilités de notification des Sujets des données, des régulateurs ou de toute autre autorité.

5.3. Si le Client reçoit une plainte, un avis ou une communication d'une autorité de réglementation, qui se relie: (i) au traitement des Informations à caractère personnel par Ecolab ou (ii) d'un défaut potentiel de conformité à la Loi relative à la protection des données, le Client devra, dans la mesure permise par la loi, transférer rapidement la plainte, l'avis ou la communication à Ecolab et, si cela se relie au traitement des Informations à caractère personnel conformément à ces DPA, fournir à Ecolab une coopération et une assistance raisonnables dans la réponse à cette plainte, cet avis ou cette communication.

5.4. Le Client déclare et certifie que les Données du Client n'incluront aucune information considérée comme sensible en vertu de quelque loi ou réglementation que ce soit (y compris les Lois relatives à la protection des données), incluant, mais sans s'y limiter les informations sur la santé, les numéros de compte, toute information du type cité à l'Article 9 du RGPD ou toutes autres Informations à caractère personnel similaires sensibles. Le Client assume tous les risques découlant de l'utilisation de ces informations sensibles avec le Programme, notamment le risque de divulgation par inadvertance ou d'accès ou d'utilisation non autorisés.

6. Sécurité

6.1. En tenant compte des normes du secteur, des coûts de mise en œuvre et de la nature, la portée, le contexte et les objectifs du traitement ainsi que du risque de variation de la probabilité et de l'importance des droits et des libertés des personnes physiques, Ecolab devra, en rapport avec les Informations à caractère personnel, mettre en œuvre des mesures techniques et organisationnelles commercialement raisonnables spécifiées à l'Annexe I et conçues pour assurer un niveau de sécurité approprié relatif à ce risque. Lors de l'évaluation du niveau adéquat de sécurité, Ecolab devra tenir compte des risques représentés par le traitement, surtout en cas d'Incident de sécurité. Les mesures techniques et organisationnelles applicables à un Programme particulier sont disponibles sur demande, conformément aux mesures de sécurité décrites dans les Conditions générales et/ou le Programme.

6.2. Si Ecolab découvre un Incident de sécurité lié aux Informations à caractère personnel traitées en vertu de ces DPA et/ou des Conditions générales, il devra en avertir le Client dans un délai raisonnable. Si un Incident de sécurité est découvert sur les systèmes de commande d'Ecolab, Ecolab (i) enquêtera sur l'Incident de sécurité, (ii) fournira des informations au Client sur l'Incident de sécurité (notamment, dans la mesure du possible, la nature de l'Incident de sécurité, les Informations à caractère personnel concernées par l'Incident de sécurité et les coordonnées de la personne chez Ecolab qui peut fournir des

informations complémentaires) et (iii) prendra des mesures raisonnables pour limiter les effets et minimiser les dommages découlant de l'Incident de sécurité.

6.3. Si une des Parties découvre une divulgation des données ou une fuite de données par inadvertance concernant les données ou les systèmes de l'autre Partie, cette Partie devra en avertir rapidement l'autre Partie et les Parties devront coopérer pour établir une notification de fuite de données et un plan de correction, conformément aux Lois en vigueur, la responsabilité d'une telle notification et d'un tel plan de correction étant assumée par la responsabilité respective et proportionnelle des Parties dans la divulgation ou la fuite et leurs obligations respectives en vertu des Lois en vigueur.

6.4. La responsabilité d'Ecolab en cas d'Incident de sécurité, de divulgation des données ou de fuite de données par inadvertance sera soumise aux dispositions des Sections 4, 12, 13 et 14 des Conditions générales.

7. Transfert international d'Informations à caractère personnel et les Clauses contractuelles standard

7.1. Si, dans le cadre des Conditions générales, Ecolab ou son ou ses Sous-traitants ultérieurs traitent les Informations à caractère personnel découlant de l'Espace économique européen dans un pays qui n'a pas prouvé fournir un niveau adéquat de protection en vertu de la Loi relative à la protection des données en vigueur, les Parties acceptent de se conformer aux Clauses contractuelles standard de l'UE (« CCS UE ») et aux Clauses contractuelles standard du Royaume-Uni (« CCS UK » et collectivement avec les CCS UE, les « CCS »), telles que décrites dans cette section.

7.2. Pour faciliter le transfert vers des pays tiers d'Informations à caractère personnel provenant de l'UE, de Suisse ou d'autres pays de l'EEE qui reconnaissent la suffisance des CCS UE, les Parties acceptent de se conformer aux CCS UE, telles que mises en œuvre par la Décision d'exécution (UE) 2021-914 de la Commission et, à ce titre, les CCS UE peuvent être révisées ou remplacées de temps à autre. Les Parties utiliseront le Module 2 des CCS UE pour les transferts du controller au responsable du traitement. Le Client, en tant qu'Exportateur des données, et Ecolab, en tant qu'Importateur des données, concluent par les présentes, à la Date de prise d'effet, les CCS UE Module 2, qui sont intégrés par cette référence et font partie intégrante de ces DPA. Les Parties sont réputées avoir accepté et signé les CCS UE dans leur intégralité, y compris les annexes. En ce qui concerne les CCS UE, les Parties accordent ce qui suit :

7.2.1. La Clause 7, « Clause d'accueil », ne s'applique pas.

7.2.2. La Clause 9, Option 2 s'applique et la « durée » sera de trente (30) jours.

7.2.3. Aucune Partie n'a engagé un organisme indépendant de résolution des différends, tel que décrit à la Clause 11 et, à ce titre, la disposition facultative ne s'applique pas.

7.2.4. L'État membre de l'UE applicable pour l'Option 1 de la Clause 17 sera (1) l'Allemagne ou (2) l'État membre de l'UE dans lequel un différend entre les Parties se produit ou l'État membre de l'UE ou un Sujet des données prend une mesure particulière.

7.2.5. L'État membre de l'UE applicable pour la Clause 18 sera (1) l'Allemagne ou (2) l'État membre de l'UE dans lequel un différend entre les Parties se produit ou l'État membre de l'UE ou un Sujet des données prend une mesure particulière.

7.2.6. L'*Annexe I* des CCS UE sera considérée comme complétée par les sections pertinentes de la Section 8 de ces DPA.

7.2.7. L'*Annexe II* des CCS UE sera considérée comme complétée par les sections pertinentes de l'Annexe I de ces DPA.

7.2.8. L'*Annexe III* des CCS UE sera considérée comme complétée par les sections pertinentes de l'Annexe II de ces DPA.

7.3. Pour faciliter le transfert des Informations à caractère personnel du Royaume-Uni vers des pays tiers, les Parties acceptent de conclure l'Addendum sur le transfert international de données aux Clauses contractuelles standard de la Commission de l'UE, tel que publié par le responsable du Commissaire à l'information (« ICO ») du Royaume-Uni en vertu de la Loi relative à la protection des données S119A(1) de 2018 (ci-après dénommées « CCS UK »). Le Client, en tant qu'Exportateur des données, et Ecolab, en tant qu'Importateur des données, concluent par les présentes, à la Date de prise d'effet, les CCS UK, qui sont intégrés par cette référence et font partie intégrante de ces DPA. Les Parties sont réputées avoir accepté et signé les CCS UK dans leur intégralité, y compris les annexes et les tableaux des CCS UK pertinents sont réputés avoir été complétés avec les informations pertinentes contenues à la Section 8 ci-dessous et les Annexes de ces DPA.

7.4. En ce qui concerne tous les transferts internationaux d'Informations à caractère personnel, incluant, mais sans s'y limiter les CCS référencées dans les présentes :

7.4.1. Lorsque la Commission de l'UE, l'ICO, une autorité de surveillance de l'UE ou tout autre régulateur concerné modifie une des CCS ou mettre en œuvre de nouvelles CCS, lesdites CCS seront appliquées à leur date de prise d'effet. Les Parties acceptent que les références fournies dans les présentes peuvent être modifiées pour inclure les nouvelles CCS sur avis de l'autre Partie sans que des DPA ultérieures soient nécessaires, sauf obligation légale contraire.

7.4.2. Si un pays avec une Loi relative à la protection des données en vigueur a établi des clauses contractuelles standard ou des documents similaires qui doivent être conclus entre les Parties, lesdites clauses seront appliquées à la date de leur entrée en vigueur. Les Parties acceptent que ces DPA puissent être modifiées pour inclure les nouvelles clauses contractuelles standard sur avis de l'une ou l'autre des Parties, sans que des Conditions générales ultérieures soient nécessaires, sauf obligation légale contraire.

7.4.3. Si une Loi relative à la protection des données similaire au RGPD exige des conditions générales pour le transfert international, mais sans que des clauses contractuelles standard soient requises (par exemple, Brésil, Afrique du Sud), les Parties acceptent que ces DPA fournissent la protection et les conditions générales requises en vertu de ladite Loi relative à la protection des données.

8. Description du traitement.

8.1. Les catégories de sujets de données dont les Informations à caractère personnel sont traitées seront les suivantes, sauf définition spécifique dans le Programme ou les Conditions : personnel (par exemple, collaborateurs, sous-traitants) du Client.

8.2. Les catégories d'Informations à caractère personnel traitées seront les suivantes, sauf définition spécifique dans le Programme ou les Conditions : coordonnées de base (par exemple, e-mail professionnel, numéro de téléphone et adresse).

8.3. Aucune Information à caractère personnel classifiée « sensible » ou « spéciale » en vertu de la Loi relative à la protection des données ne sera traitée, sauf définition spécifique dans le Programme ou les Conditions.

8.4. Les Informations à caractère personnel seront traitées et transférées de façon continue pendant la durée du Programme

et des Conditions. **8.5.** La nature du traitement des Informations à caractère personnel sera définie dans le Programme et les

Conditions.

8.6. La ou les fins du traitement et du transfert des Informations à caractère personnel seront de fournir des services, tels que décrits dans les Conditions générales et le Programme.

8.7. La période de conservation des Informations à caractère personnel sera la Durée du Programme ou une période plus courte, selon les instructions du Client.

8.8. Pour les transferts à des sous-traitants ultérieurs, le sujet et la durée du traitement sont tels que définis ci-dessus à la Section 8. La nature des services de sous-traitant ultérieur spécifiques est telle que décrite dans la liste de sous-traitants ultérieurs fournie par Ecolab.

9. Durée et cessation.

9.1. Ces DPA auront la même durée que les Conditions générales.

9.2. Sans préjudice de tout autre droit de cessation qu'une Partie pourrait avoir en vertu de ces DPA et/ou de toute loi en vigueur, chaque Partie peut mettre fin à sa participation à ces DPA si elle découvre que l'autre Partie ne se conforme pas aux conditions générales de ces DPA, à condition que la Partie qui ne se conforme pas à ces conditions générales ait la possibilité de se mettre en conformité avec les Conditions générales.

9.3. À la cessation, chaque Partie aura le droit de conserver des Informations à caractère personnel uniquement si cela est nécessaire pour poursuivre les objectifs et conformer aux exigences des Conditions générales. Toutes les Informations à caractère personnel qui ne sont plus nécessaires pour poursuivre les objectifs ou se conformer à des exigences définies dans les Conditions générales peuvent être supprimées par Ecolab dans un délai de 90 jours suivant la Cessation, à l'exception appropriée de la suppression lorsque des copies de sauvegarde des Informations à caractère personnel sont logiquement supprimées selon un délai plus long ou si la conservation pendant un délai plus long est requise ou permise par les Lois en vigueur.

10. Divers.

10.1. Ces DPA s'appliquent au profit des Parties uniquement. Aucun tiers n'a de droits en vertu des présentes, sauf disposition contraire des présentes.

10.2. Si une résolution détermine qu'une disposition des DPA n'est pas valide ou applicable, cela n'aura aucune incidence sur les autres dispositions des DPA. Dans ce cas, la disposition non valide ou non applicable sera automatiquement remplacée par une disposition valide ou applicable qui se rapproche le plus de l'objet de la disposition d'origine. Il en va de même si les DPA contiennent un vide involontaire.

10.3 Dans la mesure où il y a un conflit entre le présent Accord, ces DPA et/ou les CCS, les différents accords prévaudront dans l'ordre de préférence suivant : (i) les CCS, (ii) ces DPA, (iii) les Conditions générales.

ANNEXE I - MESURES TECHNIQUES ET ORGANISATIONNELLES

Description des mesures techniques et organisationnelles mises en œuvre par Ecolab pour assurer un niveau adéquat de sécurité, en tenant compte de la nature, de la portée, du contexte et du but du traitement, ainsi que des risques liés aux droits et aux libertés des personnes physiques :

(A) Contrôle de l'accès physique au site	Mesures techniques et organisationnelles visant à contrôler l'accès physique au site et aux installations et, en particulier, pour identifier le personnel autorisé à l'entrée : ☒ Portes verrouillées à toutes les entrées/sorties ☒ Présence de personnel de sécurité ☒ Systèmes de contrôle de l'accès ☒ Systèmes CCTV ☒ Systèmes d'alarme antivols
(B) Contrôle de l'accès aux systèmes informatiques	Mesures techniques et organisationnelles de sécurité conçues pour s'assurer que les utilisateurs qui ont accès aux systèmes informatiques concernés sont identifiés et s'authentifient : ☒ Systèmes de sécurité informatique qui exigent que les utilisateurs individuels se connectent avec des noms d'utilisateur uniques ☒ Systèmes de sécurité informatique exigeant l'utilisation de mots de passe forts/complexes ☒ Systèmes de sécurité informatique exigeant l'utilisation d'une authentification à plusieurs facteurs ☒ Exigences de connexion au système supplémentaires pour des applications spécifiques ☒ Modification obligatoire du mot de passe à des intervalles précis ☒ Cryptage appliqué aux données personnelles « en transit » ☒ Cryptage appliqué aux données personnelles « au repos » ☒ Verrouillage automatique des terminaux et dispositifs informatiques après des périodes sans utilisation, le mot de passe étant requis pour sortir le terminal ou le dispositif de veille ☒ Les bases de données de mots de passe sont soumises à un cryptage/hachage important ☒ Audits réguliers des procédures de sécurité ☒ Formation des collaborateurs concernant l'accès aux systèmes informatiques
(C) Contrôle de l'accès aux données personnelles	Mesures techniques et organisationnelles de sécurité conçues pour s'assurer que les utilisateurs qui ont accès aux données personnelles concernées sont identifiés et authentifiés. ☒ « Lecture » des droits pour les systèmes contenant des données personnelles limitées à certaines fonctions ☒ « Modification » des droits pour les systèmes contenant des données personnelles limitées à certaines fonctions ou certains profils ☒ Enregistrement des tentatives d'accès aux systèmes contenant des données personnelles ☒ Cryptage sur des mémoires et des supports contenant des données personnelles ☒ Formation des collaborateurs sur l'accès aux données personnelles

(D)	**Contrôle de la divulgation des données personnelles**	Mesures techniques et organisationnelles pour transférer, transmettre et communiquer ou stocker les données en toute sécurité sur des supports de données et pour la vérification ultérieure : ☒ Restrictions des droits de transfert aux systèmes contenant des données personnelles ☒ Sécurisation des réseaux de données ☒ Cryptage des systèmes utilisés pour envoyer des données personnelles ☒ Cryptage SSL de tous les portails d'accès à Internet ☒ Protection des supports et contenants de stockage des données pendant le transport physique ☒ Formation des collaborateurs sur le transfert des données personnelles
(E)	**Contrôle des mécanismes de saisie**	Mesures techniques et organisationnelles de sécurité pour permettre l'enregistrement et l'analyse ultérieure des informations concernant le moment de la saisie dans les systèmes de données (par exemple, édition, ajout, suppression, etc.) et la personne responsable d'une telle saisie : ☒ Enregistrement de toutes les actions de saisie dans les systèmes contenant des données personnelles ☒ « Modification » des droits pour les systèmes contenant des données personnelles limitées à certaines fonctions ou certains profils ☒ Accords contraignants écrits ou autres obligations de confidentialité avec les collaborateurs qui traitent les données personnelles ☒ Vérifications régulières de la conformité aux accord pertinents ☒ Formation des collaborateurs concernant la modification des données personnelles
(F)	**Contrôle des flux de travail entre les controllers et les responsables du traitement**	Mesures techniques et organisationnelles visant à répartir les responsabilités entre les controllers et les responsables du traitement qui traitent les données personnelles pertinentes : ☒ Accords écrits contraignants qui régissent la nomination et les responsabilités des responsables du traitement qui ont accès aux données personnelles pertinentes ☒ Accords écrits contraignants régissant l'attribution des responsabilités de conformité à la protection des données entre tous les controllers qui ont accès aux données personnelles pertinentes ☒ Vérifications régulières de la conformité aux accord pertinents ☒ Formation pour les collaborateurs relative au traitement des données personnelles

(G) Mécanismes de contrôle pour assurer la disponibilité des données personnelles pertinentes	Mesures techniques et organisationnelles qui visent à assurer la disponibilité physique et électronique et l'accessibilité des données personnelles pertinentes : ☒ Procédures de reprise après sinistre enregistrées ☒ Procédures de sauvegarde sécurisées en place avec des sauvegardes complètes régulières ☒ Installations et lieux de sauvegarde ☒ Alimentation électrique ininterrompue des installations de sauvegarde ☒ Sécurité physique des installations de sauvegarde ☒ Systèmes d'alarme de sécurité dans les installations de sauvegarde ☒ Sécurité électronique des installations de sauvegarde ☒ Contrôles environnementaux des installations de sauvegarde ☒ Protection contre l'incendie des installations de sauvegarde ☒ Anonymisation ou suppression des données personnelles qui ne sont plus requises à des fins de traitement licites ☒ Formation des collaborateurs concernant les sauvegardes et la reprise après sinistre
(H) Mécanismes de contrôle pour assurer la séparation des données personnelles pertinentes des autres données	Mesures techniques et organisationnelles qui visent à s'assurer que les données personnelles pertinentes sont stockées et traitées séparément des autres données : ☒ Séparation logique des données réelles ou de production des données de sauvegarde et des données de développement ou de test ☒ Séparation du personnel qui traite les données personnelles pertinentes du reste du personnel ☒ Formation des collaborateurs concernant la séparation des données

ANNEXE II - LISTE DES SOUS-TRAITANTS ULTÉRIEURS

Le controller a autorisé le recours aux sous-traitants ultérieurs de sa liste de sous-traitants ultérieurs disponible ci-dessous :

Sous-traitant ultérieur	Adresse du sous-traitant ultérieur
Microsoft	1 Microsoft Way, Redmond, WA 98052
Cisco AppDynamics	500 Terry A Francois Blvd, 3rd fl San Francisco, CA 94158
Salesforce	415 Mission Street, 3rd Floor, San Francisco, CA
LinkedIn Sales Navigator	1000 W. Maude Ave, Sunnyvale, CA 94085
Microsoft Dynamics CRM	1 Microsoft Way, Redmond, WA 98052
Soprano Design Pty	Level 15, 132 Arthur St North Sydney NSW 2060 Australia
ServiceNow	2225 Lawson Lane, Santa Clara, CA 95054 Hoekenroder 3, Amsterdam Zuidoost, North Holland 1102 BR 80 Robinson Road, #02-00, Singapore 068898
FiveTran	1221 Broadway Street, Floor 20, San Francisco, CA