CONTRAT DE TRAITEMENT DES DONNÉES

Le présent Contrat de traitement des données **(« CTD »)** reflète l'accord des parties concernant les conditions régissant le traitement des Données Personnelles pour le compte du Client en vertu de tout contrat écrit applicable entre le Client et Dynatrace régissant l'utilisation des Offres de Dynatrace (gratuites ou payantes), et de tous les Formulaires de Commande, annexes et SOW connexes (collectivement, le **« Contrat »**). Le présent CTD entre en vigueur à sa date de signature par les deux parties (la **« Date d'Entrée en Vigueur »**).

Le présent CTD est soumis aux conditions du l'Contrat, y est entièrement incorporé et fait partie intégrante de celui-ci. Le présent CTD remplace tout contrat de traitement des données existant, sauf indication contraire aux présentes. En cas de conflit entre le présent CTD et toute autre disposition du l'Contrat concernant les Données Personnelles, le présent CTD prévaut et s'applique. Les termes commençant par une majuscule, utilisés mais non définis dans le présent CTD, ont la même signification que celle qui leur est attribuée dans le contrat de souscription disponible à l'adresse https://assets.dynatrace.com/global/legal/Online-SA-April-2023-French-France.pdf.

1. **Définitions**.

   (a) « **APPI** » désigne la Loi Japonaise sur la Protection des Informations à caractère Personnel (Act n° 57 de 2003 telle que modifiée en 2016).

   (b) « **Loi sur la Protection des Données** » désigne toutes les lois et réglementations sur la protection des données et la confidentialité des données applicables au Traitement par Dynatrace des Données Personnelles du Client dans le cadre du l'Contrat.

   (c) « **Responsable du traitement** » a la même signification que celle donnée en vertu de la Loi sur la protection des données applicable et inclut le « Propriétaire de la Base de Données » (« Database Owner ») en vertu de la loi israélienne sur la protection de la vie privée et l'« Entreprise » (« Business ») en vertu de la loi sur la protection de la vie privée de l'État des États-Unis applicable.

   (d) « **Données Personnelles du Client** » désigne toute Donnée Personnelle soumise, stockée, publiée, affichée ou autrement transmise par ou au nom du Client dans le cadre de l'utilisation des Offres de Dynatrace ; et exclut les Données Personnelles (telles que les Informations Restreintes) soumises, stockées, publiées, affichées ou autrement transmises par ou au nom du Client en violation de toute disposition du Contrat et/ou du présent CTD.

   (e) « **Groupe Dynatrace** » désigne une ou plusieurs entités de Dynatrace LLC, une société à responsabilité limitée du Delaware, et ses Sociétés affiliées qui peuvent aider Dynatrace à fournir les Offres de Dynatrace, et/ou le support ou les services connexes, dans le cadre du Contrat et du présent CTD.

   (f) « **Europe** » désigne l'Union Européenne, l'Espace Economique Européen (« EEE »), et/ou leurs États membres, la Suisse et le Royaume-Uni.

   (g) « **RGPD** » désigne le Règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données).

   (h) « **LGPD** » désigne la Lei Geral de Proteção de Dados Pessoais (Loi Générale sur la Protection des Données à caractère Personnel, au Brésil).

   (i) « **Violation de Données Personnelles** » désigne une violation de la sécurité entraînant la destruction accidentelle ou illégale, la perte, l'altération ou la divulgation ou l'accès non autorisé aux Données Personnelles du Client lors de la transmission, du stockage ou du Traitement desdites données par Dynatrace.

   (j) « **PIPL** » désigne la Loi chinoise sur la protection des informations à caractère personnel.

(k) « **Données à caractère personnel**» ou « **Données Personnelles** » désigne les « Données à caractère personnel » ou les « Informations à caractère personnel » telles que définies en vertu des Lois applicables en matière de protection des données que Dynatrace collecte ou reçoit au nom du Client. Les Données Personnelles n'incluent pas les informations que Dynatrace obtient ou traite indépendamment de l'exécution de ses obligations dans le cadre du Contrat avec le Client.

(l) « **Sous-traitant** » a la même signification que celle qui lui est attribuée en vertu de la Loi sur la Protection des Données applicable et inclut le « Titulaire » (« Holder ») tel que défini en vertu de la Loi israélienne sur la protection de la vie privée, et le « Prestataire de Services » (« Service Provider ») dans la loi sur la protection de la vie privée de l'État des États-Unis en vigueur.

(m) « **Clauses contractuelles types** » désigne les Clauses contractuelles types promulguées par la Décision de la Commission européenne 2021/914/UE incorporées aux présentes par référence, telles que modifiées ou remplacées de temps à autre.

(n) « **Sous-traitant ultérieur** » désigne les Sous-traitants engagés par Dynatrace ou les membres du Groupe Dynatrace pour permettre à Dynatrace de livrer/fournir les Offres de Dynatrace conformément aux conditions du Contrat ou du présent CTD.

(o) « **Autorité de contrôle** » désigne l'agence gouvernementale, le ministère ou toute autre organisation compétente ayant autorité sur le traitement des Données Personnelles pertinentes pour le présent CTD.

(p) « **Addendum britannique** » désigne l'Addendum international de transfert de données aux Clauses contractuelles types de la Commission européenne publié par le bureau de l'Information Commissioner (ICO) du Royaume-Uni en vertu du S119A (1) Data Protection Act 2018, tel que mis à jour, modifié ou remplacé de temps à autre.

(q) Les termes « **Entreprise** », « **Responsable du traitement** », « **Consommateur »,** « **Sous-traitant** », « **Prestataire de services** », « **Personne concernée** », « **Vendre** », « **Autorité de contrôle** » et « **Traitement** » (et « **Traiter** ») auront la signification qui leur est attribuée en vertu de la Loi applicable en matière de protection des données.

2. Applicabilité du CTD et rôles des parties

(a) Le présent CTD s'applique au Traitement des Données Personnelles du Client par Dynatrace pour le compte du Client afin d'exécuter ses obligations et d'exercer ses droits en vertu du Contrat et du présent CTD. Afin d'éviter toute ambiguïté, le présent CTD ne s'applique pas au Traitement des Données Personnelles du Client par Dynatrace en tant que Responsable du traitement.

(b) Le Client est un Responsable de traitement ou un Sous-traitant et Dynatrace est un Sous-traitant. Dans la mesure où cela est applicable en vertu de la Loi sur la Protection des Données, le client désigne Dynatrace en tant que Sous-traitant pour traiter les Données Personnelles du Client en son nom.

3. Traitement des Données Personnelles du Client

(a) La nature et la portée du Traitement des Données Personnelles du Client par Dynatrace pour fournir les Offres de Dynatrace sont déterminées et contrôlées par le Client et sont décrites dans l'Annexe A. La nature, le but et la durée du Traitement, ainsi que les types de Données Personnelles collectées et les catégories de Personnes concernées dont les Données Personnelles peuvent être traitées par Dynatrace, sont décrits dans l'**Annexe A** du présent CTD. Le Client reconnaît que Dynatrace n'a aucune connaissance des données ou types de Données Personnelles contenus dans les Données du Client. Les parties conviennent que les instructions complètes et définitives du Client concernant la nature et les finalités du Traitement en lien avec les Offres de Dynatrace sont énoncées dans le Contrat et le présent CTD.

(b) Tout changement ou modification des instructions doit être communiqué par écrit et approuvé par les

deux parties. Dynatrace informera le Client si, de son point de vue raisonnable, les instructions de traitement du Client sont susceptibles d'enfreindre une Loi de Protection des Données applicable; dans ce cas, Dynatrace est en droit de refuser le Traitement des Données Personnelles du Client qu'elle estime être en violation d'une Loi de Protection des Données applicable, jusqu'à ce que le Client modifie ses instructions de manière à ne pas l'enfreindre.

(c) Dans la mesure où la configuration des Offres de Dynatrace par le Client entraîne la collecte par Dynatrace de Données Personnelles du Client, celui-ci déclare et garantit qu'il se conformera, à tout moment, à toutes les Lois de Protection des Données applicables. Entre le Client et Dynatrace, le Client est responsable de : (i) la protection des Données Personnelles du Client lors de l'utilisation de Dynatrace en configurant les Paramètres de confidentialité des données de Dynatrace tels que décrits à l'adresse https://docs.dynatrace.com/docs/manage/data-privacy-and-security (instructions de Dynatrace sur la manière de configurer les paramètres de confidentialité des données) pour contrôler avec précision la portée des Données Personnelles du Client qui seront collectées par les Offres de Dynatrace ; (ii) l'exactitude, la qualité et la légalité des Données Personnelles du Client, et les moyens par lesquels le Client ou tout tiers concerné a acquis ces Données Personnelles.

(d) Si le Client est un Sous-traitant agissant au nom d'un Responsable de traitement tiers, le Client garantit à Dynatrace que ses instructions et actions concernant les Données Personnelles du Client, y compris sa désignation de Dynatrace en tant qu'autre Sous-traitant, ont été autorisées par le Responsable de traitement concerné.

(e) Le Client déclare et garantit que : (i) il informera les Personnes concernées, comme l'exige la loi, de son recours à des Sous-traitants pour traiter leurs données à caractère personnel, y compris Dynatrace, y compris, le cas échéant, en informant les Personnes concernées de l'utilisation des Offres de Dynatrace ; (ii) il a obtenu, et continue d'avoir, pendant la durée du Contrat, tous les droits nécessaires, la base juridique, les autorisations et/ou le consentement valide des Personnes concernées pour le Traitement des Données Personnelles relatives au Client par Dynatrace, tel qu'envisagé par le Contrat ; (iii) l'utilisation par le Client des Offres de Dynatrace ne conduira pas Dynatrace à enfreindre les Lois de Protection des Données applicables ou toute autre loi ou règlementation applicable.

(f) Le Client ne fournira à Dynatrace que les Données Personnelles du Client nécessaires à Dynatrace pour exécuter ses obligations en vertu du Contrat concernant les Offres de Dynatrace et tous les services associés. Le Client reconnaît que l'utilisation des Offres de Dynatrace ne nécessite pas et n'est pas adaptée au Traitement de toute Information Restreinte et qu'il ne fournira pas, dans le cadre de son utilisation des Offres de Dynatrace, d'Information Restreinte à traiter par Dynatrace.

4. Demandes de tiers.

(a) Les Offres de Dynatrace fournissent au Client une fonctionnalité permettant d'accéder aux Données Personnelles du Client afin d'aider les Clients à répondre aux demandes des Personnes concernées exerçant leurs droits qui leur sont accordés en vertu de la Loi sur la Protection des Données (« Demandes des Personnes concernées ») ou aux demandes des organismes réglementaires ou judiciaires concernant le Traitement des Données Personnelles du Client. Dans la cas où le Client n'est pas en mesure d'accéder aux Données Personnelles du Client pertinentes dans les Offres de Dynatrace ou si l'accès aux Données Personnelles du Client ne permet pas une assistance suffisante pour répondre à ces demandes conformément à la Loi sur la Protection des Données, et lorsque la Loi sur la Protection des Données applicable l'exige, Dynatrace accepte, à la demande du Client, de fournir une assistance raisonnable au Client, pour permettre audit Client de répondre aux Demandes des Personnes concernées ou aux demandes des organismes réglementaires ou judiciaires relatives au Traitement des Données Personnelles du Client en vertu du Contrat. Si une demande est faite directement à Dynatrace concernant les Données Personnelles du Client pour lesquelles Dynatrace peut identifier le Client comme étant le Responsable du traitement, Dynatrace devra dans les meilleurs délais renvoyer cette communication au Client et ne devra pas répondre à une telle demande sans son autorisation expresse. Ce qui précède n'interdit pas à Dynatrace de communiquer avec une Personne concernée ou un organisme réglementaire

ou judiciaire s'il ne ressort pas raisonnablement de la communication que la demande concerne le Client ou si Dynatrace a l'obligation légale de répondre elle-même.

(b) Si Dynatrace est tenue de divulguer des Données Personnelles pour lesquelles le Client est le Responsable du traitement suite à une demande d'un organisme chargé de l'application de la loi ou d'un autre tiers, Dynatrace en informera le Client avant d'accorder l'accès et/ou de fournir les Données Personnelles, afin de permettre au Client de demander une ordonnance de protection ou toute autre mesure appropriée. Si Dynatrace ne peut pas légalement informer le client, Dynatrace prendra des mesures pour protéger les Données Personnelles d'une divulgation indue, comme s'il s'agissait de ses propres Informations Confidentielles.

5. **Assistance et coopération.** Sous réserve de la nature du traitement et des Données Personnelles dont dispose Dynatrace et lorsque la Loi sur la Protection des Données applicable l'exige, Dynatrace fournira, sur demande écrite du Client, une assistance et des informations raisonnables au Client, lorsque, de l'avis de ce dernier, le type de Traitement effectué par Dynatrace nécessite une étude d'impact sur la protection des données, et/ou une consultation préalable avec les autorités compétentes en matière de protection des données et fournira une assistance raisonnable au Client pour se conformer à ses autres obligations en vertu de la Loi sur la Protection des Données applicable concernant la sécurité des données et les notifications de Violation de Données Personnelles, dans la mesure applicable au Traitement des Données Personnelles du Client. Le Client remboursera Dynatrace de tous les coûts encourus par Dynatrace dans l'exécution de ses obligations en vertu du présent article.

6. **Conformité.** Dynatrace accepte de fournir les informations nécessaires pour démontrer la conformité au présent CTD sur demande raisonnable du Client.

7. **Audits et évaluations.**

(a) Lorsque les Lois sur la Protection des Données applicables accordent au Client un droit d'audit ou d'évaluation, et sous réserve de sa portée, le Client peut effectuer, sur demande écrite et au maximum une fois par an, un audit ou une évaluation des politiques, procédures et enregistrements de Dynatrace relatifs au traitement des Données Personnelles du Client, conformément aux Lois sur la Protection des Données applicable.

(b) Pour demander un audit, le Client doit soumettre à Dynatrace un plan d'audit détaillé au moins quatre (4) semaines avant la date d'audit proposée, décrivant la portée, la durée et la date de début de l'audit. Dynatrace examinera le plan d'audit et fera part au Client de toute préoccupation ou question. Avant le début de tout audit, les parties doivent se mettre d'accord sur un plan détaillé, précisant notamment les coûts, le calendrier, l'étendue des contrôles, les justificatifs à produire et la durée de l'audit. Si le périmètre de l'audit demandé est compris dans un rapport d'audit similaire réalisé au cours des douze mois précédents et que Dynatrace confirme qu'il n'y a pas de changements importants dans les contrôles audités, le Client accepte ces conclusions au lieu de demander un nouvel audit de ces contrôles.

(c) Tout audit ou évaluation doit être : (i) effectué pendant les heures normales d'ouverture de Dynatrace ; (ii) soumis aux obligations de confidentialité des parties. Si l'audit doit être effectué par un tiers, ledit tiers ne doit pas être un concurrent de Dynatrace, et il doit obtenir l'accord préalable de Dynatrace et signer un accord de confidentialité écrit avec les parties avant d'effectuer l'audit.

(d) Tous les audits sont à la charge du Client. Toute demande d'assistance de Dynatrace pour un audit est considérée comme un service distinct si l'assistance en question nécessite l'utilisation de ressources différentes de, ou en plus de, celles requises pour la fourniture des Offres de Dynatrace. Le Client devra confirmer par écrit à Dynatrace qu'il paiera tous les frais applicables avant que Dynatrace fournisse une telle assistance à l'audit.

8. **Confidentialité.** Dynatrace veillera à ce que toute personne qu'elle autorise à traiter les Données

Personnelles du Client (y compris son personnel, ses agents et ses sous-traitants) soit soumise à une obligation contractuelle, légale ou autre obligation contraignante de confidentialité.

9. Sécurité

(a) **Mesures de sécurité.** Compte tenu de l'état de l'art, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du risque de probabilité et de gravité variables quant aux droits et libertés des personnes physiques, Dynatrace a mis en œuvre et veillera à maintenir des mesures techniques et organisationnelles appropriées conçues pour fournir un niveau de sécurité adapté au risque que présente le Traitement des Données Personnelles des clients (« **Mesures de sécurité** »). Le Client confirme que la mise en œuvre par Dynatrace des Mesures de sécurité décrites à l'**Annexe B** est suffisante pour se conformer à ses obligations en vertu du présent CTD. Nonobstant ce qui précède, le Client reconnaît et convient qu'il est responsable de sa propre utilisation sécurisée des Offres de Dynatrace.

(b) **Violation de Données Personnelles.** En cas de violation de Données Personnelles, Dynatrace en informera le Client dans les plus brefs délais et au plus tard dans le délai imposé par la Loi sur la Protection des Données applicable, dès qu'elle en aura pris connaissance. Dynatrace diligentera rapidement une enquête sur les circonstances entourant la Violation de Données personnelles et transmettra ses conclusions au Client. Dynatrace s'efforcera de prendre toutes les mesures requises par la Loi sur la Protection des Données applicable pour atténuer les effets de ladite Violation de Données personnelles. À la demande du Client et en tenant compte de la nature du Traitement et des informations dont elle dispose, Dynatrace prendra des mesures commercialement raisonnables pour aider le Client à se conformer à ses obligations pour lui permettre de notifier les Violations de Données Personnelles pertinentes aux autorités compétentes et/ou aux Personnes concernées affectées, si ledit Client est tenu de le faire en vertu de la Loi sur la Protection des Données applicable. La notification d'une Violation de Données Personnelles sera transmise à un ou plusieurs administrateurs du Client par tout moyen choisi par Dynatrace, y compris par courriel. Il incombe au Client de s'assurer que ses administrateurs conservent des coordonnées exactes sur le portail en ligne ou tel qu'autrement requis par notification de Dynatrace adressée à son ou ses administrateur(s). Le fait que Dynatrace soit tenue de signaler ou de répondre à une Violation de Données Personnelles en vertu du présent article ne constitue pas une reconnaissance par Dynatrace d'une quelconque faute ou responsabilité en ce qui concerne la Violation de Données Personnelles.

10. Sous-traitance

(a) Le Client donne une autorisation générale pour désigner les membres du Groupe Dynatrace en tant que Sous-traitants ultérieurs en vertu du présent CTD, et autorise Dynatrace et les membres du Groupe Dynatrace à engager d'autres Sous-traitants ultérieurs. Une liste à jour des Sous-traitants ultérieurs actuels pour les Offres de Dynatrace est disponible sur https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/. Pour être informé des nouveaux Sous-traitants ultérieurs ou des changements dans les Sous-traitants ultérieurs, le Client doit s'inscrire pour recevoir les notifications disponibles sur https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ (« **Notification de protection des données** »). Dynatrace mettra à jour la Liste des Sous-traitants ultérieurs pour faire apparaître tout ajout ou changement de Sous-traitants ultérieurs tiers au moins trente (30) jours avant la date d'entrée en vigueur du changement. Les clients qui se sont abonnés aux notifications des mises à jour de la liste des Sous-traitants ultérieurs seront informés du changement.

(b) Dans la mesure requise par la Loi de Protection des Données applicable, le Client peut s'opposer au traitement de ses Données Personnelles par tout Sous-traitant ultérieur nouvellement nommé pour des motifs raisonnables relatifs à la protection des Données Personnelles du Client et en informera Dynatrace par écrit dans les quinze (15) jours suivant la publication de la notification des modifications de la Liste des Sous-traitants ultérieurs, en indiquant les raisons spécifiques de son objection. Cette objection doit être formulée par écrit et justifiée de manière commercialement raisonnable, sur la base de préoccupations raisonnables concernant les pratiques du Sous-traitant ultérieur proposé en matière de protection des données. En cas de refus, les parties collaboreront de bonne foi pour répondre aux objections raisonnables

du Client et procéder au changement de Sous-traitant. Si un accord ne peut être conclu dans les quinze (15) jours suivant l'objection, au choix de Dynatrace : (a) Dynatrace demandera au Sous-traitant ultérieur de ne pas traiter les Données Personnelles du Client, ce qui peut entraîner la suspension et l'indisponibilité d'une fonctionnalité des Offres de Dynatrace pour ledit Client, ou (b) le Client pourra résilier immédiatement le présent CTD et le Contrat et Dynatrace remboursera rapidement une partie de tous les frais prépayés au prorata de la période suivant la date de suspension ou de résiliation. Si Dynatrace ne reçoit aucune objection dans le délai indiqué ci-dessus, le Client sera réputé avoir approuvé le recours au nouveau Sous-traitant ultérieur.

(c) Dynatrace: (i) conclura un contrat écrit avec chaque Sous-Traitant dans lequel figurent des obligations relatives à la protection des données appropriées et substantiellement similaires mais non moins restrictives que celles énoncées dans le présent CTD, dans la mesure appropriée à la nature du service fourni par ledit Sous-Traitant ; et (ii) restera responsable du respect par ledit Sous-Traitant des obligations du présent CTD et de tout acte ou omission dudit Sous-Traitant entraînant la violation par Dynatrace de l'une quelconque de ses obligations au titre du présent CTD.

11. Suppression des Données du Client en fin de Contrat. Après la résiliation ou l'expiration du Contrat, les Données Personnelles du Client seront supprimées dans les trente (30) jours, ou, au choix du Client, renvoyées, sauf si la loi applicable l'exige ou en cas d'archivage sur des systèmes de sauvegarde, auquel cas les conditions du présent CTD resteront en vigueur.

12. Transferts internationaux de données

(a) Le Client autorise Dynatrace et ses Sous-traitants ultérieurs à transférer les Données Personnelles du Client au-delà des frontières internationales, y compris, mais sans s'y limiter, de l'EEE, du Royaume-Uni et/ou de la Suisse, d'Israël et de la Chine vers les États-Unis. Si les Données Personnelles du Client provenant de l'EEE ou de la Suisse sont transférées vers un pays qui n'a pas été jugé comme fournissant un niveau de protection adéquat en vertu de la Loi de Protection des Données applicable (« **Transfert restreint** »), les parties conviennent que le transfert sera régi par les Clauses Contractuelles Types qui sont incorporées par les présentes par référence au présent CTD comme suit. Les signatures figurant au CTD ou au Contrat valent signature des Clauses Contractuelles Types et de leurs annexes éventuelles. Lorsque le transfert des Données Personnelles du Client (« **Exportateur de données** ») à Dynatrace (« **Importateur de données** ») est un transfert restreint et que les Lois sur la Protection des Données exigent qu'un mécanisme de transfert valide soit mis en place, les transferts seront soumis aux Clauses Contractuelles Types.

(b) Les Clauses Contractuelles Types seront complétées comme suit :

i. Le Module 2 s'appliquera (le cas échéant) ;

ii. Dans la Clause 7 (Adhésion), la clause d'adhésion facultative s'appliquera ;

iii. Dans la Clause 8.5 et la Clause 16 (d), la certification de suppression sera fournie sur demande écrite de l'Exportateur de Données ;

iv. Dans la Clause 8.9, le droit d'audit sera effectué conformément à l'Article 7 du CTD ;

v. Dans la Clause 9 (Recours à des Sous-traitants ultérieurs), l'option 2 « Autorisation écrite générale » pour les Sous-traitants ultérieurs s'appliquera et la période de préavis sera telle qu'énoncée à l'Article 11 du présent CTD ;

vi. Dans la Clause 11 (Voies de recours), le texte optionnel ne s'applique pas ;

vii. Dans la Clause 13 (Contrôle), l'autorité de contrôle compétente sera la Commission nationale de l'informatique et des libertés (CNIL).

viii. Dans la Clause 14 (f) et la Clause 16 (c), le droit de résiliation sera limité à la résiliation des Clauses ;

ix. Dans la Clause 17 (Droit applicable), les Clauses contractuelles types seront régies par le droit français;

x. Dans la Clause 18(b) (Election de for et juridiction), les parties conviennent que les litiges seront résolus devant les tribunaux français ;

xi. L'Annexe 1 des Clauses contractuelles types sera complétée par les informations figurant à l'Annexe A du présent CTD ;

xii. L'Annexe 2 des Clauses contractuelles types sera complétée par les informations figurant à l'Annexe B du présent CTD ; et

xiii. Une nouvelle Clause 1 (e) est ajoutée aux Clauses contractuelles types comme suit : « Dans toute la mesure applicable, les présentes Clauses s'appliquent également mutatis mutandis au Traitement des Données Personnelles du Client par les Parties qui est soumis à la Loi Fédérale Suisse sur la Protection des Données. Le cas échéant, la référence au droit d'un État membre de l'UE ou aux autorités de contrôle de l'UE sera modifiée pour inclure la référence appropriée en vertu du droit suisse en ce qui concerne le transfert des Données Personnelles du Client qui sont soumises à la Loi Fédérale Suisse sur la Protection des Données, et au Commissaire Fédéral Suisse à la Protection des Données et à l'Information en tant qu'autorité de contrôle des présentes Clauses. »

(c) Dans la mesure où les Offres de Dynatrace impliquent le transfert de Données Personnelles du Client provenant du Royaume-Uni vers un pays tiers qui n'a pas été désigné comme fournissant un niveau adéquat de protection des Données Personnelles du Client en vertu du droit applicable au Royaume-Uni, les Clauses contractuelles standard doivent : (i) être utilisées et complétées comme indiqué dans l'Article 13 ; (ii) une nouvelle Clause 1(f) est ajoutée aux Clauses contractuelles standard, comme suit : « Dans toute la mesure applicable, les présentes Clauses, telles que complétées par l'Article 13, s'appliquent également mutatis mutandis au Traitement des Données Personnelles du Client par les Parties qui est soumis aux Lois Britanniques sur la Protection des données ; et (iii) l'Addendum britannique sera complété comme suit :

i. Le Tableau 1 de l'Addendum britannique est complété avec les informations figurant dans l'Annexe A.

ii. Le Tableau 2 de l'Addendum britannique est complété avec les informations figurant à l'Article 13 (c) du présent CTD.

iii. Le Tableau 3 de l'Addendum britannique est complété comme suit :

1) La liste des Parties est établie à l'Annexe A ;

2) Une description du transfert est présentée à l'Annexe A ;

3) Une description des mesures techniques et organisationnelles est présentée dans l'Annexe B ;

4) La liste des Sous-traitants ultérieurs figure à l'Article 11 du présent CTD ;

5) Aux fins de compléter le Tableau 4 de l'Addendum britannique, l'importateur et l'exportateur peuvent tous deux mettre fin à l'Addendum britannique comme indiqué à l'Article 19 dudit Addendum.

(d) Dans la mesure où la fourniture par Dynatrace des Offres de Dynatrace implique le transfert de Données Personnelles du Client provenant de la Chine vers un pays tiers qui n'a pas été désigné comme fournissant un niveau adéquat de protection des Données Personnelles du Client en vertu des Lois applicables en Chine), il incombe au Client de remplir toutes les obligations suivantes pour l'exportation des Données Personnelles du Client (lorsque le Client est le Responsable du traitement) ou de s'assurer que toutes les obligations suivantes ont été remplies par le responsable du traitement tiers concerné (lorsque le Client est le Sous-traitant) :

i. informer les personnes du nom et des coordonnées de la partie destinataire à l'étranger des Données Personnelles du Client, de la finalité et des moyens du Traitement, des catégories de Données Personnelles du Client, et des méthodes et procédures par lesquelles les personnes peuvent faire des demandes d'exercice des droits sur les Données Personnelles du Client auprès de la partie destinataire à l'étranger des Données Personnelles du Client ;

ii. obtenir une base juridique pour l'exportation des Données Personnelles du Client, et lorsque le consentement des personnes constitue la base légale, obtenir le consentement distinct des personnes ;

iii. réaliser une évaluation de l'impact de la protection des Données Personnelles sur l'exportation desdites données du Client ; et

iv. adopter la mesure de protection appropriée requise par le PIPL et les réglementations administratives qui l'accompagnent (c.-à-d. réussir l'évaluation de sécurité du gouvernement, déposer les clauses contractuelles types signées ou obtenir la certification), sauf si une exemption s'applique.

(e) En plus de ce qui précède, si une Autorité de contrôle adopte, met à jour ou remplace des clauses contractuelles types ou des mécanismes de transfert de données similaires, Dynatrace se réserve le droit d'adopter une norme de conformité alternative pour remplacer ou compléter les Clauses contractuelles types ou l'Addendum britannique pour le transfert légal de Données Personnelles, ou d'ajouter de nouveaux mécanismes de transfert de données pour d'autres pays, à condition que ceux-ci soient reconnus en vertu de la Loi sur la Protection des Données. Dynatrace émettra un préavis de trente (30) jours informant de l'adoption d'une norme de conformité alternative aux clients qui souscrivent aux Notifications de protection des données. La modification s'appliquera automatiquement comme indiqué dans la notification de Dynatrace à la fin de la période de préavis.

(f) En cas de conflit ou d'incohérence entre les documents suivants, l'ordre de priorité sera : (1) les Clauses contractuelles types (à condition toutefois que le Sous-traitant puisse nommer des Sous-traitants ultérieurs comme indiqué et sous réserve des exigences de l'Article 11 du présent CTD) ou un mécanisme similaire requis par les Lois applicables en matière de protection des données spécifiquement pour les transferts internationaux de données ; (2) le présent 'CTD ; et (3) le Contrat.

(g) Dans la mesure où Dynatrace transfère des Données du Client provenant du Brésil et protégées par la Loi sur la Protection des Données en vigueur dans ce pays, Dynatrace se conformera aux principes et aux droits des Personnes concernées ainsi qu'aux obligations de protection des données prévues par la LGPD.

(h) Dans la mesure où Dynatrace transfère des Données client provenant du Japon et protégées par la Loi sur la Protection des Données applicable dans ce pays, Dynatrace se conformera aux principes et droits des Personnes concernées et aux obligations de protection des données prévues dans l'APPI.

(i) Dans la mesure où la fourniture par Dynatrace des Offres de Dynatrace implique le transfert de Données Personnelles du Client provenant d'Israël vers un pays tiers qui n'a pas été désigné comme fournissant un niveau de protection adéquat pour les Données Personnelles du Client selon les Lois applicables en Israël, il incombera au Client d'obtenir une base juridique pour pouvoir exporter les Données Personnelles du Client. Pour plus de clarté, le présent CTD constitue l'obligation écrite de Dynatrace d'adopter les mesures de sécurité appropriées requises par le Règlement sur la Protection de la Vie Privée (Transfert International de Données) de 2001. Pour plus de lisibilité, les obligations figurant dans le présent CTD sont reconnues suffisantes par le Client pour permettre le transfert d'informations en dehors d'Israël conformément au Règlement 3 du Règlement sur la Protection de la Vie Privée (Transfert de données vers des bases de données en dehors des frontières du pays) de 2001.

13. Conditions supplémentaires spécifiques aux lois des États américains sur la Protection de la Vie Privée.

(a) La définition de « Loi applicable en matière de protection des données » comprend les lois sur la protection de la vie privée des États américains. « Lois sur la protection de la vie privée des États américains » : désigne toutes les lois des États relatives à la protection et au traitement des données à caractère personnel en vigueur aux États-Unis d'Amérique, qui peuvent inclure, sans s'y limiter, le California Consumer Privacy Act, tel que modifié par le California Privacy Rights Act (« CCPA »), et toute autre loi de protection de la vie privée des consommateurs dans d'autres états, ainsi que leurs modifications le cas échéant.

(b) Lorsque Dynatrace traite des Données Personnelles du Client soumises au CCPA ou aux lois sur la protection de la vie privée des États américains, Dynatrace agit en tant que « prestataire de services » ou « processeur » (si applicable) lors du traitement desdites Données. Le Client divulgue, ou met autrement à disposition, les Données Personnelles du Client à Dynatrace à des fins limitées et spécifiques pour fournir les Offres de Dynatrace dans les conditions du Contrat (« l'Objet »). Dynatrace devra (et exigera de même de ses Sous-traitants ultérieurs) :

i. se conformer aux obligations qui lui sont applicables en tant que prestataire de services our processeur en vertu des lois sur la protection de la vie privée des États américains ;

ii. notifier s'il ne peut plus remplir ses obligations au titre des lois sur la protection de la vie privée des États américains ;

iii. ne pas vendre ou partager le Contenu Client (« Customer Content ») ou conserver, utiliser, ou divulguer les Données Personnelles du Client : (1) à toute fin autre que la Finalité (« Purpose »), y compris la conservation, l'utilisation, ou la divulgation des Données Personnelles du Client à des fins commerciales autres que la Finalité, ou tel qu'autrement autorisé par les lois sur la protection de la vie privée des États américains ; ou (2) en dehors de la relation commerciale directe entre le Client et Dynatrace ; ou, à moins qu'il n'en soit autrement autorisé par les lois sur la protection de la vie privée des États américains, ne pas combiner les Données Personnelles du Client avec des données à caractère personnel que Dynatrace reçoit de, ou au nom d'une autre entreprise ou personne, ou qu'elle recueille à partir de ses propres interactions avec les individus, à moins qu'une telle combinaison ne soit nécessaire pour atteindre un objectif commercial tel qu'autorisé par le lois sur la protection de la vie privée des États américains.

iv. Le Client : (1) sur notification, aura le droit de prendre des mesures raisonnables et appropriées convenues par les parties pour veiller à ce que Dynatrace traite les Données Personnelles des clients d'une manière conforme aux obligations du Client en vertu des lois sur la protection de la vie privée des États américains et pour arrêter et remédier au traitement non autorisé des Données Personnelles des clients par Dynatrace ; (2) informera le Client s'il estime qu'il ne peut plus remplir ses obligations en tant que fournisseur de services en vertu des lois sur la protection de la vie privée des États américains.

v. Dynatrace reconnaît et confirme qu'elle ne reçoit pas de Données Personnelles du Client en contrepartie des Offres fournies au Client. Dynatrace certifie qu'elle comprend et respectera ses obligations en vertu de lois sur la protection de la vie privée des États américains.

15. Divers

(a) Sauf modification du présent CTD, le Contrat restera pleinement en vigueur. Toute modification apportée au présent CTD doit être faite par écrit et dûment signée par les représentants autorisés des parties.

(b) Nonobstant toute stipulation contraire de Contrat ou du présent CTD, la responsabilité de chaque Partie et de toutes ses Sociétés Affiliées, prise dans son ensemble, découlant de ou relative au présent CTD, à toute commande ou au Contrat, que ce soit soit en matière contractuelle, délictuelle ou en application d'un autre principe de responsabilité, demeurera soumise à l'Article « Limitation de responsabilité » du Contrat, et toute référence dans cet article à la responsabilité d'une Partie s'entend de l'entière responsabilité de cette partie et de toutes ses Sociétés affiliées au titre du Contrat et du présent CTD, y compris toutes leurs annexes. En aucun cas Dynatrace ne sera responsable envers le Client de pertes ou de dommages indirects ou consécutifs, de pertes de profits, de pertes de ventes, de pertes d'activité, de pertes d'économies escomptées, de pertes ou de dommages au fonds de commerce, ou autresqu'ils soient directs ou indirects, découlant du présent CTD ou en rapport avec celui-ci. Sans limiter les obligations des parties en vertu du Contrat ou du présent CTD, le Client convient que toute responsabilité encourue par Dynatrace en relation avec les Données Personnelles du Client découlant du non-respect par le Client de ses obligations en vertu du présent CTD ou de la Loi applicable en matière de protection des données sera prise en compte et réduira la limite de responsabilité de Dynatrace prévue au Contrat (ou, le cas échéant, au présent CTD) comme s'il s'agissait d'une responsabilité envers le Client. Nonobstant toute disposition contraire dans le présent CTD (y compris, mais sans s'y limiter, les obligations d'indemnisation de l'une ou l'autre des parties), aucune des parties ne sera responsable de toute amende émise ou imposée en vertu de l'article 83 du RGPD contre l'autre partie par une autorité de régulation ou un organisme gouvernemental en lien avec la violation du RGPD par ladite autre partie.

(c) Le présent CTD est régi et interprété conformément au droit applicable et à la clause attributive de compétence et de juridiction prévus dans le Contrat, étant entendu que les Clauses contractuelles types sont régies par les dispositions de l'Article 13 du présent CTD.

Accepté par :	Accepté par :
Nom_entité_client	**Nom_entité_Dynatrace**
Signature autorisée	Signature autorisée
Nom	Nom
Titre	Titre
Date	Date
Adresse	Adresse
Numéro de société (le cas échéant)	Numéro de société (le cas échéant)

ANNEXE A
INFORMATIONS RELATIVES AU TRAITEMENT

Description de l'Exportateur de données

L'Exportateur de données est l'entité identifiée comme le « Client » ou « Dynatrace », selon le cas en cas de Sous-traitance ultérieure, dans le Contrat de traitement des données existant entre l'Exportateur de données et l'Importateur de données et auquel la présente Annexe est jointe.

Description de l'importateur de données

L'Importateur de données est l'entité identifiée comme « Dynatrace » ou un Sous-traitant ultérieur dûment autorisé dans le Contrat de traitement de données en vigueur entre l'Exportateur de données et l'Importateur de données et auquel la présente annexe est jointe.

Objet et durée du traitement

L'objet et la durée du traitement sont les suivants :

De convention expresse entre les parties, le Client est le Responsable du traitement de certaines Données Personnelles du Client fournies à Dynatrace par le Client dans le cadre de son utilisation des Offres de Dynatrace. La durée du traitement correspond à la durée du Contrat.

Finalités du traitement

Le traitement est nécessaire aux finalités suivantes :

Permettre à Dynatrace de fournir les Offres de Dynatrace au Client et d'exercer ses droits et obligations au titre du Contrat.

Personnes concernées

Les personnes concernées peuvent inclure, à la seule discrétion du Client : (i) les utilisateurs autorisés par le Client à utiliser les Offres de Dynatrace et (ii) les utilisateurs ou visiteurs des applications et/ou sites Web monitorés par le Client (y compris, notamment, les employés du Client, ses clients, ses agents, ses sous-traitants et ses conseillers).

Type de données à caractère personnel

Le Client est tenu de fournir certaines Données Personnelles afin d'utiliser les Offres de Dynatrace, y compris l'adresse IP et le prénom et le nom de famille s'ils sont inclus dans l'adresse e-mail et les identifiants d'un utilisateur. Le Client peut soumettre des Données Personnelles supplémentaires aux Offres de Dynatrace, dont la mesure est déterminée et contrôlée par le Client à sa seule discrétion.

Catégories particulières de données ou données à caractère personnel sensibles (le cas échéant)

Les Données Personnelles transférées concernent les catégories particulières suivantes de données ou de données à caractère personnel sensibles :

Sans objet. Le Client n'est pas autorisé à utiliser les Offres de Dynatrace pour traiter des données classées comme « données de catégorie spéciale » ou « données sensibles » ou « Informations Restreintes » sauf accord explicite écrit.

Opérations de traitement

Les Données Personnelles transférées feront l'objet des opérations de traitement de base suivantes :

Dynatrace ne traitera les Données Personnelles du Client que dans le mesure nécessaire pour fournir les Offres de Dynatrace et exercer ses droits et obligations tels que contenus dans les conditions du Contrat et du CTD, y compris, notamment, la formation du Client, l'assistance technique, les services

professionnels, l'amélioration des performances et des fonctionnalités des Offres de Dynatrace, l'authentification et les communications des utilisateurs et l'administration des comptes.

ANNEXE B

MESURES DE SÉCURITÉ

Dynatrace (également désignée dans le présent document comme le « Sous-traitant »), mettra en œuvre, au minimum, les mesures de sécurité techniques et organisationnelles décrites ci-dessous concernant les Données Personnelles du Client qu'elle traite pour le compte du Client (également désigné dans les présentes comme le « Responsable du traitement »). Lesdites mesures de sécurité seront appliquées à toutes les Données Personnelles du Client soumises au contrat sous-jacent établi entre le Sous-traitant et le Responsable du traitement (le« Contrat »). En ce qui concerne les sous-traitants ultérieurs tiers susceptibles de traiter des Données Personnelles pour le compte de Dynatrace, lesdits tiers auront leurs propres exigences en matière de sécurité pour protéger les Données Personnelles.

Mesures techniques

1.1 Autorisation

(a) Un système d'autorisation doit être utilisé lorsque différents profils d'autorisation servent à des fins différentes.

1.2 Identification

(a) Chaque Utilisateur autorisé doit recevoir un code d'identification personnel et unique à cette fin (« ID utilisateur »). Un ID utilisateur ne peut pas être attribué à une autre personne, même ultérieurement.

(b) Un registre des Utilisateurs Autorisés et des accès autorisés dont chacun dispose sera tenu à jour, et des procédures d'identification et d'authentification pour tout accès aux systèmes d'information ou pour la réalisation d'un Traitement de Données seront établies. Tel qu'utilisé dans les présentes, le terme « Traitement » désigne toute opération ou ensemble d'opérations effectuées sur les Données, que ce soit ou non par des moyens automatisés, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction.

(c) Les mots de passe doivent être modifiés régulièrement comme indiqué dans les Politiques de sécurité de l'information.

1.3 Authentification

(a) Les utilisateurs autorisés sont habilités à traiter des données s'ils disposent d'informations d'authentification leur permettant de mener à bien une procédure d'authentification relative à une opération de traitement spécifique ou à un ensemble d'opérations de traitement.

(b) L'authentification doit être basée sur un mot de passe secret associé à un ID utilisateur, ledit mot de passe n'est connu que de l'utilisateur autorisé.

(c) Un ou plusieurs identifiants d'authentification doivent être attribués à un Utilisateur autorisé ou associés à celui-ci.

(d) Une procédure doit être mise en place pour assurer la confidentialité et l'intégrité des mots de passe. Les mots de passe doivent être stockés de manière à les rendre inintelligibles tant qu'ils restent valides. Une procédure doit être mise en place pour l'attribution, la distribution et le stockage des mots de passe.

(e) Les mots de passe sont composés d'au moins douze caractères ou, si cela n'est pas techniquement autorisé par les systèmes d'information correspondants, un mot de passe doit être composé du nombre maximum de caractères autorisé. Les mots de passe ne doivent contenir aucun élément pouvant être facilement lié à l'Utilisateur autorisé en charge du Traitement et doivent être modifiés à intervalles réguliers, lesquels intervalles doivent être définis dans le document de sécurité. Les mots de passe doivent être modifiés par l'Utilisateur autorisé selon une valeur secrète connue de lui seul lors de sa première utilisation et périodiquement par la suite.

(f) En plus d'un ID utilisateur et d'un mot de passe valides, tout accès aux données ou aux systèmes de Dynatrace doit être sécurisé par une solution d'authentification multifacteurs (« MFA »). La solution MFA peut être de nature logicielle ou matérielle.

(g) Les identifiants d'authentification doivent également être désactivés si l'Utilisateur autorisé est licencié, transféré ou privé de l'accès aux systèmes d'information ou au Traitement de Données.

1.4 Contrôles des accès

(a) Seuls les Utilisateurs autorisés ont accès aux Données, y compris lorsqu'elles sont stockées sur un support électronique ou portable ou lorsqu'elles sont transmises. Les Utilisateurs autorisés ne disposent d'un accès autorisé qu'aux données et ressources nécessaires à l'exercice de leurs fonctions.

(b) Un système permettant aux Utilisateurs autorisés d'accéder aux données et ressources désignées doit être utilisé.

(c) Il convient de vérifier deux fois par an que les conditions préalables à la conservation des profils d'autorisation pertinents sont toujours d'actualité. Cette vérification peut également porter sur la liste des utilisateurs autorisés établie par catégories homogènes de tâches et sur le profil d'autorisation correspondant.

(d) Des mesures doivent être mises en place pour empêcher un utilisateur d'accéder aux systèmes d'information ou de les utiliser sans autorisation. En particulier, des systèmes de détection d'intrusion conformes aux meilleures pratiques de l'industrie devraient être installés pour protéger les systèmes d'information contre les accès non autorisés.

(e) Les contrôles d'accès au système d'exploitation ou à la base de données doivent être correctement configurés pour ne permettre que des accès autorisés.

(f) Seul le personnel autorisé peut accorder, modifier ou annuler l'accès des utilisateurs aux systèmes d'information.

1.5 Gestion des systèmes informatiques et des supports amovibles

(a) Les systèmes d'information en réseau et les supports physiques stockant les données doivent être hébergés dans un environnement sécurisé dont l'accès physique est limité au seul personnel autorisé à y accéder. Il est nécessaire de mettre en place des contrôles d'accès et d'autorisation rigoureux.

(b) Les logiciels, les micrologiciels et le matériel utilisés dans les systèmes d'information font l'objet d'un examen annuel visant à détecter les vulnérabilités et les failles des systèmes d'information et à y remédier.

(c) Des politiques et des formations sont mises en place concernant la conservation et l'utilisation

des supports sur lesquels les Données sont stockées afin d'empêcher tout accès et Traitement non autorisés.

(d) Lorsque les supports doivent être mis au rebut ou réutilisés, les mesures nécessaires sont prises pour empêcher toute récupération ultérieure des données et autres informations précédemment stockées sur lesdits supports, ou pour rendre les informations intelligibles ou les reconstituer par tout moyen technique avant qu'ils ne soient retirés de l'inventaire. Tous les supports réutilisables utilisés pour le stockage des données seront écrasés au moins trois fois avec des données aléatoires avant d'être éliminés ou réutilisés.

(e) Le retrait des supports contenant des données des locaux désignés doit être spécifiquement autorisé par le Responsable du traitement et en conformité avec les politiques de Dynatrace.

(f) Les supports contenant des données doivent être supprimés ou rendus illisibles s'ils ne sont plus utilisés et avant d'être mis au rebut de manière appropriée.

1.6 Distribution ou transmission

(a) Seuls les Utilisateurs autorisés peuvent avoir accès aux Données.

(b) Le chiffrement (128 bits ou plus) ou une autre forme de protection équivalente doit être utilisé pour protéger les Données transmises électroniquement sur un réseau public ou stockées sur un appareil portable, ou lorsqu'il est nécessaire de stocker ou de traiter les Données dans un environnement physiquement non sécurisé.

(c) Lorsque les Données doivent quitter les locaux désignés à la suite d'opérations de maintenance, toutes les mesures nécessaires doivent être prises pour empêcher toute récupération non autorisée des Données et autres informations qui y sont stockées.

(d) Lorsque des Données sont transmises ou transférées sur un réseau de communications électroniques, des mesures doivent être mises en place pour contrôler le flux de données et enregistrer le moment de la transmission ou du transfert, les Données transmises ou transférées, la destination de toute Donnée transmise ou transférée, et les informations relatives à l'Utilisateur autorisé qui effectue la transmission ou le transfert.

1.7 Conservation, copies de sauvegarde et récupération

(a) Des procédures doivent être définies et établies pour effectuer des copies de sauvegarde et pour récupérer les Données. Ces procédures doivent permettre de reconstituer les données dans l'état où elles se trouvaient au moment où elles ont été perdues ou détruites.

(b) Les copies de sauvegarde doivent être effectuées au moins une fois par semaine, à moins qu'aucune donnée n'ait été mise à jour pendant cette période.

(c) Une copie de sauvegarde et les procédures de récupération des données doivent être conservées en un lieu différent du site des systèmes d'information traitant les Données et les présentes exigences minimales de sécurité s'appliquent à ces copies de sauvegarde.

1.8 Détection des antivirus et des intrusions

(a) Des logiciels antivirus et des systèmes de détection d'intrusion doivent être installés sur les systèmes d'information pour les protéger contre les attaques ou autres actes non autorisés. Les logiciels antivirus et les systèmes de détection des intrusions doivent être mis à jour régulièrement conformément aux meilleures pratiques du secteur pour les systèmes d'information concernés (et au moins une fois par an).

1.9 Test

(a) Les tests préalables à la mise en œuvre ou à la modification des systèmes d'information de Traitement des Données n'utilisent pas de données réelles ou « en temps réel », sauf si une telle utilisation est nécessaire et qu'il n'y a pas d'autre solution raisonnable. Lorsque des données réelles ou « en temps réel » sont utilisées, elles doivent être limitées dans la mesure nécessaire aux fins des tests et le niveau de sécurité correspondant au type de Données traitées doit être garanti.

1.10 Audit

(a) Le respect de ces exigences de sécurité doit faire l'objet d'audits réguliers, au moins une fois par an.

(b) Les résultats doivent donner un avis sur la mesure dans laquelle les mesures et contrôles de sécurité adoptés sont conformes à ces exigences de sécurité, identifier les lacunes éventuelles et (le cas échéant) proposer des mesures correctives ou supplémentaires si nécessaire. Ils doivent également présenter les données, les faits et les observations sur lesquels se fondent les opinions émises, ainsi que les recommandations proposées.

2. Mesures organisationnelles

2.1 Plan et document de sécurité

- Les mesures adoptées pour se conformer à ces exigences de sécurité feront l'objet de politiques de sécurité de l'information de l'entreprise et seront présentées dans un portail de sécurité, lequel sera tenu à jour et révisé chaque fois que des changements pertinents seront apportés au(x) système(s) d'information ou aux mesures techniques ou organisationnelles.
- Les Politiques de sécurité de l'information portent sur :

  (i) les mesures de sécurité relatives à la modification et à la maintenance du (des) système(s) utilisé(s) pour le Traitement des Données, y compris le développement et la maintenance des applications, l'assistance appropriée des fournisseurs et l'inventaire du matériel et des logiciels ;

  (ii) la sécurité physique, y compris la sécurité des bâtiments ou des locaux où le Traitement des Données a lieu, la sécurité de l'équipement de données et de l'infrastructure de télécommunication et les contrôles environnementaux ; et

  (iii) la sécurité des ordinateurs et des systèmes de télécommunication, y compris les procédures de gestion des copies de sauvegarde, les procédures relatives aux virus informatiques, les procédures de gestion des signaux/codes, la sécurité de la mise en œuvre des logiciels, la sécurité des bases de données, la sécurité de la connexion des systèmes à l'internet, l'inspection du contournement des systèmes de données, les mécanismes de comptabilisation des tentatives de violation de la sécurité des systèmes ou d'obtention d'un accès non autorisé.

- Le plan de sécurité doit inclure toutes les politiques de Dynatrace, telles que mises à jour de temps à autre, y compris, mais sans s'y limiter :

  (i) le Code de conduite professionnelle et d'éthique

  (ii) la Politique mondiale de protection des données

  (iii) la Politique d'utilisation acceptable de Dynatrace IT

  (iv) les Politiques de sécurité du système : Politique de gestion du contrôle d'accès Dynatrace ; Norme de conservation des sauvegardes ; Politique de gestion des changements ; Politique de gestion des changements - systèmes d'entreprise ; Politique de conformité ; Plan de réponse en cas d'incident lié à la cybersécurité et à la sécurité des données ; Politique de

classification des données ; Politique de prévention de la perte de données ; Politique de surveillance électronique ; Politique de chiffrement ; Politique de sécurité des ressources humaines ; Politique de gestion des ressources d'information ; Politique de gestion des risques liés à l'information ; Politique relative aux opérations informatiques ; Politique relative aux appareils mobiles ; Politique relative à l'accès au réseau ; Politique relative aux mots de passe des comptes réseau ; Politique relative aux pare-feu réseau ; Politique relative à la sécurité physique et à l'environnement ; Politique relative à la restitution des actifs pour les employés en fin de contrat ; Sécurité ; Politique relative à la sécurité contre l'hameçonnage ; Politique relative au cycle de vie des comptes de service ; Politique relative à la gestion des fournisseurs ; Politique relative à la gestion des vulnérabilités ; Politique relative à la sécurité des postes de travail.

(v) Le plan de sécurité doit être mis à la disposition du personnel ayant accès aux Données et aux systèmes d'information, et doit couvrir au minimum les aspects suivants :

(vi) La portée, avec une spécification détaillée des ressources protégées ;

(vii) Les mesures, normes, procédures, règles et normes du code de conduite pour garantir la sécurité, y compris le contrôle, l'inspection et la supervision des systèmes d'information ;

(viii) Les procédures de signalement, de gestion et de réponse en cas d'incidents ; et

(ix) Les procédures permettant d'effectuer des copies de sauvegarde et de récupérer les Données, y compris le membre du personnel qui a entrepris l'activité de Traitement, les Données restaurées et, le cas échéant, les données qui devaient être saisies manuellement dans le processus de récupération.

2.2 Fonctions et obligations du personnel

- Seuls les membres du personnel qui ont un besoin opérationnel légitime d'accéder aux systèmes d'information ou d'effectuer un Traitement des Données seront autorisés à le faire (« **Utilisateurs autorisés** »).

- Les mesures nécessaires doivent être adoptées pour former et familiariser le personnel avec ces exigences minimales en matière de sécurité, toutes les politiques pertinentes et les lois applicables concernant l'exécution de leurs fonctions et devoirs en ce qui concerne le Traitement des Données et les conséquences de toute violation de ces exigences.
- Les fonctions et obligations du personnel ayant accès aux Données et aux systèmes d'information doivent être clairement définies par les rôles de sécurité des applications.
- Les Utilisateurs autorisés doivent être informés le matériel électronique ne doit pas être laissé sans surveillance ou accessible pendant les sessions de Traitement. L'accès physique aux zones où des Données sont stockées est strictement réservé aux Utilisateurs autorisés. En cas de violation du plan de sécurité, les mesures disciplinaires sont clairement définies, documentées et communiquées au personnel.

2.3 Directeur de la sécurité

- Une ou plusieurs personnes responsables de la conformité globale à ces exigences minimales en matière de sécurité est (sont) désignée(s) comme Responsable(s) de la sécurité des systèmes de l'information(« **RSSI** »). Le RSSI doit disposer d'une formation et d'une expérience suffisantes en matière de gestion de la sécurité de l'information, ainsi que des ressources appropriées pour assurer efficacement le respect des règles.
- Les coordonnées du RSSI sont fournies au Responsable du traitement sur demande.

2.4 Tenue des registres

- L’historique de l’accès des Utilisateurs autorisés aux Données, ou de leur divulgation, est enregistré sous forme d’une piste d’audit sécurisée.
- Seul le personnel dûment autorisé peut accéder physiquement aux locaux où sont stockés les systèmes d’information et les supports de stockage des Données.
- Une procédure doit être mise en place pour signaler, répondre et gérer les incidents de sécurité tels que les violations de la sécurité des données. Cette procédure doit comprendre au minimum les éléments suivants :

  (i) Une procédure pour signaler à la hiérarchie de tels incidents/violations;

  (ii) Une équipe clairement désignée pour gérer et coordonner la réponse à donner en cas d’incident, sous la supervision du RSSI ;

  (iii) Un processus documenté de gestion de la réponse à apporter en cas d’incident, y compris l’obligation de tenir des registres où figurent les problèmes rencontrés et les mesures prises, avec mention de l’heure à laquelle l’incident s’est produit, de la personne qui l’a signalé, de la personne à qui il a été signalé et de ses conséquences ;

  (iv) L’obligation pour le Sous-traitant d’informer le Responsable du traitement dans les meilleurs délais en cas de violation de la sécurité entraînant, accidentellement ou illégalement, la destruction, la perte, l’altération, la divulgation non autorisée ou l’accès non autorisé aux Données transmises, stockées ou autrement traitées par le Sous-traitant ; et

  (v) L’équipe du Sous-traitant chargée de la gestion de la sécurité/incident doit, le cas échéant, collaborer avec les représentants de la sécurité du Responsable du traitement jusqu’à ce que l’incident ou la violation ait été résolu de manière satisfaisante.

  (vi) La procédure de signalement, de gestion et de réponse aux incidents doit être testée au moins une fois par an.