Mesures techniques et organisationnelles de NTT

A travers les technologies et innovations, la vision de NTT est de permettre un futur connecté et sécurisé. Nous avons établi ces Mesures Techniques et Organisationnelles de NTT (MTO) qui décrivent la manière dont nous assurons la protection des données à caractère personnel de manière transparente, équitable, éthique et légale.

Nos MTO sont fondées sur les meilleures pratiques de l'industrie et sur les exigences légales applicables dans les juridictions dans lesquelles nous opérons, en prenant en compte la nature des données que nous traitons et le coût de leur implémentation.

Sommaire

(A) Confidentialité des données et mesures de protection

1 Gouvernance et modèle opérationnel

1.1 NTT s'engage à faire preuve de responsabilité lorsque NTT traite des données à caractère personnel et a mis en place une structure organisationnelle, ainsi que les rôles et responsabilités pour la gestion et la supervision du traitement des données à caractère personnel.

1.2 Un certain nombre de structures de gouvernance ont été mises en place pour garantir que les questions de confidentialité et de protection des données sont examinées par la direction appropriée au sein de NTT. La responsabilité ultime de la confidentialité et de la protection des données incombe au comité de direction de NTT Ltd et est soutenue par des rôles désignés dans toute l'entreprise, y compris des délégués à la protection des données nommés ou des rôles équivalents, lorsque requis par les Lois applicables à la protection des données.

2 Politiques, processus et Lignes directrices

2.1 NTT a mis en œuvre et communiqué ses politiques, processus, normes et directives qui détaillent la manière dont les collaborateurs de NTT sont censés traiter les données à caractère personnel. Cela comprend les politiques suivantes:

2.1.1 Politique de confidentialité et de protection des données ;

2.1.2 Politique relative aux droits des personnes concernées ; et

2.1.3 Politique relative aux notifications des violations de données à caractère personnel.

2.2 NTT a défini et communiqué des instructions de confidentialité aux collaborateurs, clients ou autres parties prenantes sur la manière dont les données à caractère personnel sont traitées.

2.3 NTT a mis en œuvre un processus d'Analyse d'Impact sur la Protection des Données (IAPD) et réalise autant d'IAPD que nécessaire et en application des Lois applicables à la protection des données.

3 Protection des données dès la conception

3.1 NTT s'engage à mettre en œuvre des mesures raisonnables pour soutenir la capacité de ses clients à se conformer aux Lois applicables à la protection des données. Dans la mesure du possible, les principes de protection des données dès la conception et par défaut sont appliqués lors du développement et de la livraison des produits, services et solutions de NTT.

4 Data Landscape

4.1 NTT a mis en place des processus pour identifier, enregistrer, évaluer et maintenir une compréhension précise des données à caractère personnel traitées par NTT.

4.2 NTT tient un registre des données à caractère personnel traitées conformément aux Lois applicables à la protection des données.

5 Gestion du cycle de vie des informations

5.1 NTT a mis en place des politiques et des processus pour garantir que les données à caractère personnel sont traitées de manière appropriée tout au long de leur cycle de vie (de la collecte à l'utilisation, la conservation, la divulgation et la destruction).

5.2 Les Lois applicables à la protection des données, dans certains pays, confèrent aux personnes concernées des droits spécifiques en ce qui concerne leurs données à caractère personnel. NTT s'engage à respecter ces droits et à s'assurer que NTT réponde aux demandes des personnes concernées de manière transparente, équitable, éthique et légale.

5.3 NTT a mis en œuvre une politique sur les droits des personnes concernées et un processus de demande des personnes concernées pour faire respecter les droits des personnes concernées conformément aux Lois applicables à la protection des données.

5.4 NTT tient un registre de toutes les demandes des personnes concernées reçues et des mesures prises pour répondre à ces demandes. NTT fournira tout le soutien raisonnable aux clients pour répondre aux demandes des personnes concernées, sur demande, et conformément aux accords avec eux.

5.5 NTT maintient une politique de conservation, d'archivage et d'élimination des enregistrements qui est soutenue par des calendriers de conservation des enregistrements qui sont alignés sur les lois applicables. NTT ne conserve les données à caractère personnel que s'il existe un objectif commercial légitime et conformément à ses obligations légales. NTT détruit, supprime ou désidentifie les données à caractère personnel lorsque la période de conservation expire et qu'il n'y a aucune raison commerciale légitime de conserver les données à caractère personnel pendant une période plus longue.

5.6 NTT conservera les données à caractère personnel traitées pour le compte de ses clients conformément aux exigences du client et détruira, supprimera, désidentifiera ou restituera les données à caractère personnel sur demande, au client, et lorsqu'il n'y a plus d'obligation de conserver les données à caractère personnel en vertu de la loi applicable.

5.7 NTT a mis en œuvre tous les efforts raisonnables pour s'assurer que les données à caractère personnel sont exactes, complètes et à jour.

5.8 NTT s'appuie sur des clauses contractuelles type pour prendre en charge le transfert légal des données à caractère personnel en dehors du pays où elles ont été initialement collectées et a conclu des accords appropriés avec les filiales, sociétés affiliées, sous-traitants et clients de NTT pour prendre en charge les transferts transfrontaliers.

6 Formation et sensibilisation à la confidentialité et à la protection des données

6.1 NTT exige que tous les collaborateurs suivent une formation annuelle sur la confidentialité et la protection des données. Toutes les politiques, processus, normes et directives de confidentialité et de protection des données sont à la disposition des collaborateurs et communiqués régulièrement. Le cas échéant, une formation locale, régionale ou fonctionnelle est également proposée pour aider les collaborateurs à agir conformément aux exigences de protection des données dans des pays, régions ou fonctions commerciales spécifiques.

7 Sécurisation de la confidentialité

7.1 Les équipes NTT en charge de la confidentialité et de la protection des données et de la sécurité des informations travaillent ensemble pour garantir qu'une gouvernance et un contrôle approprié de la protection des données sont mis en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité des données à caractère personnel.

7.2 Les mesures spécifiques de sécurité de l'information sont définies en paragraphe (B) de ces MTO

8 Réponse aux incidents et notification

8.1 NTT dispose de politiques, processus et procédures pour identifier, détecter, répondre, récupérer et notifier les parties prenantes appropriées en cas de violation de données à caractère personnel. Cela comprend des mécanismes pour effectuer une analyse des causes et entreprendre des actions correctives.

8.2 NTT s'engage à s'assurer que NTT informe les autorités de protection des données applicables, les clients concernés et les personnes concernées en cas de violation de données à caractère personnel conformément aux Lois applicables à la protection des données applicables et à tout engagement contractuel.

8.3 NTT tient un registre de toutes les violations de données à caractère personnel et des mesures prises pour répondre à ces événements

8.4 Les mesures de gestion des incidents NTT pour identifier, détecter, répondre et récupérer des incidents de sécurité de l'information sont décrites dans la section B (Sécurité de l'information) de ces MTO.

9 Gestion des tierst

9.1 NTT est responsable des actions de ses sous-traitants qui traitent les données à caractère personnel au nom de NTT et évalue la capacité de ses sous-traitants à protéger les données à caractère personnel au moment de la sélection et sur une base périodique par la suite, conformément aux politiques de NTT.

9.2 Les sous-traitants de NTT sont tenus de signer des accords appropriés qui régissent le traitement et la protection des données à caractère personnel et exigent que les mêmes obligations, telles que décrites dans l'accord de protection des données, soient transférées à tout sous-traitant supplémentaire que NTT pourrait engager. NTT a déployé tous les efforts raisonnables pour s'assurer que des accords de protection des données sont en place avec ses sous-traitants.

10 Surveillance et évaluation

10.1 NTT rend compte périodiquement de la conception et de l'efficacité opérationnelle de ses activités de confidentialité et de protection des données au comité d'audit et des risques de NTT Ltd et à la direction générale. Cela comprend des tableaux de bord, des auto-évaluations de la direction, des certifications, des revues d'audit interne et des audits et évaluations indépendants.

(B) Mesures de sécurité de l'informations

NTT s'engage à veiller à ce que le contrôle de la sécurité des informations soit mis en œuvre et correctement géré, afin de protéger la confidentialité, l'intégrité et la disponibilité des données à caractère personnel traitées au nom et sous les instructions du Client.

NTT a mis en place un système de management de la Sécurité de l'information à l'échelle du groupe, qui est aligné sur les principales pratiques et

normes de sécurité de l'information du monde entier, y compris les certifications ISO27000 et le Cyber Security Framework (CSF) établis par le NIST.

11 Sécurité de l'Information

11.1 Les rôles et des responsabilités en matière de sécurité de l'information ont été officiellement attribués, avec des lignes hiérarchiques qui garantissent l'indépendance de la fonction, y compris un responsable de la sécurité des systèmes d'informations ('RSSI), et des correspondants sur la sécurité de l'information ('RSSI').

11.2 Les collaborateurs de NTT sont responsables de veiller à ce qu'ils agissent conformément aux politiques, processus, normes et directives de la sécurité de l'information dans leurs activités commerciales quotidiennes.

11.3 NTT a documenté et publié un ensemble de politiques de sécurité de l'information qui prennent en charge les exigences du ISMS. Les politiques et les pièces justificatives sont revues périodiquement.

11.4 NTT a mis en place des mesures pour garantir que les appareils mobiles (y compris les ordinateurs portables, les téléphones portables, les tablettes, les appareils permettant l'accès à distance et les programmes « Bring your own device ») et leur contenu sont protégés. Des efforts raisonnables ont été déployés par NTT pour s'assurer que les outils de gestion des appareils mobiles («GAM») est installé sur tous les appareils mobiles ayant accès au réseau d'entreprise de NTT.

11.5 Les télétravailleurs ne peuvent accéder à distance à l'infrastructure NTT qu'en utilisant les services de réseau privé virtuel («VPN»), lorsque cela est possible.

12 Ressources Humaines

12.1 NTT effectue une vérification des antécédents et de l'emploi de ses collaborateurs, dans la mesure permise par la loi applicable, afin de garantir leur aptitude à embaucher et à traiter les informations sur l'entreprise et les clients (y compris les données à caractère personnel). L'étendue du filtrage est proportionnelle aux exigences opérationnelles et à la classification des informations auxquelles le colaborateur aura accès.

12.2 NTT exige que les collaborateurs de NTT (y compris les sous-traitants et les collaborateurs temporaires) acceptent de maintenir la confidentialité des données internes et client de NTT (y compris les données à caractère personnel).

12.3 Les collaborateurs de NTT doivent suivre une formation de sensibilisation à la sécurité de l'information sur une base annuelle. Les politiques de sécurité de l'information et les procédures, processus et directives de soutien sont mis à la disposition des collaborateurs et les collaborateurs reçoivent des informations pertinentes sur les tendances, les menaces et les meilleures pratiques via les plates-formes de communication NTT.

13 Gestion des actifs

13.1 NTT a une politique d'utilisation acceptable qui prend en charge l'utilisation et la protection appropriées et efficaces des actifs de l'entreprise NTT, y compris les ressources informatiques et de télécommunications, les produits, les services, les solutions et l'infrastructure informatique.

13.2 NTT a une politique de classification des informations qui décrit les contrôles techniques et organisationnels appropriés pour traiter les informations en fonction de leur classification. Les informations et les actifs sont protégés conformément à l'étiquette de classification.

14 Contrôles des accès

14.1 NTT a une politique de contrôle d'accès, des procédures de soutien et des mesures d'accès logiques et physiques, pour garantir que seules les personnes autorisées ont accès aux informations sur la base des principes du moindre privilège.

14.2 Des revues d'accès sont effectuées périodiquement sur les actifs informatiques, les applications, les systèmes et les bases de données pour s'assurer que seules les personnes autorisées y ont accès.

14.3 Les sous-traitants de NTT doivent accéder aux systèmes NTT en utilisant des comptes nommés. Les comptes génériques et / ou le partage d'informations d'identification sont interdits, sauf exception expressément autorisée par la direction ou les clients.

14.4 NTT a déployé des efforts raisonnables pour limiter strictement le nombre d'utilisateurs privilégiés («Admin») sur ses applications, systèmes et bases de données.

15 Sécurité physique et environnementale

15.1 NTT a mis en œuvre des mesures raisonnables et appropriées conformément à la politique de sécurité physique pour empêcher l'accès physique non autorisé, les dommages ou les interférences avec les informations, applications, systèmes, bases de données et infrastructures NTT dans les domaines suivants:

(a) Contrôles des accès physiques;

(b) Surveillance et audit des accès physiques;

(c) Protection contre les risques environnementaux;

(d) Sécurisation des actifs physiques;

(e) Sécurité du câblage;

(f) Gestion des actifs physiques et informationnels;

(g) Entretien et élimination des actifs physiques;

(h) Des pratiques de bureau et d'écran claires;

(i) Accès et supervision des visiteurs; et

(j) Procédures de santé et de sécurité.

16 Sécurité opérationnelle

16.1 La fonction de NTT Information and Technology («I&T») est responsable de la gestion des applications, systèmes, bases de données et infrastructures de NTT. I&T documente, maintient et met en œuvre toutes les politiques et procédures opérationnelles informatiques qui sont alignées sur les normes COBIT et ITIL.

16.2 NTT a une politique et des procédures de support pour gérer les changements de nos processus d'affaires, applications, systèmes, bases de données et infrastructure. NTT a établi plusieurs structures de gouvernance pour examiner et approuver tout changement en fonction de la taille et de la portée du changement et des objectifs stratégiques. Toutes les demandes et leurs résultats sont enregistrés et documentés.

16.3 NTT a mis en place un programme de gestion des menaces et des vulnérabilités soutenu par des outils standard de l'industrie pour identifier, gérer et atténuer les risques pour les informations de l'entreprise, y compris les données à caractère personnel des collaborateurs et des clients Cela inclut la détection et la réponse des points finaux de nouvelle génération («EDR») pour les outils antivirus et anti-malware, l'analyse régulière des environnements, les protocoles de correction et la gestion des activités de correction et d'amélioration.

16.4 Les besoins en capacité sont surveillés en permanence et régulièrement revus. Les systèmes et les réseaux seront gérés et mis à l'échelle conformément à ces examens.

16.5 La disponibilité du système comprend l'architecture, la conception à haute disponibilité et / ou les sauvegardes en fonction des exigences de risque et de disponibilité de chaque système. Le procédé pour maintenir la disponibilité ou la restauration du système, y compris la portée et la fréquence des sauvegardes, est déterminé sur la base des exigences commerciales de NTT, y compris les exigences du client, et la criticité des informations. La surveillance des sauvegardes est effectuée pour garantir la réussite des sauvegardes, ainsi que pour gérer les problèmes, exceptions ou échecs de sauvegarde.

16.6 NTT déploie des efforts raisonnables pour maintenir la journalisation d'audit des applications et les systèmes. Ces journaux sont revus périodiquement et sont disponibles à des fins d'enquête. L'accès aux journaux est strictement limité au personnel autorisé uniquement.

17 Acquisition, développement et maintenance du système

17.1 NTT dispose d'une Architecture Securité et d'une Politique de Conception et des normes et procédures de soutien pour garantir que les principes de sécurité dès la conception sont appliqués dans le cycle de vie du développement logiciel.

17.2 NTT n'autorise pas l'utilisation de la production, du client, des données à caractère personnel ou de toute information confidentielle à des fins de test. Dans des cas exceptionnels, les données de production ou de client peuvent être utilisées avec l'accord du client ou du responsable concerné.

18 Gestion des tiers

18.1 NTT a une politique de sécurité de tiers et des procédures de soutien pour garantir que les actifs d'information sont protégés lorsque NTT engage des fournisseurs de services et / ou des sous-traitants tiers. Cela comprend des exigences de diligence raisonnable en matière de sécurité de l'information et des évaluations des risques de sécurité de l'information à réaliser, afin de garantir:

(a) Les exigences en matière de sécurité de l'information sont clairement énoncées et documentées dans les accords avec les sous-traitants de NTT;

(b) Les sous-traitants de NTT implémentent le même niveau de protection et de contrôle que NTT;

(c) Les sous-traitants sont tenus de signaler tout incident de sécurité des informations suspecté ou réel à NTT en temps opportun.

18.2 NTT a déployé des efforts raisonnables pour s'assurer que des accords appropriés sont en place avec les sous-traitants qui ont accès aux informations, applications, systèmes, bases de données et infrastructures NTT. Ces accords incluent les normes de sécurité des informations NTT pour garantir la confidentialité, l'intégrité et la disponibilité des informations NTT.

19 Gestion des incidents de sécurité de l'information

19.1 NTT dispose de politiques, processus et procédures pour identifier, détecter, répondre, récupérer et notifier les parties prenantes appropriées en cas d'incident de sécurité des informations, y compris les violations de données à caractère personnel. Cela comprend des mécanismes pour effectuer une analyse des causes et entreprendre des actions correctives.

19.2 NTT a mis en place des opérations de sécurité à l'échelle du groupe pour surveiller et gérer de manière proactive tous les actifs réseau et informatiques. Ceci est soutenu par des outils techniques pour la réponse aux incidents de sécurité de l'information et la récupération des données.

20 Continuité d'activité

20.1 NTT a établi des plans de continuité des activités. NTT a adopté une approche par couches pour garantir la disponibilité de nos systèmes et données.

21 Conformité

21.1 NTT a établi des rôles et des responsabilités pour identifier les lois et réglementations qui affectent les opérations commerciales de NTT. La responsabilité du respect des lois et réglementations est établie au niveau du groupe et régional pour garantir que NTT répond aux exigences mondiales et locales.

Pour toute question, veuillez contacter le Bureau de la protection de la vie privée à **privacyoffice@global.ntt**

Together we do great things