Annexe de Protection des Données ("Annexe")

1 La présente Annexe de Protection des Données s'applique en lien avec le Page de Couverture (y compris les Conditions Générales des voyages d'affaires et/ou les Conditions Générales des services de réunions et d'évènements) (collectivement, le "Contrat") entre Reed & Mackay France SAS ("**R&M**") (numéro d'identification unique 435 134 168) dont le siège social est situé au 15 Rue Traversière, 75012 Paris, et vous, le Client. Les termes définis utilisés ailleurs dans le Contrat ont la même signification dans la présente Annexe. Lorsque R&M traite les Données Personnelles en tant que sous-traitant pour le compte du Client, R&M s'engage à :

1.1 N'utiliser les Données que pour :

(a) S'acquitter des obligations qui lui incombent en vertu du présent Contrat et traiter ces Données conformément aux instructions écrites du Client ; et/ou

(b) Se conformer à la législation sur la protection des Données ou aux lois de tout autre État membre de l'Union européenne (à condition que R&M ait, avant le traitement concerné, informé le Client de cela, à moins que la loi concernée n'interdise une telle notification) ;

1.2 Sous réserve des paragraphes 2, 4 et 5 (inclus) de la présente Annexe, mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées pour protéger les Données traitées dans le cadre du présent Contrat contre la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés, de manière accidentelle ou illicite, et prendre toutes les mesures qu'elle exige en vertu de l'article 32 du RGPD ("sécurité du traitement") ;

1.3 Prendre toutes les mesures raisonnables pour garantir la fiabilité des employés de R&M qui ont accès aux Données et s'assurer que tous ces employés de R&M sont liés par des obligations de confidentialité exécutoires ;

1.4 Compte tenu de la nature du traitement, aider le Client par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, à s'acquitter de son obligation de répondre aux demandes des personnes concernées exerçant leurs droits en vertu du chapitre III du RGPD ;

1.5 Aider le Client à se conformer aux obligations qui lui incombent en vertu des articles 32 à 36 du RGPD ("sécurité du traitement", "notification d'une violation de données personnel ...", "analyse d'impact relative à la protection des données" et "consultation préalable"), en tenant compte de la nature du traitement et des informations dont dispose R&M ;

1.6 Notifier au Client dans les meilleurs délais, et en tout état de cause dans les 48 heures, toute violation de la sécurité entraînant accidentellement ou illégalement la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès aux Données ;

1.7 Mettre à la disposition du Client, dans un délai raisonnable suivant l'avis du Client, toutes les informations nécessaires pour démontrer la conformité avec les obligations énoncées dans la présente Annexe et permettre et contribuer aux audits, y compris les tests de sécurité ou les inspections, menés par le Client ou un autre auditeur mandaté par le Client, à condition que ces audits, tests de sécurité et/ou inspections n'aient lieu qu'une (1) fois par période de douze (12) mois, que ces inspections, tests de sécurité et/ou audits soient strictement limités aux dispositions prises par R&M pour se conformer à la présente Annexe, que ces inspections, tests de sécurité et/ou audits soient effectués pendant les heures normales de bureau, que le Client (ou le tiers concerné effectuant un tel audit, test de sécurité et/ou inspection) donne à R&M un préavis raisonnable par écrit d'un tel audit, test de sécurité et/ou inspection et que la portée d'un tel audit, test de sécurité et/ou inspection soit convenue avec R&M avant qu'il ne commence ;

1.8 Autoriser à transférer des Données en dehors de l'Espace économique européen, à condition que des garanties appropriées soient mises en place en vertu de la législation sur la protection des données, y compris, mais sans s'y limiter, le cas échéant: (a) pour les transferts de Données depuis l'Espace économique européen, les Clauses contractuelles types de l'UE sont en place; (b) pour les transferts de Données depuis le Royaume-Uni, l'Addendum Royaume-Uni est en place, à condition que cela reste un mécanisme de transfert valide en vertu du RGPD Royaume-Uni; (c) toute autre clause standard ou addendum pour le transfert de Données en dehors du Royaume-Uni, valable en vertu du RGPD Royaume-Uni, est en place; ou (d) tout autre mécanisme de transfert valable est en place en vertu de la législation sur la protection des données. Pour éviter toute ambiguïté et sous réserve du paragraphe 4 ci-dessous, le Client reconnaît et accepte que R&M n'est pas tenu de conclure des clauses contractuelles types (y compris, sans s'y limiter, les Clauses contractuelles types de l'UE ou l'Addendum du Royaume-Uni) ou d'autres accords avec les Prestataires de Services ;

1.9 Informer immédiatement le Client si, de l'avis de R&M, toute instruction ou directive du Client enfreint la législation sur la protection des données ou toute autre loi applicable en France, dans l'Union européenne ou dans un État membre en matière de protection des données ; et

1.10 Au choix du Client, supprimer ou restituer au Client toutes les Données lorsque les services cessent d'être fournis au Client, et supprimer toutes les copies existantes (sauf si R&M est tenu de les conserver en vertu de la loi applicable).

2 Le Client reconnaît et accepte, et doit s'assurer que les Voyageurs et les Utilisateurs reconnaissent et acceptent, qu'il est nécessaire pour le R&M de fournir des Données aux Prestataire de Services (qu'ils soient ou non dans l'Espace économique européen) afin de fournir ses Services.

Copyright Reed & Mackay 2025 (V082025)

3 Le Client reconnaît et accepte que R&M soit autorisé à utiliser des Sous-Traitants Ultérieurs en relation avec le traitement des Données au nom du Client pour la fourniture des Services dans le cadre de ce Contrat. Une liste des Sous-Traitants Ultérieurs utilisés par le R&M est disponible ici. R&M informera le Client de toute modification apportée à la liste des Sous-Traitants Ultérieurs, y compris l'ajout de tout nouveau Sous-Traitant Ultérieurs. Si le Client s'oppose à une modification de la liste des Sous-Traitants Ultérieurs, il doit le notifier par écrit à R&M dans les 15 jours suivant la publication de la liste mise à jour des Sous-Traitants Ultérieurs. Si le Client fournit à R&M une telle notification, R&M exécutera, dans la mesure du possible, ses obligations en vertu du présent Contrat sans que les nouveaux Sous-Traitants Ultérieurs ne traitent les Données. Toutefois, s'il n'est pas raisonnablement possible pour le R&M d'exécuter ses obligations en vertu du présent Contrat sans que les nouveaux Sous-Traitants Ultérieurs ne traitent des Données dans le cadre du présent Contrat, R&M en informera le Client, et le Client aura le droit de résilier le présent Contrat moyennant un préavis écrit de trente (30) jours adressé à R&M. Si le Client ne s'oppose pas à une modification ou à un ajout à la liste des Sous-Traitants Ultérieurs dans n les 15 jours suivant la publication de la liste mise à jour par le R&M, le Client sera réputé avoir approuvé les modifications et/ou les ajouts à la liste des Sous-Traitants Ultérieurs. R&M demeure responsable de tout acte ou omission de ses Sous-Traitants Ultérieurs. R&M s'assurera d'avoir un contrat écrit avec les Sous-Traitants Ultérieurs qui contient des conditions pour la protection des Données qui ne sont pas moins protectrices que les conditions énoncées dans la présente Annexe.

4 Sans préjudice du paragraphe 2 ci-dessus, et nonobstant toute autre disposition du présent Contrat, le Client :

(a) Consent par la présente à ce que R&M transfère les Données à tout Prestataire de Services (qu'il soit ou non situé dans l'Espace économique européen ou au Royaume-Uni) dans le but de fournir les services conformément au présent Contrat ; et

(b) S'assure que les Voyageurs et les Utilisateurs ont, le cas échéant, tous donné leur accord pour que R&M transfère les Données des Voyageurs et des Utilisateurs aux Prestataires de Services dans le but de fournir les Services conformément au présent Contrat.

5 A la lumière du paragraphe 2 ci-dessus, R&M fera tout son possible pour aider le Client à répondre à tout manquement (qu'il s'agisse d'un acte ou d'une omission) de la part d'un Prestataire de Services à traiter les Données conformément aux méthodes appropriées et standard de l'industrie, mais R&M n'aura aucune responsabilité envers le Client, tout membre du Groupe du Client ou tout Voyageur ou Utilisateur (que ce soit de manière contractuelle, délictuelle (y compris la négligence ou le manquement à une obligation légale), la fausse déclaration ou autre). R&M n'aura par ailleurs aucune responsabilité envers le Client, tout membre du Groupe du Client ou tout Voyageur ou Utilisateur (que ce soit dans le cadre d'un contrat, d'un délit (y compris la négligence ou le manquement à une obligation légale), d'une fausse déclaration ou autre) découlant de ou en rapport avec le traitement, l'utilisation, l'abus, la perte, l'endommagement ou la corruption des Données par un Prestataire de Service, ou toute autre violation des droits d'une personne en rapport avec les Données.

6 Sans préjudice des paragraphes 2, 4 et 5 ci-dessus (y compris) de la présente Annexe, le Client s'assure que toutes les bases juridiques nécessaires sont en place, y compris, le cas échéant, le consentement, et doit fournir et aux Voyageurs et aux Utilisateurs toutes les informations nécessaires pour que les Données puissent être légalement fournies aux conformément à la législation sur la protection des données.

7 Le Client reconnaît et accepte que l'Appendice 1 contient certains détails relatifs au traitement des Données.

8 Le Client reconnaît et accepte de prendre en charge et de rembourser les frais et dépenses raisonnables encourus par le Service de médiation pour fournir l'assistance décrite aux paragraphes 1.4 et 1.5 ci-dessus.

9 Si cela est nécessaire pour se conformer à la Législation sur la protection des données et à moins que la loi applicable ne l'interdise, R&M doit : (i) informer le Client sans délai excessif de toute demande, ordonnance ou demande similaire émanant d'un tribunal, d'une autorité compétente, d'un organisme d'application de la loi ou d'un autre organisme gouvernemental (" Demande d'application de la loi ") concernant le traitement des Données dans le cadre du présent Contrat et donner au Client la possibilité de s'opposer à une telle Demande d'application de la loi ; et (ii) prendre toutes les mesures raisonnables pour empêcher la divulgation de toute Donnée traitée par le R&M dans le cadre du présent Contrat en réponse à une demande d'application de la loi sans le consentement écrit préalable exprès du Client.

Copyright Reed & Mackay 2025 (V082025)

Appendice 1

Activités de traitement des données

Catégories de Données	Coordonnées du voyageur et/ou du réservataire - titre, prénom, second prénom, nom de famille, nom connu (si différent), sexe, date, lieu et pays de naissance, pays de résidence, nationalité, état civil ; lieu où se trouve le voyageur - destinations et lieux du voyage. Informations sur l'entreprise - nom de l'entreprise, département, centre de coûts, numéro de compte, titre du poste, numéro d'employé Principales coordonnées - adresses (domicile, bureaux, etc.), numéros de téléphone, numéros de télécopie, numéros de téléphone portable, adresse électronique Informations sur le réserviste de voyage / l'assistant personnel - nom, numéro de téléphone, adresse électronique Méthodes de paiement - type de carte, numéro de carte, date d'expiration, préférences d'utilisation, débit/crédit, personnel/professionnel Documents Passeport - pays du passeport, pays de délivrance, numéro du passeport, prénom, second prénom, nom de famille, date de délivrance, date d'expiration, données biométriques (O/N) Visa (y compris ESTA, Redress, Schengen, permis de travail, Global Entry) - pays du visa, pays de délivrance, type de visa, numéro du document, date de délivrance et date d'expiration. TSA - Numéro TSA, date de début, date d'expiration Permis de conduire - pays, numéro de permis, prénom, deuxième prénom, nom, date de début, date d'expiration, provisoire (O/N), international (O/N) Cartes d'identité - pays, numéro de la carte d'identité, prénom, second prénom, nom de famille, date de début, date d'expiration Vaccins, Covid et informations sanitaires requises pour les réservations Préférences en matière de voyage Avion - type de siège, aéroport d'origine, préférence d'enregistrement en ligne, type de repas Voiture - catégorie, style, transmission, carburant/climatisation, besoin de GPS (O/N), Rail (y compris Eurostar) - attribution des sièges, type de repas Hôtel - fumeur/non-fumeur, type de chambre préféré Exigences éventuelles en matière d'accessibilité pour le voyage Adhésions - cartes de fidélité - type de service, fournisseur, numéro d'adhésion, date d'expiration, statut, niveau Hobbies/intérêts personnels
Catégories de personnes concernées	Employés et invités du Client, et autres personnes pour lesquelles le Client demande de voyager
Opérations de traitement	Fourniture de services de voyage et de services connexes
Objectifs	Fourniture de services de voyage et de services connexes
Durée	Finances - durée du Contrat + 10 ans Profils - durée du Contrat, révision annuelle et suppression à la demande du Client

Copyright Reed & Mackay 2025 (V082025)

Appendice 2

Mesures techniques et organisationnelles, y compris les mesures techniques et

Organisationnelles visant à garantir la sécurité des données

Version 2.5 - juillet 2024 (telle qu'elle peut être mise à jour par R&M de temps à autre)

DÉFINITION

Le terme "personnel" désigne les employés, les sous-traitants ou les consultants de R&M qui participent au service fourni par R&M à ses clients.

INTRODUCTION

L'équipe de direction de R&M reconnaît que l'importance de la sécurité de l'information, et le maintien des normes les plus élevées de confidentialité, d'intégrité et de disponibilité des informations internes, des clients et des fournisseurs, est fondamental pour notre vision : "Être l'entreprise de voyages, de conseils et d'événements la plus appréciée, la plus recommandée et la plus entreprenante au monde".

Comme décrit dans le présent document, R&M maintient un ensemble de mesures de sécurité techniques et organisationnelles conformes aux meilleures pratiques, certifications et normes de l'industrie. Tout cela est maintenu part R&M pour atténuer les risques pour les données, les actifs d'information, le service, la performance, la confiance des clients ou d'autres domaines de l'entreprise qui peuvent résulter d'une défaillance dans la sécurité de l'information..

1. CERTIFICATIONS

1.1. Notre siège social est certifié ISO/IEC 27001, la norme internationale pour la gestion de la sécurité de l'information, ISO 22301 - Gestion de la continuité des activités, ISO 9001 - Gestion de la qualité, et ISO 14001 - Certification de la gestion de l'environnement. R&M est également certifié PCI-DSS - The Payment Card Industry - Data Security Standard (norme de sécurité des données de l'industrie des cartes de paiement), qui est également une condition préalable à l'obtention d'une licence IATA, et qui est donc prise très au sérieux par R&M.

1.2. Les certifications sont maintenues grâce à un programme d'audit externe et interne, qui comprend des audits internes périodiques et des audits externes annuels, ainsi que des activités d'amélioration continue.

2. SYSTÈME DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

2.1. Les politiques de sécurité de l'information de R&M définissent une orientation claire pour la sécurité de l'information et démontrent le soutien et l'engagement à la gestion de la sécurité de l'information dans l'ensemble de l'entreprise.

2.2. La sécurité de l'information est gérée par un ensemble de contrôles rigoureux, comprenant des politiques, des processus, des procédures, des logiciels et des fonctions matérielles qui constituent le système de gestion de la sécurité de l'information (SGSI) de R&M. Ces contrôles sont surveillés, révisés et, le cas échéant, améliorés afin de garantir que les objectifs spécifiques de sécurité et d'activité sont atteints.

2.3. Tous les membres du personnel bénéficient d'un programme complet et obligatoire d'initiation et de formation lors dès leur entrée dans l'entreprise, ainsi que d'une remise à niveau annuelle en matière de conformité, notamment en ce qui concerne la sécurité de l'information et la protection des Données.

2.4. La responsabilité ultime de la sécurité de l'information incombe au directeur de l'information, mais cette responsabilité est assumée par le directeur de la sécurité et conformité, qui est le principal responsable de la sécurité de l'information, des risques liés à la sécurité de l'information, de la cybersécurité et de la gestion des incidents de sécurité au sein de R&M et qui constitue le point de contact central pour la sécurité de l'information, tant pour le personnel que pour les organisations externes.

2.5. Les chefs de service sont responsables de l'application des politiques de sécurité de l'information dans leur domaine d'activité et du respect de ces politiques par leur personnel. Tous les membres du personnel sont responsables de la sécurité de l'information ; ils doivent s'assurer qu'ils respectent les politiques, les processus et les procédures de l'entreprise, qu'ils sont conscients de l'importance de la sécurité de l'information et des risques, et qu'ils signalent tout incident, tout événement ou toute faiblesse potentielle.

3. SÉCURITÉ DES RESSOURCES HUMAINES

3.1. R&M travaille en étroite collaboration avec ses agences de recrutement pour s'assurer que les vérifications préalables à l'embauche sont effectuées en son nom.

3.2. R&M fait appel à une société tierce de contrôle des employés pour effectuer un contrôle des antécédents pour tous les membres du personnel, quel que soit leur rôle, sous réserve des limitations prévues par la législation locale.

3.3. Les contrats du personnel contiennent des clauses de confidentialité qui assurent une protection adéquate de la confidentialité des Données.

3.4. Une procédure disciplinaire est en place pour traiter les cas de non-respect des politiques et des exigences en matière de sécurité.

3.5. En cas de cessation d'emploi, l'accès est retiré au personnel le dernier jour de travail et l'ensemble du matériel et de la propriété intellectuelle est restitué par le démissionnaire.

4. GESTION DES ACTIFS ET SÉCURITÉ DES DONNÉES

4.1. Les actifs associés à l'information et aux installations de traitement de l'information sont identifiés et un inventaire des actifs est tenu à jour.

4.2. Les informations et les données sont classées et gérées conformément à une politique de classification des informations, de gestion des actifs et des données approuvées par la direction.

Copyright Reed & Mackay 2025 (V082025)

4.3. Seuls les appareils de confiance ont accès aux ressources du réseau d'entreprise de R&M. Il s'agit notamment d'ordinateurs et d'appareils mobiles rattachés au domaine de R&M qui ont été enregistrés avec la solution de gestion des appareils mobiles de R&M et qui sont conformes aux politiques de sécurité.
4.4. Les exigences en matière de contrôles de sécurité pour les appareils mobiles personnels et ceux fournis par R&M sont définies dans la politique relative aux appareils mobiles et personnels. Ces contrôles comprennent, entre autres, le cryptage, l'effacement à distance et la désactivation des ports USB.
4.5. Tous les points d'extrémité sont cryptés. Les ports USB et l'utilisation de supports amovibles sont limités.
4.6. Des mesures techniques DLP (Data Loss Prevention) ainsi qu'une politique Clear Desk & Clear Screen sont en place pour atténuer le risque de fuite de données et de divulgation involontaire des Données.
4.7. Une politique de conservation des données et un calendrier de conservation des données sont en place pour définir les exigences de conservation des données conformément au RGPD, ainsi que les exigences d'élimination sécurisée des données sensibles sur des supports physiques ou électroniques conformément aux normes de sécurité / meilleures pratiques reconnues de l'industrie informatique .
4.8. Les supports contenant des informations sont détruits par des moyens sûrs, conformément aux normes de destruction des données approuvées par la filière de gestion des déchets d'équipements électriques et électroniques (DEEE) et le CESG (Communications Electronics Security Group). Le département des services techniques tient des registres.
4.9. La documentation est détruite en toute sécurité, soit en utilisant des déchiqueteuses à coupe transversale, soit en faisant appel à des tiers agréés qui fournissent des services conformes à la norme de déchiquetage de sécurité BS EN 15713 et au moins au niveau de sécurité DIN P-3, adapté aux documents confidentiels.

5. CONTRÔLE D'ACCÈS

5.1. Un modèle de contrôle d'accès basé sur les rôles est en place, avec des rôles attribués aux individus en fonction de leur fonction et du besoin de savoir.
5.2. Les principes de séparation des tâches et de moindre privilège sont respectés, et l'accès privilégié est accordé sur approbation documentée de la direction générale.
5.3. Les droits d'administration informatique privilégiés sont accordés par le biais d'un identifiant d'utilisateur distinct (compte élevé) de l'identifiant d'utilisateur normal de l'utilisateur.
5.4. Nous surveillons tous les événements associés à la connexion aux serveurs et aux postes de travail avec des comptes administratifs, ainsi que les changements/modifications des groupes de privilèges.
5.5. Les examens des droits d'accès sont effectués périodiquement, la fréquence dépendant de la criticité de l'actif informationnel et variant d'un trimestre à un an.
5.6. La politique de R&M en matière de mots de passe est définie comme suit : Les mots de passe doivent contenir un minimum de 12 caractères, au moins une lettre majuscule, une lettre minuscule et un chiffre ou un caractère spécial. Les mots de passe doivent éviter les caractères internationaux (non ASCII), ne doivent pas inclure de mots du dictionnaire ni d'informations sur l'utilisateur (telles que l'identifiant, les noms des membres de la famille, la date de naissance, etc.), doivent être changés au moins une fois tous les 90 jours et ne peuvent pas être identiques aux 24 mots de passe utilisés précédemment.
5.7. Les comptes d'utilisateurs sont verrouillés après cinq tentatives de connexion non valides et le restent jusqu'à ce qu'un administrateur ou l'utilisateur les déverrouille (dans ce dernier cas, il s'agit d'un libre-service et d'une authentification multifactorielle).
5.8. L'authentification multifactorielle est appliquée à tous les comptes utilisateurs et administratifs de R&M.

6. CRYPTOGRAPHIE

6.1. Comme le définit la politique de R&M en matière de cryptographie, des contrôles cryptographiques sont utilisés pour protéger les Données sensibles en transit et au repos.
6.2. Le chiffrement des appareils mobiles est appliqué via les stratégies de Microsoft Intune Endpoint Manager.
6.3. Le cryptage de la base de données PII est assuré par Thales CipherTrust (cryptage AES 256 bits, tokenisation des données et services de cryptage).
6.4. Le cryptage de la base de données est en place en utilisant le cryptage transparent des données (TDE) AES-256.
6.5. Tout le trafic en provenance ou à destination de nos applications publiques (sites web + application mobile) utilise des certificats HTTPS émis par l'autorité de certification GlobalSign et est crypté avec TLS 1.2 ou une version plus récente.
6.6. Toutes les sauvegardes sont cryptées.

7. SÉCURITÉ DES OPÉRATIONS

7.1. Les modifications apportées aux environnements de production sont contrôlées conformément à la politique de gestion des changements informatiques de R&M.
7.2. Des contrôles de détection, de prévention et de récupération des logiciels malveillants sont en place grâce à une solution anti-programmes malveillants de nouvelle génération.
7.3. Un processus complet de gestion des correctifs est en place. Les correctifs et les mises à jour de sécurité sont déployés tous les mois, ou plus fréquemment si un risque de sécurité important est identifié. La gestion des correctifs est soumise au contrôle des changements et à la politique de gestion des changements informatiques.
7.4. Un programme de gestion des vulnérabilités techniques est en place et comprend un programme permanent de remédiation. Les vulnérabilités sont identifiées par des analyses internes et externes de l'infrastructure, des analyses trimestrielles PCI-DSS ASV et des tests de pénétration.
7.5. Un programme annuel complet de tests de pénétration est en place, réalisé par des testeurs de pénétration indépendants accrédités par le CREST. Ce programme couvre toutes les infrastructures critiques de R&M.

8. JOURNALISATION, SURVEILLANCE ET GESTION DES INCIDENTS DE SÉCURITÉ

8.1. Des journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les défaillances et les événements liés à la sécurité de l'information sont générés, conservés, protégés contre la falsification et régulièrement examinés.
8.2. Un centre d'opérations de sécurité (SOC) est en place 24 heures sur 24 et 7 jours sur 7 par l'intermédiaire d'un fournisseur de services de sécurité gérés tiers de confiance. Ce service comprend la surveillance, la collecte et l'analyse de journaux, la gestion des informations et des événements de sécurité (SIEM), la réponse aux incidents de sécurité et l'atténuation de leurs effets,

Copyright Reed & Mackay 2025 (V082025)

ainsi que des capacités d'analyse médico-légale permettant de comprendre la cause des incidents de sécurité et les méthodes de réduction ou d'élimination des zones d'attaque potentielles.

8.3. Les incidents de sécurité observés ou suspectés sont signalés au niveau central, enregistrés automatiquement et suivis par l'équipe de réponse aux incidents de sécurité conformément au plan de réponse aux incidents de sécurité de l'information et au processus de gestion des violations de données, le cas échéant.

9. SÉCURITÉ CLOUD

9.1. La plateforme de gestion des voyages et l'infrastructure de serveurs de R&M sont hébergées dans le centre de données Microsoft Azure au Royaume-Uni.

9.2. Microsoft Azure est configuré pour chiffrer les informations au repos quel que soit le support de stockage, qu'il s'agisse d'un disque géré attaché à une machine virtuelle, d'un compte de stockage contenant des données de télémétrie ou le code source d'une application, ou d'un service de base de données de plateforme comme Microsoft SQL.

9.3. Une politique de sécurité de l'informatique en nuage approuvée par la direction est en place pour définir les exigences en matière de sécurité de l'informatique via le Cloud.

9.4. Une solution de gestion de la sécurité dans le Cloud est en place pour surveiller et gérer la gouvernance des actifs et des services de R&M basés sur Microsoft Azure, y compris la visualisation et l'évaluation de la posture de sécurité, la détection des erreurs de configuration et l'application des meilleures pratiques de sécurité et des cadres de conformité.

9.5. Les groupes de sécurité réseau de Microsoft et les pares-feux virtuels de nouvelle génération de Checkpoint protègent notre environnement sur le périmètre avec la prévention des intrusions activée.

10. LA SÉCURITÉ PHYSIQUE

10.1. Conformément à notre politique de sécurité physique et environnementale, des mesures de sécurité physique et environnementale adéquates sont en place pour empêcher tout accès physique non autorisé, tout dommage et toute interférence avec les données, les locaux et les installations de traitement de R&M. Les contrôles suivants sont en place :

10.1.1. Siège social : La réception de l'immeuble est surveillée 24 heures sur 24 et 7 jours sur 7. La réception du bureau de R&M fonctionne pendant les heures de bureau. La vidéosurveillance à tous les points d'accès du bâtiment couvre la plupart des zones communes et les zones d'entrée et de sortie du bâtiment. L'accès à la salle des communications informatiques se fait par un système de cartes magnétiques et un système d'entrée par clavier. L'accès est limité aux personnes autorisées ayant un besoin professionnel.

10.1.2. Bureaux régionaux : Les bureaux régionaux sont soumis aux mêmes contrôles que le siège, à quelques exceptions près. Nos plus petits bureaux ne disposent pas d'une réception surveillée 24 heures sur 24, 7 jours sur 7, ni d'un système de cartes d'accès. Toutefois, des contrôles compensatoires sont mis en place conformément à notre politique de sécurité physique et environnementale afin de garantir que la sécurité physique de ces bureaux est adéquate.

10.2. Les visiteurs n'ont accès qu'à des fins spécifiques et autorisées et sont toujours supervisés/accompagnés lorsqu'ils se trouvent dans les bureaux de R&M. Des registres des visiteurs sont tenus pour tous les accès physiques aux bureaux de R&M, aux salles de serveurs et aux centres de données hébergeant les équipements informatiques et les actifs informationnels de R&M.

11. SÉCURITÉ DES COMMUNICATIONS ET DES RÉSEAUX

11.1. Les réseaux sont gérés au moyen de contrôles de sécurité appropriés tels que la segmentation du réseau, la gestion de l'accès au réseau, les pare-feu, les normes de configuration, l'enregistrement et la surveillance.

11.2. Des procédures de transfert d'informations et des contrôles sont en place pour protéger le transfert de données par le biais de tous les types de moyens de communication.

11.3. Le protocole de transfert de données que nous recommandons pour les échanges réguliers de données (par exemple, les fichiers de données, les flux de ressources humaines) consiste à établir une connexion SFTP entre les organisations - la partie qui pousse/tire les données peuvent faire l'objet d'un accord entre les parties.

12. DÉVELOPPEMENT DE LOGICIELS

12.1. Le développement de logiciels en interne suit la méthodologie du cycle de vie Agile/Sprint et respecte les meilleures pratiques de l'OWASP (Open Web Application Security Project).

12.2. Une politique de cycle de développement des logiciels (SDLC) est en place, comprenant l'analyse des besoins et les spécifications, la sécurité dès la conception, les principes d'ingénierie sécurisée, l'environnement de développement sécurisé, le soutien aux applications, l'assurance qualité, les essais, la mise en œuvre, la formation et l'examen après la mise en œuvre.

12.3. L'intégration de l'authentification unique est disponible dans nos applications destinées aux clients. Les solutions basées sur SAML 2.0, telles qu'Azure AD, Ping Identity, Duo et Okta sont prises en charge. D'autres options tierces peuvent également être prises en charge, mais peuvent nécessiter un développement et des tests.

12.4. Les systèmes de développement, de test et de production sont séparés. Les données anonymisées sont utilisées à des fins de test dans des environnements de non-production.

12.5. Les données des clients sont séparées à l'aide d'identifiants uniques attribués au moment de la mise en place du compte. La séparation est assurée par l'utilisation d'identifiants uniques, tels que les numéros d'identification de l'entreprise, les numéros d'identification du voyageur et les numéros d'identification du compte.

13. RELATIONS AVEC LES FOURNISSEURS

13.1. Les nouveaux fournisseurs directs (y compris les sous-traitants de données) font l'objet d'un contrôle préalable portant sur la sécurité de l'information, la protection des données, la continuité des activités, la gouvernance d'entreprise et la qualité, la santé et la sécurité, l'environnement, l'égalité des chances, la diversité, la lutte contre la corruption, l'esclavage moderne et le travail des enfants, les pratiques commerciales éthiques et la responsabilité sociale des entreprises, ainsi que d'une vérification de solvabilité, d'un examen des politiques, des certifications, des rapports d'audit indépendants, des tests de pénétration indépendants (y compris le suivi des mesures correctives), etc. selon le cas.

13.2. Les fournisseurs sont soumis à des clauses de confidentialité et de droit à l'audit dans leurs contrats.

Copyright Reed & Mackay 2025 (V082025)

13.3. Les fournisseurs sont tenus de se conformer aux principes de fonctionnement des fournisseurs de R&M et les fournisseurs de produits/services qui interagissent avec les systèmes d'information de R&M ou qui traitent des Données sont contractuellement tenus d'accepter nos exigences en matière de sécurité de l'information des fournisseurs.
13.4. Les fournisseurs font l'objet d'un examen périodique. La nature, l'étendue et la fréquence de cet examen dépendent de plusieurs facteurs, dont le produit/service fourni et la criticité du fournisseur.
13.5. Les capacités de résilience et de reprise des fournisseurs critiques sont officiellement examinées chaque année dans le cadre du bilan d'"impact sur les activités (BIA) de nos capacités de rétablissement de la continuité des activités.

14. CONTINUITÉ DES ACTIVITÉS ET REPRISE APRÈS SINISTRE

14.1. Conformément à la certification ISO 22301 de notre siège social, les plans de continuité des activités, y compris le plan de gestion de crise de R&M, sont officiellement révisés chaque année, ou plus fréquemment si nécessaire (par exemple, en cas de changement important).
14.2. Un programme continu d'exercices et de tests de continuité des activités est en place. Il consiste en des exercices de scénarios sur table et des tests de sites de récupération physique.
14.3. Une analyse annuelle de l'impact sur l'entreprise est réalisée afin de définir le degré d'interruption que l'entreprise peut tolérer dans ses activités clés, le niveau minimum de ces activités requis pour fonctionner, ainsi que les ressources et les dépendances nécessaires à la reprise des activités.
14.4. L'outil propriétaire de R&M de gestion des voyages est hébergé dans Microsoft Azure, qui offre des niveaux élevés de redondance et de résilience.
14.5. Un service de sauvegarde en ligne tiers pour garantir que les informations critiques contenues dans les machines virtuelles et les comptes de stockage sont stockées en toute sécurité et indépendamment de l'environnement Azure et qu'elles peuvent être restaurées en cas de perte ou d'altération accidentelle.
14.6. Notre base de données propriétaire, qui comprend toutes les données relatives à la comptabilité, aux clients et aux rapports, fait l'objet de sauvegardes incrémentielles tout au long de l'année et d'une sauvegarde quotidienne complète. L'objectif de point de récupération (RPO) est d'une heure et l'objectif de temps de récupération (RTO) est de trois heures. Les serveurs sont sauvegardés quotidiennement sur une base "incrémentale pour toujours". Le RPO est de 1 jour et le RTO de 4 heures. Notre RTO global est de 4 heures.
14.7. Les sauvegardes sont cryptées et testées périodiquement.

15. RISQUES LIÉS À LA SÉCURITÉ DE L'INFORMATION

15.1. Le système de gestion de R&M et les processus qui le sous-tendent intègrent une réflexion et une prise de conscience fondées sur les risques.
15.2. Le programme de gestion des risques liés à la sécurité de l'information fait partie du cadre de gestion des risques de l'entreprise et couvre l'identification et l'évaluation des risques liés à la sécurité de l'information découlant à la fois de diverses activités périodiques et de changements planifiés et non planifiés. Les risques identifiés sont classés par ordre de priorité, traités/acceptés et approuvés en temps utile.
15.3. Les activités du programme de gestion de la sécurité de l'information de R&M sont classées par ordre de priorité en fonction des risques identifiés et de leur impact sur les services fournis aux clients.

Copyright Reed & Mackay 2025 (V082025)