ACCORD DE TRAITEMENT DES DONNEES PERSONNELLES

1. OBJET

1.1. Cet Accord de Traitement des Données Personnelles (l'« Accord ») complète le Formulaire de Commande et les Conditions Générales d'Utilisation Mirakl (ensemble, le « Contrat ») signés par et entre Mirakl et le Client afin de refléter leur accord concernant le Traitement des Données Personnelles incluses dans les Données Client dans le cadre de l'exécution du Contrat tel que décrit à l'annexe 1 « Détails du Traitement », ce, conformément aux exigences de la Loi Applicable en matière de Protection des Données.

1.2. Dans le cadre de leurs relations contractuelles, les Parties agissent en leurs qualités respectives :

(i) Pour les Données Personnelles de leurs contacts professionnels respectifs, traitées dans le cadre de la gestion de leur relation commerciale réciproque : de responsables de Traitement indépendants pour Mirakl et le Client ;

(ii) Pour les Données Personnelles traitées dans le cadre de la gestion administrative, technique et commerciale des Services Cloud : de responsable de Traitement indépendant pour Mirakl ;

(iii) Pour les Données Personnelles Client traitées dans le cadre de la fourniture des Services Cloud par Mirakl au Client, et l'utilisation par le Client des Services Cloud :

- ***de responsable de traitement*** pour le Client, dans la mesure où le Client détermine les finalités et moyens du Traitement des Données Personnelles Client tel que décrits à l'annexe 1 « Détails du Traitement » ; et
- ***de sous-traitant*** pour Mirakl, dans la mesure où Mirakl s'assure, pour le compte du Client et selon ses instructions documentées, de l'exécution du Traitement des Données Personnelles Client tel que décrit à l'annexe 1 « Détails du Traitement ».

2. DEFINITIONS

2.1. Les termes suivants, qu'ils soient utilisés au singulier ou au pluriel, ont la signification qui leur est donnée ci-dessous. Tout autre terme en majuscule dans l'Accord a la signification qui lui est donnée dans le Contrat.

« Donnée(s) Personnelle(s) », « Violation de données à caractère personnel », « Donnée Sensible », « Personne Concernée », « Traitement » ont le sens qui leur est donné par la Loi Applicable en matière de Protection des Données.

« Donnée Personnelle Client » désigne toute Donnée Personnelle contenue dans les Données Client.

« Loi Applicable en matière de Protection des Données » désigne la législation applicable aux données personnelles telle que résultant de toute législation ou règlement, européen ou d'un État-Membre, notamment le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données « RGPD »).

« Sous-Traitant Ultérieur » désigne tout tiers avec qui le groupe Mirakl collabore dans le cadre de la fourniture des Services Cloud, conformément à l'Accord.

2.2. Si et dans la mesure où Mirakl traite les Données Personnelles Client pour le compte et conformément aux instructions documentées du Client dans le contexte d'application d'une législation sur la protection de la vie privée d'un État Américain ("Loi État Américain"), la Loi Applicable en matière de Protection des Données, si cela est autorisé et compatible avec ladite Loi État Américain, le présent DPA doit être lu comme faisant référence à la Loi État Américain parmi la réglementation applicable aux données personnelles et les références spécifiques au RGPD sont remplacées par un article ou une section équivalente de la Loi État Américain.

L'expression "Objectif d'Affaires" a la même signification que dans la Loi État Américain ;

L'expression "Objectif Commercial" a la même signification que dans la Loi État Américain ;

"Responsable de Traitement " inclut "Entreprise" tel que défini dans la Loi État Américain ;

La "Personne Concernée" comprend le "Consommateur" tel que défini dans la Loi État Américain.

Les "Données Personnelles" comprennent les "Informations Personnelles" telles que définies dans la Loi État Américain.

" Violation des Données Personnelles " inclut la " Violation de la Sécurité du Système" telle que définie dans la Loi État Américain.

Le terme "Sous-Traitant" inclut le "Prestataire de Services" tel que défini dans la Loi État Américain.

Les parties conviennent que, en ce qui concerne le traitement des Données personnelles en vertu de la Loi État Américain, le Responsable de Traitement est une Entreprise et le Sous-Traitant est un Prestataire de Services.

Le Responsable de Traitement divulgue les Données Personnelles Client au Sous-Traitant uniquement pour : (i) des fins commerciales licites ; et (ii) pour permettre au Sous-Traitant d'exécuter les services décrits dans le Contrat et dans le présent DPA.

Le Sous-Traitant ne doit pas : (i) vendre des Données Personnelles ; (ii) conserver, utiliser ou divulguer des Données Personnelles à des fins commerciales autres que la fourniture des services spécifiés dans le Contrat et dans les Annexes du DPA ou comme autrement autorisé par la loi de l'État américain ; ni (iii) conserver, utiliser ou divulguer des Données Personnelles sauf comme autorisé par le Contrat et le présent DPA entre le Responsable de Traitement et le Sous-Traitant.

Si et dans la mesure où Mirakl traite les Données Personnelles Client pour le compte et conformément aux instructions documentées du Client dans le contexte de la Loi britannique sur la protection des données de 2018 ("Loi Britannique") la Loi Applicable en matière de Protection des Données, si cela est autorisé et compatible avec ladite Loi Britannique, le présent DPA doit être lu comme faisant référence à la Loi Britannique parmi Loi Applicable en matière de Protection des Données et les références spécifiques au RGPD sont remplacées par un article ou une section équivalente de la Loi Britannique.

3. CHAMP D'APPLICATION DE L'ACCORD

3.1. Cet Accord s'applique aux Données Personnelles Client traitées par Mirakl agissant en qualité que Sous-Traitant, et, le cas échéant, ses Sous-Traitants Ultérieurs, pour la fourniture des Services Cloud. Le Client ne doit pas utiliser de quelque manière que ce soit des environnements non productifs pour traiter ou stocker des Données Personnelles. Par conséquent, cet Accord ne s'applique pas à ces environnements.

3.2. Le Client agit en tant que point de contact unique de Mirakl et doit obtenir toute autorisation, consentement et permission pertinents pour le Traitement des Données Personnelles conformément au Contrat et notamment au présent Accord. Toute instruction du Client ou de ses Utilisateurs Autorisés à Mirakl sera réputée avoir été donnée par le Client. De la même manière, toute information donnée par Mirakl au Client sera réputée avoir également été donnée, le cas échéant, aux Utilisateurs Autorisés.

3.3. Le Client ne doit en aucun cas importer ou fournir de Données Sensibles au travers des Services Cloud.

4. CONFORMITE

4.1. Les Parties se conformeront à leurs obligations telles que prévues par la Loi Applicable en matière de Protection des Données. Le Client accepte que Mirakl ne soit pas responsable de la conformité aux lois ou règlements applicables au Client ou à l'industrie du Client qui ne sont pas généralement applicables aux fournisseurs de services de technologie de l'information. Mirakl ne détermine pas si les Données Client comprennent des informations soumises à une loi ou une réglementation spécifique.

4.2. Le Client est seul responsable :

(i) de l'exactitude, de la qualité, de la loyauté et de la licéité des Données Personnelles Client et des moyens par lesquels le Client a obtenu ces Données Personnelles ;

(ii) (a) de la vérification des bases légales du Traitement (mesures précontractuelles, contrat, intérêt légitime, sauvegarde d'intérêts vitaux, mission d'intérêt public, obligations légales) en vertu de la Loi Applicable en matière de Protection des Données pour le Traitement des Données Personnelles Client et de l'obtention, le cas échéant, du consentement libre,

éclairé, spécifique, et univoque des Personnes Concernées au Traitement en accord avec la Loi Applicable en matière de Protection des Données, (b) de la conservation de la preuve du consentement de la Personne Concernée par le Traitement, et (c) de s'assurer que les Personnes Concernées peuvent exercer leur droit de retirer leur consentement à tout instant ;

(iii) d'informer les Personnes Concernées du Traitement des Données Personnelles Client réalisé par Mirakl et ses Sous-Traitants Ultérieurs ; et

(iv) d'obtenir toute autorisation nécessaire telle qu'exigée par la loi applicable.

5. INSTRUCTIONS DOCUMENTEES

5.1. Mirakl traite les Données Personnelles Client uniquement pour le compte du Client et uniquement selon ses instructions documentées (y compris cet Accord et son annexe 1, sauf si une loi applicable n'en dispose autrement).

5.2. En signant le présent Accord, le Client donne instruction à Mirakl de traiter les Données Personnelles Client :

(i) pour la fourniture des Services Cloud ;

(ii) tel que spécifié par le Client du fait de son utilisation de toute fonctionnalité des Services Cloud ;

(iii) tel que documenté dans le Contrat, y compris le Formulaire de Commande et la Documentation ; et

(iv) tel que documenté dans toute autre instruction écrite donnée par le Client et reconnue par Mirakl comme constituant une instruction aux fins du présent Accord.

5.3. Si Mirakl estime qu'une instruction du Client n'est pas conforme à la Loi Applicable en matière de Protection des Données ou au Contrat, Mirakl ne sera pas tenue de suivre ladite instruction et en notifiera le Client.

6. SUPPORT

6.1. Sur demande du Client, Mirakl fournira les informations pertinentes et nécessaires au Client afin de lui permettre de s'assurer du respect par Mirakl de ses obligations au titre du présent Accord.

6.2. Mirakl s'engage à mettre à disposition du Client les informations pertinentes pour permettre au Client de démontrer sa conformité à ses obligations au titre de la Loi Applicable en matière de Protection des Données, notamment en assistant raisonnablement le Client aux fins de s'assurer du respect par ce dernier de ses obligations au titre des articles 32 à 36 du RGPD (sécurité du Traitement – notification d'une Violation de données à caractère personnel à l'autorité de contrôle et aux Personnes Concernées – la vérification de l'analyse d'impact et la consultation préalable de l'autorité de contrôle).

6.3. Dans la mesure où la loi applicable exige que Mirakl recueille et conserve certaines informations relatives au Client, le Client fournira ces informations à Mirakl sur demande et les gardera correctes et à jour. Mirakl peut mettre ces informations à la disposition de l'autorité de contrôle si la Loi Applicable en matière de Protection des Données l'exige.

7. SOUS-TRAITANTS ULTERIEURS

7.1. Le Client autorise Mirakl à engager des Sous-Traitants Ultérieurs dans le cadre de l'exécution des Services Cloud.

7.2. Mirakl est autorisée à utiliser les Sous-Traitants Ultérieurs avec lesquels elle travaille déjà à la date de signature du présent Accord.

7.3. Mirakl s'engage à mettre en place avec chaque Sous-Traitant Ultérieur des accords écrits contenant des obligations similaires à celles prévues dans le présent Accord concernant la protection des Données Personnelles Client au regard de la nature du service fourni par ledit Sous-Traitant Ultérieur.

7.4. Mirakl informera le Client de tout nouveau Sous-Traitant Ultérieur engagé pour le Traitement des Données Personnelles Client pendant la durée du Contrat. Si le Client a des raisons légitimes de

rejeter un nouveau Sous-Traitant Ultérieur pour des raisons de non-conformité à Loi Applicable en matière de Protection des Données, le Client aura la faculté de s'opposer à la désignation de ce nouveau Sous-Traitant Ultérieur en motivant son opposition par une notification écrite adressée à Mirakl dans les trente (30) jours à compter de la notification de Mirakl de recourir à ce nouveau Sous-Traitant Ultérieur. Mirakl déploiera alors des efforts raisonnables pour (i) proposer au Client une modification des Services Cloud si cela est techniquement et/ou commercialement raisonnable ou pour (ii) recommander au Client des modifications de sa configuration des Services Cloud ou de son utilisation des Services Cloud afin d'éviter le Traitement des Données Personnelles Client par le nouveau Sous-Traitant Ultérieur contesté. Si les Parties ne parviennent pas à trouver une solution leur convenant dans les trente (30) jours suivant la notification de Mirakl, le Client devra alors cesser toute utilisation du Service Cloud concerné et pourra résilier le Service Cloud concerné en notifiant Mirakl par écrit. Cette résiliation sera effective à la date choisie par le Client qui ne pourra excéder trente (30) jours suivant la notification de Mirakl. Si le Client ne résilie pas le Contrat durant ce délai de trente (30) jours, le Client sera réputé avoir accepté le nouveau Sous-Traitant Ultérieur.

7.5. A la demande du Client, Mirakl mettra à disposition la liste à jour des Sous-Traitants Ultérieurs des Services Cloud.

8. DIVULGATION ET CONFIDENTIALITE

8.1. Mirakl ne divulguera pas ou ne donnera pas accès aux Données Personnelles Client sauf : (i) à la demande du Client ; (ii) selon les exigences du présent DPA ; ou (iii) si la loi l'exige.

8.2. Mirakl ne divulguera pas et ne donnera pas accès aux Données Personnelles Client aux administrations compétents ou à tout autre tiers, sauf si la loi l'exige. Si les administrations compétentes contactent Mirakl avec une demande de Données Personnelles du Client, Mirakl tentera de rediriger l'administration pour demander ces données directement au Client. Dans la mesure où la loi applicable le permet, Mirakl informera le Client et lui fournira une copie de la demande, à moins qu'il ne lui soit interdit de le faire.

8.3. Mirakl s'assure que le Traitement des Données Personnelles Client est strictement limité aux personnes, y compris ses employés et les employés de ses Sociétés Affiliées et Sous-Traitants Ultérieurs, pour qui l'accès auxdites Données Personnelles est nécessaire à l'exécution du Contrat. Ces personnes devront être tenues à des obligations de confidentialité concernant les Données Personnelles qu'elles pourront traiter.

9. SECURITE

9.1. Mirakl s'engage à mettre en œuvre les mesures techniques et organisationnelles décrites en Annexe 2 « Mesures Techniques et Organisationnelles » pour assurer la sécurité, la confidentialité et l'intégrité des Données Personnelles Client, y compris leur protection contre une Violation de données à caractère personnel.

9.2. Le Client reconnaît avoir pris connaissance des mesures techniques et organisationnelles mises en œuvre par Mirakl et convient qu'elles offrent un niveau de sécurité adapté au risque en ce qui concerne le Traitement des Données Personnelles. Le Client est responsable de la mise en œuvre et du maintien de mesures de sécurité appropriées pour les composants qu'il fournit ou contrôle.

9.3. Mirakl est autorisée à modifier les mesures techniques et organisationnelles qu'elle met en œuvre sans en notifier préalablement le Client, sous réserve de maintenir le même niveau de sécurité ou un niveau de sécurité supérieur.

10. VIOLATION DE DONNEES A CARACTERE PERSONNEL

10.1. Mirakl informera le Client dès que possible après avoir pris connaissance d'un Violation de données à caractère personnel, et fournira au Client les informations disponibles au moment de la notification.

10.2. Si cela s'avère pertinent, Mirakl pourra envoyer une seconde notification au Client afin de lui fournir un second niveau d'information relatif à la Violation de données à caractère personnel.

10.3. Mirakl prendra toutes les actions correctives que Mirakl estimera nécessaires afin d'atténuer les effets négatifs de la Violation de données à caractère personnel ainsi que pour prévenir la répétition d'une autre Violation de données à caractère personnel dans la mesure où ces actions relèvent de son

contrôle raisonnable. Ces obligations ne s'appliquent pas aux Violation de données à caractère personnel causées par le Client ou par les Personnes Concernées.

11. AUDITS

11.1. A la demande du Client, et sous réserve des obligations de confidentialité stipulées dans le Contrat, Mirakl mettra à la disposition du Client ou de l'auditeur tiers indépendant du Client (qui ne devra pas être un concurrent de Mirakl), tout rapport et/ou audit relatif à la conformité de Mirakl avec les obligations énoncées dans cet Accord. Le Client accepte que tout droit d'information et d'audit accordé par la Loi Applicable en matière de Protection des Données soit couvert par ces rapports et/ou audits.

11.2. En cas de non-respect par Mirakl de l'article 11.1 et sous réserve que le Client en informe Mirakl au moins soixante (60) jours à l'avance, le Client pourra demander un audit sur site des mesures de sécurité relatives à la protection des Données Personnelles Client. Avant tout audit sur site, le Client et Mirakl s'entendront sur la portée, le calendrier et la durée de l'audit. Les Parties reconnaissent et conviennent (i) d'un maximum d'un (1) audit par an, (ii) que l'audit sera limité à un maximum de cinq (5) jours ouvrables, et (iii) que le Client prendra en charge l'ensemble des coûts associés à l'audit et devra notamment rembourser Mirakl des frais, notamment de personnel, engendrés par cet audit sur site, sauf dans l'hypothèse où l'audit révèlerait une non-conformité substantielle des mesures de sécurité qui serait imputable à Mirakl.

12. SUPPRESSION DES DONNEES PERSONNELLES CLIENT

12.1. Le Client donne instruction à Mirakl, à la fin du Contrat, de supprimer les Données Personnelles Client présentes sur les serveurs hébergeant les Services Cloud dans un délai raisonnable (qui ne saurait dépasser un délai de six (6) mois) et en tout état de cause dans le respect de la Loi Applicable en matière de Protection des Données, à moins que la loi applicable n'exige leur conservation pour une durée plus longue.

13. DEMANDE DES PERSONNES CONCERNEES

13.1. Mirakl assistera le Client, en cohérence avec la fonctionnalité des Services Cloud et le rôle de Mirakl en tant que sous-traitant, avec la réponse aux demandes d'exercice des droits des Personnes Concernées. Lorsque Mirakl reçoit une demande du Client-Final d'exercer un ou plusieurs de ses droits en rapport avec les Services Cloud pour lesquels Mirakl est un sous-traitant, Mirakl redirigera la Personne Concernée pour qu'elle exerce sa demande directement auprès du Client.

13.2. S'il est entendu que le fait de répondre aux demandes des personnes concernées relève de la responsabilité exclusive du Client, Mirakl fera néanmoins ses efforts raisonnables afin de permettre au Client de traiter les demandes des Personnes Concernées. Le Client pourra (i) gérer les demandes d'anonymisation de manière autonome au moyen d'un outil mis à sa disposition par Mirakl (tel que décrit dans la Documentation) et (ii) contacter le Service Support concernant des autres demandes des Personnes Concernées.

14. LOCALISATION DES CENTRES DE DONNEES ET TRANSFERT INTERNATIONAL

14.1. Les Données Client seront hébergées à titre principal dans le centre de données utilisé par Mirakl dans la région du Client, sauf demande contraire mentionnée dans le Formulaire de Commande.

14.2. Mirakl est autorisée à traiter les Données Personnelles Client hors de l'Union Européenne et conformément à la Loi Applicable en matière de Protection des Données.

14.3. Lorsque la Loi Applicable en matière de Protection des Données l'exige, les Parties reconnaissent et acceptent de recourir au système des clauses contractuelles types publiées par la Commission Européenne. De plus, le Client devra mettre en place, si nécessaire avec l'assistance raisonnable de Mirakl, une évaluation du régime juridique du pays destinataire afin de s'assurer de l'effectivité des droits des Personnes Concernées.

14.4. Lorsque cela est nécessaire, le Client est informé que Mirakl s'appuie sur les clauses contractuelles types au nom de ses client avec ses Sous-Traitants Ultérieurs.

15. CONTACTS EN MATIÈRE DE DONNÉES PERSONNELLES ET DE SÉCURITÉ

15.1. Contact client en matière de données personnelles : Referenced in the OF

15.2. Contact client en matière de sécurité : Referenced in the OF

15.3. DPO du Groupe Mirakl : privacy@mirakl.com

15.4. CISO du Groupe Mirakl : security@mirakl.com

ANNEXE 1 : DETAILS DU TRAITEMENT

1. DETAILS DU TRAITEMENT

1.1. Nature et finalité du Traitement. Mirakl traitera les Données Personnelles Client lorsque cela est nécessaire afin de fournir les Services Cloud conformément au Contrat et tel qu'instruit par le Client dans le cadre de son utilisation des Services Cloud.

La finalité du Traitement des Données Personnelles Client par Mirakl est la fourniture des Services Cloud au Client.

1.2. Catégories de Personnes Concernées.

1.2.1. Mirakl Core Platform : Les Personnes Concernées par le Traitement des Données Personnelles Client sont : (i) les clients finaux et (ii) les Utilisateurs Autorisés.

1.2.2. Mirakl Payout Platform : Les Personnes Concernées par le Traitement des Données Personnelles Client sont les Utilisateurs Autorisés.

1.2.3. Mirakl Ads Platform : Les Personnes Concernées par le Traitement des Données Personnelles Client sont les Utilisateurs Autorisés. Il est entendu entre les Parties que les Données Personnelles des clients finaux sont traitées et stockées uniquement dans une forme pseudonymisée ou anonymisée qui ne permet pas à Mirakl d'identifier directement ou indirectement les individus.

1.3. Catégories de Données Personnelles. Le Client importe ou fournit des Données Personnelles au travers des Services Cloud, dont l'étendue est déterminée et contrôlée par le Client à sa seule discrétion, et qui peuvent inclure, sans s'y limiter, les catégories de Données Personnelles suivantes :

- Pour les clients finaux : civilité, prénom, nom, adresse de livraison, adresse de facturation, adresse email, numéro de téléphone, historique de commandes.
- Pour les Utilisateurs Autorisés : nom, prénom, titre, nom de la société, adresse email, adresse postale, certificat de constitution ou pièce d'identité du représentant, coordonnées bancaires, coordonnées du représentant (fonction, prénom, nom, adresse email, numéro de téléphone, fax).

1.4. Catégories de destinataires. Les destinataires des Données Personnelles Client sont : (i) les employés du groupe de Mirakl, (ii) les fournisseurs du groupe de Mirakl (y compris les Sous-Traitants Ultérieurs), (iii) le cas échéant, les conseils du groupe de Mirakl et toute partie intéressée, et (iv) le cas échéant, toute autorité administrative ou judiciaire.

2. DUREE DU TRAITEMENT

2.1. La durée du Traitement des Données Personnelles Client est égale à celle du Contrat, sous réserve des obligations de Mirakl de supprimer les Données Personnelles Client tel que détaillé dans l'Accord. Cependant, le Client reconnaît qu'il est en mesure et est responsable de configurer les Services Cloud afin de limiter la durée maximale pendant laquelle les Données Personnelles Client seront stockées dans les Services Cloud.

2.2. Mirakl se réserve le droit de stocker et d'archiver toutes les informations techniques, échanges électroniques, Données Personnelles Client et toute Donnée Personnelle de quelque nature que ce soit dans le but de satisfaire à toute exigence légale applicable, à des fins de preuve, selon les politiques internes de conservation de Mirakl, conformément à la loi applicable.

ANNEXE 2 : MESURES TECHNIQUES ET ORGANISATIONNELLES

Le présent Avenant sur la sécurité de l'information, ou les “Mesures techniques et organisationnelles”, conformément au RGPD[1] ("l’Avenant"), décrit les exigences de sécurité que Mirakl maintiendra dans le cadre des Services Cloud ("Mesures de Sécurité") et est annexé au contrat ("le Contrat") conclu par Mirakl et le Client. Les termes en majuscules utilisés dans cet Avenant et qui ne sont pas définis auront la signification qui leur est donnée dans le Contrat.

1. Programme de sécurité de l'information

Mirakl s’engage à :

(i) mettre en œuvre et maintenir un programme écrit et complet de sécurité de l'information ;

(ii) mettre à jour et réviser ce programme, si nécessaire, de manière régulière et lors d'un changement important dans la fourniture des Services Cloud ; et

(iii) s'assurer que ce programme

- est conforme aux lois et aux standards de l’industrie applicables (y compris ISO 27001, ISO 27018, ISO 27701, ISO 22301, SOC 1 Type II, SOC 2 Type II),
- comprend les mesures de protection organisationnelles, logiques, techniques et physiques appropriées qui sont conformes au présent Avenant,
- est en mesure de détecter et prévenir une violation de la sécurité ("Violation de la Sécurité" signifie une violation de la sécurité des Services Cloud conduisant à la divulgation accidentelle ou non autorisée des Données Client ou à l'accès à celles-ci sur des systèmes gérés ou autrement contrôlés par Mirakl), et
- est raisonnablement conçu pour atteindre les objectifs suivants :
    - assurer la sécurité et la confidentialité, l'intégrité et la disponibilité des Données Client ;
    - protéger les Données Client contre les menaces ou les risques pour leur sécurité et leur 'intégrité ; et
    - empêcher l'accès, l'acquisition, la destruction, la perte, la suppression, la divulgation, l'altération ou l'utilisation non autorisés ou accidentels des Données Client.

Les dispositions du présent Avenant prévalent en cas de conflit entre le Contrat (y compris toute autre annexe au Contrat) et le présent Avenant.

2. Sécurité, respect de la vie privée et résilience dès la conception

Mirakl intègre la sécurité, la confidentialité et la résilience dans la conception et le fonctionnement des Services Cloud, et répond de manière continue aux changements dans les obligations légales ou réglementaires, les meilleures pratiques de l'industrie, et les risques connus et prévisibles pour les Données Client.

3. Politiques de sécurité

Mirakl maintient des politiques de sécurité de l'information couvrant au minimum les domaines clés suivants :

- Gestion des risques
- Gestion des actifs
- Sécurité des ressources humaines
- Contrôle d'accès
- Sécurité physique et environnementale
- Sécurité des opérations

[1] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, ou “RGPD”).

- Cryptographie
- Développement sécurisé
- Gestion des vulnérabilités et des correctifs
- Surveillance de la sécurité
- Gestion des incidents de sécurité
- Gestion des fournisseurs
- Résilience de l'activité

4. Gestion des ressources humaines

Vérification des antécédents : Mirakl vérifie les antécédents des candidats à l'emploi conformément aux lois et réglementations applicables.

Sensibilisation et formation à la sécurité : Mirakl délivre une formation de sensibilisation à la sécurité et à la protection de la vie privée à ses employés au moment de l'embauche et chaque année par la suite. La formation est régulièrement mise à jour afin d'inclure toute information applicable sur les sujets relatifs à la sécurité et à la vie privée, y compris les responsabilités en matière de protection des données et des systèmes, ainsi que les menaces et les tendances émergentes.

5. Gestion des identités et des accès

Mirakl n'autorise que le personnel de Mirakl et les tiers autorisés conformément au Contrat (collectivement, les "Utilisateurs Mirakl") à accéder aux Données Client. Les Utilisateurs Mirakl accèdent et traitent les Données Client uniquement dans le cadre du Contrat et du présent Avenant.

Mirakl applique le principe du moindre privilège en accordant l'accès aux Données Client. Cela signifie que seuls les Utilisateurs Mirakl qui ont besoin de connaître ou d'accéder aux Données Client se voient accorder l'accès, et seulement dans la mesure où cet accès est nécessaire pour la fonction qui leur a été attribuée.

Mirakl suit les standards de l'industrie pour authentifier et autoriser les utilisateurs.

Les Utilisateurs Mirakl n'utilisent pas d'identifiants partagés ou génériques pour accéder aux Données Client.

Mirakl exige des Utilisateurs Mirakl qu'ils utilisent une authentification à deux facteurs pour accéder aux systèmes où résident les Données Client.

Mirakl maintient un répertoire centralisé de toutes les références d'identification utilisées pour accéder au réseau de Mirakl où se trouvent les Données Client.

Mirakl révoque l'accès des Utilisateurs Mirakl qui n'ont plus besoin d'accéder aux Données Client.

Mirakl révise et révoque périodiquement les droits d'accès des Utilisateurs Mirakl, si nécessaire.

L'authentification pour accéder aux ressources réseau, plateformes, appareils, serveurs, postes de travail, applications et dispositifs du réseau de Mirakl n'est pas autorisée avec des mots de passe par défaut.

Mirakl s'assure que les connexions externes au réseau de Mirakl sont sécurisées.

Mirakl modifie les mots de passe par défaut des serveurs avant de mettre l'appareil ou le système en production.

Les postes de travail inactifs depuis un certain temps sont automatiquement verrouillés.

6. Traitement sécurisé des données

Mirakl chiffre les Données Client, pendant la transmission et au repos, en utilisant des algorithmes standards de l'industrie.

Mirakl applique et maintient un chiffrement intégral du disque au repos sur tous les systèmes de Mirakl qui accèdent, transmettent ou stockent les Données Client.

Les clés de chiffrement symétriques et les clés privées asymétriques sont chiffrées en transit et en stockage, protégées contre tout accès non autorisé, et sécurisées. Les procédures de gestion et de rotation des clés cryptographiques sont documentées. L'accès aux clés de chiffrement est limité aux dépositaires des clés. Mirakl suit les standards de l'industrie pour générer, stocker et gérer les clés cryptographiques utilisées pour chiffrer les Données Client.

Mirakl maintient des procédures sécurisées de suppression des données, y compris, mais sans s'y limiter, l'utilisation de commandes d'effacement sécurisé, la démagnétisation et le "crypto-shredding", selon les besoins, et conformément aux standards de l'industrie.

Les Données Client sont logiquement séparées de celles des autres Clients de Mirakl.

7. Sécurité des infrastructures et des réseaux

Mirakl installe, configure et maintient les Mesures de Sécurité des systèmes et du réseau afin d'empêcher tout accès non autorisé aux Données Client.

Mirakl effectue une surveillance et une journalisation continues, notamment des alertes pertinentes concernant les événements de sécurité, y compris les tentatives d'accès et les accès réussis, les changements non autorisés sur les terminaux, les périphériques réseau et les systèmes des serveurs qui contiennent les Données Client, et d'autres indicateurs de compromission. Tous les journaux sont protégés contre tout accès ou modification non autorisés.

Mirakl met en œuvre et maintien des Mesures de Sécurité et de durcissement pour les périphériques réseau, sur la base des meilleures pratiques de l'industrie.

8. Gestion des changements

Mirakl suit des procédures documentées de gestion des changements afin d'empêcher tout changement qui pourrait entraîner la divulgation, la modification ou la destruction non autorisée de données.

9. Sécurité des applications

Mirakl suit les pratiques de développement sécurisé, telles que celles définies par l'Open Web Application Security Project (OWASP) Top 10 (disponible à l'adresse www.owasp.org), afin de s'assurer qu'aucun code vulnérable n'est livré en production et que les meilleures pratiques sont respectées. Les pratiques de développement sécurisé comprennent :

(i) des environnements de développement, de test et de production séparés ;
(ii) l'évaluation des risques pendant la phase de conception ;
(iii) la revue du code par les pairs ;
(iv) l'analyse de la sécurité de tous les logiciels et/ou applications Mirakl qui stockent, traitent ou transmettent les données des clients ; et
(v) l'utilisation exclusive de données hors production, obscurcies ou anonymisées dans des environnements hors production (par exemple, développement ou test).

10. Sécurité physique

Sécurité physique. Mirakl utilise des mesures conformes aux standards de l'industrie afin d'assurer la sécurité physique de ses locaux, notamment :

(i) Mécanismes de contrôle d'accès physique (autorisations d'accès distinctes pour le personnel de Mirakl et les tiers ; clés et laissez-passer restreints, identification des personnes ayant un accès autorisé, protections des sorties, surveillance vidéo) pour s'assurer que seules les personnes autorisées peuvent obtenir un accès physique aux locaux à partir desquels les Services Cloud sont fournis.
(ii) Établir des protocoles de protection contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et d'autres formes de catastrophes naturelles ou causées par les activités humaines dans les locaux de Mirakl.

Sécurité des équipements. Mirakl protège ses systèmes et autres équipements afin de réduire les risques liés aux menaces et dangers environnementaux et aux possibilités d'accès non autorisé.

En outre, pour les équipements stockés dans les locaux de Mirakl, Mirakl s'engage à :

(i) Protéger les équipements qui dépendent de l'alimentation électrique contre les pannes de courant, les surtensions et autres anomalies électriques.

(ii) Protéger tous les câbles d'alimentation, de télécommunication et de réseau contre les accès non autorisés et les dommages.

(iii) Assurer la maintenance de ses systèmes et autres équipements afin de garantir leur disponibilité et leur intégrité.

(iv) Mettre en œuvre des procédures de sortie pour contrôler le retrait non autorisé des systèmes et autres équipements.

11. Gestion des risques ; sécurité des tiers/Mirakl

Mirakl conduit régulièrement des analyses de risques, au moins une fois par an ou lorsque des changements importants se produisent. Ces analyses couvrent les risques de sécurité de l'information et de protection de la vie privée.

Mirakl maintiendra un programme de gestion des risques liés aux tiers, qui comprendra les éléments suivants :

(i) maintien d'accords de sécurité de l'information pour s'assurer que les tiers de Mirakl ayant accès aux Données Client sont liés par des Mesures de Sécurité au moins aussi restrictives que celles énoncées dans le présent Avenant ; et

(ii) à la surveillance et l'audit des tiers ayant accès aux Données Client pour s'assurer qu'ils se conforment aux Mesures de Sécurité énoncées dans le présent Avenant.

La gestion des risques comprendra la remédiation proportionnelle au risque par Mirakl de toutes les constatations identifiées, et la preuve de l'achèvement.

Mirakl maintiendra un programme d'analyse des risques, qui définit les rôles et les responsabilités pour effectuer l'évaluation des risques et planifier leur remédiation. Mirakl procédera à des analyses de risques régulières afin de vérifier la conception des contrôles qui protègent les opérations business et les technologies de l'information.

12. Gestion des vulnérabilités et des correctifs

Scans de vulnérabilités : Mirakl effectuera régulièrement des scans de vulnérabilités et les corrigera conformément aux standards de l'industrie et aux risques de sécurité associés.

Tests d'intrusion : Mirakl engagera, au moins une fois par an, un tiers indépendant pour effectuer un test d'intrusion de l'infrastructure et des systèmes de Mirakl afin de détecter d'éventuelles faiblesses en matière de sécurité. Si des faiblesses sont identifiées, Mirakl apportera les corrections raisonnables et disponibles, en fonction des risques de sécurité associés. Mirakl fournira au Client, à sa demande et au maximum une fois par an, la synthèse de ce test d'intrusion.

Gestion des correctifs : Mirakl appliquera les correctifs de sécurité et les mises à jour système des logiciels et applications, des appareils et des systèmes d'exploitation gérés par Mirakl, conformément aux standards de l'industrie et aux risques de sécurité associés.

13. Continuité et reprise d'activité

Mirakl maintiendra des politiques et des procédures pour répondre à une urgence ou à un événement de force majeure qui pourrait endommager les Données Client ou les systèmes de production qui contiennent les Données Client. Ces procédures comprennent :

- Sauvegardes des données : Une politique de sauvegarde périodique des systèmes de fichiers et des bases de données de production pour atteindre l'objectif de point de reprise (RPO) décrit ci-dessous ;
- Plan de continuité d'activité : Un processus formel pour définir le framework via lequel un événement non planifié pourrait être géré afin de minimiser la perte de ressources vitales ;
- Plan de reprise d'activité : Un plan formel de reprise d'activité pour l'environnement de production conçu pour minimiser l'interruption du service, qui comprend des exigences pour que le plan de reprise d'activité soit testé régulièrement ;

- RPO / RTO : L'objectif de point de reprise (RPO) n'est pas supérieur à une (1) heure et l'objectif de délai de restauration (RTO) n'est pas supérieur à 24 heures.

14. Notification des violations de sécurité

Mirakl maintiendra et mettra à jour annuellement un plan d'action et de réponse documenté en cas d'atteinte à la sécurité.

Si Mirakl découvre ou est informé d'une faille de sécurité entraînant l'accès, la divulgation ou l'utilisation non autorisés des Données Client ("Violation des Données"), Mirakl s'engage, à ses frais et dans les meilleurs délais, à :

(i) notifier la Violation des Données au(x) Client(s) concerné(s) dans les plus brefs délais ;

(ii) enquêter sur la Violation des Données ;

(iii) atténuer les effets de la Violation des Données ; et

(iv) effectuer des analyses post-incident et rendre compte des résultats de ces évaluations au Client concerné.

15. Reporting & Audit

Au moins une fois par an, Mirakl fera appel à un auditeur indépendant pour :

(i) effectuer une évaluation de la conformité et fournir, sur demande, une attestation, une revue ou un rapport complet dans le cadre de la norme suivante :

a. Service Organization Control (SOC 2 Type II) ou

b. toute autre évaluation de conformité indépendante similaire reconnue par l'industrie.

(ii) effectuer une évaluation de certification et fournir, sur demande, un certificat valide couvrant la norme :

a. ISO/IEC 27001 ou

b. toute autre évaluation de conformité indépendante similaire reconnue par l'industrie.

16. Contact

Pour toute question ou demande relative à la sécurité, le Client utilisera le portail support de Mirakl (get.mirakl.help) comme point de contact unique.