Accord de traitement des données à caractère personnel

Accord de traitement des données à caractère personnel

I. PRÉAMBULE

Considérant que :

A. Les lois applicables en matière de protection des données permettent à tout responsable du traitement des données personnelles, qu'il soit une personne physique ou morale, une administration publique ou toute autre entité ou association, de désigner une personne physique ou morale agissant en tant que sous-traitant pour le traitement des données personnelles pour le compte du responsable du traitement, à condition que celle-ci puisse garantir, sur la base de son expérience, de ses compétences et de sa fiabilité, le respect des lois applicables en matière de protection des données, y compris en ce qui concerne les aspects de sécurité.
B. Le sous-traitant désigné doit fournir des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées visant à protéger les données personnelles et les droits des personnes concernées.
C. Le présent accord de traitement des données, ainsi que ses annexes (ensemble dénommés « DPA » – Data Processing Agreement), est conclu entre le client (ci-après « Client »), personne physique ou morale ayant acquis le service (tel que défini ci-après) dont les détails sont indiqués ci-dessous, et Swizzonic AG (« Swizzonic ») ; le Client et Swizzonic sont collectivement désignés par les termes « Parties » et individuellement « Partie ». Ils concluent la présente DPA afin de documenter l'accord des Parties concernant le traitement des données personnelles du Client conformément aux exigences des lois applicables en matière de protection des données.
D. Swizzonic met à disposition du Client les services activés par ce dernier (« Service(s) ») conformément aux conditions contractuelles définies dans la/les commande(s) de service et les conditions générales consultables à l'adresse https://www.swizzonic.ch/company/legal/conditions-general/?lang=fr (« CG »). Pour fournir les services mentionnés dans le cadre de cette DPA, Swizzonic peut traiter des données personnelles pour le compte du Client.
E. Plus précisément, l'objet et les finalités du traitement des données personnelles du Client liées au Service sont décrits en Annexe 1.
F. Le Client reconnaît que son utilisation du Service peut être soumise aux lois applicables en matière de protection des données de juridictions spécifiques, imposant certaines exigences relatives au traitement des données personnelles.
G. Les Parties ont conclu la présente DPA afin de garantir leur conformité aux lois applicables en matière de protection des données et de définir des mesures de protection et des procédures pour le traitement licite des données personnelles. Le Client confirme que les dispositions énoncées dans cette DPA reflètent les obligations auxquelles Swizzonic est soumise selon les lois applicables en matière de protection des

données pour le traitement des données personnelles du Client dans le cadre de la fourniture du Service. En conséquence, Swizzonic s'engage à respecter les dispositions contenues dans cette DPA.
Le préambule ci-dessus fait partie intégrante de la DPA.

1. DÉFINITIONS

Sauf définition contraire dans la présente DPA, tous les termes en majuscules utilisés ici ont la signification qui leur est attribuée dans les CG. En cas de conflit ou d'incohérence entre les dispositions relatives à la protection des données de cette DPA et celles du contrat principal de prestation de services, la présente DPA prévaut.
« Décision d'adéquation » désigne une décision juridiquement contraignante de la Commission européenne et/ou du Conseil fédéral suisse autorisant le transfert de données personnelles de l'Espace économique européen et/ou de la Suisse vers un pays tiers reconnu comme offrant un niveau de protection adéquat au regard des règles applicables en matière de protection des données.
« Lois applicables en matière de protection des données » désigne, dans les États membres de l'UE, le règlement ainsi que les lois complémentaires relatives à la protection des données dans les États membres de l'UE, y compris toutes directives et/ou codes de conduite émis par l'autorité de contrôle compétente au sein de l'UE ; et/ou dans les pays hors UE, toute loi applicable relative à la protection et au traitement licite des données personnelles.
« Client » désigne la personne ayant acquis le service.
« Données personnelles du Client » désigne les données personnelles concernant les personnes concernées et traitées dans le cadre du service fourni par Swizzonic pour le Client.
« Responsable du traitement » désigne généralement la personne physique ou morale, l'autorité, l'établissement ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.
« Exportateur de données » a la signification définie dans les clauses contractuelles types.
« Importateur de données » a la signification définie dans les clauses contractuelles types.
« Sous-traitant » désigne généralement une personne physique ou morale, une autorité, un établissement ou tout autre organisme traitant des données personnelles pour le compte du responsable du traitement.
« Personne concernée » a la signification définie dans les lois applicables en matière de protection des données.
« Droits de la personne concernée » désigne les droits dont dispose la personne concernée en vertu des lois applicables en matière de protection des données. Ces droits comprennent, par exemple, le droit d'obtenir du responsable du traitement l'accès aux données personnelles la concernant, ainsi que la rectification, l'effacement, la limitation du traitement, l'opposition au traitement et le droit à la portabilité des données.
« DPA » désigne la présente convention globale de traitement des données ainsi que ses annexes 1, 2 et 3.
« EEE » désigne l'Espace économique européen.
« UE » désigne l'Union européenne.
« Liste des sous-traitants » désigne la liste disponible sur demande écrite à legal@swizzonic.com.
« CG » désigne les conditions contractuelles contenues dans la/les commande(s) de service et les conditions générales applicables au service, convenues entre les parties et accessibles à l'adresse suivante : https://www.swizzonic.ch/company/legal/conditions-general/?lang=fr.

« Sous-traitants hors EEE/Suisse » désigne toute entité agissant en tant que sous-traitant traitant les données personnelles du Client pour fournir le service dans un pays hors EEE et Suisse.

« Responsable hors EEE/Suisse » désigne toute entité agissant en tant que responsable du traitement à laquelle Swizzonic fournit les services et qui est établie dans un pays hors EEE et Suisse.

« Données personnelles » désigne toute information se rapportant à une personne physique identifiée ou identifiable ; une personne physique est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale. Pour éviter tout doute, « données personnelles » a la signification donnée par le règlement et les lois applicables en matière de protection des données.

« Traitement » ou « traiter » désigne toute opération ou ensemble d'opérations effectuées sur des données personnelles, que ce soit ou non par des moyens automatisés, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

« Règlement » désigne 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, à la libre circulation de ces données et abrogeant la directive 95/46/CE.

« Violation de données personnelles » désigne une violation de la sécurité entraînant la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données personnelles transmises, stockées ou traitées d'une autre manière.

« Service(s) » a la signification définie au point D. du préambule.

« Services impliquant des sous-traitants hors EEE/Suisse » désigne les services « Micro Site, Simply Site et Simply Shop », dont la commande est disponible à l'adresse suivante : https://www.swizzonic.ch/company/legal/site-produits/?lang=fr.

« Catégories particulières de données personnelles » désigne les données personnelles révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que le traitement de données génétiques, biométriques aux fins d'identifier de manière unique une personne physique, de données relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle d'une personne physique, y compris les données concernant des condamnations pénales, des infractions ou des mesures de sécurité, des procédures administratives et sanctions ainsi que des mesures de sécurité sociale.

« Clauses contractuelles types » désigne les clauses types de l'Union européenne relatives au transfert de données personnelles vers des pays tiers conformément au règlement, approuvées par la Commission européenne par la décision d'exécution (UE) 2021/914 et reconnues par le Préposé fédéral à la protection des données et à la transparence (PFPDT), sous réserve de compléments éventuellement exigés par ce dernier.

« Sous-traitant » désigne toute entité mandatée par Swizzonic pour assister Swizzonic dans le traitement des données personnelles du Client en vertu des obligations de la présente DPA (ou effectuant elle-même un traitement), telle que figurant dans la liste des sous-traitants approuvée par le Client conformément à l'article 5 de la présente DPA.

« Autorité de contrôle » désigne toute autorité habilitée à superviser et à faire appliquer les lois applicables en matière de protection des données concernant le traitement des données personnelles du Client dans le cadre de la fourniture du service.

2. RÔLES EN MATIÉRE DE PROTECTION DES DONNÉES

2.1. Les Parties conviennent que :

a) Le Client est le Responsable du traitement des Données personnelles du Client, sauf dans le cas où le Client agit en tant que Sous-traitant des Données personnelles du Client pour le compte d'un tiers qui agit lui-même en tant que Responsable du traitement ou Sous-traitant. Le Client, ou le Responsable du traitement concerné, détermine les finalités de la collecte et du traitement des Données personnelles du Client ;
b) Swizzonic agit, en tout cas, en tant que Sous-traitant des Données personnelles du Client pour la fourniture du Service ; et
c) la présente DPA régit la relation entre les Parties quant à leurs devoirs et obligations respectifs concernant le traitement des Données personnelles du Client par Swizzonic, agissant en tant que Sous-traitant, dans le cadre de la fourniture du Service.

3. ENGAGEMENTS DE SWIZZONIC

3.1. Le Client ou le Responsable du traitement concerné détermine les finalités du traitement des données personnelles du Client dans le cadre de la fourniture du Service.

3.2. Dans le cadre de la fourniture du Service, Swizzonic s'engage à respecter les obligations suivantes, y compris celles définies dans les annexes 1 et 2 de la présente DPA :
a) Swizzonic ne traite les données personnelles du Client que dans la mesure nécessaire à la fourniture du Service et uniquement conformément aux instructions écrites du Client telles que définies dans cette DPA;

b) Swizzonic informe le Client s'il estime qu'une instruction écrite du Client viole les lois applicables en matière de protection des données. Toutefois, Swizzonic n'est en aucun cas tenu de procéder à un contrôle juridique complet concernant une instruction écrite du Client ;
c) En tant que Sous-traitant, Swizzonic informe immédiatement le Client de tout contact ou communication reçue d'une autorité de contrôle concernant le traitement des données personnelles du Client. Les Parties reconnaissent et conviennent que la responsabilité de répondre à ces demandes incombe au Client et non à Swizzonic ;
d) Swizzonic a mis en place des mesures opérationnelles, techniques et organisationnelles — y compris celles décrites dans l'annexe 2 de la présente DPA — visant à protéger les données personnelles du Client. Les Parties reconnaissent et conviennent que Swizzonic est expressément autorisé à mettre en œuvre des mesures alternatives appropriées ou à utiliser des sites alternatifs, à condition que le niveau de sécurité des mesures ou des sites soit maintenu ou amélioré par rapport à ceux indiqués ;
e) Si Swizzonic divulgue des données personnelles du Client à son propre personnel chargé directement et exclusivement de fournir le Service, Swizzonic s'assure que ce personnel : i) est tenu à la confidentialité ou soumis à une obligation légale de secret correspondante ; et ii) traite les données personnelles du Client conformément aux instructions de Swizzonic et en accord avec les obligations définies dans cette DPA.

4. OBLIGATIONS DU CLIENT

4.1. Le Client reconnaît et accepte que la fourniture du Service par Swizzonic nécessite le transfert de Données personnelles du Client à Swizzonic. Le Client s'engage à vérifier si les mesures de sécurité énumérées à l'Annexe 2 du présent contrat sont compatibles avec les types de données personnelles qu'il souhaite confier à Swizzonic.

4.2. Le Client déclare et garantit que :

a) il dispose d'une base légale appropriée (par exemple, consentement de la personne concernée, intérêt légitime, autorisation de l'autorité de contrôle compétente, etc.) pour traiter les Données personnelles du Client dans le cadre de la prestation du Service et pour les transférer à Swizzonic ; et
b) les dispositions énoncées dans le présent DPA reflètent les obligations que les lois applicables imposent à Swizzonic en ce qui concerne le traitement des Données personnelles du Client dans le cadre du Service.

5. CONSENTEMENT AU TRAITEMENT EN SOUSTRAITANCE

5.1. Le Client reconnaît, accepte et consent à ce que, dans le seul but de la fourniture du Service et conformément aux dispositions du présent DPA, les Données personnelles du Client puissent être traitées par Swizzonic ou par ses Sous-traitants, comme décrit dans la Liste des Sous-traitants.

5.2. Conformément à l'article 5.1, Swizzonic dispose d'une autorisation générale pour faire appel à des Sous-traitants, à condition que Swizzonic :

a) fournisse au préalable au Client des informations sur l'identité des Sous-traitants conformément à la Liste des Sous-traitants et informe le Client de toute modification, afin que celui-ci puisse s'opposer à leur désignation ;
b) conclue avec les Sous-traitants des accords imposant les mêmes obligations en matière de traitement des Données personnelles du Client que celles définies dans le présent DPA ;
c) fasse preuve d'une diligence raisonnable dans le choix des Sous-traitants et demeure responsable du respect par ces derniers des obligations prévues dans le présent DPA ;
d) fournisse au Client, sur demande, des informations appropriées concernant les mesures et dispositions mises en place par Swizzonic et ses Sous-traitants pour se conformer concrètement au présent DPA.

6. TRANSFERT DE DONNÉES À CARACTÉRE PERSONNEL

6.1. Si le Client achète un ou plusieurs Services impliquant le recours à des Sous-traitants situés en dehors de l'EEE et/ou de la Suisse, Swizzonic est autorisé, conformément aux articles 5.1 et 5.2, à transférer les Données personnelles du Client à un ou plusieurs de ces Sous-traitants. Ces entités sont considérées comme des importateurs de données au sens des Clauses contractuelles types. En l'absence d'une décision d'adéquation concernant ledit Sous-traitant non établi dans l'EEE ou en Suisse, Swizzonic garantit que des Clauses contractuelles types ont été conclues avec ce Sous-traitant, et que seules les dispositions du MODULE TROIS : Transfert entre sous-traitant et sous-traitant s'appliquent (à l'exclusion de tous les autres modules). Si cela est requis par la législation applicable en matière de protection des données, Swizzonic s'engage également à conclure des Clauses contractuelles types pour le transfert des Données personnelles du Client de la Suisse vers des Sous-traitants établis dans l'EEE.

6.2. Aucune disposition du présent DPA ne doit être interprétée comme ayant priorité sur une clause contradictoire des Clauses contractuelles types.

6.3. À la demande du Client, ce dernier peut consulter les Clauses contractuelles types. Swizzonic est toutefois autorisé à caviarder certaines parties des Clauses contractuelles types avant leur communication, dans la mesure où cela est nécessaire à la protection de secrets d'affaires ou d'autres informations confidentielles, y compris les Données personnelles.

6.4. Le Client reconnaît qu'il lui incombe de satisfaire à toutes les exigences juridiques supplémentaires applicables afin de garantir que le transfert de Données personnelles à Swizzonic et à des Sous-traitants situés en dehors de l'EEE ou de la Suisse soit conforme à la législation en vigueur en matière de protection des données.

6.5. Dans la mesure où le Client est un Responsable du traitement établi en dehors de l'EEE et de la Suisse, Swizzonic et le Client conviennent que les Clauses contractuelles types font partie intégrante du présent DPA par renvoi – pour tout transfert de Données personnelles du Responsable du traitement non établi dans l'EEE ou en Suisse à Swizzonic dans le cadre de la fourniture des Services. Dans ce cas, les dispositions suivantes s'appliquent aux Clauses contractuelles types :

(i) La clause 7 des Clauses contractuelles types s'applique ;
(ii) Seules les clauses du MODULE QUATRE : Transfert entre sous-traitant et responsable du traitement s'appliquent (à l'exclusion de tous les autres modules) ;
(iii) Les clauses 14 et 15 ne s'appliquent pas, car les Services ne prévoient pas la combinaison des Données personnelles reçues du Responsable du traitement non établi dans l'EEE ou en Suisse avec d'autres données collectées par Swizzonic dans l'UE ou en Suisse ;
(iv) Conformément à la clause 17 des Clauses contractuelles types, le droit italien est applicable ;
(v) Conformément à la clause 18 des Clauses contractuelles types, les tribunaux compétents sont ceux de Florence (Italie) ;
(vi) Seule l'Annexe 1 du présent DPA est applicable, celle-ci étant également considérée comme l'Annexe I des Clauses contractuelles types.

7. COOPÉERATION ET RESPONSABILITÉE

7.1. Les Parties coopèrent de bonne foi afin de garantir le respect des dispositions du présent DPA, y compris, sans s'y limiter, l'exercice correct et en temps utile des droits des personnes concernées ainsi que la gestion des incidents de sécurité ou des violations de données personnelles, dans le but d'en minimiser les effets négatifs potentiels.
7.2. Les Parties coopèrent de bonne foi afin de se fournir mutuellement, ainsi qu'aux autorités de contrôle, les informations nécessaires pour démontrer le respect des lois applicables en matière de protection des données.

8. DROITS DES PERSONNES CONCERNÉES

8.1. Compte tenu de la nature du traitement, Swizzonic assiste le Client, au moyen de mesures techniques et organisationnelles appropriées, dans le respect de son obligation de répondre aux demandes d'exercice des droits des personnes concernées.
8.2. Swizzonic fournit au Client une coopération et une assistance raisonnables, ainsi que les informations raisonnablement nécessaires pour répondre aux demandes des personnes concernées ou pour permettre au Client de respecter ses obligations en vertu des lois applicables en matière de protection des données en lien avec les droits des personnes concernées. Le Client reconnaît et accepte que, dans le cas où cette assistance entraînerait un effort significatif de la part de Swizzonic, des frais puissent être facturés – sous réserve d'une notification préalable et de l'accord du Client.

9. RESTITUTION ET SUPPRESSION DES DONNÉES

9.1. À la demande du Client, ainsi qu'à l'expiration ou à la résiliation anticipée du présent DPA, Swizzonic restituera ou supprimera gratuitement les données personnelles du Client, sous réserve d'une demande écrite préalable et raisonnable du Client, sauf si des lois impératives applicables (y compris, mais sans s'y limiter, les lois sur la protection des données ou des ordonnances émanant d'autorités judiciaires ou de contrôle) l'en empêchent.

9.2. Les demandes spécifiques du Client relatives à la restitution des données personnelles seront satisfaites dans la mesure du raisonnable sur les plans technique et organisationnel, en tenant compte du volume, de la catégorisation et de la quantité de données traitées.

9.3. Les données personnelles du Client restituées selon les procédures standard internes de Swizzonic sont fournies gratuitement. Dans les autres cas, la restitution peut être facturée au Client à un coût raisonnable.

9.4. Si le Client opte pour la suppression des données personnelles – sous réserve de l'article 9.5 – Swizzonic délivrera une confirmation de la suppression effectuée.

9.5. Swizzonic peut conserver les données personnelles du Client enregistrées dans le cadre de sauvegardes régulières, conformément aux protocoles internes de reprise d'activité et de continuité des activités (voir article 12), à condition que Swizzonic (et ses sous-traitants) ne traite pas activement ou délibérément ces données à d'autres fins que la fourniture du service.

10. TRANSMISSIONS

10.1. Les données personnelles transmises par Swizzonic via Internet dans le cadre du service sont convenablement chiffrées. Toutefois, les Parties reconnaissent que la sécurité des transmissions via Internet ne peut être garantie. Swizzonic n'est pas responsable de l'accès Internet du Client, de l'interception ou de l'interruption des communications sur Internet, ni des altérations ou pertes de données personnelles transmises via Internet.

10.2. En cas de suspicion de violation de la protection des données, Swizzonic peut suspendre immédiatement l'utilisation du service via Internet par le Client, jusqu'à ce qu'une enquête soit menée, à condition que Swizzonic informe le Client d'une telle suspension dans les meilleurs délais raisonnables et prenne toutes les mesures appropriées pour rétablir l'accès au service via Internet le plus rapidement possible, tout en collaborant avec le Client afin d'assurer la continuité du service via d'autres canaux de communication.

10.3. Le Client doit prendre toutes les mesures raisonnables pour préserver la confidentialité des identifiants et mots de passe de ses employés pour l'utilisation des services. Le Client est responsable des conséquences de toute utilisation abusive du service par l'un de ses employés.

11. VIOLATION DE LA PROTECTION DES DONNÉES

11.1 Le Client reconnaît et accepte que Swizzonic ne soit pas responsable des violations de la protection des données qui ne résultent pas d'une négligence de la part de Swizzonic.
11.2 Lorsqu'une violation de données personnelles est portée à la connaissance de Swizzonic, cette dernière :

a) prendra les mesures appropriées pour contenir et atténuer l'incident, et en informera immédiatement le Client afin que celui-ci puisse initier ses propres mesures de réponse. Swizzonic se réserve le droit de déterminer de manière autonome les actions nécessaires au respect des lois sur la protection des données ou à la protection de ses propres intérêts ;
b) coopérera avec le Client dans l'enquête sur l'incident — notamment en ce qui concerne la nature, l'ampleur, les catégories de données concernées et les conséquences possibles ;
c) suivra, si la loi l'exige, les instructions du Client lorsque ce dernier est tenu de notifier l'incident aux autorités de contrôle ou aux personnes concernées. Le Client est seul responsable de :

i. décider s'il y a lieu de notifier l'incident, et à qui (par exemple, aux autorités, aux personnes concernées) ;
ii. déterminer le contenu de la notification ainsi que les éventuelles mesures correctives proposées.

12. Reprise des activités en cas d'urgence et garantie de la continuité des activités

12.1 Swizzonic maintient des protocoles appropriés de reprise d'activité et de continuité des opérations, qui varient selon le service fourni. Le Client peut en obtenir un résumé sur demande. Swizzonic peut modifier ces plans à tout moment, à condition de ne pas réduire le niveau de capacité de reprise par rapport à celui en vigueur au début du contrat.

13. Demandes

13.1 En signant la présente DPA, y compris les annexes 1, 2 et 3, le Client autorise expressément Swizzonic à effectuer les activités mentionnées à l'article 5 pour son compte.
13.2 En signant la présente DPA, Swizzonic accepte ce mandat, qui est exécuté sans rémunération dans le cadre du service, et confirme légalement avoir lu et compris les instructions qui lui sont confiées.

ANNEXE 1

1. PERSONNES CONCERNÉES

Les données personnelles traitées peuvent concerner, selon le service activé, les catégories suivantes de personnes concernées, qui ne peuvent pas être déterminées à l'avance :

- Client et/ou employés du client ;
- Fournisseurs du client ;
- Utilisateurs du client ;
- Clients du client ;
- Personnes concernées dont les données personnelles sont traitées par le client via les services fournis par Swizzonic :

2. CATÉGORIES DE DONNÉES À CARACTÈRE PERSONNEL TRAITÉES POUR CHAQUE SERVICE

Les données personnelles traitées pour chaque service, qui peuvent être mises à la disposition du client et ne sont pas déterminables à l'avance, se rapportent exclusivement aux données personnelles au sens des lois applicables en matière de protection des données, à l'exclusion expresse des données personnelles relatives aux condamnations pénales et infractions ainsi qu'aux autres catégories particulières de données personnelles.

En particulier, les catégories suivantes de données personnelles sont transmises/traitées :

- Données de contact (nom et prénom, adresse e-mail, adresse postale, numéro de téléphone) ;
- Date de naissance ;
- Âge ;
- Sexe ;
- Autres catégories de données personnelles traitées par le Client via les services fournis par Swizzonic.

3. CATÉGORIES PARTICULIÈRES DE DONNÉES

Les données personnelles traitées ne concernent pas les données personnelles liées aux condamnations pénales et aux infractions, ni les catégories particulières de données personnelles.

4. FINALITÉS DU TRAITEMENT

Les données personnelles ne peuvent être traitées que pour la prestation du service décrit dans les CGV.

5. TYPE DE TRAITEMENT

Le type de traitements varie en fonction du service spécifique activé via les CGV.

6. FRÉQUENCE DE TRAITEMENT

La fréquence des opérations de traitement varie en fonction du service spécifique activé via les CGV.

7. DAUER DER VERARBEITUNG

Les données personnelles du client sont conservées aussi longtemps que le service est actif.

ANNEXE 2

Description des mesures techniques et organisationnelles de sécurité

Swizzonic et les sous-traitants s'engagent à respecter au minimum les mesures techniques et organisationnelles décrites ci-dessous.

Informations sur les mesures de sécurité

Procédures de sécurité de l'information
Organisation interne
Des rôles et responsabilités distincts en matière de sécurité de l'information ont été définis et attribués aux personnes en charge des activités de traitement au sein de l'entreprise (ci-après également « utilisateurs »), afin d'éviter les conflits d'intérêts et de prévenir les activités inappropriées.

Sécurité du personnel
Appareils mobiles et télétravail
Une politique de sécurité régit l'utilisation de tous les équipements d'entreprise, en particulier les appareils mobiles, et des contrôles appropriés sont mis en œuvre.
Fin ou modification de la relation de travail
À la fin d'une relation de travail ou en cas de changement significatif du rôle assumé, les droits d'accès sont immédiatement mis à jour, tandis que les outils professionnels sont retournés physiquement et remis à zéro au niveau système.

Gestion des ressources de l'entreprise
Responsabilité des ressources et des actifs de l'entreprise
Tous les outils et actifs de l'entreprise sont soigneusement inventoriés, et leur attribution aux utilisateurs responsables de leur sécurité est suivie. Une politique d'utilisation appropriée a également été définie.

Classification des informations
Toutes les informations sont classifiées et cataloguées par les utilisateurs concernés selon les exigences de sécurité, et traitées en conséquence.

Gestion des supports
Les informations stockées sur les supports sont gérées, contrôlées, modifiées et utilisées de manière à ne pas compromettre leur contenu, et sont effacées de façon appropriée.

Contrôle d'accès
Exigences organisationnelles en matière de contrôle d'accès
Les exigences organisationnelles relatives à la surveillance de l'accès aux ressources d'information sont documentées dans une politique et mises en œuvre par un procédé de contrôle d'accès, limitant ainsi l'accès au réseau et aux connexions.

Gestion des accès utilisateurs
L'attribution des droits d'accès est contrôlée depuis l'enregistrement initial de l'utilisateur jusqu'à la suppression des droits lorsqu'ils ne sont plus nécessaires, y compris des restrictions spécifiques pour les droits d'accès privilégiés et la gestion des « informations d'authentification secrètes ». Cette gestion fait l'objet de vérifications régulières, notamment des mises à jour des droits d'accès. Le principe du moindre privilège est appliqué, accordant aux utilisateurs uniquement l'accès aux données nécessaires à leurs fonctions. Tout accès supplémentaire requiert une autorisation spéciale.

Responsabilité des utilisateurs
Les utilisateurs sont conscients de leur responsabilité en maintenant un contrôle d'accès efficace, par exemple en choisissant un mot de passe complexe, dont la complexité est vérifiée par le système, et en le gardant confidentiel.

Systèmes et applications de contrôle d'accès
L'accès aux informations est soumis à des restrictions conformément à la politique de contrôle d'accès,

via un système d'accès sécurisé, la gestion des mots de passe, le contrôle des outils privilégiés, et l'accès restreint à tout code source.

Chiffrement
Contrôle cryptographique
Une politique régit l'utilisation du chiffrement des supports et des données utilisateur. Les authentifications sont chiffrées.

Sécurité physique et environnementale
Des mesures de sécurité physiques et environnementales sont mises en œuvre pour prévenir tout accès non autorisé ou accidentel, perte ou diffusion des données.

Zones sécurisées : centre de données
Les services sont fournis et hébergés dans plusieurs centres de données dans le monde, dont celui qui stocke les données personnelles des clients est l'un des rares centres de données certifiés Tier IV en Italie, garantissant le plus haut niveau possible. Tous les centres de données offrent une redondance complète des circuits électriques, de refroidissement et réseau, disposent d'éclairage périmétrique, de systèmes de détection de présence avec caméras CCTV, et les sorties de secours sont équipées d'alarmes. Tous les signaux d'alarme sont centralisés dans des salles de contrôle.
L'accès physique est régulé par des procédures d'autorisation, d'identification et d'enregistrement, limité aux zones où une autorisation est accordée grâce à un système de contrôle d'accès.

Équipement
Une politique encadre la mise au rebut sécurisée des équipements hors d'usage, afin de détruire de manière sûre toutes les informations qu'ils contiennent.

Sécurité des opérations
Procédures et responsabilités opérationnelles
Les responsabilités opérationnelles en informatique sont documentées, et les modifications des installations et systèmes informatiques sont contrôlées. Les systèmes de développement, de vérification et d'exploitation sont séparés. Des utilisateurs sont responsables du bon fonctionnement des procédures. La gestion de la sécurité logique des systèmes d'exploitation et des applications installées par le client incombe au client lui-même.

Protection contre les logiciels malveillants
Les antivirus et contrôles antimalware sont actifs sur les équipements d'entreprise, et les utilisateurs sont sensibilisés.
Pour les services de serveurs virtuels ou dédiés, le client est responsable de l'installation des logiciels antivirus, antimalware et, si le service n'a pas été acquis, d'un pare-feu. Le service d'hébergement bénéficie d'une protection en temps réel sur les équipements frontaux.
Le service de messagerie analyse en temps réel les courriels entrants et sortants pour détecter virus, malwares, spams, par analyse automatisée basée sur le contenu, la consultation de bases de données internationales et la réputation obtenue par divers paramètres.

Sauvegarde
Des sauvegardes périodiques sont effectuées, sauf pour les services où le client est responsable des sauvegardes (serveurs dédiés et virtuels). Pour les services d'hébergement et de messagerie, des sauvegardes périodiques sont effectuées, accessibles au client dans le cas des services d'hébergement. Des sauvegardes supplémentaires, non accessibles au client, sont réalisées uniquement pour la reprise après sinistre.

Authentification et surveillance
Authentification et synchronisation
Toute activité et tout événement lié à la sécurité de l'information par les utilisateurs et administrateurs/opérateurs système requiert la saisie d'identifiants d'authentification ou de certificats d'identité. Les horloges de tous les dispositifs sont synchronisées.

Contrôle des logiciels systèmes
L'installation de logiciels sur les systèmes d'exploitation est contrôlée et surveillée.
Les systèmes d'exploitation des serveurs virtuels et dédiés sont fournis avec des images d'installation mises à jour, y compris pendant l'installation par le client. Le client est également responsable de la mise à jour du firmware et des applications ou logiciels installés.

Gestion des vulnérabilités techniques
Gestion des correctifs
Chaque vulnérabilité technique est corrigée par des patchs appropriés, avec des procédures pour toutes les phases de test et d'installation des mises à jour, qui ne sont appliquées que si tous les tests sont concluants.

Audits des systèmes d'information
Des contrôles réguliers sont effectués pour minimiser les impacts négatifs sur les systèmes de production et prévenir les accès non autorisés aux données.

Sécurité des communications
Gestion de la sécurité réseau
Les réseaux et services en ligne sont sécurisés par séparation et segmentation.

Transmission d'informations
Des accords sont en place concernant la transmission d'informations vers et depuis des tiers.

Sécurité dans les processus de développement et de support
Les règles assurant la sécurité des développements logiciels et systèmes sont définies dans une politique. Les modifications des systèmes (applications et systèmes d'exploitation) sont contrôlées. La sécurité des systèmes est testée, et des critères d'acceptation incluant la sécurité sont définis.

Relations avec les fournisseurs
Sécurité de l'information dans la relation fournisseurs
Des contrats ou accords régissent la protection et la gestion des informations de l'organisation et des clients accessibles aux tiers dans le domaine informatique et autres fournisseurs dans la chaîne d'approvisionnement.

Gestion des services fournis par les fournisseurs
La fourniture des services est surveillée et vérifiée conformément aux contrats ou accords. Toute modification du service est contrôlée.

Gestion des incidents de sécurité
Gestion des incidents de sécurité de l'information et amélioration
Des responsabilités spécifiques et procédures sont en place pour gérer de manière cohérente et efficace tous les événements et incidents liés à la sécurité de l'information (par exemple la procédure dite de violation de données).

Aspects de sécurité de l'information liés à la continuité des activités
Redondances
Tous les équipements informatiques critiques sont redondants pour répondre aux exigences de disponibilité. Lorsque la redondance n'est pas présente, des mesures appropriées sont mises en œuvre pour assurer la continuité du service ou minimiser la perte de données.

Conformité
Respect des exigences légales et contractuelles
L'entreprise identifie et documente ses obligations envers les autorités externes et tiers concernant la sécurité de l'information, y compris la propriété intellectuelle, les documents comptables et les données personnelles.

Revue de la sécurité de l'information
Les projets liés à la sécurité de l'information et les politiques de sécurité de l'organisation sont revus, et des mesures correctives sont prises si nécessaire.

ANNEXE 3

Annexe 3 (Liste des sous-traitants) peut être demandée par e-mail à : legal@swizzonic.com.