

ANNEXE RELATIVE AU TRAITEMENT DE DONNÉES PERSONNELLES (V1. 2023 FR EMEA)

La présente Annexe relative au Traitement des Données (« **l'Annexe** ») fait partie du Contrat et des documents contractuels signés entre l'une des entités Botify suivantes : Botify SAS, Botify Ltd., Botify Corp., Botify Australia Pty. Ltd., Botify Asia Pte Ltd. et Botify Japan K.K. (« **Botify** », « **Sous-Traitant** » ou (« **Prestataire** ») et (« **Client** » ou « **Responsable de Traitement** » ou l'« **Entreprise** ») comme indiqué dans le bloc de signature du Bon de commande applicable et entre en vigueur à la dernière date de signature du Bon de commande applicable (« **Date d'entrée en vigueur** »).

Les termes en majuscules qui ne sont pas définis dans la présente Annexe ont la signification qui leur est donnée dans le Contrat. Toutefois, les termes " Responsable de Traitement ", " Sous-Traitant ", " Personne Concernée ", " Données à caractère personnel " et " Traitement " ont la signification qui leur est donnée dans les Lois applicables en matière de protection des données.

La présente Annexe est conclue entre Botify et le Client afin de définir les obligations des Parties conformément à l'Article 28 du Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 (« **Règlement Général relatif à la Protection des données** » ou « **RGPD** »), le RGPD tel que modifié et transposé aux lois du Royaume-Uni à la suite du « European Union (Withdrawal) Act 2018 » et du « European Union (Withdrawal Agreement) Act 2020 » (le « **RGPD UK** »), la loi « California Privacy Rights Act » (« **CPRA** ») ainsi que toutes autres Lois Applicables à la Protection des Données applicable, et a pour but de définir les conditions dans lesquelles Botify est habilitée, dans le cadre des Services Souscrits fournis en exécution du Contrat, à traiter les données à caractère personnel selon les instructions du Client. Toute référence à la CPRA est interprétée, jusqu'au 31 décembre 2022, comme une référence aux dispositions correspondantes de la CCPA en vigueur, le cas échéant. À partir du 1er janvier 2023, toute référence antérieure à la CCPA sera interprétée comme une référence aux dispositions pertinentes de la CPRA.

Le Client déclare que toutes les Données Personnelles transférées par le Client ou sur instruction du Client à Botify ont été collectées conformément aux Lois Applicables à la Protection des Données.

1. Champ d'Application et Applicabilité de l'Annexe

Botify fournit des services tels que définis par le Contrat, portant notamment sur l'analyse des performances de référencement dans les moteurs de recherches du (des) Site(s) Internet du Client (les « **Services** »).

Afin de fournir les Services, Botify traite les données de logs ainsi que les données d'analyses externes provenant d'outils de tiers (Google Analytics, GA 360, Google Search Console, Adobe Analytics ou tout autre fournisseur de données que le Client souhaite intégrer) (les « **Données Analytiques** ») concernant le Site Internet du Client, comme précisé dans le Contrat. Les données de logs ainsi que les adresses IP des visiteurs du Site Internet (« **Utilisateurs** ») du Client concerné par les Services (« **Données Personnelles des Utilisateurs** ») peuvent être communiquées à Botify, qui agira en qualité de Sous-Traitant des Données Personnelles des Utilisateurs et agira sur les instructions du Client, en tant que Responsable de Traitement.

Le Client a été avisé par Botify que la communication des Données Personnelles des Utilisateurs n'est pas nécessaire à la fourniture des Services par Botify, et qu'il est entièrement responsable de leur communication.

Compte tenu de l'absence de nécessité de communiquer les Données Personnelles des Utilisateurs, Botify recommande au Client de procéder à une anonymisation de ces données préalablement à l'envoi des registres à Botify.

S'agissant des Données Analytiques, elles ne contiennent aucune Donnée Personnelle des Utilisateurs.

La présente Annexe s'applique à Botify lorsque Botify traite des données à caractère personnel provenant de l'EEE ou qui sont par ailleurs soumises aux lois et règlements relatifs à la protection des données applicables à l'EEE, y compris (i) le RGPD ; et (ii) la directive 2002/58/CE relative à la protection de la vie privée et aux communications électroniques (telle que mise à jour par la directive 2009/136/CE) ; et en ce qui concerne le

Royaume-Uni, toute législation nationale applicable qui remplace ou retranscrit en droit interne le RGPD ou toute autre loi relative aux données et à la vie privée du fait de la sortie du Royaume-Uni de l'Union européenne, y compris (i) la Loi sur la protection des données de 2018 ; et (ii) le Règlement sur la vie privée et les communications électroniques de 2003 (SI 2003/2426) (ensemble, les "**Lois Applicables à la Protection des Données**") pour le compte du Client en tant que Sous-Traitant dans le cadre de la fourniture de Services conformément au Contrat.

2. Rôle des Parties

Traitement des Données Personnelles des Utilisateurs par le Client :

En tant que Responsable de Traitement, le Client s'engage à :

- (i) respecter ses obligations conformément aux Lois Applicables à la Protection des Données lorsqu'il traite les Données Personnelles des Utilisateurs ou toutes autres données personnelles qu'il peut être amené à traiter et communiquer à Botify, ainsi que lorsqu'il donne des instructions de traitement à Botify; et
- (ii) fournir des informations complètes et obtenir tous les consentements et droits nécessaires, conformément aux Lois Applicables à la Protection des Données, au traitement des Données Personnelles des Utilisateurs par Botify et la fourniture des Services conformément au Contrat et à la présente Annexe.

En tant que Responsable de Traitement, le Client est responsable du respect des obligations prévues par les Lois Applicables à la Protection des Données. A ce titre, le Client est tenu de respecter les obligations qui lui incombent en vertu des Lois Applicables à la Protection des Données. Le Client devra indemniser Botify et le dégager de toute responsabilité en cas de dommages et poursuites (y compris, mais sans s'y limiter, les coûts et les dommages et intérêts, frais de toute nature, y compris les frais d'avocat) liés à toute réclamation ou action découlant de la violation par le Client de la présente Annexe ou des Lois Applicables à la Protection des Données.

Traitement des Données Personnelles des Utilisateurs par Botify :

Botify ne traite les Données Personnelles des Utilisateurs qu'aux fins décrites par l'Annexe et uniquement selon les instructions documentées du Client.

Les Parties reconnaissant que l'Annexe et le Contrat définissent les instructions de manière exhaustive et complète du traitement des Données Personnelles des Utilisateurs du Client à Botify, et que tout éventuel traitement en dehors des limites de ces instructions fera l'objet d'un accord écrit entre le Client et Botify.

Traitement des données d'une autre entreprise par le Client :

Dans le cas où le Client traite les données d'une autre entreprise en qualité de sous-traitant au sens des Lois Applicables à la Protection des Données, Botify agira en tant que sous-traitant ultérieur.

Dans ce cas, le Client garantit qu'il a transmis toutes les informations relatives au traitement de données par Botify et a obtenu toutes les autorisations nécessaires de la part du Responsable de Traitement.

Dans les cas où le Client traiterait les données d'une autre entreprise et les communiquerait à Botify, le Client s'engage à :

- (i) obtenir toutes les autorisations nécessaires à la conclusion de l'Annexe auprès du Responsable de Traitement,
- (ii) s'assurer qu'un contrat, entièrement conforme aux conditions de l'Annexe, a été conclu avec le Responsable de Traitement,
- (iii) ce que toutes les instructions données à Botify par le Client dans le cadre de l'exécution du Contrat soient conformes aux instructions du Responsable de Traitement et,
- (iv) ce que toutes les informations communiquées ou rendues accessibles par Botify et destinées au Responsable de Traitement, conformément à l'Annexe, soient communiquées de façon appropriée au Responsable de Traitement.

Botify traite les données du Responsable de Traitement uniquement selon les instructions qui lui sont données par le Client et ne reçoit aucune instruction directement du Responsable de Traitement, lorsque celui-ci n'est

pas le Client.

3. Finalités et description du traitement

La finalité de ces clauses est de définir les conditions dans lesquelles Botify en sa qualité de Sous-traitant est autorisé à réaliser, pour le compte du Client en sa qualité de Responsable du traitement, les opérations de traitement de données à caractère personnel définies (“**Données Personnelles**”) ci-dessous en Annexe A1 : Finalité, Description des Traitements et Liste des Sous-Traitants de Botify.

4. Engagements de Botify en tant que Sous-Traitant

Botify s’engage à :

- Traiter les Données Personnelles des Utilisateurs uniquement aux fins du Contrat conclu entre Botify et le Client dans l’EEE ou dans un pays tiers, pour autant que les conditions de l’article 5 (Transferts de données à caractère personnel vers des pays tiers ou une organisation internationale) du RGPD soient respectées ;
- S’assurer que les personnes autorisées à traiter les Données Personnelles des Utilisateurs sont tenues par une obligation de confidentialité de nature contractuelle ou légale ;
- Conserver un registre des activités de traitement pour tous les types de traitement réalisés au nom du Client ;
- Obtenir l’accord général du Responsable de Traitement pour faire appel à des sous-traitants ultérieurs conformément à l’article 5 de la présente Annexe ;
- Imposer à ses sous-traitants ultérieurs les mêmes obligations relatives à la protection des données que celles qui sont à sa charge ;
- Au choix du client, restituer ou supprimer toutes les données à caractère personnel à la fin des services de traitement ou sur instruction du client ;
- Compte tenu de la nature du traitement, assister le Client par des mesures techniques et organisationnelles appropriées dans la mesure du possible pour l’exécution des obligations du Client de répondre aux demandes d’exercice des droits de la personne concernée prévues au chapitre III (Droits de la personne concernée) du RGPD ;
- Aider le responsable du traitement à assurer le respect des obligations en vertu des articles 35 (Analyse d’impact sur la protection des données) et 36 (Consultation préalable) du RGPD en tenant compte de la nature du traitement et des informations dont dispose Botify ;
- Mettre à la disposition du Client toutes les informations nécessaires pour démontrer le respect de ses obligations et permettre et coopérer pleinement avec les audits, y compris les inspections, menés par le Client ou une autre personne autorisée à cette fin par le Client.
- Mettre en œuvre et maintenir des mesures de sécurité technique et organisationnelle appropriées afin de protéger les Données Personnelles des Utilisateurs des incidents de sécurité et de préserver leur sécurité et confidentialité ;
- Signaler au Client sans retard excessif tout incident de sécurité dès qu’il en a connaissance, et fournir en temps opportun toute information relative à l’incident de sécurité dès qu’il en a connaissance.

5. Sous-Traitance Ultérieure

Le Client accepte que Botify puisse faire appel à des sous-traitants ultérieurs afin de traiter les Données Personnelles des Utilisateurs au nom du Client. Les sous-traitants ultérieurs auxquels Botify a actuellement recours et sont autorisés par le Client sont indiqués à l’Annexe A3 de la présente Annexe. En cas de demande écrite du Client, Botify s’engage à fournir une liste à jour des sous-traitants qu’il a désignés. En cas d’ajout ou de modification de la liste des sous-traitants ultérieurs, Botify (i) fournira une liste actualisée des sous-traitants ultérieurs qu’elle a désignés sur demande écrite du client et (ii) communiquera trois mois à l’avance tout sous-traitant ultérieur, en mettant à jour la présente Annexe. Si Botify souhaite faire appel à des sous-traitants ultérieurs il devra se conformer aux obligations relatives aux transferts de données personnelles, et répercuter ses propres obligations à ses sous-traitants ultérieurs. Botify est expressément autorisée à avoir librement recours à des fournisseurs tiers, sans avoir à en informer le Responsable de Traitement ou obtenir son

approbation au préalable, sous réserve que ces fournisseurs tiers n'accèdent pas aux Données Personnelles des Utilisateurs.

6. Transferts de Données Personnelles des Utilisateurs

Botify peut procéder à un transfert de Données Personnelles relatives à des Personnes Concernées situées au sein d'un Etat Membre de l'Union Européenne hors de l'Union Européenne vers un pays n'assurant pas un niveau de protection adéquat, après avoir obtenu préalablement le consentement du Client par écrit.

Dans ce cas, à la demande du Client, Botify conclura des Clauses Contractuelles Types (« CCT ») avec le sous-traitant et/ou un de ses affiliés.

Les parties reconnaissent que les Lois Applicables à la Protection des Données n'exige pas que des CCTs soient conclues pour que les Données Personnelles du Client soient traitées dans ou transférées vers un Etat membre de l'Union Européenne ou un pays ayant fait l'objet d'une décision d'adéquation conformément à l'article 45 du RGPD (un "Pays Adéquat").

Si les Données à caractère personnel du Client sont transférées vers ou traitées dans un pays qui n'est pas un Pays Adéquat et que la législation européenne sur la protection des données s'applique aux transferts (ci-après un " **Transfert Restreint de l'UE** ") ou si la réglementation applicable au transfert de données personnelle britannique s'applique aux transferts (ci-après un " **Transfert Restreint du Royaume-Uni** ") (un "**Transfert Restreint**"), les CCTs (Responsable de traitement à Sous-traitant) ou les CCTs (Responsable de traitement à Sous-traitant) britanniques s'appliqueront à l'égard de ces Transferts Restreints entre Botify et le Client. Dans ce cas, le présent DPA incorpore lesdites CCTs par référence dans les conditions prévues ci-après.

Aucune disposition du Contrat (y compris la présente Annexe) n'est destinée à modifier ou à contredire les CCTs ou à porter atteinte aux droits fondamentaux ou aux libertés des personnes concernées en vertu de la législation européenne sur la protection des données.

Dans le cas où les présentes CCTs seraient invalidées, Botify et le Client négocieront de bonne foi une méthode alternative acceptable pour régir le transfert de données conformément aux lois applicables en matière de protection des données.

6.1 Clauses contractuelles types de l'Union européenne :

Le terme CCTs de l'UE (Responsable de traitement à Sous-traitant) fait référence aux clauses contractuelles types adoptées par la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des prestataires établis dans des pays tiers dont il a été établi qu'ils offrent un niveau de protection des données inadéquat, le module 2 étant sélectionné.

Les parties conviennent que les CCTs de l'UE (Responsable de traitement à Sous-traitant) s'appliqueront aux Transferts Restreints de l'UE.

Lorsqu'un Transfert Restreint a lieu, les CCTs (du contrôleur au sous-traitant) sont réputés avoir été conclus (et intégrés au présent DPA par cette référence) et complétés comme suit (lorsqu'applicable) :

- Pour la Clause 7, la « **Clause d'adhésion** » facultative est applicable ;
- Pour la Clause 9, l'**Option 2 « AUTORISATION ÉCRITE GÉNÉRALE » est sélectionnée**, et le délai pour notifier de tout changement concernant l'ajout ou le remplacement de sous-traitants ultérieurs est de **trois (3) mois** ;
- Pour la Clause 11, la **partie optionnelle de la Clause ne s'applique pas** ;
- Pour la Clause 17, l'**Option 1 est sélectionnée**, et il est prévu que les CCTs sont régies par le droit **de la France** ;
- Pour la Clause 18(b), les juridictions compétentes sélectionnées sont les juridictions **de la France** ;

- L'Annexe I, Partie A est remplie comme suit :
 - Exportateur de données : le Client tel que défini au sein de ce DPA ;
 - Les coordonnées de l'Exportateur de données : celles mentionnées au sein de ce DPA ;
 - Rôle de l'exportateur de données : Responsable de traitement ;
 - Signature et date de signature de l'Exportateur de données : En concluant le présent DPA, l'Exportateur de données est réputé avoir signé les présentes Clauses contractuelles types, lesquelles sont incorporées par référence aux présentes, y compris leurs Annexes, à la Date d'entrée en vigueur du présent DPA ;
 - Importateur de données : l'entité Botify signataire du Contrat pouvant être soit : Botify Ltd., Botify Corp., Botify Australia Pty. Ltd., Botify Asia Pte Ltd. ou Botify Japan K.K.
 - Adresse de l'Importateur de données :
 - Botify SAS, 7 rue d'Amsterdam, 75009, Paris, France ;
 - Botify Ltd., 23 Copenhagen Street, London N1 0JB, United Kingdom ;
 - Botify Corp., 3 World Trade Center, 49th Floor, New York, NY 10007 ;
 - Botify Australia Pty. Ltd. (ABN 41 652 816 610), 6 Middlemiss St Lavender Bay, Sydney Nsw 2060, Australia ;
 - Botify Asia Pte Ltd., 1 George St, Level 10, Singapore 049145 ;
 - Botify Japan K.K., c/o SU Partners Godo Gaisha Ark Hills Front Tower RoP 701, 2-23-1 Akasaka, Minato-ku Tokyo, Japan.
 - Nom, fonction et coordonnées de la personne de contact de l'Importateur de données : Katia Bellon, Déléguee à la Protection des Données, dpo@botify.com;
 - Signature et date de signature de l'Importateur de données : En concluant le présent DPA, l'Importateur de données est réputé avoir signé les présentes Clauses contractuelles types, lesquelles sont incorporées par référence aux présentes, y compris leurs Annexes, à la Date d'entrée en vigueur du présent DPA.
- L'Annexe I, Partie B est remplie conformément aux éléments mentionnés à l'Annexe A1 du présent DPA de la manière suivante :
 - La clause "Catégories de personnes concernées dont les données à caractère personnel sont transférées" est complétée conformément à l'article 4 de l'Annexe A1 du présent DPA ;
 - La clause "Catégories de données à caractère personnel transférées" est complétée conformément à l'article 5 de l'Annexe A1 du présent DPA ;
 - La clause "Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que la limitation stricte des finalités, les restrictions d'accès (notamment l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, les"

restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires n'est pas applicable ;

- La clause "Fréquence du transfert (indiquez, par exemple, si les données sont transférées sur une base ponctuelle ou continue)" est complétée conformément à l'article 2 de l'Annexe A1 du présent DPA ;
 - La clause "Nature du traitement" est complétée conformément à l'article 6 de l'Annexe A1 du présent DPA ;
 - La clause "Finalité(s) du transfert et du traitement ultérieur des données" est complétée conformément à l'article 1 de l'Annexe A1 du présent DPA ;
 - La clause "Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères utilisés pour déterminer cette durée" est complétée conformément aux informations mentionnées au sein du tableau de l'article 7 de l'Annexe A1 du présent DPA ;
 - La clause "Pour les transferts à des sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature et la durée du traitement" est complétée conformément aux articles 3 et 6 de l'Annexe A1 du présent DPA ;
- Au sein de l'Annexe I, Partie C, la CNIL (<https://www.cnil.fr/>) est désignée comme étant l'autorité de contrôle compétente.
 - L'Annexe II est remplie conformément à l'Annexe A2 du présent DPA.
 - L'Annexe III est complétée conformément aux informations mentionnées au sein du tableau de l'article 7 de l'Annexe A1 du présent DPA.

Aucune disposition du Contrat – en ce compris le présent DPA – n'est destinée à modifier ou à contredire les CCTs, ou à porter atteinte aux droits fondamentaux ou aux libertés fondamentales des personnes concernées découlant des Lois Applicables à la Protection des Données.

Dans le cas où les CCTs actuelles devaient être invalidées, Botify et le Client négocieront de bonne foi une méthode alternative acceptable permettant d'encadrer le transfert des données conformément aux Lois Applicables à la Protection des Données.

6.2 Transferts depuis le Royaume-Uni :

Les parties conviennent que les CCTs britanniques (Responsable de traitement à Sous-traitant) s'appliqueront aux Transferts Restreints Britanniques.

Dans le cas d'un transfert restreint au Royaume-Uni, les CCTs britanniques (de Responsable de Traitement à Sous-Traitant) seront réputées conclues (et incorporées dans le présent DPA par référence).

Le terme CCTs britanniques (Responsable de traitement à Sous-traitant) fait référence aux CCTs de l'UE (Responsable de traitement à Sous-traitant) tels que définis dans la présente Annexe, complétée par l'avenant du Royaume-Uni sur le transfert international de données ("l'**Avenant du Royaume-Uni**") publié par le Commissaire Section 119A du Data Protection Act 2018 qui est entré en vigueur le 21 mars 2022. Concernant les Données Personnelles protégées par le RGPD britannique, les CCT de l'UE, complétées comme le prévoit l'article 6 de la présente Annexe, s'appliquent aux transferts de ces Données Personnelles, sauf dans les cas où :

- (i) Les CCT de l'UE sont réputés modifiés comme spécifié par l'Avenant du Royaume-Uni, qui est réputé exécuté entre le Client cédant (ou le membre concerné du Groupe de Clients) et Botify ;

(ii) Tout conflit entre les termes des CCT de l'UE et de l'Avenant du Royaume-Uni sera résolu conformément à la section 10 et à la section 11 de l'Avenant du Royaume-Uni ;

(iii) Aux fins de l'Avenant du Royaume-Uni, les tableaux 1 à 3 de la partie 1 de l'Avenant du Royaume-Uni sont réputés remplis à l'aide des informations contenues au sein de l'article 6.2 de la présente annexe ; et

(iv) le tableau 4 de la partie 1 de l'Avenant du Royaume-Uni est réputé rempli en sélectionnant "aucune partie".

Les Parties acceptent d'être liées par l'Avenant du Royaume-Uni. En ce qui concerne tout transfert sous restriction au Royaume-Uni auquel elles s'appliquent, lorsque le contexte le permet et l'exige, toute référence aux CCAP dans le DPA doit être interprétée comme une référence à ces CCAP telles que modifiées de la manière indiquée dans la présente section 2.

7. Dispositions supplémentaires concernant les Données Personnelles relatives à la Californie

Champ d'application. La présente section s'applique uniquement aux données personnelles californiennes.

Rôles des parties. Lors du traitement des Données à Caractère Personnel de Californie conformément aux Instructions du Client, les parties reconnaissent et conviennent que le Client est une Entreprise et que Botify agit en tant que Prestataire de services aux fins de, et tel que défini dans la CPRA.

Responsabilités. Les Parties conviennent que Botify traitera les Données à Caractère Personnel relatives à la Californie en tant que Prestataire de services strictement dans le but d'exécuter les Services et tout autre service connexe en vertu du Contrat ou comme le permet autrement la CPRA, y compris comme décrit dans la Politique de confidentialité de Botify.

8. Liste des sous annexes :

- Annexe A1 : Finalités, Description des Traitements et Liste des sous-traitants de Botify
 - Annexe A2 : Mesures de sécurité techniques et organisationnelles
-

Annexe A1

Finalités, Description des Traitements et Liste des sous-traitants de Botify

Description du traitement

1. Finalités du Traitement

Les traitements des données du Client ont pour principale finalité l'exécution des Services tels que décrits au sein du Contrat.

Il est précisé Botify peut traiter les données du Client pour les finalités commerciales légitimes additionnelles suivantes :

(a) L'hébergement, le stockage, et le Traitement nécessaires à la continuité et à la reprise de l'activité, y compris la création de copies de sauvegarde et d'Archivage des Données Personnelles ;
(b) L'administration et la sécurité du système et du réseau, y compris le contrôle de l'infrastructure, la gestion de l'identité et des identifiants, la vérification et l'authentification, et le contrôle d'accès ;
(c) La gestion et l'exécution du processus commercial interne Botify conduisant au Traitement indirect des Données du Client en vue de :

- L'audit interne et l'information consolidée ;
- La conformité juridique, y compris les dépôts impératifs, les utilisations et les divulgations des informations requises par les Lois Applicables à la Protection des Données ;
- L'anonymisation des Données et l'agrégation des données anonymisées pour permettre la minimisation des données et les analyses des services ;
- L'utilisation de données anonymisées et agrégées, tel que permis par les Clients, pour faciliter l'analyse, la continuité et l'amélioration des produits et services de Botify
- La facilitation de la gouvernance d'entreprise, y compris les fusions, acquisitions, désinvestissements, et co-entreprises.

2. Fréquence du transfert (indiquez, par exemple, si les données sont transférées sur une base ponctuelle ou continue)

Les Données à Caractère Personnel des Utilisateurs du site internet du Client peuvent être transférées à l'Importateur des données de temps à autre, si cela est nécessaire pour assurer la fourniture correcte du Service, en vertu du Contrat et de la présente Annexe.

3. Durée du Traitement

La durée du Traitement correspond à la durée du Contrat.

4. Catégories de personnes concernées

Les Utilisateurs du site internet du Client.

5. Catégories de données à caractère personnel traitées

Données de connexion (adresse IP, logs...)

6. Nature des opérations de traitement réalisées par le Sous-traitant pour le compte du Responsable du traitement :

Le traitement des Données Personnelles réalisé par le Sous-traitant consiste à la consultation des Données à Caractère Personnel dans le cadre de l'exécution des Services en vertu du Contrat ou tout autre accord entre les Parties.

7. Liste des Sous-Traitants :

Sous-traitants autorisés

Le Responsable de Traitement a autorisé le recours aux sous-traitants suivants :

Sous-traitant	Pays	Rôle	Durée de conservation des données	Type de garantie (si transfert hors UE)
Botify SAS (lorsque qu'intervenant en qualité de filial)	France	Support Optionnel	https://www.botify.com/data-retention-policy	DPA et CCTs intragroupe
Botify UK Ltd (lorsque qu'intervenant en qualité de filiale)	Royaume-Uni	Support Optionnel	https://www.botify.com/data-retention-policy	DPA et CCTs intragroupe
Botify Corp. (lorsque qu'intervenant en qualité de filiale)	US	Support Optionnel	https://www.botify.com/data-retention-policy	DPA et CCTs intragroupe
Botify Australia Pty. Ltd. (lorsque qu'intervenant en qualité de filiale)	Australie	Support Optionnel	https://www.botify.com/data-retention-policy	DPA et CCTs intragroupe
Botify Japan K.K. (lorsque qu'intervenant en qualité de filiale)	Japon	Support Optionnel	https://www.botify.com/data-retention-policy	DPA et CCTs intragroupe
**OVH (OVH Groupe SAS)	France, UE	Hébergement	21 jours*	DPA
AWS (Amazon Web Services, Inc.)	Irlande, UE	Sauvegarde de secours	6 mois d'archivage*	DPA
***AWS (Amazon Web Services, Inc.)	Allemagne, UE	Hébergement	Traitement ponctuel, 15 jours puis suppression	DPA
***AWS (Amazon Web Services, Inc.)	USA	Hébergement	Traitement ponctuel, 15 jours puis suppression	DPA CCTs

****Cloudflare Inc.	US	Hébergement	Traitement ponctuel, 15 jours puis suppression	DPA CCTs
---------------------	----	-------------	--	---

**Les durées de stockage et de sauvegarde sont des durées par défaut, définies pour faciliter le retraitement si nécessaire. Toutes les durées de stockage peuvent être raccourcies jusqu'à un minimum de 14 jours à la demande du Client.*

***Botify peut obtenir les Données du Responsable de Traitement de deux manières ("Méthode de Transfert") : (a) par transfert FTPS ou SFTP, ou par extraction de ces données par Botify à partir des systèmes du Responsable de Traitement ("Méthode Directe") ; et (b) par envoi de ces données par le Responsable de Traitement sur le système AWS S3 de Botify ("Méthode Indirecte"). OVH n'est utilisé que dans le cadre de la Méthode Directe, et AWS est toujours utilisé quel que soit le mode de transfert utilisé.*

****Les données en provenance des États-Unis peuvent être traitées aux États-Unis et/ou dans l'Union européenne sauf demande particulière visée dans le Bon de Commande applicable. Les données en provenance d'une entité du Client située dans l'Union Européenne ne seront traitées que dans l'Union Européenne.*

*****Cette sous-traitance est uniquement applicable lorsque le Client fait le choix de la solution Botify PageWorkers.*

Remarque : les données en provenance de pays ayant fait l'objet d'une décision d'adéquation par la Commission Européenne en application de l'article 45 du RGPD sont traitées de la même manière que les données en provenance de l'Union Européenne.

Annexe A2 : Mesures de sécurité techniques et organisationnelles

En tant que sous-traitant agissant au nom de nos clients, les responsables de traitement, nous nous engageons à mettre en œuvre et maintenir des processus et procédures de sécurité robustes.

Ce document résume les mesures techniques et organisationnelles qui sont mises en place dans un objectif de sécurité et de protection des données partagées par nos clients.

A. Mesures de contrôle liées à l'accès aux locaux

Exigences	Mesures
Identifier les personnes autorisées (employés et non employés)	Une liste du personnel autorisé est tenue à jour
Identifiants d'accès	Tous les employés reçoivent un badge personnel permettant l'accès aux bureaux L'accès est contrôlé sur la base de l'identité de l'utilisateur
Réglementation sur l'accès aux clés des bureaux et locaux	Les employés reçoivent des clés électroniques qui, en cas de départ de l'employé, sont récupérées dans le cadre de la procédure de départ des RH. Les clés perdues sont désactivées.
Réglementation de l'accès des non-employés	Les visiteurs sont accompagnés à tout moment et ont un accès limité aux installations.
Historique des visiteurs	Les visiteurs doivent s'enregistrer dans le registre à l'accueil.
Identifiants des visiteurs	Les visiteurs ne peuvent accéder aux bureaux et locaux que s'ils sont annoncés et enregistrés par un membre du personnel et fournissent une preuve de leur identité.
Mesures de sécurité et sécurité des locaux	Les locaux sont fermés en dehors des horaires de travail et l'accès est soumis à la présentation d'une clé électronique. Les entrées sont surveillées par un dispositif de caméra surveillance. Des rondes de nuit sont assurées par une entreprise de sécurité.

B. Mesures de contrôle liées à la localisation des serveurs de données

Exigences	Mesures
Accès contrôlé aux installations d'hébergement des données de tiers	<p>L'accès aux installations d'hébergement des données de tiers est contrôlé sur la base de l'identité de l'utilisateur.</p> <p>Tout le personnel doit être enregistré auprès de ces installations par un processus officiel.</p>
Créer des périmètres de sécurité et des voies d'accès limitées	<p>Des contrôles d'accès électroniques limitent les mouvements à des zones spécifiques du bâtiment.</p> <p>Tous les points de passage entre les zones sont contrôlés.</p>
Entrée sécurisée pour les livraisons et retrait	<p>Les livraisons et retraits ne peuvent être effectués qu'à la réception et durant les horaires de travail.</p>
Portes sécurisée (mécanisme de fermeture électronique, vidéosurveillance)	<p>Les portes sont équipées de serrures électroniques. Les installations sont surveillées par des caméras.</p>
Installation de dispositifs de contrôle d'accès	<p>Les bureaux et installations de stockage des données sont protégés par des clés, des dispositifs biométriques, des lecteurs de badges.</p>
Double système de contrôle	<p>L'entrée dans les serveurs d'hébergement des données est protégée par des contrôles d'accès.</p>
Mesures visant à protéger les locaux (système d'alarme, surveillance)	<p>Les bureaux et installations de stockages des données sont protégés par des contrôles d'accès : clés, des lecteurs de badges, des dispositifs biométriques.</p>

C. Mesures de contrôle d'accès aux systèmes d'information

Exigences	Mesures
Les terminaux permettant l'accès aux données peuvent être verrouillés	Les postes de travail, les ordinateurs portables et les appareils mobiles sont automatiquement verrouillés lorsqu'ils sont inactifs
Identification d'un terminal et/ou de l'utilisateur d'un terminal pour le système informatique	L'accès des utilisateurs aux systèmes informatiques nécessite des identifiants valables. L'authentification multi-facteurs est activée si nécessaire.
Contrôle d'accès basé sur les attributions	Les droits des utilisateurs pour tous les comptes sont gérés par des profils attribués en fonction des attributions et du besoin d'accès de l'activité
Vie privée et obligation de confidentialité	<p>Les données ne sont accessibles que si le client enregistre un formulaire de demande d'assistance pour une aide qui nécessite l'accès aux données.</p> <p>Les données personnelles sont supprimées ou rendues anonymes si elles sont reçues directement du client et ne sont autrement accessibles que si le client le demande.</p> <p>Les accords de confidentialité contractuels sont exécutés comme prévu.</p>
Directives pour la classification des documents	Les politiques internes couvrent le classement des dossiers et des documents par niveau de sensibilité.
Historique de l'accès aux données	Les outils de contrôle permettent de suivre l'accès aux données.
Systèmes d'inspection et de contrôle	Les outils d'audit et de journalisation permettent de suivre l'utilisation du système. Les serveurs, les réseaux et les composants logiciels sont surveillés.
Gestion des modifications	Le processus de gouvernance informatique gère le contrôle des changements du code et de l'infrastructure.

D. Mesures de contrôle d'accès aux données

Exigences	Mesures
Cryptage	<p>Le cryptage est activé si nécessaire.</p> <p>Les clés de cryptage de la base de données sont stockées de manière cryptée dans un emplacement séparé</p>
Contrôle d'accès aux postes de travail	<p>Des identifiants de connexion sont nécessaires pour accéder à tout système.</p> <p>L'authentification multi-facteurs est activée si nécessaire</p>
Contrôle de l'authentification par signature unique	<p>Authentification unique est mise en œuvre afin d'avoir une authentification centralisée sur toutes nos plateformes.</p> <p>Les exceptions sont documentées et suivies afin d'assurer un processus de départ approprié.</p>
Options de limites de temps d'accès	<p>Les temporisations de session sont activées pour tous les logiciels. Les sessions inactives sont automatiquement fermées.</p>
Options d'accès partiel pour l'inventaire des données	<p>Des systèmes de contrôles d'accès basés sur les rôles sont utilisés</p> <p>Les fonctions d'inventaire et de révision ont un accès en lecture seule aux métadonnées et aucun accès aux données</p>

E. Mesures de contrôle liées à la transmission de données

Exigences	Mesures
Cryptage des données mobiles et immobiles	<p>Cryptage TLS de bout en bout entre les composants de l'application.</p> <p>Cryptage des lecteurs et des supports, cryptage des fichiers d'intégration de données si nécessaire.</p> <p>Le cryptage acceptable est indiqué dans une politique ad hoc.</p>
Confirmation des personnes autorisées	Canaux de transfert sécurisés, authentification par certificat et/ou justificatifs.
Contrôle des supports de données	<p>Services de transport/expédition limités aux prestataires autorisés avec les documents correspondants (par exemple, bon de commande, manifeste de transport, etc.)</p> <p>Aucun transport physique de supports contenant des données du client n'est autorisé.</p>
Réglementation sur les supports de données	Pas de transport physique de supports contenant des données de clients.
La destruction contrôlée des supports de données (par exemple, les coquilles)	<p>Les copies papier des informations sur les clients sont très limitées. De nombreux documents sont mis sous clé.</p> <p>Les copies papier inutiles sont déchiquetées et collectées pour être éliminées.</p>
Gérer la production de copies	La copie de sauvegarde est réalisée selon un processus prédéfini.
Flux de données documentés	Toutes les transmissions de données sont identifiées et documentées.
Livraison des données	Pas de transport physique des supports contenant les données des clients
Contrôle de l'intégrité des données	Effectué au niveau du serveur de validation et après le transit.

F. Mesures de contrôle liées aux entrées de données

Exigences	Mesures
Documentation de la responsabilité de saisie des données	Processus documenté du système d'attribution des rôles et configuration des droits d'utilisation
Historiques des entrées	Les accès sont enregistrés
Organisation des programmes et flux de travail	Les processus et les responsabilités sont définis à l'avance et attribués par des rôles et des droits.
Obligation de confidentialité des données	Les employés signent des contrats comprenant des obligations de confidentialité des données

G. Mesures de contrôle liées à la disponibilité

Exigences	Mesures
Plan de continuité des activités	Des politiques existent et sont révisées chaque année
Plan de reprise d'activité en cas de sinistre	Des politiques existent et sont révisées chaque année

H. Mesures de contrôle liées à la séparation des données

Exigences	Mesures
Séparation des clients	Chaque client dispose de son propre ensemble de bases de données séparées
Séparation des fonctions	Chaque gestionnaire de compte client se voit attribuer un ensemble spécifique de clients
Séparation des fonctions	Les employés font partie d'équipes distinctes et exercent des fonctions distinctes