Accord annexe relatif à la sous-traitance de traitement(s) conformément à l'art. 28 du RGPD en tant qu'annexe à un ou plusieurs contrats utilisés par le donneur d'ordre

06 pages accord
+ Annexes (05 pages)

Accord annexe relatif à la sous-traitance de traitement(s) conformément à l'art. 28 du RGPD en tant qu'annexe à un ou plusieurs contrats utilisés par le donneur d'ordre

Entre la société
1&1 Internet SARL
7 place de la Gare - BP 70109
57201 Sarreguemines Cedex
France
– ci-après le **« mandataire »** –

et

Groupe : TTG Alliance
Entreprises-marques: TEAM TATOO GESTION SAS, TTG CONCIERGERIE SASU, MSV ASSOCIATION, KOTS, BNB GESTION
Identité confirmée: Anthony Jacques, qualité: membre conseil d'administration, DG gestionnaire sécurité
N°, rue: Rue Léon Geffroy 15

Code postal, ville: 94400 Vitry-sur-Seine
Pays: FRANCE
Numéro client: 639544217, 510433504

– ci-après le groupe **« donneur d'ordre »" –**

Préambule

La présente annexe précise les obligations des parties contractantes en matière de protection des données qui découlent du traitement du contrat ou des contrats décrits en détail dans le ou les contrats individuels (ci-après le « contrat »). Elle s'applique à toutes les activités en rapport avec le contrat et pour lesquelles les employés du mandataire ou les personnes qu'il a mandatées traitent des données personnelles (ci-après « données ») du donneur d'ordre.

Cette annexe est applicable au(x) contrat(s) en vigueur entre les parties relatif aux produits suivants :

Managed Cloud, Serveur Virtuel, Dynamic Cloud Server, Hébergement Dédié, Bons plans Serveurs, Serveurs Virtuels (VPS), Serveurs Cloud, Serveurs Dédié

Hébergement Web, Hébergement WordPress, MyWebsite Now, MyWebsite Creator, MyWebsite Essential, MyWebsite e-Commerce, MyWebsite, MyWebsite One, Boutique en ligne

E-Mail Marketing, Stockage en ligne HiDrive, Carnet d’adresses

§1 Objet, durée et spécification du traitement du contrat

(1) L'objet et la durée du mandat ainsi que les finalités et les modalités du traitement découlent du contrat. L'objet de cette annexe n'est pas l'utilisation initiale ou le traitement des données personnelles par le mandataire. En tant que prestataire d'hébergement et administrateur de systèmes de serveurs, un accès à des données personnelles par le mandataire ne peut toutefois pas être exclu.
La durée d'application de la présente annexe est couplée à la durée de validité du contrat dans la mesure où aucune obligation sortant de ce cadre ne découle des dispositions de la présente annexe .

§2 Champ d'application et responsabilité

(1) Le mandataire traite sur mandat les données personnelles du donneur d'ordre. Cela comprend les activités qui sont définies dans le contrat et dans la description des prestations. Dans le cadre de ce contrat, le donneur d'ordre est seul responsable du respect des dispositions des lois et réglementations relatives à la protection des données, en particulier pour la légitimité du traitement des données (« responsable » au sens de l'art. 4, nº 7 du RGPD).

(2) Les instructions sont initialement fixées dans le contrat et peuvent être ensuite modifiées, complétées ou remplacées par le donneur d'ordre par écrit ou sous forme électronique (« forme écrite ») grâce à des instructions spécifiques données au service désigné par le mandataire (« instructions spécifiques»).

§3 Obligations du mandataire

(1) Le mandataire est uniquement en droit de traiter des données des personnes concernées dans le cadre du mandat et des instructions du donneur d'ordre, sauf cas exceptionnel au sens de l'art. 28, paragraphe 3, lettre a) du RGPD. Le mandataire doit informer le donneur d'ordre dans les plus brefs délais s'il considère qu'une instruction contrevient aux lois ou réglementations applicables. Le mandataire est en droit de refuser l'exécution d'instructions illégales.

(2) Le mandataire concevra l'organisation interne de son domaine de responsabilité de sorte à répondre aux exigences spécifiques de la protection des données. Il prendra des mesures techniques et organisationnelles visant à garantir une protection adéquate des données du donneur d'ordre selon les exigences du règlement de base sur la protection des données (art. 32 du RGPD). Le mandataire doit prendre des mesures techniques et organisationnelles afin d'assurer à long terme la confidentialité, l'intégrité, la disponibilité, la capacité de charge des systèmes et services en rapport avec le traitement.

(3) Le mandataire prend les mesures nécessaires de sauvegarde des données et d'atténuation des conséquences préjudiciables possibles pour les personnes concernées .

(4) La description des mesures techniques et organisationnelles conformément à l'**annexe 1** fait partie du présent accord.

Le mandataire se réserve le droit de modifier les mesures de sécurité conclues tout en garantissant que le niveau de protection convenu dans le contrat est bien respecté.

Le mandataire se réserve le droit de modifier les mesures de sécurité conclues tout en garantissant que le niveau de protection convenu dans le contrat est bien respecté.

Si nécessaire, le mandataire apporte son soutien au donneur d'ordre dans le cadre de ses possibilités afin de satisfaire aux demandes et exigences des personnes concernées conformément au chapitre III du RGPD et de remplir les obligations mentionnées aux art. 33 et 34 du RGPD

(5) Le mandataire s'assure que le personnel chargé du traitement des données du donneur d'ordre et toute autre personne travaillant pour le mandataire ont l'interdiction de traiter les données en dehors du cadre de l'instruction. Le mandataire veille en outre à ce que les personnes autorisées à traiter les données personnelles s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité. L'obligation de confidentialité/discrétion subsiste même après l'exécution du mandat.

(6) Le mandataire informe le donneur d'ordre dans les meilleurs délais s'il a connaissance de violations de la protection des données personnelles du donneur d'ordre.

(7) Interlocuteur pour toute question relative à la protection des données dans le cadre de la présente annexe :

1&1 Internet SARL
Service protection des données
7 place de la Gare - BP 70109
57201 Sarreguemines Cedex
legal@1and1.fr

(8) Le mandataire s'assure de s'acquitter de ses obligations selon l'art. 32 al. 1 d) du RGPD, en mettant en œuvre une procédure visant à tester régulièrement l'efficacité des mesures techniques et organisationnelles permettant d'assurer la sécurité du traitement.

(9) Le mandataire rectifie ou supprime les données faisant l'objet du contrat si le donneur d'ordre l'y enjoint et que ces procédures font partie du cadre des instructions. Si une solution conforme à la protection des données ou une restriction correspondante du traitement des données n'est pas possible, le mandataire se charge de la destruction conforme à la protection des données des supports de données et autres matériels en vertu d'un mandat spécifique donné par le donneur d'ordre ou les restitue au donneur d'ordre sauf disposition contraire du contrat .

Dans certains cas à déterminer par le donneur d'ordre, une conservation ou une remise, une rémunération et des mesures de protection à cet effet doivent être convenues séparément pour autant qu'elles ne sont pas déjà convenues dans le contrat .

(10) A la demande du donneur d'ordre, les données, supports de données et tous les autres matériels doivent être transmis ou supprimés à la fin du mandat .

(11) Dans le cas où une personne concernée ferait valoir son droit auprès du donneur d'ordre pour d'éventuelles réclamations en vertu de l'art. 82 du RGPD, le mandataire s'engage, dans la mesure de ses moyens, à assister le donneur d'ordre dans sa défense face au droit revendiqué.

§4 Obligations du donneur d'ordre

(1) Le donneur d'ordre doit informer le mandataire dans les plus brefs délais s'il constate une erreur ou des irrégularités concernant les dispositions relatives à la loi et aux réglementations sur la protection des données dans les résultats du mandat .

(2) Dans le cas où une personne concernée ferait valeur son droit auprès du donneur d'ordre pour d'éventuelles réclamations en vertu de l'art. 82 du RGPD, le § 3 al. 11 de cette annexe s'applique .

§5 Demandes des personnes concernées

(1) Si une personne concernée s'adresse au mandataire pour exiger la rectification, la suppression ou des renseignements, le mandataire renverra la personne concernée au donneur d'ordre à condition qu'une attribution au donneur d'ordre soit possible selon les indications données par la personne concernée. Le mandataire communique sans délai la demande de la personne concernée au donneur d'ordre. Sur ordre du donneur d'ordre et si convenu, le mandataire l'assiste dans la mesure de ses moyens. Dans le cadre de l'accomplissement de ses obligations, le mandataire ne peut pas être tenu responsable dans le cas où le donneur d'ordre ne répond pas à la requête de la personne concernée, n'y répond pas correctement ou pas en temps voulu.

§6 Moyens de preuve

(1) Si, dans un cas précis, des inspections par le donneur d'ordre ou par un contrôleur chargé par celui-ci sont requises, ces inspections seront réalisées aux heures ouvrables normales sans perturber le fonctionnement de l'entreprise, après notification et en tenant compte d'un délai raisonnable. Le mandataire est en droit de faire dépendre ces inspections d'une notification préalable avec un préavis suffisant et de la signature d'une déclaration de confidentialité en ce qui concerne les données d'autres clients et des mesures techniques et organisationnelles aménagées. Le mandataire est en droit d'exiger une rémunération pour son soutien dans le cadre de la réalisation d'une inspection. Les moyens mis en œuvre par le mandataire pour une inspection sont limités par principe à un jour par année civile.

(2) Si une autorité de surveillance de la protection des données ou toute autre autorité de surveillance souveraine du donneur d'ordre devait procéder à une inspection, le **paragraphe 1** s'applique en principe de façon correspondante. La signature d'une déclaration de confidentialité n'est pas nécessaire si cette autorité de surveillance est soumise à une confidentialité professionnelle ou légale pour laquelle une infraction est assortie d'une sanction selon le code pénal.

§7 Sous-traitants

(1) Le donneur d'ordre accepte que le mandataire ait recours à des entreprises affiliées ou étrangères de maintenance, d'entretien de l'infrastructure de centres de données, de prestations de service de télécommunication et de service utilisateur .

(2) Une liste des sous-traitants actuellement engagés et de leur siège social respectif peut être récupérée à tout moment par le donneur d'ordre dans le portail client. Cette liste est actualisée tous les trois mois .

(3) Si le mandataire recrute lui-même des sous-traitants, il incombe alors au mandataire d’imposer, par contrat ou au moyen d’un autre acte juridique, à ces autres sous-traitants les mêmes obligations en matière de protection des données que celles figurant aux présentes. Le mandataire assume l'entière responsabilité pour les sous-traitants qu'il a engagés.

§8 Obligations d'information, clause relative à la forme écrite, choix du droit applicable

(1) Si les données du donneur d'ordre devaient être en danger chez le mandataire en raison d'une saisie ou d'une réquisition, en raison d'une procédure de redressement judiciaire ou d'une procédure de concordat ou encore en raison d'événements divers ou de mesures de tiers, le mandataire devra en informer le donneur d'ordre dans les plus brefs délais. Le mandataire informera immédiatement tous les responsables dans ce contexte du fait que la souveraineté et la propriété des données incombent exclusivement au donneur d'ordre en tant que « responsable » au sens du règlement de base sur la protection des données .

(2) En cas d'éventuelles contradictions, les dispositions de cette annexe relative à la protection des données prévalent aux dispositions du contrat. Si des clauses de la présente annexe s'avéreraient nulles, la validité de l'annexe sur la protection des données n'en est pas affectée pour autant.

(3) Le droit français s'applique.

(4) Cette annexe remplace tous les accords précédents de ce type.

§9 Responsabilité et indemnisation

(1) Le donneur d'ordre et le mandataire sont responsables envers les personnes concernées de façon correspondante à la réglementation convenue dans l'art. 82 du RGPD.

Le présent contrat est conclu par voie électronique et est valable sans signature.
Bordereau d'annexe
Annexe 1 : Mesures techniques et organisationnelles

Mesures techniques et organisationnelles conformément à l'art. 32 du RGPD

Informations sur le document	
Version	1.0
Date	7.2.2019
Classification du document	Public
Statut de validation	Approuvé
Version originale publiée par	Délégué à la protection des données 1&1
Version actuelle publiée par	Délégué à la protection des données du groupe United Internet AG
Publié le	7.2.2019

Remarque
Ce document contient des informations qui sont mises à la disposition des partenaires commerciaux, des clients et d'autres parties externes qui disposent d'un droit de regard légal ou justifié.
Pour des raisons de lisibilité, la forme masculine a été choisie dans ce document, mais ce dernier concerne en réalité tous les sexes.

Préambule

L'entité responsable a mis en œuvre des mesures appropriées en matière de confidentialité, d'intégrité, de disponibilité et de fiabilité, ainsi que des procédures régulières d'examen, d'évaluation et d'appréciation.
La partie générale décrit les mesures techniques et organisationnelles qui s'appliquent à tous les services, lieux et clients. Les annexes décrivent les mesures qui s'appliquent au-delà de celles qui sont documentées dans la partie générale.

1. Confidentialité

Des données personnelles sont dites confidentielles lorsqu'elles ne sont pas rendues disponibles ou divulguées à des personnes, entités ou processus non autorisés.

Contrôle des entrées

- Service d'accueil et de sécurité
- Autorisations d'accès individuelles, documentées et différentes selon le rôle (cartes, transpondeurs et clés)
- Laissez-passer pour les employés et les visiteurs
- Les visiteurs ne sont autorisés à rester dans le bâtiment que s'ils sont accompagnés d'un employé
- Système d'alarme en cas de cambriolage/effraction extérieure
- Les bureaux sont fermés à clé en dehors des heures de travail

Contrôle des accès aux systèmes

- Procédures formelles d'utilisation et d'autorisation
- Connexion uniquement avec un nom d'utilisateur, un mot de passe et, le cas échéant, une authentification à deux facteurs
- Politiques de mots de passe systématiquement appliquées
- VPN pour les accès à distance et à travers des dispositifs gérés par le responsable
- Gestion des appareils mobiles
- Les supports de données mobiles sont cryptés
- Verrouillage automatique des postes de travail après quelques minutes d'inactivité
- Politique de bureau propre

Contrôle des accès aux données

- Tenue de registres des actifs et élaboration de mesures sur la base de la classification des données
- Utilisation de procédures de chiffrement (p. ex. cryptage)
- Mise en œuvre des concepts d'autorisation selon le principe du "need-to-know"
- Séparation entre les accès aux applications et les accès à l'administration des applications
- Enregistrement des tentatives d'accès
- Configuration des postes de travail des administrateurs
- Nombre minimum défini d'administrateurs
- Destruction des documents jetés

Pseudonymisation

- Dans la mesure du possible ou si nécessaire, les données personnelles seront traitées avec un pseudonyme (séparation des données d'attribution et stockage dans un système séparé)

Contrôle par séparation

- Séparation de l'environnement de développement, de test et de production
- Les données personnelles ne peuvent pas être utilisées à des fins de test
- Multi-tenancy / séparation logique des données dans les applications concernées : bases de données séparées, séparation des schémas dans les bases de données, concepts d'autorisation et/ou stockage structuré des fichiers

2. Intégrité

L'intégrité des données personnelles est préservée si elles sont exactes, inchangées et complètes.

Contrôle des transferts

- Mise à disposition de données via des connexions cryptées (par ex. SFTP)
- Divulgation de données à caractère personnel selon le principe "Need-to-Know ou "Need-to- Do"
- Les données personnelles sont classées en fonction de leur besoin de protection, les données confidentielles ne pouvant être transmises que par des voies de communication sécurisées
- Le chiffrement des emails est utilisé dans la mesure du possible
- Dans la mesure du possible, les données personnelles ne sont transmises que sous forme anonyme ou avec un pseudonyme
- Documentation de la distribution des supports de stockage physiques
- Divulgation de documents papier contenant des données à caractère personnel dans une enveloppe opaque scellée

Contrôle des saisies

- Enregistrement technique de la saisie, de la modification et de l'effacement des données personnelles et contrôle des enregistrements
- Traçabilité de la saisie, de la modification et de la suppression des données via des noms d'utilisateur individuels (et non via des groupes d'utilisateurs)
- Concept d'autorisation basé sur les rôles (droits de lecture, d'écriture et de suppression)
- Enregistrement des modifications administratives

3. Disponibilité et fiabilité

La disponibilité des données personnelles est assurée si elles peuvent toujours être utilisées comme prévu par les utilisateurs

- Utilisation de pare-feu matériels et logiciels
- Systèmes de détection d'intrusion
- Protection contre les surtensions de l'enveloppe extérieure du bâtiment contre la foudre
- Alimentation sans interruption
- Manuels d'urgence pour la récupération des données, la protection contre la destruction accidentelle et la perte
- Réalisation de tests de récupération
- Si nécessaire, utilisation de systèmes redondants (par ex. RAID)
- Tests réguliers des sauvegardes de données
- Audits externes et tests de sécurité

4. Procédures régulières d'examen, d'évaluation et d'appréciation

Comment s'assure-t-on que les mesures de protection des données mentionnées sont régulièrement réexaminées ?

Gestion de la protection des données

- Des responsables de la protection des données et un responsable de la sécurité de l'information sont nommés
- Mise en place d'une organisation de protection des données et de sécurité de l'information
- Tous les employés sont tenus à la confidentialité lors du traitement des données personnelles et sont informés du secret des télécommunications
- Les employés sont sensibilisés au traitement des données personnelles
- Les nouveaux employés reçoivent du matériel d'information sur le traitement des données personnelles
- Un registre des activités de traitement est tenu à jour et des évaluations sur la protection des données sont effectuées si besoin
- Des processus pour l'exercice des droits des personnes concernées ont été mis en place

Contrôle des commandes

- Les données traitées pour le compte du client ne sont traitées que selon les instructions du client
- Les mandataires sont soigneusement sélectionnés en fonction des mesures techniques et organisationnelles prises pour protéger les données à caractère personnel
- Les instructions relatives au traitement des données personnelles sont documentées sous forme de texte
- Le cas échéant, des accords de traitement ou des garanties appropriées pour le transfert de données vers des pays tiers sont conclus

Réglages par défaut respectant la vie privée

- Il est garanti que les systèmes et les produits sont développés dans le respect de la protection des données
- Seules les données personnelles nécessaires à la réalisation de l'objectif visé sont collectées

Gestion des interventions en cas d'incident

- Processus documenté de détection, de déclaration et de documentation des atteintes à la protection des données avec la participation du responsable de la protection des données
- Procédure documentée du traitement des incidents de sécurité avec la participation du responsable de la sécurité de l'information

Annexe 1 : Mesures techniques et organisationnelles spécifiques pour les centres de calcul

- Tous les centres de calcul sont certifiés selon la norme ISO 27001
- Les systèmes électroniques de contrôle d'accès surveillent et garantissent l'accès au centre de calcul correspondant uniquement aux personnes autorisées
- Portail de sécurité
- Des caméras vidéo ainsi que des détecteurs de cambrioleurs surveillent l'enveloppe extérieure du bâtiment
- Zones de sécurité définies
- Infrastructure réseau hautement redondante
- Le détecteur d'incendie et/ou de fumée est directement relié aux pompiers locaux
- Système de refroidissement dans le centre de calcul / salle des serveurs
- Surveillance de la température et de l'humidité de la salle des serveurs
- Pas de connexions sanitaires dans ou au-dessus des centres de calcul
- Message d'alarme en cas d'accès non autorisé aux centres de calcul