



NEFTIS

AGENCE
DE
COMMUNICATION
DIGITALE

Politique de Données Personnelles Sous-Traitant

25 Mai 2018

NEFTIS

2 rue de la plaine
54320 MAXEVILLE
SIRET : 440 715 670 00046

Représentée par
M. Christophe RISCH, gérant

NEFTIS SARL au capital de 138 560 €

N° Siret : 44071567000046 - N.A.F. : 6202A - N° intracommunautaire : FR65440715670

Déclaration d'activité de formation enregistrée sous le numéro 41 54 02895 54 auprès du Préfet de la Région Lorraine.

PREAMBULE

La présente politique de Données Personnelles Sous-Traitant a pour objet d'apporter des précisions sur les traitements des données effectués par NEFTIS (Sous-traitant) auprès de ses Clients (Responsables de Traitement), conformément aux dispositions du Règlement (UE) 2016/679 du 27 avril 2016, applicable à compter du 25 Mai 2018 dans l'ensemble des pays de l'Union Européenne, dit Règlement Européen pour la Protection des Données (ci-après repris sous les initiales « RGPD »).

DEFINITIONS

Contrat: désigne le ou les contrats unissant le Client et le Prestataire;

Données Personnelles: désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui 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, psychique, économique, culturelle ou sociale ;

Incident de sécurité (ci-après désigné « Incident ») désigne toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée à des tiers de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

Loi Applicable: désigne les loi et règlements relatifs au traitement et à la protection de Données à Caractère Personnel applicables dans le pays où le Prestataire est établi. Loi Applicable signifie en particulier

- (a) le règlement européen 2016/679 (Règlement Général relatif à la Protection des personnes physiques à l'égard du traitement des Données à Caractère Personnel ; RGPD) ;
- (b) les lois et règlements d'un état membre relatifs au traitement et à la protection des Données à Caractère Personnel, intégrant ou complétant la RGPD;
- (c) toute autre loi ou règlement applicable relatifs au traitement et à la protection des Données à Caractère Personnel dans le cadre du Contrat.

Personne physique identifiée ou identifiable: désigne une personne physique qui 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, psychique, économique, culturelle ou sociale.

Traitement de données personnelles: désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de Données Personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

Responsable de Traitement : désigne le Client ;

Sous-traitant : désigne le Prestataire, NEFTIS

ARTICLE 1 : OBLIGATIONS DES PARTIES

1.1 OBLIGATIONS DU RESPONSABLE DE TRAITEMENT – CLIENT

1.1.1. Instructions du Responsable de traitement

En tant que Responsable de Traitement, le Client fournit au Prestataire des instructions expresses (ci-après «les Instructions»), concernant au traitement des Données à Caractère Personnel. Les Parties conviennent que la fourniture par le Client des dites Instructions est nécessaire afin que le Prestataire puisse assister de manière adéquate le Client dans le respect de ses obligations au titre de la Loi Applicable.

Les Instructions comprendront a minima une description des finalités du Traitement, du type de Traitement effectué, la liste des catégories de Données à Caractère Personnel traitées, les catégories de Personnes Concernées dont les Données sont traitées, et les durées de conservation des dites Données.

Les instructions sont transmises au Prestataire par tout moyen écrit à sa convenance permettant de valider leur bonne réception par le Prestataire.

Dans le cas où le Client souhaiterait modifier ses Instructions, il en notifie au Prestataire au moins trente (30) jours à l'avance afin de permettre aux Parties d'évaluer les modifications proposées. Dès lors le Client reconnaît que:

- L'intégration des modifications peuvent avoir un impact direct sur les Prestations, rendant nécessaire une modification des termes du contrat

unissant le Client et le Prestataire, y compris en particulier du périmètre du service et des conditions financières associées;

- Les Parties négocieront de bonne foi les modifications du Contrat rendues nécessaires, y compris le délai d'intégration des dites modifications;
- Les Parties utiliseront les procédures de contrôle des modifications conformément au Contrat en vue de réaliser les modifications objet des deux points ci-dessus repris.

1.1.2. Garanties concernant les traitements

Le Client, en sa qualité de Responsable de Traitement, s'assurera que toute Donnée à Caractère Personnel traitée pour son compte par le Prestataire au titre du Contrat le sera conformément à la Loi Applicable.

Le Client confirme donc que:

- tout traitement de Données à Caractère Personnel repose sur un fondement juridique adéquat, tel que résultant des Lois de protection des Données à Caractère Personnel applicables;
- tout traitement est effectué pour une finalité définie, expresse, et légitime;
- tout traitement de Données à Caractère Personnel est pertinent et non-excessif au regard de la finalité du traitement;
- toute Donnée à Caractère Personnel est et sera tenue à jour pour toute la durée de la prestation des services;
- la durée de conservation est légitime au regard de la finalité poursuivie et de la nature de la Donnée concernée;
- des informations complètes, claires, et exactes sont fournies aux Personnes Concernées s'agissant des données traitées au titre du Contrat, y compris le cas échéant l'information concernant le fait que les données sont transférées à des tiers;
- Les Personnes Concernées dont les Données à Caractère Personnel sont traitées en application du Contrat bénéficient de moyens adéquats et efficaces leur permettant d'exercer leurs droits au regard du traitement de données effectué, conformément à la législation applicable (les droits d'accès, de rectification, de mise à jour, d'effacement, etc., lorsqu'ils sont applicables). Lorsque la demande de la Personne Concernée est adressée directement au Prestataire, le Prestataire en informera le Client. La

responsabilité du Prestataire ne pourra être retenue en cas de défaillance du Client à fournir une réponse complète, exacte et en temps utile;

- Le Client considère que le Prestataire fournit des garanties suffisantes aux fins de traitement des Données à Caractère Personnel du Client conformément à la Loi Applicable notamment au regard des mesures de sécurité décrites dans la matrice de conformité ;
- Le Client doit tenir un registre des traitements des Données.

1.2 OBLIGATIONS DU PRESTATAIRE

Les Parties conviennent expressément que le Prestataire est le Sous - Traitant au sens de la Loi Applicable et traite (notamment pour stocker) des Données personnelles pour le compte du Client dans le cadre de l'exécution des Prestations objet du Contrat.

1.2.1. Traitement conforme aux instructions

Le Prestataire traite les Données à Caractère Personnel pour le compte du Client exclusivement et uniquement en application des instructions fournies par le Client.

Si le Prestataire ne peut s'engager à se conformer à ces Instructions pour un quelconque motif, le Client en est informé sans délai. Dans un tel cas les Parties conviendront de modifications que le Prestataire sera en mesure de mettre en œuvre.

Si le Prestataire estime que tout ou partie des Instructions du Client constituent ou peuvent constituer une violation de la Loi Applicable, il en informe le Client sans délai afin d'obtenir des instructions modifiées, sauf à ce que la Loi Applicable interdise la fourniture de telles informations. Le Client procède aux adaptations des Instructions, avec l'assistance raisonnable du Prestataire en vue de la mise en conformité à la Loi Applicable. Ces modifications sont susceptibles d'avoir un impact substantiel sur la fourniture des Prestations, ce qui peut nécessiter un examen et une modification des termes du Contrat, y compris, notamment, le périmètre des Services et les conditions financières. Dans cette hypothèse, les Parties négocient de bonne foi les révisions nécessaires, le cas échéant, y compris, notamment, le délai de mise en œuvre des modifications demandées.

Le Prestataire ne sera en aucun cas responsable de toute violation de la Loi Applicable dès lors que le traitement respecte les instructions du Client ou que le client n'a transmis aucune instruction.

En tout état de cause, le Client reconnaît expressément et accepte que le Prestataire ne soit pas lié par les instructions du Client en violation de la Loi Applicable (y compris la Loi Applicable sur la Protection des Données). En tant que tel, le Prestataire se réserve le droit de suspendre l'exécution des Services jusqu'à ce que les Instructions soient modifiées pour être conformes à la Loi Applicable. Dans une telle hypothèse le Prestataire informe le Client de la mise en œuvre de la suspension.

1.2.2. Assistance

Les droits des Personnes Concernées

Le Client définit les moyens mis en œuvre pour adresser les demandes d'exercice de leurs droits par les Personnes concernées, mais le Prestataire doit, conformément à la Loi Applicable et compte tenu du type de traitement, assister dans la mesure du possible le Client dans l'exécution de ses obligations, par la mise en œuvre de mesures techniques et organisationnelles adéquates.

Lorsque la demande de la Personne Concernée est adressée directement au Prestataire, de dernier doit en informer le Client sans retard injustifié. Dans un tel cas, et sauf stipulation contraire, le **Prestataire ne doit pas répondre directement aux demandes de données.**

Le Prestataire ne saurait être tenu responsable en l'absence de réponse par le Client à une demande dûment transmise, correctement, ou en temps utile.

Sécurité du traitement

Lorsque le Client le demande et le juge nécessaire, le Prestataire doit, conformément à la Loi Applicable, et compte tenu du type de traitement considéré, aider le Client à se conformer à son obligation de définition de mesures techniques et organisationnelles adéquates pour assurer la sécurité et la confidentialité des Données à Caractère personnel traitées dans le cadre du Contrat.

Etude d'impact sur les Données à Caractère Personnel

Le Prestataire fournira au Client les informations raisonnablement accessibles et pertinentes concernant les traitements effectués, afin de permettre au Client de remplir les documents requis tels que l'étude d'impact sur les Données à Caractère

Personnel, et de se conformer à ses obligations de démonstration de la mise en oeuvre de mesures de sécurité techniques et organisationnelles adéquates.

L'assistance du Prestataire sera facturée au Client dans les conditions tarifaires applicables.

1.2.3. Tenue d'un registre des traitements

Sans préjudice des obligations énoncées à l'article « Obligations du Responsable de Traitements », le Prestataire s'engage à tenir à jour son registre des traitements et mettra à disposition du Client à première demande ledit registre. Ce registre contient :

- Les catégories de données et les types de traitement réalisés pour le compte du Client ;
- Le cas échéant, tout transfert international de Données à Caractère Personnel ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en oeuvre.

Le Client pourra obtenir une copie du registre sur demande écrite au Prestataire par mail à l'adresse suivante : vieprivee@neftis.com. Celui-ci communiquera ladite copie dans les 15 jours ouvrables suivant cette demande.

1.2.4. Autres obligations

Le Prestataire confirme que **son personnel en charge du traitement des Données à Caractère Personnel est tenu par une obligation de confidentialité appropriée**. Le Prestataire veille à ce que ledit personnel soit obligatoirement formé au traitement et la protection des Données à Caractère Personnel.

Le Prestataire informera le Client de tout changement substantiel prévu à la prestation des services qui aurait un impact significatif sur le traitement des Données à Caractère Personnel.

1.3 Obligations communes

1.3.1. Coopération avec les autorités

En cas de contrôle d'une autorité compétente, **les Parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.**

Dans le cas où le contrôle mené ne concerne que les Traitements mis en oeuvre par le Prestataire en tant que responsable du Traitement, le Prestataire fera son affaire d'un tel contrôle et s'interdit de communiquer ou de faire état des Données Personnelles du Client.

Dans le cas où le contrôle mené chez le Prestataire concerne les Traitements mis en oeuvre au nom et pour le compte du Client, le Prestataire s'engage à en informer immédiatement ce dernier et à ne prendre aucun engagement pour lui.

En cas de contrôle d'une autorité compétente chez le Client portant notamment sur les prestations réalisées par le Prestataire, ce dernier s'engage à coopérer avec le Client et à lui fournir toute information dont ce dernier pourrait avoir besoin ou qui s'avèrerait nécessaire.

1.3.2. Assurances

Chacune des Parties déclare être assurée pour sa responsabilité civile professionnelle auprès d'une compagnie notoirement solvable et s'engage à maintenir cette garantie pendant toute la durée du Contrat, afin de couvrir tout dommage qui pourrait être causé à l'autre Partie ou à tout tiers, consécutivement à l'exécution ou à l'inexécution du Contrat, y compris en cas de dommage résultant du Traitement de Données Personnelles.

Le Prestataire s'engage à fournir, à première demande du Client, une attestation avec le nom de la compagnie, le numéro de la police d'assurance, ainsi que la nature et le montant des garanties.

Il s'engage également à signaler au Client toute modification, suspension ou résiliation desdites polices d'assurance, quelle qu'en soit la cause, dans les plus brefs délais.

1.4 Remontée des violations et plaintes

Le Prestataire s'engage à prendre toutes les mesures nécessaires pour remédier à une situation de violation de données à caractère personnel ou de plainte.

Le Prestataire s'engage à communiquer au Client toute violation de Données à Caractère Personnel, même si cette dernière vient d'une instruction émise par le Client lui-même, ainsi que la survenance de toute plainte qui lui serait adressée par tout individu concerné par le traitement réalisé dans le cadre du Contrat.

Cette communication devra être effectuée dans les plus brefs délais, au maximum quarante-huit heures suivant l'identification de l'incident susceptible d'entraîner une violation des données personnelles, et devra être accompagnée de toute documentation utile afin de permettre au Client d'agir en conséquence et, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Le Client, en tant que Responsable du Traitement, reconnaît expressément qu'il est responsable du respect des exigences de la Loi Applicable (y compris notamment les formalités telles que les notifications).

1.5 Référent Protection des données

En cas de question(s) ou demande(s), le Client peut contacter le référent à la protection des données aux adresses suivantes :

- Par courrier envoyé à l'adresse suivante : NEFTIS - Référent Données Personnelles – 2 rue de la plaines - 54320 - MAXEVILLE;
- Par email envoyé à l'adresse suivante : vieprivee@neftis.com.

1.6 Audits

Le Client se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le Prestataire de ses obligations au titre du Contrat, par le biais d'un audit.

Le Client s'engage à avertir le Prestataire de sa décision de procéder à un audit en respectant un préavis minimum de 15 jours, et à ne procéder à cet audit qu'en heures et jours ouvrés.

Le Prestataire s'engage à répondre aux demandes d'audit du Client, effectuées uniquement par l'intermédiaire d'un auditeur. Cet auditeur devra :

- Avoir été sélectionné et engagé par le Client, qui en supportera seul les frais ;
- Être indépendant du Prestataire ;
- Avoir une qualification adéquate ;
- Être libre de fournir les détails de ses remarques et conclusions d'audit au Client.

Les audits doivent permettre une analyse du respect du Contrat et de la Loi Applicable, notamment :

- Par la vérification de l'ensemble des mesures de sécurité mises en oeuvre par le Prestataire ;
- Par la vérification des journaux de localisation des données, de copie, et de suppression des données.

L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

L'audit ne pourra concerner que le périmètre du Contrat.

Les frais engagés par le prestataire ainsi que son assistance dans le cadre d'un audit non initialement prévu au contrat seront facturés au Client dans les conditions tarifaires applicables.

ARTICLE 2 : CONFIDENTIALITE ET SECURITE

2.1 Confidentialité des données

Le Prestataire s'engage à garantir la confidentialité des données hébergées pour le Client, plus particulièrement pour ce qui est des données à caractère personnel.

Il reconnaît être soumis au secret professionnel concernant les données hébergées dans le cadre de l'exécution du Contrat.

Il s'engage à faire respecter cette obligation de confidentialité par les personnes placées sous son autorité, et à former ces personnes pour ce qui est de la protection des données à caractère personnel.

2.2 Mesures de sécurité des données

Dans le cadre de l'exécution du Contrat, le Prestataire agira uniquement sur les instructions du Client. A ce titre, le Prestataire s'engage à ne pas utiliser les données pour son propre compte ou pour celui d'un tiers.

Seul le personnel qualifié, habilité, et sensibilisé aux procédures de sécurité par le Prestataire pourra être amené à intervenir sur demande du Client.

Le Prestataire s'engage :

- à ne pas utiliser les données pour son propre compte ou pour celui d'un tiers ;
- à ne pas insérer dans les fichiers des données étrangères autres que celles autorisées dans l'exécution du Contrat, et s'interdit la consultation et le

traitement des données autres que celles concernées par l'exécution du Contrat et ce même s'il y a accès ;

- à traiter lesdites données dans les règles de l'art et avec le même soin que celui attaché à ses propres données ;
- à préserver la sécurité desdites données et, plus spécifiquement, leur confidentialité, à savoir à les protéger contre toute destruction (accidentelle ou illicite), perte accidentelle, modification accidentelle ou non autorisée, altération, diffusion ou accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées, et ce conformément aux dispositions de l'article 34 de la Loi n° 78-17 du 6 janvier 1978, dite Loi Informatique et Libertés;
- à communiquer sans retard au Client toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre (sauf disposition contraire), ainsi que toute demande reçue directement des personnes concernées, sans répondre à cette demande, à moins qu'il n'ait été expressément autorisé à le faire par le Client ;
- à traiter rapidement et comme il se doit toutes les demandes émanant du Client relatives à son traitement des données à caractère personnel.

Le Prestataire fournira au Client sur simple demande une annexe de sécurité, et l'informerait de ses évolutions.

Les supports informatiques et documents fournis par le Client au Prestataire restent la propriété du Client.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (conformément à l'article 226-13 du Code pénal). Il en va de même pour toutes les données dont le Prestataire prend connaissance à l'occasion de l'exécution du contrat.

Le Prestataire s'engage à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'information qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation prévue au Contrat ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au Contrat ;

- ne pas divulguer ces documents ou informations traités à des fins autres que celles spécifiées au Contrat (en sachant que la divulgation par le Prestataire d'informations relatives uniquement à l'identité du Client ne saura être considérée comme étant constitutive d'une violation des règles de confidentialité ici définies) ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du Contrat.

2.2.1 Application des mesures de sécurité techniques et organisationnelles

Le Prestataire appliquera les mesures de sécurité techniques et organisationnelles appropriées visant à empêcher la destruction accidentelle ou illicite, la perte, la modification, la divulgation non autorisée ou l'accès aux Données Personnelles Client, décrites dans le document de sécurité désigné.

Le Client reconnaît expressément que :

- les mesures de sécurité techniques et organisationnelles définies et appliquées par le Prestataire sont basées sur les Instructions et informations reçues du Client qui sont utilisées pour évaluer avec le Client les risques associés au traitement des Données Personnelles du Client ;
- il juge les mesures de sécurité techniques et organisationnelles adéquates compte tenu des risques du traitement et des finalités définies. Le Prestataire ne diminuera pas la sécurité globale du Service pendant la durée du Contrat, sans le consentement écrit préalable du Client.

2.2.2 Modification des mesures de sécurité techniques et organisationnelles suite à la modification des instructions du Client

Le Client reconnaît et accepte que, dans le cas où il modifierait ses Instructions de traitement, les mesures de sécurité techniques et organisationnelles initialement définies et mises en oeuvre peuvent ne plus être adaptées aux risques du traitement.

Dans un tel cas, le Client reconnaît et accepte que des mesures de sécurité techniques et organisationnelles puissent nécessiter des adaptations et que de telles adaptations peuvent avoir un impact sur la fourniture du Service et les termes du Contrat, notamment les dispositions financières.

ARTICLE 3 : SOUS TRAITANCE

Le Prestataire pourra sous-traiter une partie de ses prestations au titre du Contrat, et conformément aux réglementations prévues dans le cadre du RGPD.

Le Prestataire demeure seul responsable envers le Client de l'exécution des Prestations sous-traitées et du respect de l'ensemble du Contrat par ses sous-traitants.

En cas de sous-traitance, le Prestataire demeure le seul et unique garant de la bonne exécution du Contrat ainsi que le seul interlocuteur du Client.

ARTICLE 4 : TRANSFERT DE DONNEES

Le Client autorise expressément le traitement de ses Données à Caractère Personnel par un sous-traitant tiers situé dans un pays de l'UE. Le Prestataire fournira une liste de ces sous-traitants sur simple demande.

Le Prestataire doit s'assurer que les sous-traitants tiers fournissent un niveau de protection adéquat dans le cadre du traitement des Données à Caractère Personnel du Client. À cette fin, le Prestataire doit veiller à ce que tout sous-traitant dûment autorisé à traiter des Données à Caractère Personnel respecte les obligations stipulées dans les clauses contractuelles standard appropriées pour le transfert des données personnelles établies par la Commission européenne (ou toute autorité compétente), en particulier les clauses contractuelles types « Sous-traitant » de la Commission Européenne conformément à la décision 2010/593, avec le Client ou avec le Prestataire conformément à l'autorisation ci-dessus mentionnée ;

ARTICLE 5 : INCOMPATIBILITE

La présente Politique a été annexée aux conditions générales du Prestataire.

En cas de conflit entre le Contrat et la présente Politique, les dispositions de la Politique primeront sur celles du Contrat.

ARTICLE 6 : CONTINUITE

La présente Politique n'affectera pas l'exécution du Contrat et ne modifie pas la durée initiale du Contrat.