

CONDITIONS COMPLEMENTAIRES AUX CONDITIONS GENERALES D'ACHATS
APPLICABLES AUX PRESTATIONS D'ASSISTANCE TECHNIQUE

Préambule

Les présentes Conditions Complémentaires applicables aux prestations d'assistance technique (ci-après les « **Conditions Complémentaires Prestations d'Assistance Technique** ») s'appliquent aux commandes émises par toute société membre du réseau Deloitte Touche Tohmatsu Limited (« DTTL ») en France ainsi que par leurs filiales et affiliées (ci-après désigné le « Client ») pour la fourniture de services relatifs à des Prestations d'Assistance Technique par un prestataire (ci-après désigné le « Prestataire »).

Les services relatifs à des Prestations d'Assistance Technique s'entendent de toutes prestations de nature immatérielle impliquant la mise en œuvre d'un savoir-faire ou d'une technicité particulière.

Les Conditions Complémentaires Prestations d'Assistance Technique complètent les Conditions Générales d'Achats du Client (les « CGA »).

En cas de discordance entre les Conditions Complémentaires Prestations d'Assistance Technique et les CGA, les Conditions Complémentaires Prestations d'Assistance Technique priment sur les CGA.

Les termes commençant par une majuscule ont la signification qui leur est donnée dans le préambule des CGA.

Article A : Durée des Services

La durée des Services convenue entre les Parties est mentionnée au Bon de Commande, et sauf accord contraire entre les Parties mentionné au Bon de Commande, cette durée ne saurait excéder un (1) an.

Le Client conserve la faculté de mettre fin à la Prestation préalablement à l'échéance convenue à tout moment, moyennant l'observation d'un préavis d'un (1) mois.

Article B : Réalisation des Services

Les Parties conviendront du lieu d'exécution des Services selon leur objet : dans les locaux du Prestataire, dans les locaux du Client, et/ou à distance dans un ou des lieux à convenir avec le Client.

Le Prestataire est responsable des outils/logiciels/équipements que son Intervenant utilise dans le cadre de l'exécution des Services. Il garantit que son(ses) intervenant(s) dispose(nt) de toutes les licences et autorisations nécessaires à cette utilisation. Le Prestataire garantit également Deloitte contre tout recours ou revendication de toute nature émanant de tout tiers en relation avec ces outils/logiciels/équipements.

Dans tous les cas où la réalisation des Services impliquerait l'utilisation d'outils/logiciels/équipements du Client, le Prestataire communiquera à son(ses) intervenant(s) concerné(s) les « Règles d'Usage TIC » figurant en Annexe ci-après et sera garant de leur respect.

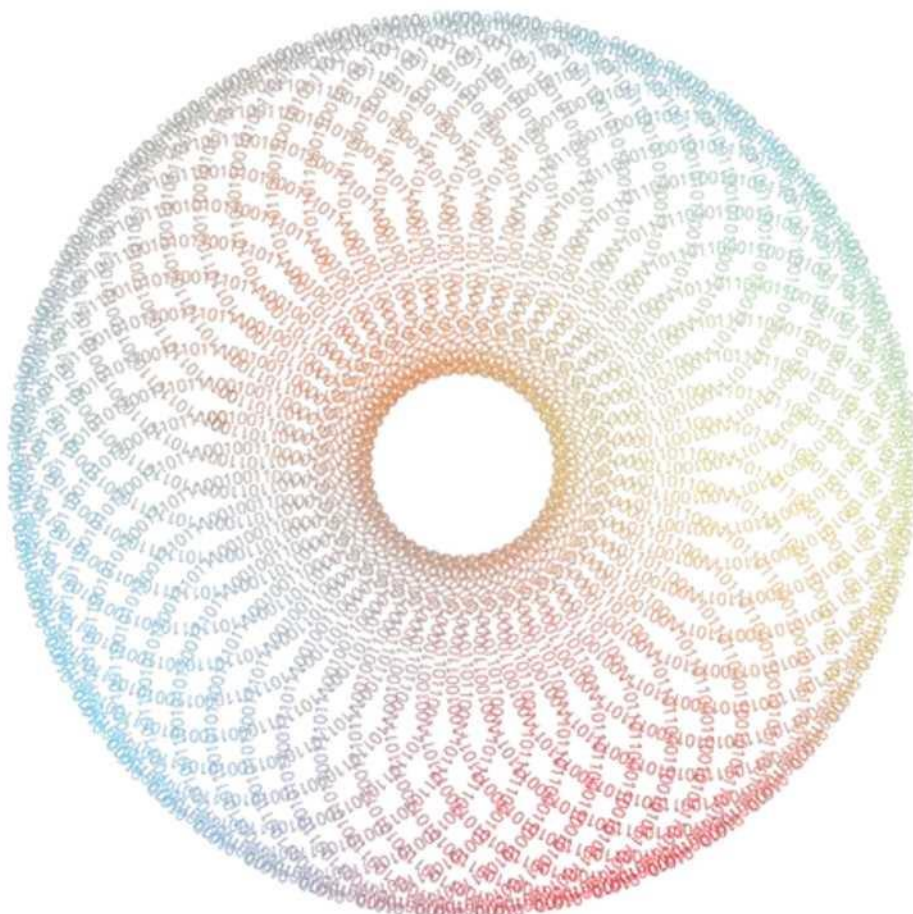
Article C : Indépendance du Prestataire

Le Prestataire exerce son activité sans aucun lien de subordination à l'égard du Client, en tant que prestataire indépendant. Il jouit de l'indépendance propre à toute entreprise dans l'organisation de son activité.

Il organise par conséquent ses activités librement et en supporte tous les frais.

Le(s) intervenant(s) du Prestataire demeurent sous sa seule autorité hiérarchique et disciplinaire.

Le Prestataire s'engage à ne pas consacrer l'ensemble de ses ressources à l'exécution de ses obligations au titre des Services et conserve toute faculté pour assurer la diversification de sa clientèle ou accroître sa part de marché notamment pour ce type de prestation ; il lui appartient de faire le nécessaire en ce sens afin notamment d'éviter toute situation pouvant l'amener à dépendre principalement de l'activité du Client.



Règles d'Usage des Technologies de l'Information et de la Communication
Applicables aux fournisseurs, prestataires et sous-traitants de Deloitte
Octobre 2018

| | |
|--|-----------|
| <u>1. Introduction</u> | 5 |
| <u>2. Statut du document</u> | 5 |
| <u>2.1 Les Règles d'Usage TIC tendent ainsi :</u> | 6 |
| <u>2.2 Champ d'application des Règles d'Usage TIC</u> | 6 |
| <u>2.3 Application des Règles d'Usage TIC</u> | 6 |
| <u>3. Règles d'utilisation des ressources TIC</u> | 7 |
| <u>3.1 Règles générales</u> | 7 |
| <u>3.2 Règles particulières d'utilisation quotidienne des ressources TIC</u> | 10 |
| <u>3.3 Mesures de sécurité</u> | 15 |
| <u>4. Mesures de contrôle</u> | 16 |
| <u>4.1 Respect de la vie privée et finalités du contrôle</u> | 16 |
| <u>4.2 Mesures générales de contrôle</u> | 16 |
| <u>4.3 Mesures de contrôle de l'utilisation d'internet</u> | 17 |
| <u>4.4 Mesures de contrôle de la messagerie électronique</u> | 17 |
| <u>4.5 Mesures de contrôle du trafic téléphonique</u> | 17 |
| <u>4.6 Mesures d'individualisation et sanctions</u> | 18 |
| <u>4.7 Mesures de contrôle en fin d'intervention ou de contrat de prestation</u> | 18 |
| <u>5. Contacts</u> | 19 |
| <u>5.1 Questions relatives à l'application des Règles d'Usage TIC</u> | 19 |
| <u>6. Date d'entrée en vigueur des Règles d'Usage TIC</u> | 19 |

1. Introduction

L'ensemble des sociétés de Deloitte SAS ci-après dénommées la « Firme », met à la disposition de ses fournisseurs, prestataires ou sous-traitants autorisés ci-après dénommés les « Utilisateur(s) Externe(s) », pour l'accomplissement de leurs missions professionnelles, des Ressources relevant des Technologies de l'Information et de la Communication, ci-après dénommées les « Ressources TIC ». Ces Ressources TIC comprennent notamment : les matériels informatiques, entendus comme l'ensemble des éléments physiques employés pour le traitement des données, tels que les ordinateurs, fixes ou portables, les tablettes numériques et tout autre matériel informatique, connectique ou bureautique en ce compris des serveurs, commutateurs, câbles du réseau, fax, photocopieurs, téléphones, fixes ou portables notamment, ainsi que l'ensemble des logiciels de la Firme contenus dans ou faisant fonctionner, interopérer ou protégeant en totalité ou en partie lesdits matériels informatiques. Ces Ressources TIC permettent notamment la création, la consultation, la modification, la suppression, l'échange, la circulation, la diffusion, la duplication, la reproduction et le stockage de données, de fichiers, de bases de données, sous forme d'images, de sons, de textes, ou tous flux quelconques d'information entre les Utilisateurs internes ou externes entre eux (Intranet) ou les Utilisateurs internes ou externes et l'extérieur (Extranet).

L'utilisation des Ressources TIC est strictement professionnelle. Les Ressources TIC font partie du patrimoine de la Firme. A cet égard, toute information émise, reçue ou stockée sur les équipements informatiques et les moyens de communication mis à la disposition de l'Utilisateur Externe est et demeure la propriété de la Firme.

L'usage des Ressources TIC de la Firme obéit à des règles qui s'inscrivent dans le respect de la loi, des réglementations, de la déontologie, de la Charte Ethique et comportement professionnel, des instructions internes, des notices techniques, de la sécurité et du bon usage, gage d'efficacité opérationnelle.

L'Utilisateur Externe doit être conscient que, par sa négligence ou sa mauvaise utilisation des Ressources TIC, il fait encourir des risques et responsabilités à la Firme, à ses membres ainsi qu'à lui-même.

L'emploi par les Utilisateurs Externes de tout autre matériel non fourni par la firme relevant des TIC et utilisé à des fins professionnelles (exemples : accéder à sa messagerie professionnelle avec son ordinateur personnel, son téléphone personnel, sa tablette personnelle selon la pratique « Bring your own device », ...), qu'il appartienne à l'Utilisateur Externe ou à un tiers doit respecter les règles décrites dans la présente Charte.

2. Statut du document

Le présent document, ci-après dénommé « les Règles d'Usage TIC », précise les principales règles et

précautions que tout Utilisateur Externe doit respecter dès lors qu'il fait usage des Ressources TIC de la Firme.

Les Règles d'Usage TIC précisent les mesures de contrôle que la Firme met en œuvre pour s'assurer du respect de ces règles et précautions.

2.1 Les Règles d'Usage TIC tendent ainsi :

- A protéger la disponibilité des données et des Ressources TIC de la Firme,
- à protéger l'intégrité des données et du fonctionnement des Ressources TIC de la Firme,
- à protéger la confidentialité des données en empêchant la diffusion, non autorisée, accidentel ou non, des informations non publiques de toutes natures appartenant à la Firme ou ses clients,
- à empêcher l'intrusion dans les Ressources TIC de la Firme, de matériels et de logiciels, de données et de fichiers de nature à porter préjudice à la Firme,
- à empêcher une utilisation des Ressources TIC de la Firme non-conforme aux lois et règlements en vigueur.
- à définir les conditions d'utilisation, de mises à jour, de maintenance, de correction, de réparation des Ressources TIC de la Firme.

2.2 Champ d'application des Règles d'Usage TIC

Les Règles d'Usage TIC concernent tous les Utilisateurs Externes et à ce titre doivent être communiquées à chacun avant d'accéder aux ressources TIC.

Est considéré comme « Utilisateur Externe » toute personne en contrat de prestation ou de sous-traitance avec Deloitte ou réalisant des prestations/missions d'un commun accord avec la Firme et tout salarié ou sous-traitant d'une société en contrat avec Deloitte ou réalisant des prestations/missions d'un commun accord avec la Firme et qui est amené à utiliser les Ressources TIC pour toute action de consultation, de création, de modification ou de suppression de données.

Les Règles d'Usage TIC sont mises à la disposition des Utilisateurs Externes sur l'Intranet de la Firme.

A son arrivée, chaque Utilisateur Externe est invité à prendre connaissance des Règles d'Usage TIC en consultant l'Intranet de la Firme.

2.3 Application des Règles d'Usage TIC

En qualité d'Utilisateur Externe des Ressources TIC de la Firme, chaque Utilisateur Externe s'engage à connaître et à appliquer l'ensemble des dispositions décrites dans ce présent document.

La Firme s'engage, pour sa part, à mettre en œuvre les moyens appropriés, compte tenu de l'état de la technique, afin de garantir la sécurité des Ressources TIC mises à la disposition des Utilisateur Externes.

3. Règles d'utilisation des ressources TIC

3.1 Règles générales

3.1.1 Accès au système d'information

Le contrôle de l'accès aux Ressources TIC permet d'identifier toute personne utilisant tout support informatique permettant d'accéder à ces mêmes ressources. Cette identification permet, à chaque connexion, l'attribution de droits propres à chaque Utilisateur Externe sur les ressources TIC dont il a besoin pour son activité professionnelle.

3.1.1.1 Accès par identifiant unique

Lorsqu'un identifiant nominatif est attribué à un Utilisateur Externe ; il sera unique pour toute la durée de sa prestation prévue au contrat que son employeur a établi avec la firme. L'Utilisateur Externe devra définir son mot de passe lors de sa première connexion au réseau de la Firme. Il est seul et personnellement responsable de l'utilisation qui peut en être faite et ne doit en aucun cas le communiquer à qui que ce soit (un collègue, binôme, tiers y compris les proches), ni les noter sur un document.

3.1.1.2 Accès par identifiant partagé

Pour certaines prestations de service, la DSI confie un compte partagé qui peut être utilisé par plusieurs Utilisateurs Externes. Le mot de passe est défini et confié au prestataire qui transmet de façon sécurisé le mot de passe qui ne doit en aucune façon être écrit. Chacun est responsable individuellement de l'utilisation faite du compte et du mot de passe.

En cas d'oubli de mot de passe, seule la Firme peut permettre à l'Utilisateur Externe d'en disposer d'un nouveau. La Direction des Systèmes d'Information communiquera un mot de passe temporaire à l'Utilisateur Externe qui en fait la demande pour lui permettre de saisir son nouveau mot de passe personnalisé dès la première connexion au réseau de la Firme.

Dans le cas d'un identifiant partagé, l'Utilisateur Externe a la charge et la responsabilité de le transmettre de façon sécurisée aux autres.

Le mot de passe réseau ainsi que l'ensemble des mots de passe nécessaires à l'accès aux ressources TIC doivent être modifiés selon une fréquence déterminée par la Firme. Les mots de passe doivent respecter les caractéristiques définies par la Firme. Ils ne doivent pas être, notamment, identiques à l'identifiant, même en inversant les caractères, comporter le nom et/ou prénom de l'Utilisateur Externe ou de membres de sa famille, le numéro de téléphone ou toute référence à quelque chose appartenant à l'Utilisateur Externe pour éviter leur découverte. La politique de mot de passe est disponible sur l'Intranet de la firme.

La Firme se réserve le droit de retirer l'ensemble des ressources TIC ainsi que l'accès aux données dans l'hypothèse d'une rupture du contrat à venir, pour quelque raison que ce soit et sans préavis.

3.1.2 Protection des données personnelles

La Firme et les Utilisateurs externes s'engagent à respecter la législation et la réglementation applicables en matière de protection des Données Personnelles, notamment le Règlement (UE) 2016/679 du Parlement européen 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 (ci-après dénommé le « **RGPD** »), ainsi que la loi n°78-17 du 6 janvier 1978 dans sa dernière version en vigueur (ci-après dénommés ensemble la « **Règlementation applicable en matière de protection des Données Personnelles** »). Les termes commençant par une majuscule au sein du présent article ont le sens qui leur est attribué par le RGPD.

La Firme traitera les Données Personnelles qu'elle collecte en tant que Responsable du Traitement et s'assurera de la base légale de Traitement des Données Personnelles de ses collaborateurs, associés et des Utilisateurs Externes.

La Firme prend des mesures techniques et organisationnelles appropriées pour protéger les Données Personnelles contre la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à de telles Données et ce compte tenu de l'état de l'art et de la technique, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du (des) Traitement (s) de Données Personnelles, mais également des risques, dont le degré de probabilité et de gravité varie, pour la protection des droits et libertés des personnes physiques.

Dans l'hypothèse où des Données Personnelles seraient transférées hors de l'Union Européenne dans un pays considéré par la Commission Européenne comme n'assurant pas un niveau de protection adéquat des Données Personnelles, la Firme mettra en œuvre l'un ou l'autre des dispositifs suivants : (i) signature d'un contrat conforme aux clauses contractuelles types adoptées par la Commission Européenne (« **Clauses contractuelles types** »), (ii) mise en place de règles internes d'entreprise contraignantes (« **Binding Corporate Rules** » ou « **BCR** »), ou (iii) tout autre dispositif de protection conforme à la Réglementation applicable en matière de protection des Données Personnelles.

L'Utilisateur Externe dès lors qu'il traite des Données Personnelles de collaborateurs, associés ou clients de la

Firme doit se mettre en conformité avec la Réglementation applicable en matière de protection des Données Personnelles, notamment tenir le registre des traitements mis en œuvre dans le cadre du contrat de prestation à disposition de Deloitte, collaborer au titre des analyses d'impact, informer sans délai Deloitte en cas de violation de données.

Pour satisfaire à ses obligations légales et réglementaires, la Firme pourrait être tenue de communiquer les Données Personnelles des Utilisateurs Externes à des autorités judiciaires ou administratives légalement habilitées.

Par principe, il est interdit à tout Utilisateur Externe de collecter et de traiter des Données Personnelles sensibles c'est-à-dire qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci.

Chaque Utilisateur Externe peut contacter le DPO pour toute question concernant la politique de protection des Données Personnelles mise en œuvre par la Firme, à l'adresse suivante : dpo@deloitte.fr

3.1.3 Règles d'interdiction générales

L'Utilisateur Externe est responsable de l'usage qu'il fait des Ressources TIC de la Firme dans l'exercice de sa mission. Cet usage s'effectue dans le respect des règles techniques applicables et des normes définies par la Firme.

L'Utilisateur Externe utilise les Ressources TIC pour son activité professionnelle. L'usage personnel des Ressources TIC est interdit.

Il est strictement interdit d'utiliser les Ressources TIC de la Firme en vue, notamment, de :

- La diffusion d'informations confidentielles relatives à la Firme, à ses membres et à ses partenaires commerciaux, sauf dans le cadre strict de la réglementation et du contrat de prestation, dans le respect des règles de protection de l'information définies par la firme.
- Le téléchargement, le stockage, l'utilisation ou encore la transmission de programmes, logiciels ou données protégés par les droits de la propriété intellectuelle sauf à disposer des autorisations ou des droits d'usage nécessaires.
- La participation à une activité professionnelle autre que celle exercée au titre du contrat de prestation.
- La diffusion d'informations ou de propos de nature à porter préjudice à l'image de la Firme ou de ses partenaires commerciaux.
- Le stockage, la consultation, l'envoi ou la réception délibérés de logiciels, programmes, fichiers, vidéo, images ou messages électroniques ou vocaux dont le contenu est susceptible d'être illégal ou d'être contraire à l'ordre public ou aux bonnes mœurs ou de porter atteinte à la dignité d'autrui. Il est notamment strictement interdit d'envoyer des messages ou de consulter des sites ou encore de publier des contenus à caractère érotique, pornographique, pédophile, révisionniste ou prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, de la race ou de l'origine nationale ou ethnique ou des convictions politiques ou religieuses d'une personne ou d'un groupe de personnes.
- L'utilisation à des fins de diffamation, harcèlement, menace ou d'injure.
- L'achat ou la location de biens ou de services aux frais de la Firme, sans l'accord préalable et écrit de ses responsables autorisés.
- L'utilisation dans le cadre d'une activité illégale, quelle qu'elle soit.

3.1.4 Sanctions concernant les règles d'interdiction générales

Le non-respect des dispositions ci-dessus engage la responsabilité de l'Utilisateur Externe et l'expose notamment de manière appropriée et proportionnée au manquement commis, à la mise en cause de sa responsabilité civile, pénale ou administrative. L'Utilisateur Externe est informé que la Firme pourra mettre fin au contrat et/ou aux prestations/missions réalisées par lui, avec effet immédiat après notification écrite - de plein droit et sans qu'aucune formalité judiciaire ne soit nécessaire -, sans préjudice de toute action que la Firme pourrait engager à l'égard de l'Utilisateur Externe et notamment

toute action en justice devant le tribunal compétent en vue d'obtenir les condamnations qui s'imposent et la réparation des dommages subis.

3.2 Règles particulières d'utilisation quotidienne des ressources TIC

3.2.1 Messagerie

La Messagerie comprend le système de messagerie électronique et celui de messagerie instantanée. L'utilisation de la Messagerie est professionnelle et s'effectue selon les normes définies par la Firme et propres à chaque activité ; règles d'envoi, de réception, de stockage et d'archivage, règles relatives aux formats et volumes des fichiers joints aux messages, etc. et disponibles sur l'intranet de la Firme.

Lorsque l'Utilisateur Externe dispose d'une adresse de Messagerie Deloitte, son utilisation doit être conforme aux modalités prescrites dans les politiques et procédures de sécurité de la firme et selon les modalités définies au contrat de prestation ou d'intervention définies au contrat du Client. L'échange d'informations par email pour le compte de Deloitte envers l'un de ses clients ou d'un tiers doit être exclusivement réalisé depuis la Messagerie Deloitte afin de garantir la confidentialité des messages. L'utilisation d'un dispositif de Messagerie publique (Gmail, Yahoo, Hotmail...) n'est pas autorisée.

La Firme répondra à toute injonction délivrée par des autorités judiciaires ou administratives.

La Firme pourra détruire tout mail envoyé ou reçu quel que soit son objet y compris s'il comporte une mention « Personnel » ou « Privé » et qui entraverait le trafic normal des messages. L'Utilisateur Externe concerné en sera préalablement informé par les administrateurs de la messagerie.

Aucun message électronique ne doit comporter d'éléments sous forme de texte, d'image, de son à caractère violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, pornographique, ou susceptible de porter atteinte au respect et à la dignité de la personne humaine et ce, tant à l'égard des autres Utilisateur Externes que de tout tiers extérieur à la Firme.

Aucun message électronique ne doit comporter d'éléments de nature à porter atteinte à l'image de la Firme et de sa clientèle.

Aucun message électronique ne doit comporter d'éléments protégés par des droits de propriété intellectuelle, autres que ceux expressément autorisés par la Firme.

Les Utilisateur Externes s'interdisent de solliciter l'envoi par d'autres utilisateurs ou par des tiers de messages comportant des éléments de cette nature et s'engagent à les détruire immédiatement s'ils sont amenés à en recevoir à leur insu.

A des fins de statistiques, de qualité de service et de sécurité, le trafic de la Messagerie est sujet à une supervision et à des vérifications et audits réguliers par la Firme, dans les limites prévues par la réglementation en vigueur. Ces opérations de contrôle sont décrites au chapitre 4.4.

3.2.2 Internet

La Firme fournit aux Utilisateur Externes l'accès à Internet à des fins professionnelles. La Firme admet une consultation non abusive de l'internet à des fins personnelles, à condition que cet usage ne perturbe pas l'accès professionnel au réseau pour tous les autres Utilisateur de la Firme et qu'il ne

constitue pas une infraction à la Loi, aux réglementations, au contrat et à aux Règles d'Usage TIC.

En aucun cas, l'accès à Internet ne pourra être utilisé à l'une des fins prohibées décrites dans les Règles d'Usage TIC.

A l'occasion de ses connexions, l'Utilisateur Externe s'interdit notamment de :

- consulter et de télécharger des contenus à caractère raciste, antisémite, xénophobe, pornographique, ou susceptibles de porter atteinte au respect et à la dignité de la personne humaine ;
- participer à des forums de discussion ou à des dialogues en direct de type « Chat » au nom de la Firme sans disposer au préalable des autorisations internes nécessaires ;
- inscrire son adresse électronique professionnelle sur des sites Internet sans liens directs avec ses fonctions et ses attributions ;
- alimenter des sites, des blogs ou des pages personnelles en contenus à caractère violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, pornographique, ou susceptibles de porter atteinte au respect et à la dignité de la personne humaine.
- télécharger des fichiers, des logiciels, progiciels, programmes protégés par les lois en vigueur sur la propriété intellectuelle, sans autorisation préalable de la Direction des Systèmes d'Information.
- déposer et échanger des contenus professionnels sur des sites non autorisés par la DSI.

La Firme pourra, de façon unilatérale, interdire l'accès à certains sites internet, sans avoir aucune justification à donner.

A des fins de statistiques, de qualité de service et de sécurité, le trafic Internet est sujet à une supervision et à des vérifications et audits réguliers par la Firme, dans les limites prévues par la réglementation en vigueur. Ces opérations de contrôle sont décrites au chapitre 4.3.

3.2.3 Intranet

La Firme met à la disposition de tous les Utilisateurs un Intranet.

L'Intranet est notamment constitué d'un réseau social d'entreprise permettant aux Utilisateur Externes :

- De partager des documents en lien avec les activités de la Firme et de publier et commenter des messages sur un « mur de discussion » accessible sur son propre profil ou sur les « murs de discussion » accessibles sur les profils d'autres Utilisateur Externes.

L'Intranet permet également aux Utilisateur Externes de consulter et visualiser un certain nombre de contenus et notamment des documents. Leur utilisation doit être limitée au strict cadre du contrat de prestation.

L'ensemble des informations contenues dans l'Intranet de la Firme et notamment, les données à caractère personnel figurant dans l'annuaire de la Firme ainsi que les documents non rendus publics et figurant dans l'Intranet revêtent un caractère confidentiel ou très confidentiel.

Aucune diffusion de ces informations en dehors de la Firme n'est autorisée sans l'accord préalable de la Direction de la Communication.

3.2.4 Internet, intranet et réseaux sociaux

Dès lors qu'il est amené à utiliser les réseaux sociaux mis à disposition par la Firme pour un usage interne ou externe et si son identification en tant que membre de la Firme y figure ou peut être déduite, l'Utilisateur Externe s'engage à respecter les règles de bonne conduite ci-dessous :

3.2.4.1 Respect de l'audience

Lors de l'utilisation des réseaux sociaux et communautés virtuelles, l'Utilisateur Externe sera attentif à la façon dont il se présente et à la façon dont il communique. Il pourra exprimer ses points de vue et affirmer sa personnalité mais en veillant à toujours respecter son audience et rester fidèle à l'image de la firme.

3.2.4.2 Honnêteté, transparence, responsabilité

Lors de l'utilisation des médias sociaux de la Firme à usage interne ou externe, l'Utilisateur Externe s'interdira de participer de façon anonyme ou sous un pseudonyme, sauf s'il lui en est fait spécifiquement la demande, par exemple : pour une enquête. Il s'exprimera toujours à la première personne.

S'il se retrouve dans une situation de conflit d'intérêts¹, il devra le préciser immédiatement.

L'Utilisateur Externe est responsable de ce qu'il publie ou édite quel que soit le média utilisé. Il devra notamment s'assurer que l'ensemble des contenus qu'il publie sont libres de tout droit² (image, vidéo, articles ...). En cas d'utilisation de contenus associés à la marque Deloitte (logo, images, vidéos, écrits...), il devra au préalable obtenir l'autorisation de la Direction de la communication.

En cas d'autorisation accordée par la Direction de la Communication, L'Utilisateur Externe devra reproduire le(s) logo(s) de la Firme de façon claire et visible et sans altération, c'est-à-dire dans un strict respect des libellés, proportions, graphismes et couleurs définis dans la charte graphique de la Firme. Dans ce cadre, le droit d'usage est consenti à titre gratuit, précaire et non exclusif.

L'Utilisateur Externe veillera à mesurer la portée des contenus qu'il publie et les conséquences inattendues liées à leur durée de vie prolongée sur Internet. C'est pourquoi, il s'obligera à les nettoyer régulièrement.

L'Utilisateur Externe devra s'assurer que l'utilisation qu'il fait des médias sociaux est compatible avec la façon dont il souhaite être perçu au sein de la Firme et en dehors de la Firme.

S'il a la moindre hésitation avant de publier un contenu, l'Utilisateur Externe ne devra pas hésiter à en discuter avec la personne la plus appropriée au sein de la Firme pour éviter toute erreur. S'il ne sait pas identifier cette personne, il pourra s'adresser à la Direction de la Communication.

S'il commet des erreurs dans les contenus qu'il produit, l'Utilisateur Externe devra les reconnaître et

¹ Un **conflit d'intérêts** apparaît quand un individu ou une organisation est impliqué dans de multiples intérêts, l'un d'eux pouvant mettre en péril l'intégrité de la motivation à agir. En cas de doute, il convient de consulter l'article 6.1 de la Charte.

² Article L122-4 du Code de la propriété intellectuelle :

« Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque. »

les corriger rapidement.

3.2.4.3 Un usage à vocation professionnelle et à valeur ajoutée

Les médias sociaux de la Firme à usage interne ou externe doivent permettre :

- d'aider les collaborateurs et les clients de la Firme à trouver des solutions ;
- d'accroître le savoir et les compétences ;
- d'améliorer les services et les processus de Deloitte ;
- de renforcer la communauté "Deloitte" et le partage du savoir.

3.2.5 Téléphones & télécopieurs

La Firme peut mettre des téléphones fixes et des téléphones logiciels (Skype For Business) et des télécopieurs à la disposition des Utilisateurs Externes dans le cadre de leur mission. Ces téléphones doivent être utilisés dans le respect des normes définies par la Firme.

La Firme admet toutefois l'utilisation des téléphones fixes et téléphones logiciels à des fins personnelles dans le cadre des nécessités de la vie courante et familiale, à condition que cet usage exceptionnel, n'entrave en rien la sécurité de la Firme et qu'il ne constitue pas une infraction aux dispositions légales et réglementaires et aux Règles d'Usage TIC.

A des fins de statistiques, de qualité de service, de sécurité et de suivi des dépenses, l'utilisation des téléphones fixes et téléphones logiciels et des télécopieurs est sujet à une supervision et à des vérifications et audits réguliers par la Firme, dans les limites prévues par la réglementation en vigueur. Ces opérations de contrôle sont décrites au chapitre 4.5.

3.2.6 Matériels, programmes et logiciels

La Firme met à la disposition de l'Utilisateur Externe des Ressources TIC pour exercer sa mission conformément aux prescriptions définies par la Firme, ci-après dénommées « Standards ».

L'utilisation des matériels, programmes et logiciels de la Firme doit être effectuée conformément aux Standards. L'Utilisateur Externe s'interdit de modifier d'une façon quelconque ces Standards.

Les Matériels, programmes et logiciels mis à la disposition des Utilisateurs Externes doivent être utilisés à titre professionnel. Les fichiers et dossiers créés à partir de ces matériels, programmes et logiciels doivent avoir un caractère professionnel de sorte que la Firme peut y avoir accès hors sa présence.

Une utilisation privée des matériels, programmes et logiciels de la Firme n'est pas autorisée.

L'Utilisateur Externe s'interdit d'utiliser les matériels, programmes et logiciels en violation des droits de la Firme et des tiers notamment, au regard des lois et réglementations en vigueur notamment sur la propriété intellectuelle.

Il est donc notamment interdit à l'Utilisateur Externe :

- de contourner ou de tenter de contourner les mesures techniques de protection des logiciels et des programmes appartenant à la Firme ou qui lui sont concédés par des licences d'utilisation ;

- d'effectuer des copies permanentes ou temporaires des logiciels et des programmes appartenant à la Firme ou qui lui sont concédés par des licences d'utilisation sur quelque support d'enregistrement que ce soit ;
- de diffuser auprès de tiers les logiciels et programmes appartenant à la Firme ou qui lui sont concédés par des licences d'utilisation ; de modifier les programmes et logiciels appartenant à la Firme ou qui lui sont concédés par des licences d'utilisation.

Seule la Direction des Systèmes d'Information de la Firme est autorisée à effectuer des copies de sauvegarde des logiciels et programmes utilisés par la Firme ou d'effectuer des modifications ou des corrections sur ceux-ci dans les conditions fixées par l'article L.122-6-1 du Code de la propriété intellectuelle.

Chaque Utilisateur Externe dispose d'un droit d'accès qui est propre aux Ressources TIC de la Firme et qui est conditionné par la mission qu'il exerce pour la Firme. L'Utilisateur Externe s'interdit donc d'accéder ou de tenter d'accéder à des dossiers ainsi qu'à des fichiers contenus dans les Ressources TIC de la Firme, pour lesquels il ne bénéficie pas des droits d'accès correspondants.

A ce titre, l'Utilisateur Externe est averti que l'intrusion non autorisée dans les Ressources TIC de la Firme peut être considérée comme une infraction au sens de l'article 323-1, alinéa 1 du Code pénal.

La firme interdit l'utilisation d'ordinateur personnel pour le traitement d'information appartenant à Deloitte ou à l'un de ses clients. Le stockage et l'archivage sur support numérique de données professionnelles appartenant à Deloitte ou à l'un de ses Clients doit respecter les politiques de sécurité et particulièrement la politique de classification. L'utilisation d'ordinateurs personnels dans les locaux de Deloitte est interdite. Deloitte met à disposition des Utilisateurs Externes, un réseau WIFI pour invités afin qu'ils puissent utiliser un téléphone personnel ou une tablette.

L'utilisation d'un ordinateur public pour réaliser des tâches professionnelles n'est pas autorisée.

3.2.7 Introduction de nouveaux Matériels, programmes et logiciels

Toute introduction de nouveaux Matériels, programmes, logiciels dans les Ressources TIC de la Firme nécessite une autorisation préalable de la Direction des Systèmes d'Information de la Firme.

L'Utilisateur Externe s'interdit donc notamment de télécharger tout programme ou élément de programme, application, "plugin" ou mise à jour à partir d'un support magnétique (CD, DVD, clés USB, disque dur externe...) ou d'un serveur Internet quelle qu'en soit la raison sans autorisation.

3.2.8 Informations, données et fichiers

L'Utilisateur Externe est responsable de la bonne conservation des fichiers, dossiers et messages qu'il utilise dans le cadre de sa mission, ainsi que des accès de lecture et de modification qu'il peut donner à d'autres personnes ou Utilisateurs Externes. A ce titre, il s'engage à :

- Identifier et protéger les informations, données et fichiers contenant des données confidentielles conformément aux modalités prescrites par le Guide Confidentialité et protection de l'information et aux règles de protection associées.

- Classer, sauvegarder et archiver les dossiers, fichiers et données selon les normes définies au sein des différentes activités et fonctions support de la Firme et selon les modalités prescrites dans le guide Confidentialité et Protection de l'information.
- Ne pas conserver de copie ou donner communication des documents, fichiers et messages qu'il aura restitués au jour de son départ, sans l'accord exprès des responsables des données autorisés de la Firme.
- Ne pas copier des données professionnelles sur un support ne présentant pas des garanties de sécurité validées par la firme.
- Ne pas transférer des données via un service online stockant les données sur le cloud ou sur internet autre que ceux autorisés par la DSI.

3.2.9 Virus informatiques et pare-feu

Le poste de travail de chaque Utilisateur Externe est systématiquement équipé de logiciels anti-virus et pare-feu installés et configurés par la Firme qui permettent de sécuriser le poste de travail et de tracer toutes les transactions. Il est strictement interdit de désinstaller ou d'altérer ce ou ces logiciels.

L'Utilisateur Externe s'interdit de télécharger ou transmettre, de façon délibérée, tout fichier contenant des virus ou des données altérées.

En cas de doutes sur la présence potentielle de virus, l'Utilisateur Externe doit stopper toute utilisation et prévenir immédiatement les services d'assistance informatique de la Firme.

3.2.10 Sanctions concernant les règles particulières d'utilisation quotidienne des ressources TIC

Le non-respect des dispositions ci-dessus engage la responsabilité de l'Utilisateur Externe et l'expose notamment de manière appropriée et proportionnée au manquement commis, aux sanctions définies par le Règlement Intérieur de la Firme lorsqu'il lui est applicable et/ou à la mise en cause de sa responsabilité civile ou pénale.

3.3 Mesures de sécurité

Dans un souci de sécurité et de préservation des Ressources TIC et conformément aux politiques de sécurité, l'Utilisateur Externe doit respecter les prescriptions définies par la Firme. Il s'engage notamment à :

- Se prémunir contre tout risque de vol ou de dégradation des Ressources TIC en respectant les consignes de sécurité en vigueur.
- Protéger les informations à caractère confidentiel ou très confidentiel dans le respect des procédures en vigueur au sein de la Firme.
- Se conformer aux instructions émises par la Firme notamment en matière de stockage et classification des données et en matière d'antivirus.
- Ne pas prêter son matériel professionnel à des personnes ne faisant pas partie de la firme, notamment à ses proches.
- Déclarer à la Firme :
 - Le vol ou la perte de matériel non fourni par la Firme relevant des TIC et utilisé à des fins professionnelles tel que par exemple le vol d'un smartphone personnel sur lequel l'Utilisateur Externe accède aux applications professionnelles.
 - Le vol ou la perte de matériel fourni par la Firme relevant des TIC.

- Tout incident conformément à la procédure de déclaration des incidents, ce sans délai.

Ces règles peuvent être consultées sur l'intranet de la Firme.

L'absence de respect des prescriptions et consignes définies par la Firme pourra être sanctionnée dès lors que les manquements observés ont nui ou sont susceptibles de nuire à la Firme.

4. Mesures de contrôle

4.1 Respect de la vie privée et finalités du contrôle

La Firme est attachée au principe du respect de la vie privée des Utilisateurs Externes sur le lieu de travail.

La Firme répondra à toute injonction délivrée par des autorités judiciaires ou administratives.

La Firme s'assure du respect par l'Utilisateur Externe de la réglementation en vigueur par la mise en œuvre des contrôles détaillés ci-après, notamment en matière de :

- Prévention et de répression de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou à l'ordre public ou de faits susceptibles de porter atteinte à la dignité d'autrui.
- Prévention et de répression des atteintes aux droits de propriété intellectuelle d'autrui³.

La Firme veille par ailleurs :

- A la protection de ses intérêts économiques, commerciaux et financiers et notamment au respect des règles de confidentialité.
- A la sécurité et au bon fonctionnement technique de ses Ressources TIC, y compris le contrôle des coûts y afférant.

Les contrôles sont effectués dans le respect des dispositions légales et réglementaires en vigueur.

4.2 Mesures générales de contrôle

Tous les fichiers, dossiers, courriers envoyés, reçus ou stockés dans les Ressources TIC de la Firme sont réputés avoir un caractère professionnel et sont la propriété de la Firme.

Aussi, à tout moment et éventuellement sans information, la Firme se réserve le droit d'examiner, supprimer ou révéler le contenu de ces fichiers.

Toutefois, il pourra être demandé à l'Utilisateur Externe la destruction des fichiers ou messages à caractère personnel qui perturberaient le bon fonctionnement ou risqueraient de mettre en péril les Ressources TIC de la Firme.

³ Article L122-4 du Code de la propriété intellectuelle : « Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque. »

Contre toutes intrusions ou malveillances, la Firme utilise des outils de sécurité de type anti-spyware, firewall, détection d'intrusion qui génèrent un reporting de l'activité sécuritaire.

4.3 Mesures de contrôle de l'utilisation d'internet

La Firme maintient automatiquement une liste générale des sites Internet consultés via son réseau, indiquant le moment et la durée des visites.

Lorsque, à l'occasion de ce contrôle général ou au départ d'autres sources d'information, la Firme constate un manquement à la Loi, la réglementation, au contrat de travail, aux Règles d'Usage TIC et aux prescriptions définies par note de service, elle se réserve le droit, dans le cadre de la poursuite des finalités décrites au point 4.1 du présent chapitre, de procéder à l'identification de l'Utilisateur Externe concerné, conformément à la procédure d'individualisation décrite au point 4.6 du présent chapitre.

Les données permettant d'identifier le poste de l'Utilisateur Externe sont conservées pendant une durée d'1 an.

Contre toute utilisation abusive d'internet, la Firme utilise des moyens de contrôle du contenu des sites internet visités et le reporting des firewalls.

La Firme se réserve le droit de bloquer, sans information préalable, l'accès aux sites dont elle juge le contenu illégal, offensant ou inapproprié par des mesures de filtrage adaptées.

4.4 Mesures de contrôle de la messagerie électronique

La Firme réalise un suivi d'indices généraux des messages tels que la fréquence, le nombre, la volumétrie, les type de pièces jointes, etc.

Les données permettant d'identifier l'émetteur des messages sont conservées pendant une durée d'1 an.

Certaines mesures de contrôle plus spécifiques portant notamment sur la volumétrie et le nombre de mails échangés pourront être prises par la Firme vis-à-vis de ces messages, dans le cadre de la poursuite des finalités décrites au point 4.1 du présent chapitre.

La Firme utilise des outils de contrôle, de reporting et d'analyse du trafic.

Si la Firme présume un usage anormal ou interdit de la Messagerie, elle procédera à l'identification de l'Utilisateur Externe concerné dans le respect de la procédure de contrôle individuel décrite au point 4.6 du présent chapitre.

4.5 Mesures de contrôle du trafic téléphonique

La Firme dispose de moyens de suivi du trafic téléphonique des postes fixes ou logiciels et des téléphones mobiles qui permettent l'enregistrement des numéros des postes appelants et des numéros de téléphone appelés.

Les données enregistrées concernent les six premiers chiffres du numéro appelant ou appelé, le jour et l'heure de l'émission ou de la réception de l'appel. Elles sont conservées pendant une durée maximale d'1 an.

Des informations synthétiques concernant les téléphones fixes et logiciels sont transmises périodiquement aux responsables de la Firme afin d'assurer le suivi des coûts.

Toutefois, si la Firme constate un usage anormal de l'utilisation du téléphone, notamment un recours abusif à des fins personnelles, elle procédera, dans le cadre de la poursuite des finalités décrites au point 4.1 du présent chapitre, à l'identification de l'Utilisateur Externe concerné, dans le respect de la procédure de contrôle individuel décrite ci-dessous.

La Firme utilise des logiciels de gestion des coûts et de reporting téléphonique.

Les informations concernant les téléphones mobiles ne sont quant à elles utilisées qu'à des fins de négociations commerciales et de vérification d'application des conditions contractuelles.

4.6 Mesures d'individualisation et sanctions

Par "individualisation", on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un Utilisateur Externe identifié ou identifiable.

La Firme pourra procéder à une individualisation de l'Utilisateur Externe en vue d'identifier l'auteur d'une transgression des règles légales, règlementaires, conventionnelles, contractuelles ou issues des procédures internes.

La Firme pourra répondre aux injonctions des autorités judiciaires et prendra les mesures appropriées vis-à-vis de l'auteur de faits ou de son employeur (cf. 3.1.4).

4.7 Mesures de contrôle en fin d'intervention ou de contrat de prestation

Lors du départ de la Firme, qu'elle qu'en soit la cause, l'Utilisateur Externe s'engage à :

- Restituer tous les matériels, documents, fichiers et messages électroniques appartenant à la Firme.
- Classer ces documents, fichiers et messages selon les normes en vigueur au sein de la Firme et à en informer les responsables autorisés au plus tard au jour où il cessera effectivement ses fonctions.
- Ne pas conserver de copie ou donner communication des documents, fichiers et messages qu'il aura restitués au jour de son départ, sans l'accord exprès des responsables autorisés de la Firme.
- Respecter les procédures de contrôle prévues au départ de la Firme.

La DSI supprimera à distance les applications et programmes contenus sur tout matériel non fourni par la Firme mais inscrit dans l'application Windows Intune et qui permettent d'accéder à des informations professionnelles selon la pratique « Bring your own device ». Cette opération sera réalisée le lendemain du départ de l'Utilisateur Externe de la Firme.

Droits de l'Utilisateur Externe

En cas de Traitement de leurs Données Personnelles par la Firme, lorsque cela est rendu possible par la Règlementation applicable en matière de protection des Données Personnelles, les Utilisateurs Externes peuvent exercer leur droit d'accès, de rectification, d'effacement, de limitation du traitement ainsi que de portabilité de leurs Données.

Pour ce faire, l'Utilisateur Externe adressera une demande écrite à la Direction des Ressources Humaines de la Firme, (FrHotlineRh@deloitte.fr) qui s'engage à lui répondre dans le mois suivant la réception de la demande.

Par ailleurs, la Firme lorsqu'elle agit en tant que Responsable du Traitement, s'engage à informer les Utilisateurs Externes dans les meilleurs délais de toute violation de leurs Données Personnelles pouvant exposer à un risque élevé leurs droits et libertés.

Les Utilisateurs Externes peuvent introduire une réclamation auprès d'une autorité de contrôle concernant le Traitement de leurs Données Personnelles.

5. Contacts

5.1 Questions relatives à l'application des Règles d'Usage TIC

Chaque Utilisateur Externe peut s'adresser à son contact Deloitte pour toute question concernant l'application des Règles d'Usage TIC. Assistance technique

Chaque Utilisateur Externe peut contacter le service d'assistance informatique de la Firme pour des questions techniques concernant l'utilisation des Ressources TIC de la Firme.

6. Date d'entrée en vigueur des Règles d'Usage TIC

Le présent document fait partie intégrante de la Politique de Sécurité de l'Information de la firme et est applicable dès la première utilisation des ressources TIC de la firme à partir du 01 octobre 2018.

Deloitte.

Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited (DTTL), société de droit anglais (« private company limited by guarantee »), et à son réseau de cabinets membres constitués en entités indépendantes et juridiquement distinctes.

DTTL (ou « Deloitte Global ») ne fournit pas de services à des clients. Pour en savoir plus sur notre réseau global de firmes membres : www.deloitte.com/about. En France, Deloitte SAS est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.

© 2023 Deloitte SAS. Membre de Deloitte Touche Tohmatsu Limited