

## **Charte de l'Utilisateur pour l'usage des Ressources Informatiques et des médias sociaux**

- 1. Statut de la Charte**
- 2. Règles d'utilisation des Ressources Informatiques**
- 3. Règles d'utilisation des médias sociaux**
- 4. Entrée en vigueur**

## **PREAMBULE**

Les sociétés du Groupe constitué par JCDecaux S.E et l'ensemble de ses filiales directes et indirectes françaises (ci-après désignées, avec JCDecaux S.E, collectivement ou individuellement l'« **Entreprise** ») mettent à disposition de leurs collaborateurs et de certains tiers des Ressources Informatiques nécessaires à l'accomplissement de leur mission.

La présente Charte de l'utilisateur pour l'usage des Ressources Informatiques et des médias sociaux (la « **Charte** ») a pour objet de porter à la connaissance des collaborateurs de l'Entreprise et de certains tiers les informations essentielles à la bonne utilisation de ces Ressources Informatiques.

Cette charte a également pour objet de sensibiliser les utilisateurs aux possibles conséquences préjudiciables que pourraient engendrer pour eux-mêmes et l'Entreprise une utilisation abusive ou imprudente des Ressources Informatiques en termes de sécurité, confidentialité et d'intégrité.

### **Les Ressources Informatiques**

Il s'agit du système d'information et de communication de l'Entreprise, de l'ensemble des données informatisées (bases de données, images, vidéos, documents dématérialisés...), des matériels (postes de travail fixes ou portables, imprimantes, tablettes, téléphones mobiles et smartphone...), des logiciels (messagerie, logiciels « métiers », navigateur d'accès à Internet, logiciels bureautique, gestionnaires de documents dématérialisés, réseau social interne...) et des services (possibilité d'accès à Internet, stockage, partage, interaction autour des documents, communication instantanée, visio-conférence...) mis à disposition des Utilisateurs par l'Entreprise ou depuis Internet grâce à des accès sécurisés dans et en dehors des locaux professionnels.

### **L'Utilisateur**

Est considéré comme Utilisateur toute personne physique disposant d'un identifiant fourni et géré par l'Entreprise.

Cette Charte est affichée dans les sites centraux, sites secondaires et agences des différentes entités de l'Entreprise ; elle est par ailleurs disponible sur les différents sites Intranet de l'Entreprise et remise aux salariés à l'embauche.

# 1 STATUT DE LA CHARTE

## 1.1 Les objectifs de la Charte

Cette Charte a pour objectifs :

- d'exposer les principales règles et précautions d'utilisation des Ressources Informatiques et des médias sociaux, dans des conditions de sûreté, de sécurité et de confidentialité optimales ;
- de rappeler le devoir d'information auprès des Directions des Systèmes d'Information en cas d'incertitude quant à la nature des contenus ou des usages des applications ;
- de définir les responsabilités respectives de l'Entreprise et de l'Utilisateur ;
- d'informer chaque Utilisateur sur les risques encourus et les éventuelles sanctions applicables en cas d'utilisation non-conforme des Ressources Informatiques ou des médias sociaux et de non-respect de la Charte.

## 1.2 Le champ d'application de la Charte

La Charte s'impose à tous les Utilisateurs à travers le monde en fonction de la législation applicable localement, le socle commun de la Charte Internationale des Valeurs Sociales Fondamentales demeurant une référence applicable à tous les Utilisateurs. Ces derniers devront en prendre connaissance et se conformer à l'ensemble de ses dispositions.

L'ensemble des contrats conclus entre l'Entreprise et tout tiers Utilisateur (sous-traitant, client, prestataire, partenaire,...) donnant accès aux Ressources Informatiques doivent stipuler expressément que les utilisateurs externes concernés s'engagent à respecter la présente Charte, ces derniers étant dès lors considérés comme des Utilisateurs au sens de la Charte.

Cependant, dans les cas où la réglementation locale impose des règles et pratiques différentes aux Utilisateurs situés hors de France que celles énoncées dans la Charte, c'est cette réglementation locale qui sera appliquée aux Utilisateurs de l'entité de l'Entreprise dans le pays concerné. Si un principe énoncé dans la Charte n'est pas autorisé par une loi ou une réglementation locale, l'entité locale de l'Entreprise devra, dans la mesure du possible, le mettre en œuvre d'une manière compatible localement.

## 1.3 La responsabilité de l'Entreprise et de ses Utilisateurs

En cette qualité, chaque Utilisateur s'engage à connaître et à appliquer l'ensemble des dispositions de la Charte.

L'Entreprise s'engage, d'une part, à mettre à disposition des Utilisateurs des Ressources Informatiques adaptées à leurs besoins professionnels et offrant la meilleure sécurité possible et, d'autre part, à préserver l'autonomie des Utilisateurs en leur garantissant en particulier la possibilité de communiquer librement au sein de l'Entreprise dans les limites fixées dans la Charte.

En contrepartie, chaque Utilisateur doit utiliser les Ressources Informatiques sans abus et dans le strict respect de son obligation de discrétion et de secret professionnel résultant de son contrat de travail et/ou de la nature de ses fonctions.

## 1.4 Les sanctions et risques encourus

L'Utilisateur qui aura, par son action, contrevenu aux règles de bon usage, en particulier celles définies dans la Charte, peut s'exposer à des sanctions disciplinaires telles que prévues dans le Règlement intérieur de l'Entreprise. En outre, en cas d'utilisation non-conforme des Ressources Informatiques, l'Utilisateur s'expose à différents risques :

**Risques de nature pénale.** Il existe sur Internet des sites aux contenus illicites, c'est-à-dire contraires à la loi (notamment pédophilie, terrorisme, jeux d'argent illégaux, téléchargement illégal de fichiers musicaux ou de films, négationnisme historique,...). Le simple accès à ce type de site est condamné par la plupart des lois. Si ces actes sont commis au sein de l'Entreprise, la justice peut, dans de nombreux pays, poursuivre le collaborateur ainsi que l'Entreprise et son management.

**Risques concernant la sécurité.** Ne pas se plier aux règles de protection en vigueur (secret des mots de passe, protection des fichiers confidentiels, ...) accroît les risques de diffusion non-maitrisée d'informations confidentielles.

**Risques concernant le fonctionnement des Ressources Informatiques.** Utiliser de manière abusive les Ressources Informatiques (téléchargement massif de fichiers depuis Internet, envoi de messages très volumineux) peut très notablement pénaliser le travail des autres Utilisateurs et porter ainsi atteinte à l'efficacité des services.

**Dans le cas où la responsabilité de l'Entreprise et/ou de son management serait engagée, celle-ci pourra se retourner contre l'Utilisateur ayant enfreint les présentes dispositions.**

## 1.5 Le respect des règles de protection des données personnelles

**Rappel des règles applicables et des sanctions encourues en cas de non-respect.** Pour tout traitement de données personnelles (en ce compris toute collecte, accès, utilisation, modification, transmission, suppression ou autre opération effectuée sur lesdites données), l'Utilisateur s'engage à se conformer aux règles définies par la Loi Informatique et Libertés (Loi n°78-17 du 6 janvier 1978) et du Règlement Général relatif à la Protection des Données « RGPD » (Règlement (UE) 2016/679 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données).

L'Entreprise a désigné un **Délégué à la Protection des Données** dont le rôle est, notamment, d'informer et de conseiller les Utilisateurs qui procèdent à des traitements de données personnelles sur les obligations qui leur incombent. Il **doit être consulté préalablement à la mise en œuvre d'un traitement de données personnelles** et peut être contacté à l'adresse suivante : DPO\_F@jcdecaux.com.

L'Utilisateur est informé que le non-respect des termes de la Charte peut constituer un manquement aux dispositions du RGPD. Dans ce cas, l'Entreprise encourt un risque de sanction pénale (notamment pour non-respect des obligations de sécurité des données), civile (indemnisation des personnes concernées) et administrative (sanctions prononcées par la CNIL, incluant des sanctions pécuniaires pouvant s'élever jusqu'à 4% du chiffre d'affaires annuel mondial de l'Entreprise). L'Utilisateur peut également voir sa responsabilité personnelle directement engagée s'il a agi en dehors de ses fonctions sans autorisation ou des fins étrangères à ses attributions.

**Information des Utilisateurs quant au traitement de leurs données personnelles.** Les informations relatives aux traitements de données personnelles des Utilisateurs, tant au regard de la gestion de la sécurité informatique ou qu'au regard de leur qualité de collaborateurs de JCDecaux, sont communiquées dans la rubrique « Liens utiles » de l'intranet de l'Entreprise (Annexe 1 de la Charte : Information et droits des Utilisateurs : Traitement de données personnelles relatifs à la sécurité informatique et Politique de Protection des Données – Collaborateurs).

Les Utilisateurs peuvent prendre contact avec le Délégué à la Protection des Données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le RGPD.

## 1.6 Le droit à la déconnexion

En application de la loi, l'Utilisateur dispose d'un droit à la déconnexion de ses outils numériques professionnels en vue d'assurer le respect de ses temps de repos et de congé ainsi que de sa vie personnelle et familiale. Ce droit est exerçable dans le cadre d'accords collectifs d'entreprises ou autrement.

# 2 REGLES D'UTILISATION DES RESSOURCES INFORMATIQUES

## 2.1 Les règles générales d'utilisation

**L'Utilisateur** est responsable de l'usage qu'il fait des Ressources Informatiques mises à sa disposition dans l'exercice de ses fonctions au sein de l'Entreprise. Par conséquent, il **ne doit se livrer, en aucune circonstance, à l'une des activités suivantes** :

### **2.1.1 Télécharger, stocker, envoyer, transférer par courrier électronique ou de toute autre manière tout contenu illicite au sens de la loi et de la réglementation applicables**

Par « contenu illicite », on entend généralement :

- ce qui pourrait être qualifié de crime ou de délit ou d'incitation à en commettre un, d'atteinte à la vie privée, de fabrication, de transport et de diffusion de message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine ;
- tout contenu qui serait contraire à une loi en vigueur (relatifs à la pédophilie, aux ventes d'organes, aux ventes de substances illicites ou de tout autre objet et/ou prestation illicite) ou faisant l'apologie du terrorisme ou de crimes de guerre.

L'Utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous quelque forme que ce soit (information, image, vidéo, fichier...).

### **2.1.2 Utiliser les Ressources Informatiques de l'Entreprise à des fins de harcèlement, menace ou injure et, de manière générale, de violation des lois en vigueur**

### **2.1.3 Télécharger, stocker ou transférer sur des supports externes tiers à l'Entreprise des fichiers contenant des données propriété de l'Entreprise**

On entend par là des contenus propriété de l'Entreprise, qu'ils soient régulièrement utilisés ou pas par l'Utilisateur, ou qu'ils soient ou pas dans le périmètre contractuel/habituel de responsabilité/compétence de l'Utilisateur.

### **2.1.4 Télécharger, stocker ou transférer des fichiers contenant des éléments protégés par les lois sur la propriété intellectuelle**

### **2.1.5 Utiliser les Ressources Informatiques de l'Entreprise à des fins de harcèlement, menace ou injure et, de manière générale, de violation des lois en vigueur**

On entend par là :

- tout contenu dont la diffusion serait interdite par une disposition légale ou un acte juridique, notamment des informations internes, privilégiées, confidentielles apprises ou divulguées dans le cadre d'un contrat de travail ou d'un accord de confidentialité,
- tout contenu violant tout brevet, marque déposée, secret de fabrication, droit de propriété intellectuelle ou tout autre droit de propriété appartenant à autrui.
- tout programme, logiciel, progiciel, etc., qui est protégé par les lois sur la propriété intellectuelle, autres que ceux qui sont expressément autorisés par l'Entreprise.

L'Utilisateur s'interdit de solliciter l'envoi par des tiers, sous quelque forme que ce soit, de tels fichiers, programmes, logiciels, etc.

### **2.1.6 Altérer le bon fonctionnement des Ressources Informatiques**

A ce titre, il est particulièrement interdit de télécharger, afficher, transmettre par courrier électronique ou de toute autre manière tout contenu susceptible de contenir des virus informatiques ou tout autre code, dossier ou programme conçus pour interrompre, détruire ou limiter la fonctionnalité de logiciel, ordinateur ou outil de télécommunication sans que cette énumération ne soit limitative ; d'entraver ou perturber le service, les serveurs, les réseaux connectés de l'Entreprise, ou de refuser de se conformer aux conditions requises, aux procédures, aux règles générales ou aux dispositions réglementaires applicables aux réseaux connectés de l'Entreprise, d'envoyer des messages en masse à plus de 50 destinataires (hors diffusion sur des listes de l'Entreprise pour raisons de service) ou en chaîne (message reçu individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement) ; d'utiliser les Ressources de l'Entreprise de manière à gêner l'accès des autres Utilisateurs.

Certaines des activités énoncées ci-dessus peuvent constituer des infractions de nature pénale et sont susceptibles d'engager, par voie de conséquence, la responsabilité personnelle de leurs auteurs.

L'Entreprise se réserve la possibilité d'effectuer, si nécessaire, des vérifications et contrôles, dans le respect des dispositions légales et réglementaires en la matière et conformément aux conditions prévues dans le Règlement Intérieur de l'Entreprise.

## 2.2 Conditions d'accès et de sécurité

L'usage de certaines Ressources Informatiques ou le droit d'accès à ces dernières peut être soumis à un processus de validation (exemple : création d'un compte NT, droit d'accès à un dossier partagé...).

Ce droit d'accès est personnel, incessible, et n'est autorisé que dans le cadre exclusif de l'activité professionnelle des Utilisateurs.

L'Entreprise s'engage à mettre en œuvre tous les moyens pertinents afin de garantir la meilleure sécurité possible des Ressources informatiques mises à la disposition des Utilisateurs.

De son côté, chaque Utilisateur se doit de contribuer, à son niveau, à la sécurité générale et à celle l'Entreprise et s'oblige ainsi à respecter les règles suivantes :

- ne jamais « divulguer » son « compte / mot de passe » (le compte qui a été attribué et le mot de passe associé sont strictement confidentiels) ;
- ne jamais chercher à s'approprier le mot de passe d'autrui ;
- activer sans délai tout système d'authentification multi facteur (MFA) ou système équivalent ;
- ne pas valider de demande MFA ou d'un système équivalent sans en avoir identifié l'origine de la demande ;
- changer de mot de passe conformément aux règles en vigueur ;
- protéger spécifiquement les fichiers à caractère confidentiel, stratégique et/ou sensible de l'Entreprise ;
- signaler immédiatement à la Hot Line tout message apparaissant à l'écran et pouvant avoir un rapport avec un virus informatique (bien que chaque poste soit équipé d'un logiciel anti-virus, l'utilisation d'outils tels que la messagerie ou Internet, celle de supports de stockage de type CD-Rom et clés USB, peuvent, malgré les précautions prises, provoquer la transmission de virus informatiques qui risquent d'endommager gravement les données de l'Entreprise) ;
- ne pas quitter son poste de travail en laissant accessible une session ouverte, et donc verrouiller sa session avant de quitter son poste de travail ;
- ne pas laisser à disposition des supports informatiques (CD-Rom, clés USB, disque dur...) contenant des données confidentielles, dans un bureau ouvert.

**Les Utilisateurs de postes informatiques portables, quel que soit l'endroit où ils se trouvent, ont la responsabilité de sécuriser leur matériel et l'accès aux données qu'il contient.**

L'Utilisateur ne doit jamais transporter l'intégralité des fichiers qui auraient une valeur stratégique pour l'Entreprise.

Les informations et données sensibles, stratégiques ou confidentielles stockées et/ou gérées par l'Utilisateur doivent être sécurisées conformément aux directives, le cas échéant, données par la direction ou l'Entreprise dont relève l'Utilisateur.

Il appartient, par ailleurs, à chaque Utilisateur de signaler toute tentative de violation de son poste de travail ou de ses fichiers ou données, ou toute perte ou vol de son matériel, dès qu'il en a connaissance, auprès de son responsable hiérarchique ainsi que du service de support informatique, afin notamment de prendre les mesures nécessaires de sécurité.

## 2.3 L'utilisation des Ressources Informatiques

Les Ressources Informatiques mises à disposition des Usagers sont destinées à un usage professionnel dans le cadre de leurs fonctions. Toutefois, un usage personnel limité et raisonnable est toléré, dans la mesure où il ne perturbe pas le travail et ne nuit ni à la sécurité ni au fonctionnement du système d'information de l'Entreprise.

Les données, y compris personnelles, messages ou fichiers sont présumés professionnels. L'Utilisateur qui souhaite, à titre exceptionnel, faire usage des Ressources Informatiques à des fins privées doit indiquer clairement dans l'objet du message, dans le nom du fichier ou du dossier la **mention « personnel et confidentiel »**.

### **2.3.1 L'usage des listes de diffusion est strictement réservé aux utilisations professionnelles de la messagerie**

Dans ce cadre, l'utilisation des listes de diffusion telles que « Utilisateurs NT » ainsi que de celles regroupant tous les utilisateurs d'un site (agence ou site central) est strictement réservée aux services ou aux personnes responsables de diffusions périodiques d'information.

Pour les listes de diffusion « Métiers » (de type « Directeurs techniques », « R.A.R. », utilisateurs d'une application...), un propriétaire est nommé comme responsable de cette liste, et doit déterminer la liste des personnes habilitées à utiliser ces listes.

### **2.3.2 Il appartient à l'Utilisateur de ne pas effectuer des opérations pouvant nuire au bon fonctionnement de la messagerie. A ce titre, il lui appartient notamment de :**

- limiter l'envoi de messages aux seuls destinataires réellement intéressés ou concernés, et d'utiliser les plateformes d'échange de fichiers mises à disposition par l'Entreprise pour partager des fichiers volumineux pour éviter la saturation du réseau et des serveurs ;
- ne pas procéder à des envois massifs de courrier ;
- ne pas utiliser la messagerie électronique à des fins promotionnelles ou marchandes, et notamment ne pas se livrer à du « spam », à la transmission de chaînes de lettres ou de toute autre forme de sollicitation ;
- détruire les messages alarmants (non-envoyés par la Hot Line) l'invitant à une rediffusion générale de ces messages, ce qui risque d'entraîner une saturation de la messagerie ;
- (dans la mesure du possible) ne pas communiquer son adresse e-mail sur des serveurs Web qui le demanderaient (en particulier lorsqu'il s'agit de remplir un formulaire), pour éviter de l'exposer à la réception de nombreux messages publicitaires ;
- ne pas ouvrir de messages, de pièces attachées ou de cliquer sur un lien venant de personnes ou de sociétés non identifiées, pour éviter des risques de virus ou de « phishing » (hameçonnage : technique de fraude sur Internet visant à obtenir des renseignements confidentiels comme les mots de passe, les informations bancaires afin d'usurper l'identité de la victime).

Il est rappelé que les messages électroniques envoyés à l'intérieur de l'Entreprise sont sécurisés. Néanmoins, dans le cas de l'envoi de messages électroniques à l'attention de destinataires externes (sous-traitants, partenaires, clients, collectivités...), les messages transitent par Internet et peuvent donc, à tout moment, être interceptés, visualisés, enregistrés et utilisés à d'autres fins par un tiers. L'Utilisateur se doit donc de prendre des dispositions particulières en lien avec sa Direction des Services Informatiques afin d'échanger en toute sécurité avec des tiers des fichiers contenant des informations sensibles (données à caractère personnel, financières, stratégiques, commerciales...).

L'utilisation de services de messagerie électronique (comme Gmail, Yahoo Mail, Orange Mail...) autres que ceux fournis par l'Entreprise ou l'utilisation de son adresse de messagerie personnelle à des fins d'échanges professionnels sont interdites.

L'Utilisateur doit être vigilant à ne pas écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie, etc.), car ce message pourrait :

- être stocké, réutilisé, exploité à des fins auxquelles l'Utilisateur n'aurait pas pensé en le rédigeant ;
- constituer une preuve ou un commencement de preuve par écrit.

**Le non-respect de ces dispositions expose l'Utilisateur à d'éventuelles sanctions disciplinaires figurant dans le Règlement intérieur de l'Entreprise.**

## **2.4 L'usage d'Internet**

**L'accès à Internet est mis à la disposition de l'Utilisateur à titre professionnel et individuel.**

Sont ainsi notamment constitutifs d'abus sanctionnables par des mesures disciplinaires et/ou des poursuites judiciaires les visites de sites à caractère pornographique, pédophiles, racistes, antisémites ou négationnistes, de jeux, de sport, la participation à des forums de discussion sans lien direct avec l'activité professionnelle, ainsi que les téléchargements de musique et de vidéo.

Toutes les activités de l'Utilisateur sur Internet ainsi que les données le concernant (sites consultés, cookies, messages échangés, données fournies à travers des formulaires, données collectées à l'insu de l'utilisateur,

etc.) peuvent être, à son insu, enregistrées par des tiers, analysées pour en déduire ses centres d'intérêt, les préoccupations de l'Entreprise, etc., et utilisées à des fins commerciales ou autres. L'utilisation de services de partage ou de stockage de fichiers (comme Google Drive, Dropbox, WeTransfer...) autres que ceux fournis par l'Entreprise à des fins d'échanges professionnels est interdite.

Par ailleurs et avant tout téléchargement, l'Utilisateur doit, dans la mesure du possible, s'assurer de la fiabilité et de la notoriété du site sur lequel il a trouvé le document.

L'accès à Internet à des fins personnelles est toléré dans le cadre d'une utilisation limitée et raisonnable ne nuisant pas au temps de travail de l'Utilisateur, au bon fonctionnement des Ressources informatiques et respectant les conditions ci-dessus.

## **2.5 Les informations, données et fichiers**

L'Entreprise est responsable de :

- la mise à disposition de Ressources Informatiques sécurisées conformes aux règles juridiques et techniques applicables et aux prescriptions définies par l'Entreprise (standards) ;
- la maintenance technique des Ressources Informatiques et leur sécurisation.

L'Utilisateur est responsable de la pérennité de ses fichiers, données, informations, etc. Il est également garant des accès de lecture et de modification qu'il peut donner à d'autres personnes ou Utilisateurs et s'engage à respecter les consignes de sécurité.

## **2.6 L'usage des matériel et logiciels**

L'Entreprise met à la disposition de l'Utilisateur des outils informatiques et des équipements (PC fixe ou portable, station, serveur, téléphone, smartphone, etc.) pour exercer son activité professionnelle. Ces matériels et ces logiciels sont conformes aux normes juridiques et techniques applicables et aux prescriptions définies par l'Entreprise (standards).

Il est formellement interdit de modifier ces standards, notamment par l'ajout de logiciels hors standards pour lesquels l'Entreprise pourrait être accusée de piratage ou contrefaçon, ou qui pourraient perturber le bon fonctionnement des Ressources Informatiques

Il est formellement interdit de souscrire à un service en ligne (y compris SAAS), gratuit ou non, sans validation préalable de la Direction Informatique et de la Direction Juridique.

Le non-respect de ces dispositions expose l'Utilisateur à d'éventuelles sanctions disciplinaires figurant dans le Règlement intérieur de l'Entreprise.

## **2.7 Les contrôles**

Pour des nécessités de maintenance, de gestion technique, de sécurité et de contrôle de la bonne application de la présente Charte, les Ressources Informatiques peuvent être analysées et contrôlées dans le respect de la législation applicable.

Ces opérations d'analyse et de contrôle sont effectuées par le personnel habilité ou par le Directeur des Systèmes d'Information habilité, dans le respect de la confidentialité et de la vie privée des salariés sur leur lieu de travail, et peuvent avoir notamment pour objet :

- de compresser les fichiers trop volumineux ou de les supprimer avec préavis et, plus généralement, de prendre toutes les dispositions permettant de garantir le bon fonctionnement des outils et l'intégrité des données ;
- d'analyser le contenu des messages et fichiers afin de procéder à des vérifications anti-virus ainsi qu'à un contrôle « anti-spam » ;
- de mettre en œuvre les moyens nécessaires pour faire respecter le droit relatif aux contenus illicites, notamment par filtrage de l'accès aux sites Internet à contenu illicite et/ou contraires aux bonnes mœurs ou par filtrage des messages électroniques à contenu suspect ;
- d'établir des diagnostics en cas de dysfonctionnement ;
- d'évaluer l'impact de nouveaux outils ou de nouvelles pratiques.

Dans les limites légales et réglementaires applicables, ces contrôles ne peuvent porter sur les données personnelles (messages électroniques ou fichiers) émises et reçues par les salariés, identifiées et classées par ces derniers comme telles, dans un dossier personnel, portant clairement en objet la mention « personnel et confidentiel ».

Les administrateurs de réseaux et systèmes de l'Entreprise sont tenus à obligation de discrétion et de secret professionnel et ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des Utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'Entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

L'Entreprise se réserve le droit de pouvoir s'assurer à tout moment du contenu des équipements (PC, portable, smartphone,...) mis à la disposition de l'Utilisateur, dans le respect des dispositions légales et réglementaires en la matière et conformément aux conditions de vérification prévues dans le Règlement Intérieur de l'Entreprise.

Dans l'hypothèse où, à l'occasion d'opérations d'analyse et de contrôle, des éléments objectifs seraient de nature à établir une utilisation abusive, la Direction pourrait évaluer avec l'Utilisateur si son utilisation du matériel informatique a été conforme à la Charte, notamment si ces contrôles devaient révéler que des sites ont été visités en infraction avec cette dernière. L'Entreprise se réserve le droit d'identifier l'ordinateur au départ duquel ces visites ont été effectuées, d'entendre l'Utilisateur à ce propos et, le cas échéant, de le sanctionner.

### **3 REGLES D'UTILISATION DES MEDIAS SOCIAUX**

#### **3.1 Principes généraux**

On entend par « médias sociaux » l'ensemble des sites et plateformes web qui proposent des fonctionnalités dites « sociales » aux utilisateurs :

- création collaborative de contenus (sites Web) ;
- échange d'information entre individus (forums, blogs ouverts aux commentaires, etc.) ;
- partage de contenus (articles, photos, vidéos, messages...).

Dans le cadre de l'utilisation de ces médias sociaux, chaque Utilisateur s'engage à respecter la Charte dès lors qu'il y est question notamment de l'Entreprise, de ses salariés, de ses clients ou de ses activités.

#### **3.2 Protection des informations confidentielles**

Dans le cadre de l'utilisation des médias sociaux, l'Utilisateur ne doit pas partager d'informations sensibles, confidentielles ou stratégiques relatives à l'Entreprise, ses clients, ses partenaires, ses fournisseurs, des tierces parties ou encore ses salariés.

Toute utilisation ou diffusion via les médias sociaux d'images ou de vidéos disponibles sur les plateformes de partage internes à l'Entreprise (Bee, Mediacenter, Alexandria...) doit avoir fait l'objet d'une communication à l'externe de l'Entreprise voire, dans certains cas, (campagne publicitaire, design des mobiliers urbains en cours de création, ...) de la validation expresse préalable de la Direction de la Communication du Groupe.

#### **3.3 L'image et la réputation de JCDecaux**

Dans l'utilisation d'un média social, l'Utilisateur doit exprimer ses avis et ses opinions en son nom propre, et non au nom de l'Entreprise, afin d'éviter toute confusion entre sa position et celle de l'Entreprise.

En outre, toute photo, image et/ou vidéo du lieu de travail ou prise(s) sur le lieu de travail, contenu ou propos dénigrant, insultant ou diffamatoire, et qui serai(en)t de nature à nuire à la réputation de l'Entreprise, de ses salariés, clients, fournisseurs, prestataires ou partenaires est (sont) strictement interdit(es) et est (sont) passible(s) de sanctions disciplinaires telles que prévues par le Règlement Intérieur.

### **3.4 Le respect d'autrui**

Dans un environnement international complexe d'un point de vue légal, opérationnel, commercial et social, l'Utilisateur s'engage à respecter une éthique professionnelle ainsi qu'à observer la Charte Ethique Groupe et la Charte Internationale des Valeurs Sociales Fondamentales applicables au sein de l'Entreprise.

Ainsi, l'Utilisateur d'un média social s'engage à ne pas publier de contenus insultants, diffamatoires, menaçants ou discriminatoires en ligne.

## **4 ENTREE EN VIGUEUR**

La présente Charte entre en vigueur après l'accomplissement de toutes les formalités requises.

Les Utilisateurs sont informés de l'existence et du contenu de la présente Charte par voie d'affichage et sur le réseau social interne Bee.

En outre, tout nouvel embauché au sein de l'Entreprise se verra remettre un exemplaire de la présente Charte.

**Pour toute question relative à cette Charte et ses dispositions,  
n'hésitez pas à vous rapprocher de votre interlocuteur Ressources Humaines habituel,  
présent au sein de votre entité de travail JCDecaux.**

## Annexe 1 – Information et droits des Utilisateurs : Traitement de données personnelles relatifs à la sécurité informatique

JCDecaux SE, RCS Nanterre B 307 570 747), 17 rue Soyer, 92200 Neuilly-sur-Seine, est le responsable des traitements de données à caractère personnel concernant les Utilisateurs détaillés ci-après :

N°	Finalité	Base légale	Données traitées	Durée de conservation	Destinataires
1	<b>Détection des incidents</b> de sécurité informatique, à l'exclusion du contrôle individuel de l'activité des Utilisateurs	Intérêt légitime à sécuriser les Ressources Informatiques par la détection d'incidents de sécurité informatique	Civilité, nom, prénom, adresse électronique professionnelle, adresse IP, identifiants de connexion, adresses des sites Internet consultés, applications utilisées, date et heure de chaque événement collecté, adresse MAC, nom de machine, localisation indiquée par l'adresse IP.	six (6) mois à compter de la date de réalisation de l'évènement traité par le dispositif	personnes habilitées au sein des équipes de la DSI de JCDecaux SE sous-traitants techniques qui fournissent le dispositif de détection d'incidents et qui sont en charge du traitement d'un incident et/ou de l'hébergement du dispositif et de la sécurité des postes de travail
2	<b>Protection de la messagerie</b> et des messages	Intérêt légitime à sécuriser les Ressources Informatiques par la protection des emails contre des menaces informatiques	Email du ou des destinataire(s) et de l'expéditeur, identifiants uniques, contenu des emails et des pièces jointes, métadonnées.	[à compléter] à compter de [à compléter]	personnes habilitées au sein des équipes de la DSI de JCDecaux SE au sous-traitant technique qui fournit le dispositif de détection d'incidents
3	<b>Contrôle d'accès à Internet</b>	Intérêt légitime à sécuriser les Ressources Informatiques par le contrôle d'accès à Internet	Nom de l'Utilisateur, identifiant de l'ordinateur, date et heure de la consultation du site Internet, adresse du site Internet consulté (URL), taille de la page et des éléments consultés	[à compléter] à compter de [à compléter]	personnes habilitées au sein des équipes de la DSI de JCDecaux SE au sous-traitant technique qui fournit le dispositif de contrôle d'accès à Internet
4	<b>Accès au VPN</b>	Intérêt légitime à sécuriser les Ressources Informatiques par le contrôle d'accès à Internet	Login de l'utilisateur, identifiant de l'ordinateur, adresse IP publique	six (6) mois à compter de la date de réalisation de l'évènement traité par le dispositif	personnes habilitées au sein des équipes DSI
5	Préparation, exercice et suivi d'une <b>procédure disciplinaire et/ou judiciaire</b>	Intérêt légitime de mener une procédure disciplinaire et/ou de se défendre ou d'agir dans le cadre d'une procédure judiciaire	Les données issues des traitements 1) à 4) susceptibles de prouver le manquement d'un collaborateur	Durée de la procédure disciplinaire et/ou judiciaire, puis durée de prescription légale ou délai de recours	dans les limites de leurs attributions et dans le cadre de leurs fonctions, les collaborateurs de l'Entreprise habilités à préparer, exercer et suivre des procédures disciplinaires et/ou des procédures judiciaires impliquant un Utilisateur auxiliaires de justice et officiers ministériels l'autorité saisie d'un litige

Dans le cadre des traitements 1) à 4), les données peuvent être transférés aux Etats-Unis d'Amérique. JCDecaux s'engage, conformément au RGPD, à assurer un niveau de protection adéquat des données personnelles, notamment par la mise en place de clauses contractuelles types approuvées par la Commission Européenne. L'Utilisateur peut obtenir une copie de ces clauses en s'adressant au DPO : par email : DPO\_F@jcdecaux.com - par courrier : JCDecaux France – Service DPO – 17 rue Soyer 92200 Neuilly sur Seine.

L'Utilisateur dispose d'un certain nombre de droits concernant le traitement de ses données personnelles, et en particulier :

- **Le droit d'être informé** : L'Utilisateur a le droit d'être informé d'une façon concise, transparente, compréhensible et aisément accessible de la manière dont ses données personnelles sont traitées.
- **Le droit d'accès** : L'Utilisateur a le droit d'obtenir (i) la confirmation que ses données personnelles sont ou ne sont pas traitées et, lorsqu'elles le sont, d'obtenir (ii) une copie de ces dernières.
- **Le droit de rectification** : L'Utilisateur a le droit d'obtenir la rectification des données personnelles le concernant qui sont inexactes, incomplètes ou pas à jour.
- **Le droit à l'effacement** : Dans certains cas, l'Utilisateur a le droit d'obtenir l'effacement de ses données personnelles. Ce droit n'est cependant pas un droit absolu dans la mesure où JCDecaux SE peut avoir des raisons légales ou légitimes de conserver lesdites données.
- **Le droit à la limitation du traitement** : Dans certains cas, l'Utilisateur a le droit d'obtenir la limitation du traitement de ses données personnelles. Cela signifie que le traitement des données personnelles de l'Utilisateur par JCDecaux SE sera limité, de sorte que JCDecaux SE pourra conserver ces données, mais ne pourra les utiliser ni les traiter autrement.
- **Le droit d'opposition** : L'Utilisateur a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, au traitement de ses données personnelles. JCDecaux SE peut cependant invoquer des motifs légitimes et impérieux qui prévalent sur les intérêts, droits et libertés de l'Utilisateur, nécessitant la poursuite du traitement. JCDecaux SE peut également le poursuivre si les données personnelles de l'Utilisateur sont nécessaires pour la constatation, l'exercice ou la défense d'un droit en justice.
- **Le droit d'introduire une réclamation auprès d'une autorité de contrôle** : L'Utilisateur a le droit de contacter la CNIL afin d'introduire une réclamation.
- **Le droit de transmettre des instructions concernant l'utilisation des données après la mort** : l'Utilisateur a le droit de donner à JCDecaux SE des directives concernant l'utilisation de ses données personnelles après son décès.

Pour exercer ces droits, l'Utilisateur peut adresser une demande à l'adresse suivante : **JCDecaux, Délégué à la Protection des données** : par email : DPO\_F@jcdecaux.com - par courrier : JCDecaux SE – Service DPO – 17 rue Soyer 92200 Neuilly sur Seine.