MINISTÈRE
DE LA JUSTICE

Liberté
Égalité
Fraternité

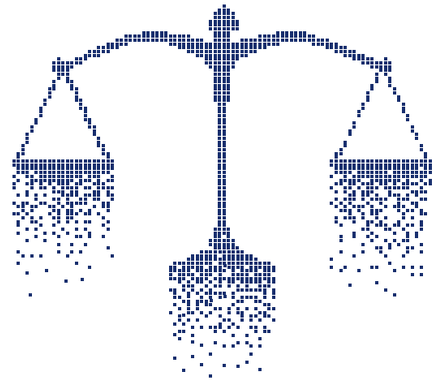
CHARTE D'USAGE

des services numériques du ministère de la Justice

Sommaire

Sommaire

CHARTE D'USAGE



des services numériques
du ministère de la Justice

Préambule

Le plan Action publique 2022 constitue une nouvelle étape dans la transformation numérique des services publics.

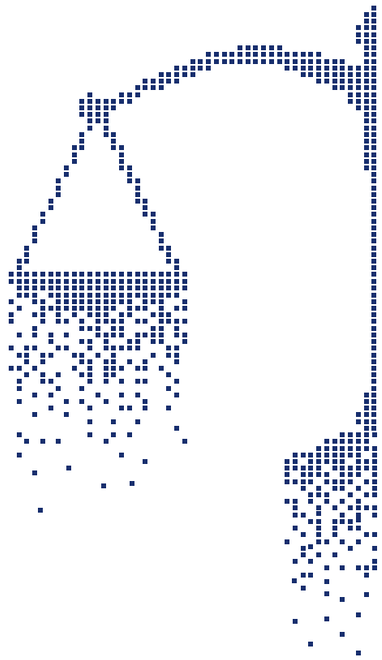
Le déploiement de l'administration électronique, des services en ligne et des télé procédures a été initié à la fin des années 1990, notamment par le programme d'action gouvernemental pour la société de l'information (PAGSI). Aujourd'hui, l'objectif est la dématérialisation de 100% des démarches administratives d'ici 2022.

Les systèmes d'information, de communication et les services numériques sont donc de plus en plus interconnectés et les réseaux de plus en plus imbriqués, la transformation numérique est à la fois marqueur de progrès et catalyseur de risques. Si les bénéfices apportés par le numérique ne sont plus à prouver, la fiabilité de ces derniers sera garantie à la seule condition que les systèmes soient sécurisés et que les données soient protégées.

De par ses activités régaliennes et sa mission de service public impliquant des prérogatives particulières, le ministère doit garantir un niveau de sécurité adapté aux informations qu'il est amené à traiter.

Prenant en compte les préconisations de l'agence nationale de la sécurité des systèmes d'information (ANSSI)[1] et de la commission nationale de l'informatique et des libertés (CNIL)[2], ce texte s'inscrit dans le cadre législatif et réglementaire en vigueur relatif à la protection des données à caractère personnel, à l'utilisation des logiciels, aux droits et obligations des utilsateurs des services numériques. Il s'inscrit dans les politiques de sécurité du système d'information du ministère de la Justice.

Les dispositions de la présente charte s'exercent dans le respect de la liberté syndicale et des droits des lanceurs d'alerte.



Portée et opposabilité

La présente charte et les modifications ultérieures qui pourraient intervenir sont publiées au bulletin officiel du ministère de la Justice. En conséquence, elle s'impose à l'utilsateur *(cf. § Définitions)* des services numériques *(cf. § Définitions)*.

Elle est communiquée à l'utilsateur au moment de sa prise de fonction et à chaque modification.

La présente charte et, toutes les explications techniques à sa bonne compréhension, sont consultables de manière permanente sur l'Intranet du ministère de la Justice

Champ d'application

L'objet de la présente charte est d'informer les utilsateurs des services numériques du ministère de leurs droits et obligations.

Elle a été élaborée dans le souci de concilier les intérêts du ministère, de l'indépendance de la Justice, des utilsateurs et des justiciables en particulier, de respecter leur vie personnelle, et d'assurer un usage loyal et transparent des services numériques.

Elle décrit ainsi l'ensemble des règles générales et spécifiques que chaque Utilsateur doit respecter dans l'utilisation des ressources et services numériques du ministère, de manière à éviter de porter atteinte à la sécurité du ministère, à la sécurité publique ou à la sécurité des usagers.

Chaque utilsateur doit être conscient de l'impact de son usage quotidien ou occasionnel sur la sécurité des services numériques, et s'engage à accepter ce règlement dans tous ses éléments et à le respecter dans tous ses termes.

Définitions

Les définitions suivantes s'appliquent dans la suite du document :

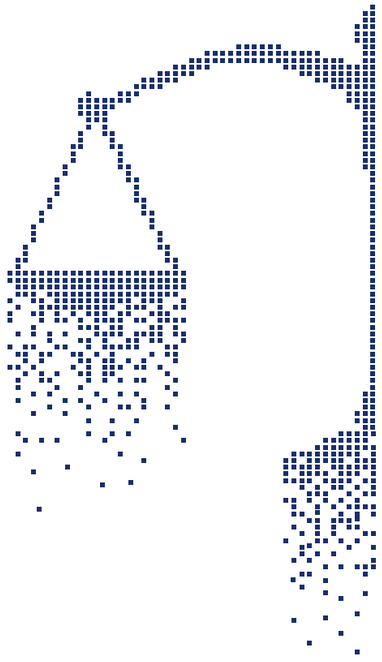
Utilsateur(s) : tout agent du ministère de la Justice, qui est amené à utiliser les services numériques du ministère de la Justice. Le terme « utilsateur » ne s'applique pas aux prestataires ou aux personnes extérieures dont l'accès aux services susvisés fait l'objet d'un lien contractuel spécifique avec le ministère (contrat de prestation, marchés public…).

Administrateur : toute personne (ou groupe de personnes) chargée(s) de l'exploitation, de la maintenance et de la supervision d'un service numérique, ou d'une partie de ce dernier.

Services numériques : ensemble de processus et de ressources permettant d'acquérir, de générer, de traiter, de stocker, de détruire, de diffuser, de transmettre ou d'accéder à des informations électroniques au sein du ministère de la Justice.

Ressources numériques : ensemble de moyens informatiques et de télécommunications, matériels ou logiciels, que le ministère met à disposition des Utilsateurs afin que ceux-ci puissent accomplir leurs tâches professionnelles. Ainsi, les micro-ordinateurs fixes ou portables, les moyens de communication (messagerie, accès à l'Internet, réseaux de transmission voix ou données, téléphones fixes ou portables, télécopieurs, service de visio-conférence,

1. https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/
2. https://www.cnil.fr/fr/donnees-personnelles



etc.), les équipements de stockage de données (disques durs externes, clés USB, supports optiques tel que le DVD etc.), les données contenues sur les équipements précédemment cités, les applications informatiques et autres logiciels font partie des ressources du système d'information du ministère.

Principes directeurs

Il appartient à chacun d'adopter un comportement professionnel et responsable lors de l'utilisation des services et des ressources numériques afin de ne pas perturber ou entraver leur bon fonctionnement, ni entrainer un détournement des activités à des fins non-professionnelles ou illégales.

Usage des services et des ressources numériques

L'ensemble des services et des ressources numériques est mis à disposition des utilsateurs pour un usage professionnel, en tant que moyen utile à l'accomplissement des tâches ou des missions qui leur sont confiées au titre de leur emploi.

L'utilisation à des fins privées des services et ressources numériques est tolérée dans la limite des nécessités de la vie courante et familiale.

Cet usage à titre extra-professionnel doit être mesuré et ne peut en aucun cas se faire au détriment des tâches ou missions professionnelles incombant à l'utilsateur. Il ne doit en aucun cas nuire au bon fonctionnement de l'ensemble des ressources numériques du ministère de la Justice ou altérer son image.

Confidentialité des informations et des données

La protection du patrimoine numérique du ministère de la Justice et de ses intérêts suppose le respect par chaque utilsateur d'une obligation de confidentialité à l'égard des informations dont il a connaissance dans l'exercice de ses activités professionnelles. Les agents d'État sont notamment soumis à une obligation particulière de secret professionnel mais également de discrétion.

Dans ce cadre, l'Utilsateur se doit de respecter certaines règles :

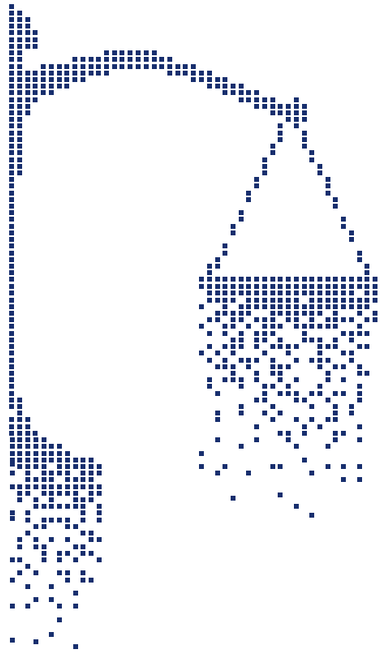
- L'utilsateur est soumis à une obligation de confidentialité. Il ne doit transmettre aucune information à caractère confidentiel, sans y être formellement autorisé ;
- La diffusion des informations classifiées relevant du secret de la défense nationale obéit à des règles restrictives qui relèvent notamment du code pénal ;
- L'utilsateur ne doit pas tenter d'accéder ou de prendre connaissance d'un message électronique qui serait adressé à un autre destinataire sans l'autorisation formelle de ce dernier ;
- En aucun cas, l'Utilsateur ne doit révéler à quiconque les moyens d'accès aux services et aux ressources numériques du ministère (mots de passe, code PIN ou tout autre secret d'authentification délivrés pour un usage professionnel) qui sont strictement personnels et incessibles.

Dispositions législatives et réglementaires

Tout utilsateur, tout comme l'administration, doit respecter les dispositions législatives et réglementaires relatives à l'utilisation des technologies de l'information et de la communication.

Celles-ci prévoient en particulier les mesures interdisant :

- L'atteinte à la vie privée (i.e. opinions politiques, syndicales, philosophiques ou religieuses, aux origines, au sexe, à l'orientation sexuelle ou identité de genre, à la situation de famille ou l'état de santé, à l'apparence physique ...) ;
- Les actes de violence écrite ou verbale ou contraire aux règles éthiques ou aux bonnes mœurs, notamment :
  - La diffamation et à l'injure ;
  - Le révisionnisme et l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité ;
  - L'incitation aux crimes et délits (i.e. l'incitation au suicide, à la haine ou à la violence) ;
  - L'atteinte aux mineurs (i.e. exposition à des messages à caractère violent, pornographique ou pédopornographique ;
  - L'incitation à la consommation de substances interdites.
- Les atteintes aux systèmes d'information, incluant des actes tels que :
  - L'accès ou le maintien frauduleux dans un système de traitement automatisé de données ;
  - La falsification, la modification, la suppression et l'introduction d'information avec l'intention de nuire.
- La violation du secret professionnel, des affaires, des enquêtes et de l'instruction ;
- La violation de la propriété intellectuelle et du droit à l'image ;
- Le non-respect de la réglementation relative à la protection des données à caractère personnel.

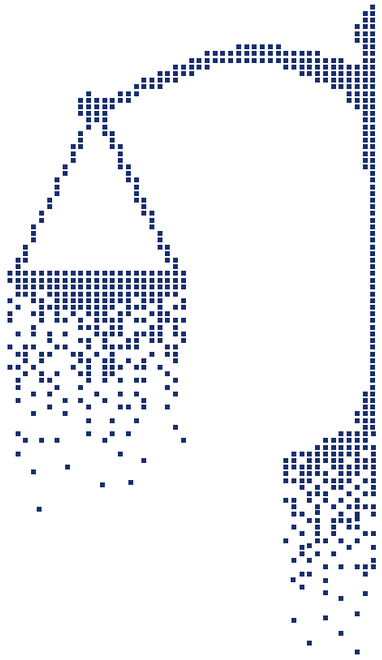


Règles d'utilisation générales

Accès aux ressources et aux services numériques

Par principe, chaque Utilsateur n'a accès qu'aux services ou aux ressources numériques qui lui sont nécessaires dans le cadre de son activité professionnelle. Les droits d'accès à tout ou partie des services ou des ressources numériques reposent sur une identification/authentification de chaque Utilsateur qui ne doit en aucun cas chercher à accéder par des moyens détournés ou fortuits à des informations et/ou des ressources pour lesquelles il n'est pas habilité.

Les moyens d'authentification (i.e. mots de passe, code PIN ou tout autre moyen d'authentification) aux services ou aux ressources numériques sont strictement personnels et incessibles. Le respect de ces principes est de la responsabilité de l'Utilsateur.



Données personnelles de l'Utilsateur

Les dispositions de la présente charte s'exercent dans le respect des droits syndicaux et des droits des lanceurs d'alerte.

La conservation de données, de documents, de fichiers et de messages électroniques à titre privé est tolérée dans la limite des nécessités de la vie courante et familiale. Ainsi, cela ne doit pas nuire au bon fonctionnement et à la sécurité des services numériques. Enfin, les données personnelles de l'utilsateur ne doivent pas contrevenir aux lois et à la réglementation en vigueur (i.e. données à caractère pédopornographique, pornographique, injurieux, diffamatoire, raciste, violent, faisant l'apologie du terrorisme ou d'actes illicites, etc.).

Ces données sont considérées comme privées dans la mesure où le marquage spécifique « PERSONNEL » ou « personnel » est employé pour les identifier explicitement (dans le nom des fichiers, le nom du répertoire de stockage ou dans l'objet du message électronique).

Tout document, contenu ou message électronique qui ne comporterait pas ce marquage, sera alors considéré comme professionnel. Le ministère pourra y avoir accès même en l'absence de l'utilsateur.

L'utilsateur ne doit, en aucun cas transformer et/ou qualifier des données, documents, fichiers ou messages de nature professionnelle en données, documents, fichiers ou messages personnels ou privés.

Au départ définitif d'un utilsateur, ses droits d'accès et habilitations seront suspendus immédiatement. Ses ayants droits ne seront pas autorisés à accéder aux contenus de l'utilsateur à l'exception des données marquées comme personnelles.

Protection du patrimoine numérique

Le ministère sauvegarde de manière automatique tout ou partie des données (répertoires, messages électroniques, ...) présentes sur ses services et ses ressources numériques de manière à en garantir la disponibilité en cas d'incident. Les sauvegardes sont faites sans distinction des répertoires (privés ou non) de l'utilsateur.

L'utilsateur est responsable de la sauvegarde et de la récupération de ses données, ses fichiers, ses documents et ses messages électroniques marqués « PERSONNEL » ou « personnel ».

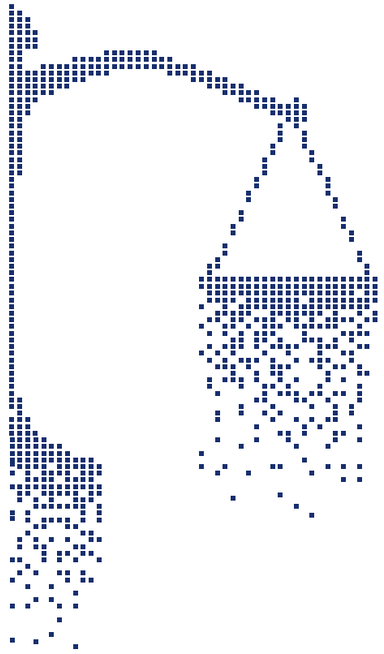
Protection des informations contenues dans les équipements informatiques et les supports amovibles

Le matériel informatique et de télécommunication que le ministère de la Justice fournit est placé sous la responsabilité de l'utilsateur, en tous lieux et en toute circonstance.

À ce titre, l'utilsateur doit utiliser les moyens de protection mis à sa disposition (câble antivol, armoire sécurisée, etc.) et appliquer les consignes de sécurité (verrouillage de l'ordinateur) afin de se prémunir contre le vol d'information. Lors de l'utilisation d'équipements nomades ou mobiles (notamment lors de voyages ou déplacements), les risques de compromission potentielle de l'information sont plus élevés. L'utilsateur doit donc faire preuve d'une vigilance accrue pour en assurer la surveillance. En cas de perte ou de vol, il doit le signaler dans les plus brefs délais à son responsable hiérarchique et à son service informatique de proximité, qui lui indiquera la procédure à suivre.

Enfin, l'utilsateur doit faire preuve d'une attention particulière lors de l'emploi des supports amovibles de stockage de masse (tels clés USB, disques durs externes, ...) et limiter autant que possible les supports non fournis par les services du ministère. En effet, ces supports peuvent être porteurs de programmes malveillants.

Ainsi, il ne doit pas connecter sur ses équipements informatiques des supports amovibles dont l'origine lui paraît suspecte. À toutes fins utiles, les utilsateurs qui le peuvent, sont invités à faire vérifier la sécurité de leurs matériels amovibles auprès de leur service de soutien informatique de proximité. En cas de perte ou de vol, le centre de service informatique doit être informé et l'agent doit déposer plainte dans les meilleurs délais. L'utilsateur doit se référer aux dispositions en vigueur dans son administration.



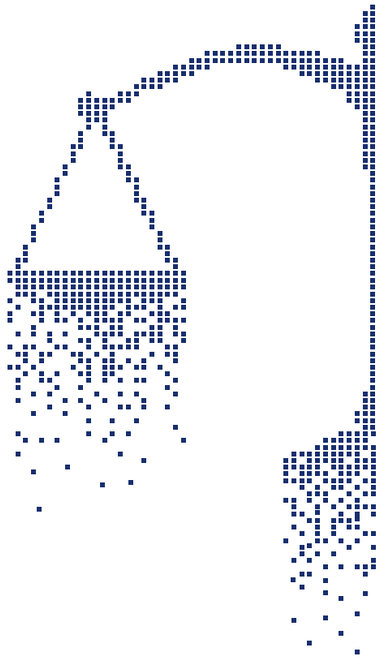
Protection du matériel

Chaque utilsateur contribue à la protection des informations conservées sur les équipements mis à sa disposition. Dans cette perspective, il se doit notamment de respecter toutes les mesures élémentaires visant à ne pas introduire et diffuser de programmes malveillants, à ne pas entraver le bon fonctionnement des contrôles de sécurité ou y porter atteinte de manière volontaire. En particulier, l'utilsateur s'assure de :

- ne pas mettre en œuvre d'outils susceptibles de contourner ou d'affaiblir la sécurité des services numériques du ministère ;
- ne pas stocker, transférer ou transmettre des informations professionnelles, qu'elle qu'en soit leur nature, via des dispositifs non autorisés par le ministère ;
- ne pas exploiter les éventuelles failles de sécurité, en faire la publicité ou les divulguer à des tiers ;
- ne pas altérer la configuration de ses équipements notamment en ce qui concerne le paramétrage des dispositifs de sécurité tels que l'antivirus, le pare-feu, le verrouillage de l'écran de veille ... ;
- ne pas installer, copier, modifier, supprimer des logiciels sans autorisation.

Seul le matériel mis à disposition par les services informatiques internes peut être connecté aux infrastructures informatiques et de télécommunication du ministère de la Justice. Le matériel, propriété des prestataires intervenant pour le compte du ministère et ceux des visiteurs, n'est pas autorisé à y être connecté.

Enfin, l'utilsateur doit restituer tout matériel informatique et de télécommunication confié par les services Informatiques (poste de travail portable, téléphone mobile...) lorsqu'il quitte définitivement ses fonctions (retraite, démission,...) ou lorsqu'il change d'affectation (en dehors ou au sein du ministère).



Services de l'Internet

L'utilisation de l'Internet n'est autorisée que dans le cadre exclusif de l'activité professionnelle. Toutefois, un usage de l'Internet est toléré dans le cadre des nécessités de la vie courante et familiale, à condition que son utilisation n'affecte pas les performances des services numériques du ministère ou ne perturbe pas le travail de l'agent.

Le ministère bloquera ou limitera l'accès, au travers de dispositifs de filtrage ou de sécurité, tout contenu présentant un risque légal, d'image ou d'atteinte à la sécurité de l'administration ou des Utilsateurs tels qu'un site malveillant, pornographique, ou incompatible avec l'activité professionnelle.

Les contenus en ligne susceptibles d'entrainer une consommation importante des ressources de l'Internet peuvent également être réglementés par le ministère.

Par ailleurs, l'utilsateur des services de l'Internet s'engage à ne pas utiliser les ressources de l'administration pour tenir des propos (oraux ou écrits) qui seraient considérés comme illicites ou contraires à l'ordre public, à ne pas porter atteinte à l'intégrité d'un autre Utilsateur ou à sa sensibilité notamment par des messages, textes ou images provocants et à ne pas émettre d'opinion personnelle étrangère à son activité professionnelle ou susceptible de porter préjudice à l'administration. Les Utilsateurs sont fortement encouragés à respecter les règles de politesse d'usage sur l'Internet.

Messagerie électronique

L'utilsateur se voit attribuer une adresse électronique professionnelle lors de sa prise de fonction. Celle-ci est mise à sa disposition pour un usage strictement professionnel.

Cependant, un usage ponctuel de la messagerie électronique dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que cet usage n'affecte pas le trafic normal des messages professionnels. Tous les courriels, reçus ou sauvegardés depuis les ressources et les services numériques du ministère sont présumés être professionnels, à défaut d'avoir été clairement identifiés comme « PERSONNEL » ou « personnel » par l'utilsateur.

L'utilsateur ne doit pas transmettre d'information professionnelle sur sa messagerie électronique privée ou celle d'un tiers, ou au travers de services numériques de l'Internet, sauf autorisation préalable et écrite de son supérieur hiérarchique ou sauf autorisation express par un accord dans le cadre d'une situation exceptionnelle (par exemple en cas de gestion de crise déclarée ainsi par les services compétents).

Si l'utilsateur reçoit par erreur un message dont il n'aurait pas dû être destinataire, toute utilisation, copie ou diffusion, même partielle de ce message est interdite. Il a l'obligation de le détruire et d'en informer immédiatement son expéditeur.

Par ailleurs, l'utilsateur est informé de la mise en place de quotas individuels en terme de capacité de stockage au niveau de chaque boîte aux lettres électronique et d'un filtrage des courriels reçus et envoyés (quotas d'envoi ou de réception, fichiers autorisés, etc.).

En cas d'absence planifiée, l'Utilsateur active, dans la mesure du possible, le dispositif de notification d'absence.

Messagerie instantanée

L'utilisation des messageries instantanées grand public est fortement déconseillée, du fait des risques de captation ou de fuite d'information. Il est recommandé à l'agent d'utiliser les outils collaboratifs mis à disposition par le ministère[3] ou par les services de l'État..

L'utilisateur est informé que l'usage de ces services peut être réglementé de manière plus stricte (limitation ou interdiction d'usage) en fonction de son emploi, de sa structure d'accueil ou d'appartenance (ex : service national du renseignement pénitentiaire...)

Rèles d'utilisation spécifiques

Accès distant et mobilité

En accédant aux services numériques du ministère à distance, l'utilisateur emprunte des infrastructures de télécommunication publiques, non maitrisées par le ministère et qui, par défaut, sont réputées peu sûres (WiFi public, aéroport, gare, etc.). Cet accès ne peut donc se faire que dans un cadre précis :

- l'utilisateur doit utiliser les mécanismes d'accès fournis par le ministère pour se connecter à distance aux ressources du ministère.
- le ministère se réserve le droit de conserver et d'analyser les traces relatives aux accès distants des utilisateurs et aux actions effectuées sur les services et les ressources numériques.

L'attention de l'utilisateur est appelée sur l'emploi des ressources et des services numériques en mobilité qui présente des risques plus élevés et des conséquences plus importantes, notamment lors des déplacements à l'étranger, compte-tenu des formalités douanières de certains pays étrangers (Etats-Unis et Chine en particulier).

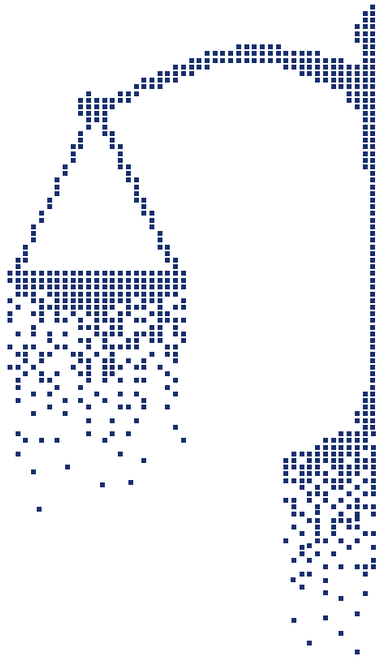
Pour éviter toute captation d'information par les autorités douanières, l'Utilisateur veille à emporter avec lui uniquement le matériel professionnel et la quantité d'information utiles à sa mission. En cas d'interception par les autorités douanières, l'utilisateur doit signaler l'incident dans les plus brefs délais à son responsable hiérarchique et à son service informatique de proximité, qui lui indiquera la procédure à suivre.

Modalités relatives aux missions ou aux fonctions itinérantes

Les dispositions de la présente charte s'appliquent aux usages en mobilité des services numériques du ministère. Pour des raisons de sécurité, l'accès aux ressources ou aux services numériques en nomadisme[4] peut être limité en accès, voire interdit par le responsable de traitement ou le service du haut fonctionnaire de défense et de sécurité.

3 http://intranet.justice.gouv.fr/site/informatique-telecom/produits-et-services-9268/soutien-aux-utilisateurs-17139/des-outils-pour-faciliter-le-travail-collaboratif-a-distance-124791.html

4 Selon l'ANSSI, le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité. Un des cas les plus sensibles est celui où l'utilisateur travaille depuis un espace complètement ouvert au public (cafétéria, bibliothèque, aéroport, etc.).



Objets connectés

Les objets connectés personnels (montres, écouteurs sans fil, smartphones, etc.) utilisés à titre privé ne doivent pas être branchés aux équipements professionnels. L'utilisateur doit être conscient que l'introduction dans l'enceinte du ministère d'objets connectés peut engendrer des risques supplémentaires tels que la captation d'informations, la géolocalisation des biens et des personnes, ou la propagation de programmes malveillants.

L'utilisateur est informé que l'utilisation de ce type de matériel peut être réglementée de manière plus stricte (limitation ou interdiction d'usage) en fonction de son emploi, de sa structure d'accueil ou d'appartenance. Ces dispositions s'appliquent aux agents appelés à se déplacer dans une de ces structures comme aux agents qui y sont affectés.

Signature électronique

La signature électronique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur. Elle a une valeur légale et produit des effets juridiques qui peuvent être équivalents aux signatures manuscrites.

L'utilisation des moyens de signature électronique mis à disposition d'un Utilisateur engage à la fois sa responsabilité et celle du ministère.

Conditions d'utilisation spécifiques

Droit à la déconnexion

Il convient de respecter les périodes de congés ou d'interruption du travail durant lesquelles les agents ne sont pas censés répondre aux sollicitations de leur employeur.

Au demeurant, ces sollicitations ne peuvent se justifier qu'en raison des nécessités de services pour faire face à une situation d'urgence (à apprécier selon les fonctions exercées).

L'usage de la messagerie électronique ou du téléphone, en dehors des horaires de travail, doit se faire en respectant la vie privée du destinataire et de l'émetteur ainsi que le droit à la déconnexion du destinataire et de l'émetteur, sauf pour faire face à une situation d'urgence.

Modalités relatives au Télétravail

Le télétravail fait l'objet de modalités définit réglementairement par arrêté du 31 juillet 2019 portant application du décret n°2016-151 du 11 février 2016 modifié et fixant les modalités de mise en œuvre du télétravail au ministère de la Justice et la note d'application du 23 octobre 2020 relative aux conditions et modalités de mise en œuvre du télétravail au ministère de la Justice.

Cette circulaire précise les règles de sécurité informatique à respecter par les agents en télétravail.

Nécessité impérieuse de service

En cas d'absence prolongée, l'accès aux ressources informatiques de l'utilisateur (messagerie électronique, base collaborative, répertoire réseau, poste de travail, ou tout service numérique ou matériel informatique et de communication), peut être autorisé en cas de nécessité par son supérieur hiérarchique. Ce dernier doit pour cela en faire la demande expresse au responsable de l'administrateur du système, et en informer en parallèle le responsable des ressources humaines.

Dans tous les cas, l'intéressé est averti au préalable, dans toute la mesure du possible, des demandes d'autorisation d'accès à ses ressources.

Protection des propriétés intellectuelles, des informations et des données

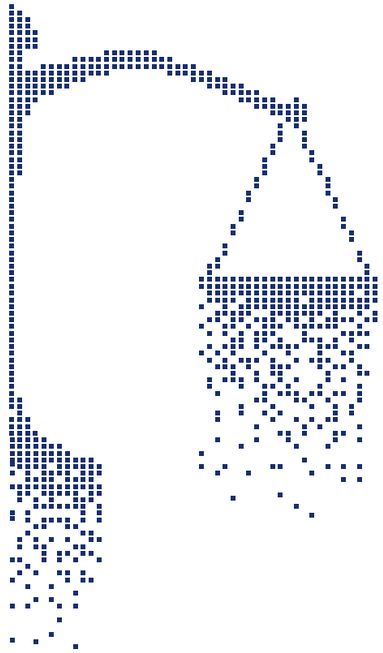
Données à caractère personnel

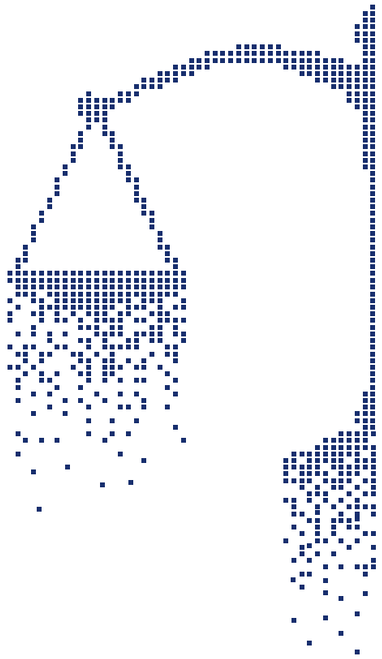
Tout traitement de données doit être mis en œuvre conformément au règlement général sur la protection des données (RGPD) et la loi dite « Informatique et Libertés ». L'utilisateur s'engage à préserver les données à caractère personnel, traitées par les services numériques du ministère. La perte, la destruction ou la divulgation frauduleuse, accidentelle ou non autorisée de données personnelles pourraient avoir des conséquences graves pour le ministère.

L'utilisateur se doit de :

- respecter les finalités définies, explicites et légitimes d'un traitement de données à caractère personnel ;
- protéger les données personnelles afin qu'elles ne soient pas utilisées par des personnes non autorisées ou habilitées, ni divulguées, supprimées ou détruites, perdues, volées, même de manière accidentelle (cela suppose le contrôle rigoureux de la diffusion de données à caractère personnel à destinataire de tiers extérieurs au ministère) ;
- lorsqu'une application permet la saisie de données dans un champ libre, celles-ci doivent être objectives, non excessive et conformes à la finalité du traitement ;
- respecter et donc ne pas contourner, ni désactiver, les mesures techniques, organisationnelles et juridiques, prises par le ministère pour assurer la protection des données à caractère personnel.

Les manquements à la réglementation en vigueur peuvent donner lieu à des sanctions à l'encontre du ministère de la justice de la part de la CNIL.





Propriété intellectuelle et droit à l'image

En dehors des cas d'usages autorisés dans le cadre de ses missions au sein du ministère, l'utilisateur s'interdit de produire, de collecter ou de transmettre des données, des fichiers, des logiciels, des applications, des messages, des œuvres ou des contenus protégés, quel qu'en soit le support, la nature ou la forme (par exemple des photographies, des dessins, des écrits, des enregistrements musicaux ou de vidéos, des images, des logos, des logiciels, etc.), dans le respect du droit de propriété intellectuelle, du droit à l'image ou du droit à la vie privée.

L'attention de l'utilisateur est appelée sur les poursuites pénales et/ou civiles dont lui-même et/ou l'administration pourraient faire l'objet du fait de la rediffusion, par quelque moyen que ce soit, de messages répréhensibles captés sur le réseau de l'internet ou de l'utilisation, de la diffusion, voire du simple enregistrement informatique, d'œuvres ou de données en contravention avec les législations existantes ou sans l'autorisation des titulaires des droits.

Sécurité et cyber-surveillance

Signalement

L'utilisateur se doit de signaler dans les plus brefs délais tout constat, tentative ou soupçon de violation de ses droits d'accès à son service informatique de proximité lequel sera chargé d'avertir sans tarder les acteurs responsables de la sécurité des services et des ressources numériques. La participation des utilisateurs à la détection d'anomalies et d'un incident de sécurité sur les services numériques est déterminante dans la rapidité de mise en œuvre des mesures de protection.

En cas de perte ou de vol de moyens d'authentification, de matériels, l'utilisateur doit en informer sans délai son supérieur hiérarchique et le service informatique de proximité et mettre en œuvre les démarches nécessaires, notamment pour limiter l'accès aux données professionnelles et aux services numériques du ministère.

Surveillance des ressources et services numériques

Pour garantir la sécurité des services et des ressources numériques et la protection des informations nécessaires au bon fonctionnement du ministère, ce dernier peut, sans préavis, limiter ou bloquer l'accès à certains services numériques, sites Web, ressources ou à certaines parties de l'Intranet, à tous ou bien certains utilisateurs, pour une durée indéterminée.

Il met en œuvre des mécanismes de filtrage et d'analyse du trafic réseau, même chiffré (HTTPS). Des moyens de déchiffrement pourront être appliqués à l'ensemble des flux de connexion des Utilisateurs, à l'exception de ceux qui seront inclus au sein d'une « liste blanche de sites ». Ce traitement permettra l'identification de logiciels malicieux, la protection du patrimoine informationnel ou la détection de flux sortants anormaux de nature à porter atteinte à l'intégrité du système d'information du ministère. Les données collectées sont conservées pour une durée maximale de 6 mois.

Il est interdit de les contourner ou de tenter de les contourner, sous peine de sanction.

Traçabilité

Pour garantir une traçabilité et être en mesure de fournir des preuves, notamment en cas d'enquête judiciaire ou administrative ou d'autocontrôle, le ministère conserve, en fonction de la finalité et des durées fixées par les textes applicables, les journaux d'accès et d'utilisation générés dans les services ou ressources numériques qu'il met en œuvre. Cette conservation est réalisée dans le respect des dispositions réglementaires relatives à la protection des données personnelles.

Suivi des acquis en matière de sécurité numérique

Le ministère informe les utilisateurs des campagnes de sensibilisation à la sécurité des services numériques et de vérification générale de leur bonne utilisation qu'il organise. Les résultats de ces campagnes seront anonymisés et ne pourront pas conduire à une sanction quelconque.

Contrôle, maintenance et gestion des services et des ressources numériques

Opérations de maintenance et de contrôle automatisé

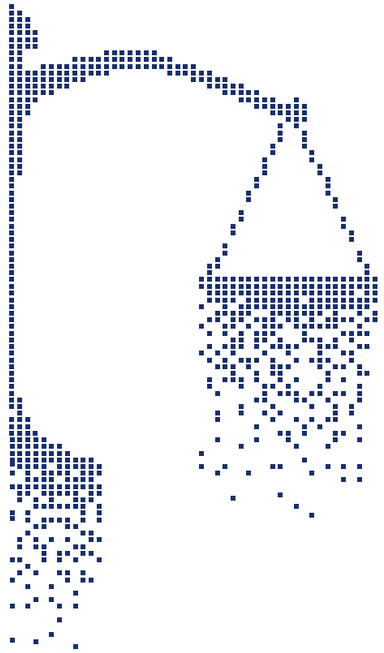
Une opération de maintenance s'inscrit dans le cadre d'une opération programmée de maintien en bon état de fonctionnement des moyens considérés. La maintenance peut être opérée par des personnels internes ou des prestataires extérieurs, aussi bien sur le lieu de travail, à distance (télémaintenance) ou encore au domicile de l'utilisateur (cas particulier du télétravail).

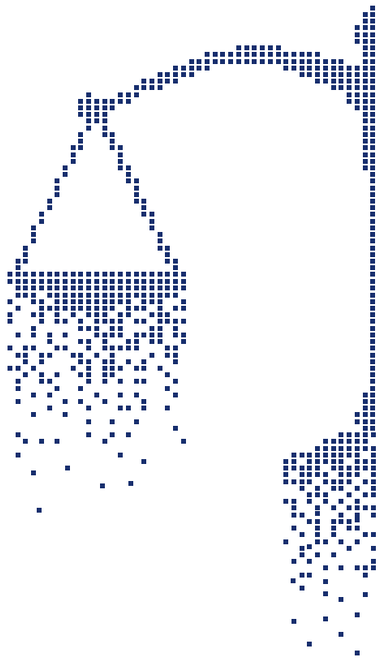
Les ressources numériques du ministère font l'objet de contrôles ayant comme unique finalité d'assurer la sécurité et la continuité des ressources et des données du ministère. En cas d'événement ou d'anomalie liés à la sécurité ou à la continuité de ses systèmes, le ministère s'autorise à prendre toutes les mesures nécessaires pour en identifier les causes.

Le ministère se réserve le droit de consulter de manière exceptionnelle le contenu des documents, des fichiers ou des messages identifiés « PERSONNEL » ou « personnel » de l'Utilisateur en cas de risque de mise en péril de son activité (par exemple la présence de code malveillant, ou dans le cas d'une enquête judiciaire en cours).

La collecte de données personnelles sera limitée aux informations nécessaires à la sécurité des services et des ressources numériques. Ces données sont conservées pour une durée maximale de 6 mois après collecte.

Les éléments découverts à l'occasion d'une opération de contrôle ou de maintenance sont susceptibles de constituer des moyens de preuves licites contre les agissements d'un Utilisateur.





L'utilisateur s'engage à ne pas entraver toute opération de contrôle ou de maintenance effectuée par les services informatiques du ministère. En outre, toute personne physique a le droit d'accéder aux données personnelles qui la concernent.

Moyens de télécommunication.

La mise à disposition au bénéfice de l'Utilisateur d'une ligne téléphonique, fixe et/ou mobile, conduit le ministère à disposer des données relatives à l'utilisation de ces moyens de communication, que ces données soient issues des autocommutateurs téléphoniques ou de leur transmission par l'opérateur auprès duquel le ministère est client.

Les smartphones, pouvant être mis à disposition de l'utilisateur par le ministère, entrent dans ce cadre. Ces matériels qui permettent, de plus, le stockage de données, l'accès à Internet et à la messagerie électronique professionnelle, sont également soumis aux dispositions du présent document.

Des contrôles sont effectués pour détecter les lignes inutilisées ou les consommations anormales et déclencher éventuellement des analyses détaillées. Par ailleurs, des analyses globales portant sur les volumes des consommations et des coûts sont effectuées en vue d'optimisation économique.

En cas d'abus ou de dépassement non justifié de forfait, le ministère se réserve la possibilité d'enquêter.

Responsabilités et sanctions

Le non-respect des règles d'utilisation et des mesures de sécurité figurant dans la présente charte est susceptible de justifier la suspension immédiate, sur décision du chef de service, de l'utilisation de tout ou partie des services et des ressources numériques.

L'agent dispose de la possibilité d'exercer un recours hiérarchique contre cette décision ou d'exercer les voies de recours dont il dispose devant le juge administratif.

Le non-respect des règles d'utilisation et des mesures de sécurité figurant dans la présente charte est susceptible d'entraîner l'engagement de poursuites disciplinaires adaptées à la gravité des agissements constatés, sans préjudice d'éventuelles actions pénales ou civiles à l'encontre de l'utilisateur.