Données personnelles et sécurité

Vérifié le 20 juin 2017 - Direction de l'information légale et administrative (Premier ministre)

La plateforme technique de service-public.fr a fait l'objet d'un travail préparatoire approfondi avec la CNIL (Commission nationale de l'informatique et des libertés) en vue d'offrir aux usagers toutes les garanties en matière de sécurité et de confidentialité de leurs données.

L'hébergement de la plateforme service-public.fr est réalisé sur un site dont les locaux et l'accès aux machines d'exploitation sont contrôlés. Les flux de données et les données personnelles sont chiffrés afin de prévenir des tentatives de détournement d'information. Les accès à la plateforme sont conservés afin de garantir leur traçabilité.

Données personnelles

Politique de confidentialité

Le site service-public.fr est déclaré à la Commission nationale de l'informatique et des libertés (Cnil) et enregistré sous le numéro 712957.

La base de données diffusée dans la rubrique Annuaire de l'administration a fait l'objet d'une déclaration spécifique sous le numéro 1546654.

Conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460) , aucune information personnelle n'est collectée à votre insu ou cédée à des tiers. Vous disposez d'un droit d'accès, de rectification et d'opposition aux données vous concernant que vous pouvez exercer en contactant le correspondant informatique et libertés de la CNIL. Pour cela, il vous suffit d'envoyer un courrier par voie électronique ou postale à la Direction de l'information légale et administrative (DILA) en justifiant de votre identité.

Utilisation de témoins de connexion (« cookies »)

Lors de la consultation du site service-public.fr, des témoins de connexions, dits « cookies », sont déposés sur votre ordinateur, votre mobile ou votre tablette.

Ces cookies permettent essentiellement à service-public.fr :

- d'afficher, lors de votre première visite, le bandeau signalant la présence de cookies et la faculté que vous avez de les accepter ou de les refuser ;
- d'établir des mesures statistiques de fréquentation des espaces de communication à caractère publicitaire présents sur le site : communication gouvernementale, promotion des ouvrages commercialisés par la DILA ;
- d'établir des mesures statistiques de fréquentation et d'utilisation du site. Pour information, le tiers émetteur, AT Internet, est également soumis à la loi informatique et libertés.

L'outil de mesure d'audience At Internet (Xiti) est déployé sur ce site afin d'obtenir des informations sur la navigation des visiteurs et d'en améliorer l'usage. Pour en savoir plus sur la gestion des cookies de statistiques d'AT Internet : www.atinternet.com/politique-du-respect-de-la-vie-privee (http://www.atinternet.com/politique-du-respect-de-la-vie-privee/) .

À savoir :

- les données collectées ne sont pas recoupées avec d'autres traitements ;
- le cookie déposé sert uniquement à la production de statistiques anonymes ;
- le cookie ne permet pas de suivre la navigation de l'internaute sur d'autres sites.

Vous pouvez paramétrer votre navigateur afin qu'il vous signale la présence de cookies et vous propose de les accepter ou non. Vous pouvez accepter ou refuser les cookies au cas par cas ou bien les refuser une fois pour toutes. Il est rappelé que ce paramétrage est susceptible de modifier vos conditions d'accès aux services du site nécessitant l'utilisation de cookies.

Le paramétrage des cookies est différent pour chaque navigateur et en général décrit dans les menus d'aide.

Sécurité

Accès au site

Le site service-public.fr est protégé par un certificat électronique, matérialisé pour la grande majorité des navigateurs par un cadenas.

Cette protection participe à la confidentialité des échanges, mais permet aussi aux usagers de s'assurer de l'authenticité du site au regard d'éventuelles tentatives de filoutage :

http://www.ssi.gouv.fr/entreprise/glossaire/h/ (https://www.ssi.gouv.fr/entreprise/glossaire/h/)

En aucun cas les services associés à service-public.fr ne seront initiateur d'envois de courriels pour demander la saisie d'informations personnelles. En particulier, le mot de passe qui reste sous le contrôle exclusif des usagers. Seuls et dans certaines circonstances identifiables par l'usager, des courriels légitimes pourraient lui être adressés à des fins d'information ou d'invitation à poursuivre une démarche engagée par voie électronique.

Lors de la connexion au site service-public.fr, il est recommandé de copier ou de saisir manuellement l'adresse réticulaire (URL) dans le navigateur, et d'éviter de cliquer sur des liens qui auraient été reçus par messagerie ou qui seraient accessibles à partir de sites non réputés.

Le certificat qui sert le site est conforme aux exigences du Référentiel général de sécurité (RGS) et est émis par un Prestataire de certification électronique qualifié (PSCE). La liste des prestataires qualifiés est disponible sur :

http://lsti-certification.fr/index.php/fr/certification/psce (http://lsti-certification.fr/index.php/fr/certification/psce)

Protection des données

La protection des données est une exigence forte de la CNIL (Commission Nationale Informatique et Liberté). Dans le cas de service-public.fr, l'une des mesures de protection repose sur un chiffrement du stockage de toutes les données à caractère personnel (nom, prénom, mot de passe, documents déposées, etc.) par des ressources cryptographiques qualifiées par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ou ayant à minima une évaluation Critères Communs au niveau EAL4+.

Pour l'usager, service-public.fr présente l'avantage d'un parcours en ligne simplifié, personnalisé et enrichi de nouveaux services, allant de la recherche d'informations administratives jusqu'à la réalisation et le suivi de démarches en ligne.

Dans ce contexte, l'usager maîtrise seul, directement ou indirectement via les démarches, les données stockées dans son espace que ce soit en dépôt ou en suppression.

Néanmoins, les données de l'espace usager restent directement exploitables par les démarches en ligne initiées par son compte. En dehors de ces démarches aucune administration ne peut accéder aux données , excepté dans le cadre d'une instruction judiciaire.

service-public.fr est donc conçu pour répondre au besoin de simplification exprimé par les usagers pour la réalisation de leurs démarches en ligne, tout en leur offrant les garanties nécessaires en matière de respect des libertés individuelles.

Naviguer en confiance

Choisir son mot de passe

Pour protéger vos accès et vos données, il est nécessaire de choisir et d'utiliser des mots de passe robustes, qui sont difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne. La force d'un mot de passe dépend de sa longueur et des caractères le composant. Le site service-public.fr exige 8 caractères minimum, comportant au moins une lettre en majuscule, au moins une lettre en minuscule et au moins un chiffre

Pour information les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour le choix d'un mot de passe sont :

- Avoir des mots de passe de 12 caractères minimum, si possible de 16 caractères ;
- Utiliser, en alternant, des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux)
- Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance...)
- Choisir un mot de passe unique pour chaque système ;

Pour en savoir plus sur les mots de passe :http://www.ssi.gouv.fr/guide/mot-de-passe/ (http://www.ssi.gouv.fr/guide/mot-de-passe/)

Protéger ses moyens d'authentification

Afin de ne pas compromettre la sécurité de vos moyens d'authentification et de votre environnement d'utilisation, il est recommandé de :

- Ne jamais demander à un tiers de créer pour vous un mot de passe ;
- Changer de mot de passe régulièrement ;
- Eviter de configurer les logiciels, y compris votre navigateur web, pour qu'ils retiennent les mots de passe ;
- Ne pas envoyer ses mots de passe en clair sur Internet, par exemple sur sa messagerie personnelle ;
- Ne pas noter ou stocker en clair les mots de passe dans un fichier ou un document en libre accès, ou sur un poste informatique connecté à Internet ;
- Naviguer avec un navigateur à jour. Avant toute utilisation d'un navigateur, quel qu'il soit, il convient de s'assurer le plus tôt possible que celui-ci est à jour. Les navigateurs les plus récents proposent tous une fonctionnalité de mise jour automatique et des moyens de protection contre les malveillances, comme le filoutage. Ce qui est vrai en termes de mise à jour pour un navigateur, l'est également pour le système d'exploitation et les logiciels qui y sont installés.

Une solution pratique pour répondre à ces exigences avec un minimum de confort est d'utiliser un coffre-fort logiciel de type Keepass pour stocker les mots de passe : http://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/ (http://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/)

Consulter l'infographie de l'Agence nationale de sécurité des systèmes d'snformation « Les bons réflexes sur Internet » : http://www.ssi.gouv.fr/uploads/2016/06/surfezzen_mini.jpg (http://www.ssi.gouv.fr/uploads/2016/06/surfezzen_mini.jpg)

Détecter un courriel malveillant sur les conseils de la CNIL :

https://www.cnil.fr/fr/detectez-un-courrier-electronique-malveillant (https://www.cnil.fr/fr/detectez-un-courrier-electronique-malveillant)

Menaces sur Internet

En complément de l'attention portée à la sécurité, voici quelques principales menaces d'Internet à surveiller :

- Les codes malveillants : les postes utilisés pour accéder à l'espace personnel doivent être protégés (anti-virus et correctifs de sécurité à jour) contre les codes malveillants afin d'assurer la légitimité des accès au compte. Le principal risque sur service-public.fr serait le piratage de son mot de passe.
  http://www.ssi.gouv.fr/entreprise/glossaire/c/#code-malveillant-logiciel-malveillant-malicious-software-malware (http://www.ssi.gouv.fr/entreprise/glossaire/c/#code-malveillant-logiciel-malveillant-malicious-software-malware)

- Le filoutage : le site pourrait être copié avec pour simple objectif d'attirer les usagers à s'y connecter et récupérer leurs mots de passe. Pour service-public.fr, un certificat électronique émis par une autorité reconnue dans les navigateurs et qualifiée au sens du Référentiel général de sécurité, permet aux usagers et à leur navigateur de vérifier la légitimité du site auquel ils accèdent.
  http://www.ssi.gouv.fr/entreprise/glossaire/h/ (http://www.ssi.gouv.fr/entreprise/glossaire/h/)
- Les pourriels (SPAM) : l'envoi de courriels non sollicités (SPAM) serait le principal vecteur pour inciter les usagers à s'authentifier sur des sites illégitimes (filoutage) ou infecter leurs postes via des liens ou des pièces jointes malveillants.
  http://www.ssi.gouv.fr/entreprise/glossaire/p/#pourriel-polluriel-spam (http://www.ssi.gouv.fr/entreprise/glossaire/p/#pourriel-polluriel-spam)

Textes de référence service-public.fr

- Ordonnance n°2005-1516 du 8 décembre 2005 (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&fastPos=1&fastReqId=861641718&categorieLien=cid&oldAction=rechTexte) relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Décret n° 2016-186 du 24 février 2016 (https://www.legifrance.gouv.fr/eli/decret/2016/2/24/PRMX1522705D/jo) modifiant le décret n° 2009-730 du 18 juin 2009 relatif à l'espace de stockage accessible en ligne pris en application de l'article 7 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Arrêté du 6 novembre 2000 (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000586125&dateTexte=) relatif à la création d'un site sur internet intitulé « service-public.fr ».
- Arrêté du 24 février 2016 (https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=A931A24E05A2AF866EE6A1F31330C29D.tpdila12v_3?cidTexte=JORFTEXT000032106812&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000032106756) portant intégration au site internet « service-public.fr » d'un téléservice permettant à l'usager d'accomplir des démarches administratives en tout ou partie dématérialisées et d'avoir accès à des services d'informations personnalisés.
- Délibération n° 2015-411 du 12 novembre 2015 (https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=A931A24E05A2AF866EE6A1F31330C29D.tpdila12v_3?cidTexte=JORFTEXT000032107742&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000032106756) portant avis sur un projet d'arrêté relatif à la mise en œuvre de traitements de données à caractère personnel intégrés au dispositif dénommé « service-public.fr » pour permettre, en un point d'accès unifié pour l'usager, d'accomplir des démarches administratives en tout ou partie dématérialisées et de bénéficier de services d'informations personnalisées (demande d'avis n° 1878256).