APPLICATIONS MOBILES & SITES INTERNET

GUIDE DE BONNES PRATIQUES

ÉDITION 2020

Des solutions numériques pour bien vivre sa retraite

avec le soutien de Sécurité sociale L'Assurance Retraite Île-de-France

MEDAPPCARE

DEKRA

PRÉFACE

PAR **CHRISTIANE FLOUQUET**
Directeur de l'action sociale
Ile-de-France - la Cnav

L'Assurance retraite en Ile-de-France a pour objectif d'offrir à ses retraités l'accès à des solutions numériques innovantes, structurantes et fonctionnelles leur permettant de mieux vivre leur retraite dans des conditions maximales de confort et d'autonomie.

Ces solutions numériques, qu'il s'agisse d'applications mobiles et/ou de sites Web, sont appelées à être de plus en plus prégnantes et incontournables. Elles sont portées par de très nombreux éditeurs partenaires de l'Assurance retraite Ile-de-France, qui est ainsi depuis l'origine un acteur engagé dans la promotion et le développement de la « silver économie ».

Afin d'évaluer la pertinence et d'améliorer la qualité des services qu'elle soutient dans ce cadre, l'Assurance retraite Ile-de-France a travaillé avec Medappcare et initié la confection de ce Guide des bonnes pratiques pour les applications mobiles et sites internet que vous avez entre les mains.

Sa vocation est de vous aider à bâtir les meilleurs produits numériques à destination des retraités, en identifiant les principales problématiques et en proposant les meilleures solutions.

Il a ainsi pour objectif premier d'accompagner la démarche qualité des projets en faveur du « bien vivre sa retraite » et pour ambition de vous éclairer utilement sur les meilleures solutions pour construire des produits numériques :

- Qui renforcent l'autonomie des retraités utilisateurs en leur permettant de « surfer » sans recours nécessaire à un aidant ou une tierce personne,
- Qui leur donnent accès rapidement et facilement à des informations pertinentes, adaptées à leurs besoins et actualisées,
- Dont le contenu est conforme aux exigences légales sur le double versant de la protection des données personnelles et de la sécurité numérique globale.

Nous espérons que vous y trouverez toute la matière pour vous aider à concevoir, développer et diffuser des solutions numériques pro-actives et différenciantes qui aideront les retraités franciliens à pleinement s'inscrire en complète autonomie dans leur environnement.

SOMMAIRE

Entraide, solidarité, communication familiale, lien social, accès à l'information... le numérique facilite et transforme la vie quotidienne des personnes âgées et l'offre digitale pour les retraités est en plein essor.

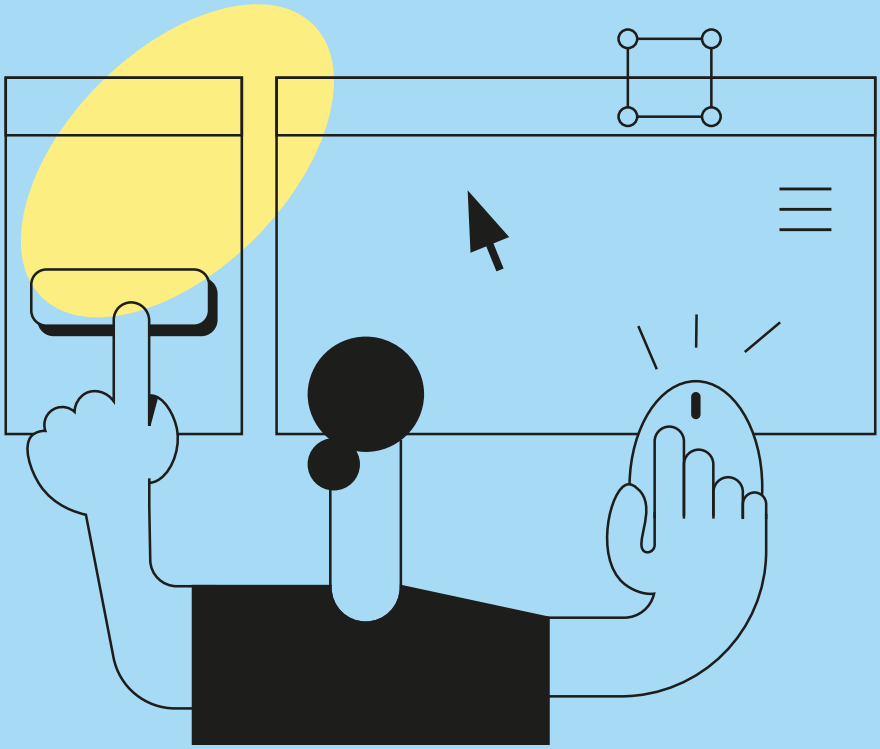
PAR **GILLES BRAUD**
Docteur en pharmacie
Head of development Health & well being connected
MEDAPPCARE (Groupe DEKRA)
gilles.braud@dekra.com

Cette année encore, l'Assurance retraite Ile-De-France (IDF) soutient des solutions innovantes qui ont pour objectif d'apporter du confort et de l'autonomie aux populations les plus fragiles à l'aide de leurs services structurants et différenciants. Grâce à ce soutien, certaines structures ont pris une dimension nationale, connue et reconnue. C'est une fantastique opportunité pour soutenir le secteur de la silver économie ! Mais la qualité est-elle toujours au rendez-vous ? La question mérite d'être posée. Comme l'indique un éditeur, il est normal que l'Assurance retraite IDF veuille évaluer les services qu'elle soutient. C'est la mission qu'elle a confié à Medappcare de procéder à l'évaluation de la qualité de ces services. Pertinence du contenu, design et ergonomie, protection des données personnelles, sécurité numérique, les éditeurs ne maîtrisent pas toujours la réglementation et les bonnes pratiques pour élaborer un service innovant de qualité.

Ce guide de bonnes pratiques, soutenu par l'Assurance retraite IDF, s'adresse à l'ensemble des parties prenantes du secteur de la silver économie : institutions, éditeurs et fabricants, financeurs, associations... Nous avons mobilisé nos experts qui présentent ici les bonnes questions à se poser et les exigences à respecter. Certes, ce guide n'a pas vocation à être exhaustif mais vous y trouverez une mine d'informations pratiques et utiles. L'essentiel est de rester innovant et créatif et ce, dans l'intérêt du bien commun

BONNE LECTURE !

DESIGN & ERGONOMIE



« Une situation et un contexte d'usage doivent faire sens avec nos gestes et nos actions »

L'EXPERT :
GAËL GUILLOUX

Designer (espace, numérique, produit et service) et chercheur en design social (doctorat en ingénierie de l'innovation, design et développement durable), Gaël Guilloux possède une expertise spécifique sur les enjeux de la santé et du mieux-vivre connecté, le parcours des soins des patients, l'ergonomie et les usages à destination des personnes fragiles, en perte d'autonomie et en situation de handicap.
Fondateur de Les Bolders, il co-designe des solutions spatiales, numériques, produits et services dans les champs médico-social et de la santé, dans le cadre de projets de design ou de recherche en design.
Gaël Guilloux est expert design pour le Forum des Living Labs en Santé et Autonomie, correspondant recherche pour le réseau Leroy Merlin Source (leroymerlinsource.org) et chercheur associé au laboratoire PROJEKT de l'Université de Nîmes.

Le design a évolué du développement de sites web et d'applications au développement de services puis vers l'expérience utilisateur. Rendre l'expérience de l'usager fragile réussie oblige à concevoir le service comme un parcours où l'ergonomie est une composante essentielle. L'évaluation de l'ergonomie dans le domaine de l'autonomie repose sur 4 catégories de critères : la présentation, le fonctionnement, l'accompagnement et la navigation du parcours proposé. Cette évaluation s'appuie sur des critères d'accessibilité et sur une méthodologie de vérification de leur conformité issus du Référentiel Général d'Accessibilité pour les Administrations (RGAA). Le RGAA se base sur l'initiative pour l'accessibilité du web (WAI), lancée par le World Wide Web Consortium (W3C), dont l'objectif est de rendre le web accessible aux personnes dont les capacités changent avec l'âge.

Pour savoir si un service fait gagner en autonomie et permet de s'autodéterminer sans avoir recours à un aidant ou une tierce personne, ce guide a pour objectif de mettre en avant les bonnes pratiques à l'heure de développer de nouveaux services en ligne.

DESIGN :
Les incontournables

PRÉSENTATION

L'IDENTITÉ GRAPHIQUE

Pour créer un univers propre et pertinent au service, assurer une bonne navigation :

- Veiller à l'uniformité graphique de l'ensemble des pages.
- Insérer des repères graphiques pour faciliter la navigation de l'usager
- Indiquer les changements de sens de lecture.
- Préférer le mode paysage.

HIÉRARCHISATION DE L'INFORMATION

Pour un parcours de lecture efficace :

- Limiter les thématiques, aller à l'essentiel.
- Hiérarchiser pour conduire l'utilisateur dans le parcours et l'appropriation des éléments, et l'appréhension des fonctionnalités.
- Soutenir et renforcer la hiérarchisation des informations par l'identité graphique.

LES COULEURS

- Proscrire l'association du vert et du jaune, notamment pour les personnes ayant des problèmes de mal voyance.
- Eviter les typographies blanches sur fond coloré clair ou à motifs, ou celles de couleur similaires au fond (exemple des niveaux de gris).

LA (OU LES) TYPOGRAPHIES

- Choisir une typographie aérée pour faciliter la lecture (25 % d'aération), avec une graisse pas trop fine.
- Préférer une taille de 13.
- Limiter les blocs de textes à maximum 80 caractères.
- Favoriser les doubles colonnes.

LES IMAGES, PICTOGRAMMES, ICÔNES, PHOTOGRAPHIES

Les illustrations ne sont pas choisies au hasard et sont liées à une information présente sur le site/l'application.

- Les mettre en relation avec le texte et le sujet abordé.
- Clairement signifier ce qu'ils indiquent, et avoir un équivalent textuel.
- Pouvoir les agrandir pour permettre à l'utilisateur de mieux les visualiser.

LE LANGAGE

S'assurer que tous les usagers comprennent les informations et données du site ou de l'application mobile :

- S'appuyer sur des formules simples et compréhensibles pour un usager ayant un niveau scolaire équivalent à la seconde.
- Donner l'accès, rendre compréhensible, référencer et dater les sources d'information et de données utilisées.

LE CANAL DE COMMUNICATION

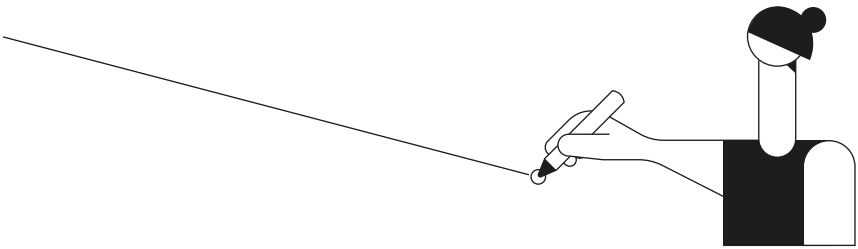
Les usagers selon leur situation sont plus sensibles à un ou plusieurs canaux de communication. Pour s'adresser à tous :

- Permettre le choix du canal de communication (écrit, Langue des Signes Française LSF, visuel, image, Langage Parlé Complété LPC, audio).
- Indiquer clairement ces options.
- Les croiser/associer pour les renforcer.

LA PLATEFORME DE TÉLÉCHARGEMENT

Pour les applications mobiles, certaines informations doivent être présentes sur la plateforme de téléchargement :

- Indiquer clairement le caractère payant ou gratuit de l'application.
- Indiquer les informations concernant l'éditeur et l'historique des versions.



FONCTIONNEMENT

LE SITE WEB OU L'APPLICATION NE DOIT PAS IMPOSER UNE MODALITÉ DE FONCTIONNEMENT QUI NE CORRESPONDRAIT PAS AUX USAGES RÉELS, ET DOIT PROPOSER UN PARCOURS.

Les actions minimales suivantes doivent être mises en oeuvre :

- Répondre à la question suivante : le service rendu correspond-il aux attentes, aux besoins et aux habitudes ou fonctionnements numériques de l'usager ?
- Si le service remplit une mission pédagogique, l'identifier clairement, et, si c'est applicable, faire mention des recommandations de la Haute Autorité de Santé.
- Proposer un moteur de recherche.

ACCOMPAGNEMENT

L'USAGE DU SITE WEB OU DE L'APPLICATION DOIT INTÉGRER DES ÉLÉMENTS D'ACCOMPAGNEMENT DE L'USAGER DANS LA DÉCOUVERTE, L'APPRENTISSAGE ET L'UTILISATION DU SERVICE.

Les actions minimales suivantes doivent être mises en oeuvre :

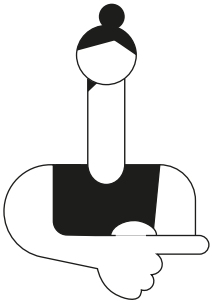
- Faciliter l'accès au plan du site, une Foire Aux Questions (FAQ), voire un glossaire quand le sujet abordé demande une certaine appropriation.
- Proposer des alertes si les données à compléter ne le sont pas comme il le faudrait.
- Mettre en avant des rubriques nouveautés.
- Rendre récurrent les contenus importants ou prioritaires.
- Indiquer que l'application est payante, ou qu'elle contient des publicités pour des services payants.
- Faciliter le zoom sur les pages et les textes avec le navigateur, ou avec l'ajout d'une fonction grossissante.

NAVIGATION

RENDRE LE PARCOURS ET L'EXPÉRIENCE UTILISATEUR RÉUSSIS

Les actions minimales suivantes doivent être mises en oeuvre :

- Le processus d'inscription doit être simplifié.
- Un plan du site est accessible.
- L'objectif du service doit être atteint en maximum 3 clics.
- Le retour à la page d'accueil doit être atteinte en 1 clic maximum.
- La page accueil doit être mentionnée dans le menu.
- Le menu doit être fixe, quelle que soit la page où l'on se trouve.
- Une tâche ou une action doit pouvoir être arrêtée en cours et pouvoir être reprise, et ne doit pas avoir une limite de temps pour être accomplie.



SOURCES & LIENS UTILES

Introduction au RGAA Lien

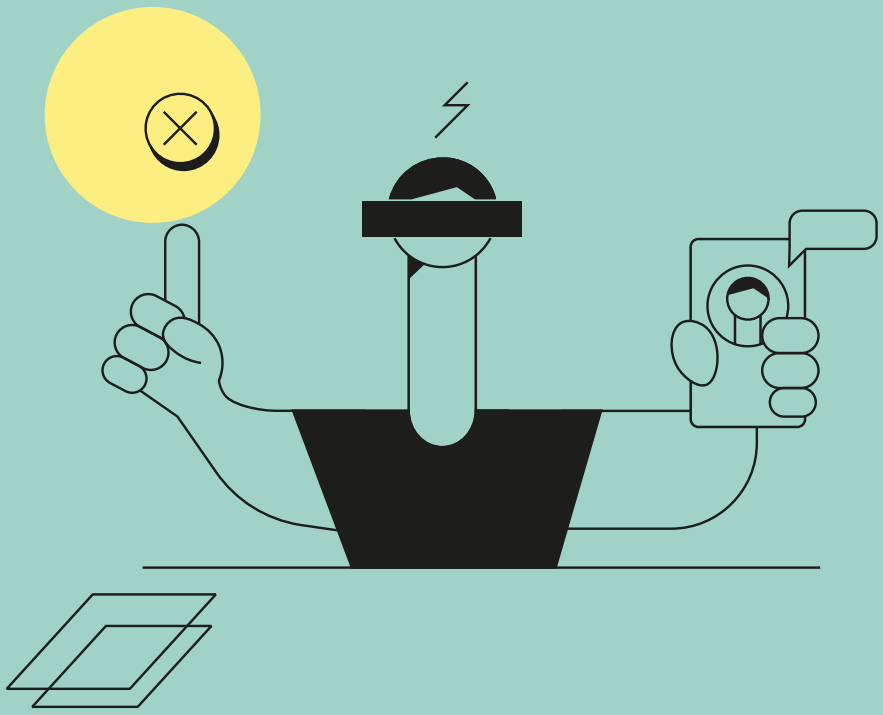
Web Accessibility Initiative, 1996.

Reconnaissance des WCAG 2.0 comme standard de référence par l'Europe.

En conformité avec les critères des WCAG 2.0. La Direction interministérielle du numérique et du système d'information et de communication de l'État (DInSIC) organise et anime le cadre de concertation nécessaire à l'évolution du RGAA.

Critères du RGAA Lien

JURIDIQUE & RGPD



« Le respect de la vie privée de l'utilisateur est une caractéristique indispensable d'un service de confiance »

Le volet juridique de l'évaluation porte notamment sur la vérification de la conformité des services soumis par les éditeurs au cadre juridique applicable aux CGU, CGV, mentions légales, et protection des données personnelles le cas échéant. Les données personnelles sont en effet soumises à un régime juridique particulier : le Règlement Général sur la Protection des Données (RGPD) du 27 avril 2016, entré en vigueur le 25 mai 2018, dispense les entreprises des formalités préalables à la mise en œuvre des traitements, mais impose d'autres obligations tournées vers le management qualitatif de la «data», assorties de sanctions plus fortes. Des spécificités françaises sont également prévues par la Loi Informatique et Libertés du 6 janvier 1978 modifiée.
C'est dans ce contexte complexe que les avocats Fidal interviennent en qualité d'évaluateurs sur les aspects juridiques. Ainsi, Fidal met à disposition des éditeurs partenaires de la CNAV des informations pratiques relatives à la conformité juridique en matière de protection des données personnelles dans l'environnement des sites web et des applications mobiles.

LES EXPERTS

GUILLAUME PEZZALI

Expert du droit de la distribution et de la consommation, il dirige le département de Droit économique de Fidal Paris. Ses domaines d'intervention : distribution, droit de la consommation, réglementaire santé, droit des technologies de l'information, propriété intellectuelle, concurrence et ce notamment pour des industriels du secteur de la santé.

MORGANE MOREY

Elle intervient sur des problématiques réglementaires pouvant se poser tout au long du cycle de vie des produits de santé et assimilés (de la qualification des produits aux contrôles post-market). Elle conseille les entreprises françaises et internationales de toute taille dans le secteur des Life Sciences (notamment les DM et produits frontière).

CAMILLE GAFFIOT

Experte en droit informatique et droit des données à caractère personnel, elle conseille les entreprises dans leurs stratégies d'e-commerce, de dématérialisation des processus internes ou d'utilisation de technologies innovantes, et dans le déploiement d'activités en ligne. Elle assiste les clients de Fidal dans leur mise en conformité juridique et opérationnelle au RGPD.

QUESTIONS Juridiques

CGU ET MENTIONS LÉGALES

EN MA QUALITÉ D'ÉDITEUR D'UNE APPLICATION EN LIGNE, DOIS-JE PUBLIER DES MENTIONS LÉGALES SUR MON SERVICE ? DE QUOI S'AGIT-IL ?

Les mentions légales au sens de la Loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) doivent obligatoirement être publiées par tout service de communication en ligne telle qu'une application ou un site internet, à savoir :

- l'identité et les coordonnées de la personne physique ou morale qui édite l'application ;
- le « directeur de la publication » ou, plus simplement, la personne physique qui détermine le contenu disponible ;
- l'identité et les coordonnées de l'hébergeur.

Ces informations doivent être aisément accessibles.

DOIS-JE RÉDIGER DES CONDITIONS GÉNÉRALES D'UTILISATION (CGU) ?

Pour tout service mis à disposition d'un utilisateur, la bonne pratique est de rédiger des CGU qui vont régir les relations entre l'éditeur de l'application et l'utilisateur. Afin que les CGU soient opposables à l'utilisateur, il est notamment requis que ces CGU soient portées à la connaissance de l'utilisateur lors de l'accès au service et que l'utilisateur accepte expressément ces conditions.

À RETENIR

- **Publier et mettre à jour régulièrement des mentions légales et des CGU sur une page dédiée.**
- **Recueillir le consentement de l'utilisateur aux CGU par le biais d'une case à cocher avec la mention « J'ai pris connaissance et j'accepte les conditions générales d'utilisation ».**

À ÉVITER

- **Absence de mentions légales ou des mentions légales difficiles à trouver.**
- **Mentions légales incomplètes ou obsolètes, non mises à jour.**
- **Accès au service proposé via l'application sans CGU ou sans recueillir le consentement de l'utilisateur aux CGU.**

COLLECTE DES DONNÉES PERSONNELLES DES UTILISATEURS DU SERVICE

JE COLLECTE DES DONNÉES PERSONNELLES RELATIVES AUX UTILISATEURS DE MON SERVICE. DOIS-JE RECUEILLIR LE CONSENTEMENT DES UTILISATEURS À CETTE COLLECTE, ET SOUS QUELLE FORME DOIS-JE RECUEILLIR CE CONSENTEMENT ?

Toute information relative à une personne physique qui permet de l'identifier (personne concernée) est une donnée personnelle – même « pseudonymisées » ou « anonymisées ».

En cas de traitement de données personnelles, il faut:

- Identifier la base légale appropriée. Les données personnelles ne peuvent être traitées que sur l'une des bases légales prévues par le RGPD. Il s'agit, à titre non exhaustif, de l'exécution d'un contrat (ex. : des CGU), du respect d'une obligation légale ou du consentement de l'utilisateur. Le fondement peut également être l'intérêt légitime de l'entreprise vis-à-vis de ses utilisateurs, mais il requiert une analyse au cas par cas pour s'assurer de sa réalité.
- D'autre part, définir les finalités du traitement. Ici, il faut analyser quelles données des personnes concernées sont collectées pour le bon fonctionnement du service proposé et déterminer la nécessité de leur collecte au regard du service rendu. Si ces données ne sont pas nécessaires aux finalités identifiées, il ne faut pas les collecter.

À RETENIR

- **La collecte de données personnelles doit être justifiée au regard des objectifs poursuivis et doit être fondée sur l'une des bases légales du RGPD.**
- **En cas de collecte de données sensibles : identifier la base légale, les finalités, l'exception applicable au regard du RGPD et évaluer la nécessité de collecter ces données et de mener une AIPD (Analyse d'Impact relative à la Protection des Données).**
- **En cas de recueil du consentement : distinguer le recueil du consentement pour le traitement des données personnelles, du consentement aux CGU.**

Le RGPD pose le principe du recueil du consentement des personnes concernées pour la collecte de leurs données, mais en pratique, le consentement est l'exception et s'applique le plus souvent pour la collecte de données dites sensibles. Enfin, le consentement de l'utilisateur doit être une manifestation de volonté :

(i) libre – l'utilisateur doit être en mesure de refuser ;

(ii) spécifique – l'utilisateur consent pour une finalité précise et non pour une finalité trop large ou vague. L'écueil classique ici est de cumuler le consentement pour les CGU avec celui pour le traitement de données personnelles. Ces deux consentements doivent être distincts ;

(iii) éclairée – l'utilisateur a été informé valablement au titre du RGPD ;

(iv) univoque – sans ambiguïté, souvent matérialisée par une case à cocher.

À ÉVITER

- **Collecter des données personnelles sans objectif précis.**
- **Conserver les données personnelles collectées sans limitation de durée.**
- **Recueillir le consentement pour la collecte des données via l'acceptation des CGU.**

QUE DOIS-JE FAIRE SI LES UTILISATEURS DE MON SERVICE SONT AMENÉS À ME COMMUNIQUER DES DONNÉES « SENSIBLES » ?

La collecte de données sensibles ne peut être fondée que sur des exceptions prévues par le RGPD. Il faudra donc, d'une part, mener le travail classique d'identification de la base légale appropriée et des finalités, et ensuite, identifier l'exception applicable à la collecte de données sensibles, telle que le consentement.

Il peut aussi être nécessaire de mener une « AIPD » (Analyse d'Impact relative à la Protection des Données, PIA étant l'acronyme anglais de « Privacy Impact Assessment ») préalablement à la mise en œuvre du service.

QU'EST-CE QU'UNE DONNÉE DE SANTÉ ? SI MON SERVICE COLLECTE DES DONNÉES DE SANTÉ, QUELLES SONT LES OBLIGATIONS LÉGALES À RESPECTER ?

Une donnée de santé est une information relative à la santé physique ou mentale d'une personne concernée. Il s'agit également des informations obtenues lors de tests ou d'examens d'une partie du corps ou d'une substance corporelle. A titre d'exemple, il peut s'agir d'une maladie, d'un handicap, d'un risque de maladie, d'antécédents médicaux ou d'un traitement clinique ou de l'état physiologique ou biomédical de la personne concernée. Ce type de données entre dans la catégorie des données « sensibles ».

LES FINALITÉS DE MON TRAITEMENT DE DONNÉES PERSONNELLES DOIVENT ÊTRE EXPLICITES, DÉTERMINÉES ET LÉGITIMES. QU'EST-CE QUE CELA SIGNIFIE ?

Afin de respecter ces critères, le responsable du traitement doit analyser les objectifs de la collecte et les identifier précisément. Ces objectifs doivent également être légitimes, c'est-à-dire qu'une base légale doit justifier le traitement. Enfin, ces finalités et la base légale appropriée doivent être portées à la connaissance de l'utilisateur et ce préalablement à l'utilisation du service – par exemple, via l'acceptation d'une Politique de confidentialité.

COMMENT DOIS-JE DÉTERMINER ET AFFICHER LES DURÉES DE CONSERVATION APPLICABLES AUX DONNÉES PERSONNELLES QUE JE COLLECTE ?

La durée de conservation doit correspondre à la période nécessaire à la réalisation des finalités du traitement. Au-delà de cette durée, les données personnelles doivent être détruites ou archivées.

Cette période peut s'aligner sur les délais de prescription en matière contractuelle, ou correspondre à des besoins opérationnels que l'entreprise doit impérativement justifier.

TRAITEMENT DES DONNÉES PERSONNELLES ET INFORMATION DES UTILISATEURS DU SERVICE

À RETENIR

- **L'information relative aux données personnelles doit être mise à disposition de l'utilisateur au plus tard lors de la validation de son inscription ou de la création de son compte.**
- **L'information doit figurer dans un document distinct des CGU et être présentée et rédigée de manière claire.**

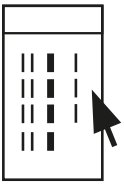
QUELLES INFORMATIONS DOIS-JE FOURNIR EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES ?

Préalablement à la collecte de données, l'utilisateur doit être informé du traitement de données personnelles le concernant, à savoir :

- l'identité et les coordonnées du responsable de traitement (l'éditeur de l'application) ;
- les coordonnées du Délégué à la protection des données (DPO) ;
- les finalités et les bases légales des traitements des données personnelles ;

- les destinataires des données personnelles (il peut s'agir des prestataires techniques, tels que les hébergeurs, qui pourront être amenés à traiter ces données) ;
- les éventuels transferts de données personnelles hors de l'UE ainsi que le cadre juridique de ces transferts ;
- les durées de conservation ;
- les droits dont disposent les personnes concernées sur les données personnelles.

Ces informations doivent être aisément accessibles à l'utilisateur.



À ÉVITER

- **Intégrer l'information relative aux données personnelles au sein des CGU.**
- **Des CGU ou une Politique de confidentialité introuvables ou difficilement accessibles pour les utilisateurs.**

COMMENT CETTE INFORMATION DOIT-ELLE ÊTRE RENDUE ACCESSIBLE À L'UTILISATEUR DE MON SERVICE ? A QUEL MOMENT ?

Elle doit être fournie avant la collecte ou au plus tard lors de la collecte. A titre d'exemple, l'accès à la Politique de confidentialité doit être donné au plus tard lors de la validation d'un formulaire d'inscription.

La bonne pratique en matière d'accessibilité de l'information est que la Politique de confidentialité ne doit jamais être à plus de deux clics. En outre, l'information relative aux données personnelles, pour être accessible, doit être distincte des CGU qui est un document considéré comme peu lisible. Pour un site internet, les différents liens vers les mentions légales, les CGU, et la Politique de confidentialité pourra figurer en pied de page.

TRANSFERT – HÉBERGEMENT INTERFACES TIERCES

JE FAIS APPEL À DES PRESTATAIRES OU ENTREPRISES EXTERNES POUR DES SERVICES QUI IMPLIQUENT DE TRAITER DES DONNÉES PERSONNELLES. QUE DOIS-JE FAIRE ?

Selon le pouvoir décisionnel de ces différents acteurs sur la donnée, ils peuvent être qualifiés de coresponsable du traitement ou bien de sous-traitant au sens du RGPD. En cas de relation de sous-traitance, il est obligatoire de mettre en place un contrat de sous-traitance selon les termes du RGPD.

À RETENIR

- **Identifier les transferts hors UE.**
- **Mettre en place les garanties appropriées telles que les Clauses Contractuelles Type de la Commission européenne.**
- **Informer les utilisateurs de ces destinataires et de ces transferts**

MON ENTREPRISE EST ÉTABLIE HORS DE L'UNION EUROPÉENNE (UE) OU DE L'ESPACE ECONOMIQUE EUROPÉEN (EEE) OU CERTAINS PRESTATAIRES OU ENTREPRISES EXTERNES À MON ENTREPRISE QUI SONT AMENÉS À TRAITER DES DONNÉES PERSONNELLES DES UTILISATEURS DE MON SERVICE SONT ÉTABLIS HORS DE L'UE OU DE L'EEE. QUE DOIS-JE FAIRE ?

On parle de transfert de données personnelles lorsque les données personnelles sont transférées depuis le territoire européen vers un ou des pays situés hors de l'UE ; le transfert peut s'effectuer par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre. Il peut s'agir d'un prestataire d'hébergement de données situé à l'étranger.

Dans une telle hypothèse, le transfert de données doit être encadré par ce que le RGPD appelle une « garantie appropriée ».

Ce terme désigne les mécanismes d'encadrement juridique des flux de données personnelles hors UE : Privacy Shield, Clauses Contractuelles Types, Règles d'Entreprise Contraignantes, décision d'adéquation.

En cas de transfert hors UE, l'éditeur doit mettre en place une telle garantie, mais aussi fournir aux utilisateurs un moyen de consulter le texte de ces garanties – il s'agit d'une mention obligatoire imposée par le RGPD. Concrètement, cela peut être un lien URL vers le site du Privacy Shield, ou bien vers les Clauses Contractuelles Types de la Commission européenne, ou bien vers la décision d'une autorité de contrôle qui valide les Règles d'Entreprise Contraignantes autorisant les transferts hors UE au sein d'une même entreprise, ou encore vers une décision d'adéquation de la Commission européenne qui autorise les transferts de données vers un Etat tiers à l'UE.

À ÉVITER

- **Recourir à des prestataires ou des partenaires qui traitent de la donnée sans s'informer du lieu de leur activité ou des modalités d'hébergement des données.**
- **Ne pas informer les utilisateurs de ces destinataires ou de ces transferts.**

COOKIES ET TRACEURS PUBLICITÉ

QUELLE INFORMATION DOIS-JE FOURNIR CONCERNANT LES COOKIES ET SOUS QUELLE FORME ?

Les données collectées via les cookies et traceurs sont considérées comme des données personnelles. La personne concernée doit donc être informée de cette collecte, notamment par le biais d'un bandeau d'information lors de l'arrivée sur le site ou sur l'application, ou par un dispositif de *consent management platform*.

Certains cookies et traceurs, nécessaires au bon fonctionnement du site ou de l'application ou utilisés pour mesurer l'audience, ne nécessitent pas le consentement de l'utilisateur, dans des conditions strictes définies par la Commission Nationale de l'Informatique et des Libertés (CNIL). Hors de ces critères, le consentement doit obligatoirement être recueilli.

DE LA PUBLICITÉ CIBLÉE EST PROPOSÉE VIA MON SERVICE. QUE DOIS-JE FAIRE ?

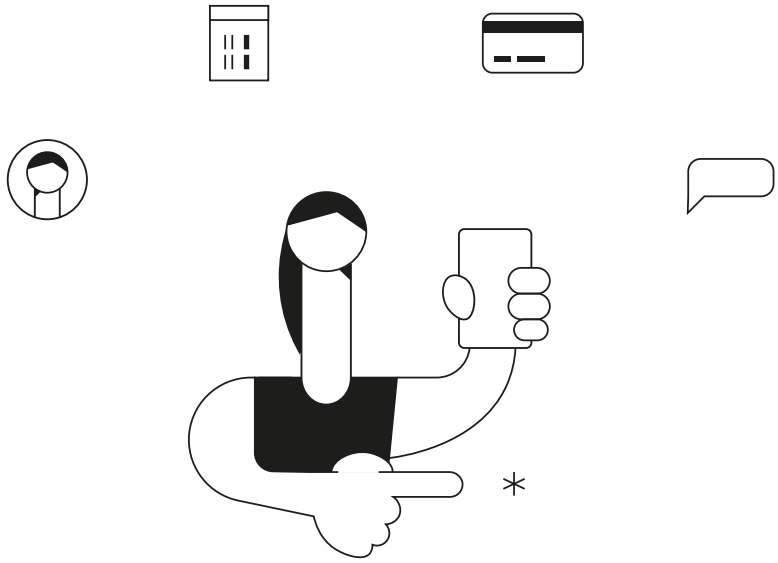
L'utilisateur doit obligatoirement être informé de l'utilisation faite de ses données personnelles aux fins de lui proposer de la publicité ciblée. Il doit être en mesure de refuser librement cette utilisation.

À RETENIR

- **Informer l'utilisateur du traitement de cookies et/ou autres traceurs dès son arrivée sur le site ou sur l'application.**
- **Recueillir le consentement de l'utilisateur lorsque cela est nécessaire, c'est-à-dire en particulier en matière de publicité ciblée.**

À ÉVITER

Un bandeau d'information cookies « creux » qui ne permet que d'accepter, sans information sur le traitement ou lien vers une Politique de confidentialité qui aborde les cookies, et sans possibilité de sélectionner les cookies acceptés ou refusés.



SOURCES & LIENS UTILES

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) Lien

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Lien

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique Lien

Groupe de travail de l'article 29, Lignes directrices sur la transparence Lien

CNIL, Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) Lien

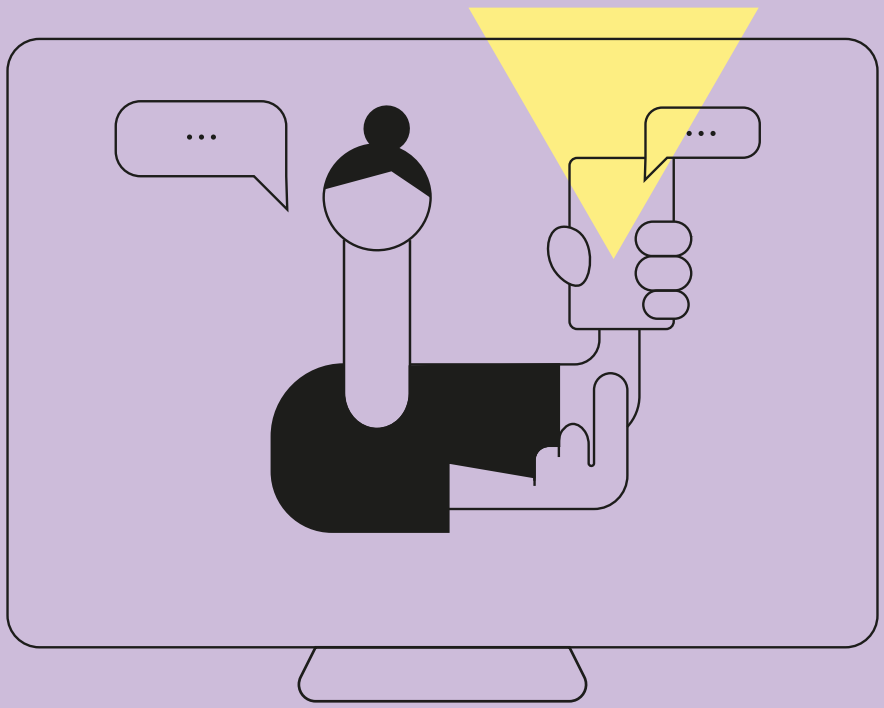
CNIL – Applications mobiles en santé et Données personnelles Lien

CNIL – Site web, cookies et traceurs Lien

CNIL – Atelier RGPD Lien

HAS – Applis Santé : Règles de bonnes pratiques Lien

PERTINENCE DU CONTENU



« “Il n’y a pas de vie minuscule”. Inventer des services innovants permet à la société inclusive de développer l’accessibilité universelle. »

Le contenu doit être pertinent et correspondre au profil de la personne à qui il s'adresse et apporter une amélioration notable de sa vie quotidienne, ainsi que celle des aidants et de son entourage. Le contenu proposé dans les services doit être facilement accessible sans contrainte technique particulière. Fort de notre expérience dans l'évaluation d'applications mobiles et de sites web, nous proposons des éléments de réflexions afin d'aider les concepteurs de solutions innovantes, actuels et futurs, à améliorer le contenu de leurs sites ou d'applications.

L'EXPERT :
JACQUES BERMONT

Professeur spécialisé pour les élèves à besoins éducatifs particuliers (BEP) retraité, Jacques Bermont a créé « illuminer le flou », microentreprise de conseil sur la déficience visuelle (DV). Il exerce une veille sur les produits technologiques à destination des personnes DV de tous âges et conseille ces personnes sur les outils de compensation. Il forme les usagers à l'utilisation de ceux-ci et accompagne les Institutions dans leurs démarches vers l'accessibilité universelle, via des sensibilisations, des rencontres, des documentations, des formations.
Ses partenaires : Les associations pour déficience visuelle UNADEV, Ouvrir Les Yeux.
Les universités : Université d'Artois, ULCO, Université Jules Vernes, bibliothèque universitaire d'Artois, bibliothèque municipales de Douai.

PANORAMA DES SOLUTIONS PROPOSÉES aux personnes âgées et/ou en situation de handicap

COMMUNICATION FAMILIALE
Conserver les liens familiaux à distance par le partage de photos, de vidéos, édition de livres, journaux familiaux.

ENTRAIDE À DISTANCE
Gestion des documents administratifs avec transmission simplifiée.

SOLIDARITÉ, RENCONTRE, ENTRAIDE
Services de voisinage de la tasse de thé à la petite réparation.

SURVEILLANCE SANTÉ
Solution domotique de surveillance avec alerte à distance (capteurs dans les lieux de vie et liaison à distance avec aidants).

ACQUISITION DE SAVOIRS À DISTANCE
Culture numérique et formation aux technologies du numérique, amélioration des savoirs et savoirs faire, lutte contre l'illettrisme numérique. Échanges culturels, conférences en direct ou en différé. Sujets allant de l'acquisition de savoirs pratiques, couture, tricot, cuisine, aux cours du collège de France.

DES EXIGENCES À RESPECTER, des questions à se poser

ACCESSIBILITÉ

RESPECTER LES PRINCIPES ET LES RÈGLES POUR L'ACCESSIBILITÉ DES CONTENUS WEB

Il y a 4 principes & 12 règles à suivre (voir sources et liens utiles).

CANAUX DE COMMUNICATION ALTERNATIFS

Favoriser l'accessibilité de l'application mobile ou du site en proposant :

- Un accès audio, avec une alternative vocale aux images, schémas, tableaux, un réglage du débit de l'option audio.
- Un accès en LSF, Langue des Signes Française et/ou en LPC, Langage Parlé Complété.
- Proposer la personnalisation du site par le choix de la police, l'augmentation de la taille des polices, en modifiant les couleurs, les contrastes.
- Proposer des articles rédigés selon les règles du facile à lire et à comprendre.
- Les contenus proposés avec les outils d'accessibilité sont identiques à ceux du site originel.

COMPATIBILITÉ AVEC DES OUTILS EXTERNES DE L'ACCESSIBILITÉ

L'utilisateur doit pouvoir naviguer dans l'application ou le site en utilisant uniquement le clavier ou avec une plage braille et un lecteur d'écran (VoiceOver, TalkBack, NVDA). Via un écran tactile, en commandant à la voix, en utilisant une boucle magnétique, ou tout autre périphérique adapté.

COMPATIBILITÉ AVEC LES PLATEFORMES (ORDINATEUR, TABLETTE, SMARTPHONE)

Conception du site en Responsive Web Design RWD2.

SIMPLICITÉ D'USAGE DE L'APPLICATION

Temps d'apprentissage et de prise en main simple, prévoir une démonstration simple et accessible à tous.

PRÉREQUIS

La prise en main doit être simplifiée avec peu de prérequis quant à l'usage de l'outil informatique. Il est indispensable de proposer un mode d'emploi détaillé en plus de la démo, une FAQ et un contact avec les concepteurs.

À ÉVITER

- **Demander de saisir des adresses de liens ou des lignes de code pour obtenir l'information.**
- **Demander des captcha complexes, lettres entremêlées ou reconnaissance d'image. En fonction du public cible, cela peut être rédhibitoire.**

CIBLE

- Étudier la population concernée pour être en adéquation avec ses besoins et proposer des contenus de qualité.
- Faire tester l'application ou le site par un échantillon cible.

COÛT, PÉRIODE D'ESSAI

Une période d'essai gratuite doit apparaître clairement ainsi que le coût de l'application en cas de souscription avec les conditions de celle-ci (achat définitif, abonnement simple, reconductible, avec mise à jour ou pas).

RÔLE DES AIDANTS

(FAMILIAUX OU PROFESSIONNELS)

- Quel bénéfice l'application/le site leur apporte-t-il ? Exemple : conservation des liens familiaux, interaction avec les services d'aide à domicile
- Quelle place ont-ils dans le projet ?

AUTONOMIE DE L'USAGER

- Peut-il gérer seul l'application ? Entrer des paramètres de personnalisation, des informations, des documents ?
- L'application augmente-t-elle la charge des aidants (familiaux, professionnels) ?
- Quelles compétences sont requises de la part des aidants pour le paramétrage de l'application ?
- Peut-on gérer le service à distance ? Obtenir un dépannage / réinitialisation ?

ESTHÉTIQUE / PRÉSENTATION

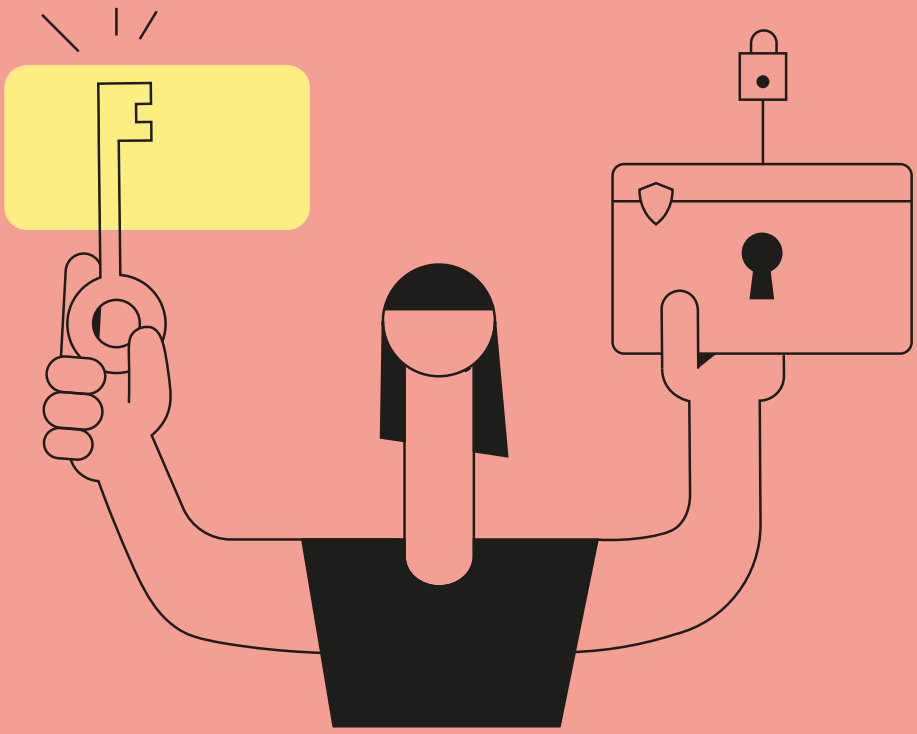
GÉNÉRATEUR DE BIEN ÊTRE VS STRESS !

- S'assurer de la compatibilité des couleurs en cas de contraste de texte sur un fond coloré.
- Présentation gaie, colorée avec un fond musical agréable (déconnectable).
- Fonds d'écran personnalisables avec des photos personnelles ou proposées par l'application.
- Options de personnalisation avec enregistrement du profil et paramètres automatiques.
- Conserver du lien avec ses proches ne doit pas générer de stress dans la relation à distance ou dans l'utilisation de l'outil.

SOURCES & LIENS UTILES

Accessibilité : WCAG 2.0 Règles pour l'accessibilité des contenus Web (WCAG) 2.0 / Responsive Web Design / Les couleurs / JAWS / NVDA

SÉCURITÉ NUMÉRIQUE



« Le moindre maillon défaillant de la chaîne de la sécurité risque la compromission de tout le système »

LES EXPERTS

RAPHAËL WALTER

Ingénieur de formation,
il est Responsable RedTeam
chez SEKOIA.

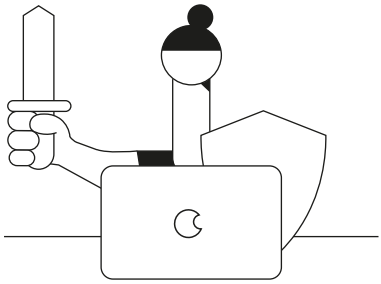
YOHANN FALLOURD

Ingénieur de formation,
il est Ingénieur Cybersécurité
chez SEKOIA.

SEKOIA est un acteur francophone majeur, dédié uniquement au domaine de la cybersécurité accompagnant au quotidien des grands comptes, des institutions et des entreprises innovantes pour les conseiller sur leur stratégie, les préparer et leur offrir support et assistance dans l'exercice de leurs métiers comme dans les phases les plus critiques d'exposition aux menaces cybers.

Lors du développement d'applications mobiles ou web, le moindre maillon défaillant de la chaîne de la sécurité risque la compromission de tout le système. Ainsi, il est important de considérer la sécurisation de chaque potentiel point d'entrée pour un attaquant.

Notre propos a pour but de présenter des bonnes pratiques de développement permettant de se protéger des vulnérabilités le plus souvent observées par les experts de Sekoia qui travaillent sur l'évaluation des applications et des sites web.



Comment SE PROTÉGER DES VULNÉRABILITÉS ?

LES MOTS DE PASSE

EXEMPLES

- **Une politique de mot de passe faible facilite la tâche d'un attaquant car les utilisateurs se cantonnent généralement au niveau de sécurité minimal.**
- **Une non-invalidation du jeton de réinitialisation de mot de passe peut permettre à un attaquant y accédant, par exemple par compromission de la boite mail liée au compte, de redéfinir un nouveau mot de passe et donc voler le compte.**

UNE POLITIQUE SOLIDE ET UN TRAITEMENT SÉCURISÉ

Un des principaux risques pour les applications web et mobiles d'aujourd'hui est le vol de compte. En effet, il est généralement plus facile pour un attaquant d'exploiter l'utilisation d'un mot de passe faible ou facilement devinable que de découvrir des vulnérabilités techniques et risquées d'exploitation.

Ainsi, la définition d'une politique de mot de passe adaptée est une étape primordiale lors du développement d'une application. Selon les pratiques communément admises, une bonne politique de mot de passe se doit de vérifier les points suivants:

- Elle doit imposer une complexité suffisante pour limiter les possibilités de définir un mot de passe trivial (azerty, aaaaaa, motdepasse, 123456, etc.)
- Elle doit être suffisamment permissive pour éviter à l'utilisateur de devoir recourir à un canal auxiliaire pour se souvenir de son mot de passe (post-it, agenda, ...)
- Elle doit s'adapter à l'application et au contexte. Ainsi, un utilisateur accédant à une application vitrine sans données personnelles n'a pas besoin d'un mot de passe aussi complexe qu'un administrateur accédant à l'interface de configuration.

S'il n'existe donc pas une politique de mot de passe « miracle », un compromis de complexité peut être trouvé afin d'offrir un niveau de sécurité acceptable. Ainsi, l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI)

recommande, au vu des puissances de calcul actuelles, « un mot de passe d'au moins 10 caractères en s'autorisant à utiliser un éventail large de caractères (majuscule, minuscule, chiffre et caractères spéciaux) ».

Un autre aspect vulnérable d'une application est la fonctionnalité de réinitialisation de mot de passe. Ici, la bonne pratique est d'envoyer un mail à l'utilisateur contenant un lien unique et valable pendant 24h. Lorsque le lien est cliqué, l'utilisateur est amené à définir un nouveau mot de passe en accord avec la politique de mot de passe définie précédemment et le lien de réinitialisation est invalidé.

L'AUTHENTIFICATION

EXEMPLES

- **Un attaquant ayant volé un jeton de session peut naviguer indéfiniment si ce dernier n'est jamais invalidé par le serveur.**
- **Un message de réinitialisation de mot de passe non-uniformisé permet à un attaquant de découvrir des identifiants de connexion valides et l'absence de protection anti-bruteforce lui permet d'essayer de se connecter avec les mots de passe les plus souvent utilisés.**

ACCÈS SÉCURISÉ ET CYCLE DE VIE D'UNE SESSION

L'authentification sert à reconnaître un utilisateur et à lui offrir un accès à des fonctionnalités et données spécifiques à son identité. Ainsi, la sécurité de ce mécanisme doit être adaptée au caractère sensible ou non de ces fonctionnalités. L'authentification, c'est-à-dire l'identification de la personne accédant à l'application, peut se faire via trois moyens :

- Ce que l'utilisateur sait (mot de passe, code PIN, ...)
- Ce que l'utilisateur a (token, carte, smartphone, ...)
- Ce que l'utilisateur est (empreinte digitale, rétinienne, ...)

L'authentification généralement est réalisée via un seul facteur, souvent un mot de passe (ce que l'utilisateur sait). Cependant, dans les cas où l'accès concerne des données sensibles ou des fonctionnalités à fort impact sur l'application, la bonne pratique est de mettre en place une solution d'authentification à deux facteurs, soit utilisant deux des moyens cités plus haut.

Une fois l'authentification effectuée, plusieurs possibilités existent pour que le serveur garde en mémoire l'identité de l'utilisateur. Deux exemples sont :

- **Avec état :**

Le serveur garde une trace de l'authentification de son côté et stocke des informations concernant l'utilisateur et sa navigation sous la forme d'une

session. L'utilisateur se voit affecter un jeton aléatoire et non prédictible servant à identifier l'objet de session côté serveur.

- **Sans état :**

Le serveur affecte un cookie contenant des informations sur l'utilisateur, par exemple au format JWT. Ces informations sont signées pour éviter leur modification et sont lues par le serveur à chaque requête par le client.

Quelle que soit la solution retenue, le cycle de vie de la connexion doit rester le même. Lorsque l'utilisateur s'authentifie, une date d'expiration est définie après laquelle ce dernier doit se réauthentifier. De plus, lorsque l'utilisateur change son mot de passe ou se déconnecte, toute session (avec ou sans état) doit être invalidée et l'application doit redemander une authentification afin de limiter l'impact d'un vol de session.

Il est également à noter que le portail d'authentification est une cible privilégiée pour les attaques de type bruteforce ou d'énumération de compte valides. L'uniformisation de la réponse du serveur permet d'éviter de révéler l'existence d'un compte en base de données, par exemple lors d'une réinitialisation de mot de passe où la réponse doit toujours être un message de la forme « Si ce compte existe, un message concernant la réinitialisation du mot de passe vient d'être envoyé à l'adresse mail fournie ».

Une protection contre le bruteforce doit également être mise en place afin de compliquer les attaques automatisées. Cela peut se faire via l'utilisation d'une solution telle que ReCAPTCHA v3 ou en imposant manuellement une limite sur le nombre de tentatives de connexions possibles.

SÉCURISATION DES COMMUNICATIONS

EXEMPLES

- **L'utilisation de protocoles dépréciés tels que TLS 1.0 expose l'application a des interceptions de données sensibles par des attaquants sur le réseau.**
- **L'absence de l'entête HSTS permet à un attaquant en interception réseau de faire naviguer la victime en HTTP et donc voir le trafic en clair.**

PROTOCOLES & BONNES PRATIQUES

Lors de l'utilisation de l'application, des données sensibles peuvent transiter entre le client et le serveur. Le trafic réseau passant via des canaux non-maîtrisés, il est important de s'assurer qu'il n'est pas possible pour un attaquant en interception d'accéder aux données sensibles en transit.

L'utilisation correcte du protocole HTTPS permet de chiffrer les données en transit et donc empêcher leur vol par un attaquant en interception réseau. Il est cependant nécessaire de s'assurer que la configuration du protocole est aussi sécurisée que possible sans sacrificier de façon excessive l'accessibilité de votre application. Ainsi, conformément aux bonnes pratiques communément reconnues, l'utilisation du protocole TLS v1.2, plus sécurisé que la version 1.1 et 1.0 qui sont en fin de vie du fait des vulnérabilités qui y ont été découvertes, est à privilégier si possible.

Après configuration du protocole HTTPS, il est nécessaire de rendre son utilisation obligatoire afin d'éviter les attaques par redirection HTTP. Une redirection du trafic HTTP vers le HTTPS et l'en-tête de réponse HSTS permettant de forcer la navigation sécurisée au niveau du navigateur du client doivent être mis en place.

TRAITEMENT DES ENTRÉES UTILISATEUR

PAS DE CONFIANCE AVEUGLE & CONTRÔLE CÔTÉ SERVEUR

Une règle d'or de la sécurité applicative est de ne jamais faire confiance à l'utilisateur et de toujours considérer qu'il essaiera de contourner le fonctionnement normal de l'application.

EXEMPLES

- **Les injections SQL sont possibles lorsqu'un utilisateur entre du code SQL (ex : Robert') ; DROP TABLE Users;--) dans un champ dont le contenu est passé à une requête SQL sans filtrage.**
- **Les XSS sont dues à une absence de filtrage des caractères utilisés pour le code client. Un attaquant peut entrer du code HTML/JavaScript qui sera exécuté sur le navigateur de tout utilisateur visitant une page qui affiche la charge utile.**

Ainsi, chaque champ acceptant des valeurs fournies par l'utilisateur doit faire l'objet de considérations réfléchies sur les contraintes appliquées à la donnée. Par exemple, il est nécessaire de filtrer certains caractères dangereux permettant les injections SQL (', « , \, ...) ou les caractères utilisés pour le code côté client (<, >, « , ', ...) afin d'éviter les attaques XSS.

Quelle que soit la technologie utilisée, il existe des librairies introduisant des protections automatiques qu'il est préférable d'utiliser plutôt que de reprogrammer soi-même un filtrage.

Il convient également d'imposer un certain format de données quand cela est possible afin de limiter les abus. Cela passe par limiter le nombre total de caractères ou imposer un schéma, par exemple en n'acceptant que des chiffres pour un numéro de téléphone.

Pour finir, il est important de se rappeler que toute sécurité ou contrainte placée côté client peut être contournée. Il est donc nécessaire d'appliquer aussi certaines vérifications côté serveur afin de s'assurer que la donnée est correctement traitée.

CLOISONNEMENT & SÉCURISATION DES DONNÉES

VÉRIFICATION DES PERMISSIONS ET TRAÇABILITÉ

Une application web ou mobile héberge en général un grand nombre de données sensibles réservées à certains utilisateurs seulement. Ainsi, un cloisonnement solide des données repose sur le fait que seuls les utilisateurs ayant un besoin-d'en-connaître peuvent accéder à certaines données ou fonctionnalités. Plusieurs points doivent donc être mis en place et être non-contournables :

- Les permissions de l'utilisateur doivent être vérifiées avant chaque accès à une ressource sensible.
- Aucune donnée sensible ne doit être publiquement accessible, au risque de finir indexée sur les moteurs de recherche. Leur accès doit donc nécessiter une forme d'authentification préalable.
- Une journalisation des accès à la donnée doit être mise en place afin de garder une traçabilité et de pouvoir réagir rapidement à tout accès non-autorisé.
- Les objets sensibles hébergés sur l'application tels qu'un fichier téléversé par l'utilisateur doivent voir leur nom remplacé par un ID non prédictible, par exemple un UUID-4 pour rendre leur accès direct quasiment impossible.
- Pour les applications mobiles, aucune donnée sensible ne doit être stockée sur la carte SD et leur manipulation ne devrait être faite que par les fonctions fournies par le SDK Android ou iOS.
- Une application correcte et exhaustive de ces points empêche toutes les vulnérabilités habituellement liées aux fuites d'informations personnelles d'utilisateurs.

EXEMPLE

Une référence directe et non-sécurisée à un objet est une vulnérabilité où n'importe quel utilisateur en possession de l'URL d'un objet, via son ID unique par exemple, peut accéder à la ressource indépendamment de ses permissions.

Par exemple, si l'application transmet la facture de l'attaquant à l'adresse */facture?id=23* **que se passe-t-il si l'attaquant accède directement à** */facture?id=22* **?**

POLITIQUE DE MISE À JOUR

LOGICIEL & SYSTÈME

Une application repose généralement sur un grand nombre de composants logiciels différents, que ce soit sur le système qui l'héberge ou au sein même de la couche applicative. Lorsqu'une vulnérabilité est découverte dans un de ces composants logiciel par le fournisseur, ce dernier met une nouvelle version à disposition contenant un correctif.

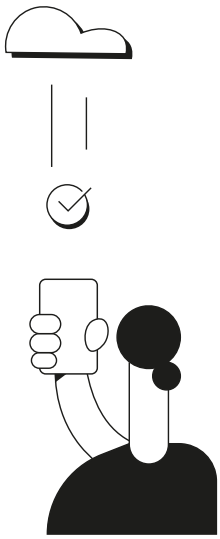
Dans le but d'éviter la présence de vulnérabilités publiquement connues sur l'application, il est important de définir une politique de mise à jour imposant certains délais à respecter pour mettre à jour les logiciels applicatifs et systèmes. Une politique de mise à jour est généralement définie comme suit :

- La découverte d'une vulnérabilité Critique au sein de la pile logicielle utilisée nécessite une mise à jour dans la semaine.
- Une mise à jour totale du système d'exploitation doit être effectuée toutes les deux semaines (cycle automatique pour Windows et recommandé pour Linux).
- Une mise à jour des logiciels applicatifs (Wordpress, plugins, etc..) est effectuée tous les deux mois sauf dans le cas d'une vulnérabilité critique.

Une politique de mise à jour dûment suivie protège contre un grand nombre des attaques automatisées visant à exploiter des vulnérabilités publiques.

EXEMPLE

Des scans existent pour les sites WordPress permettant d'obtenir la liste des plug-ins et leurs versions. Dans le cas où une vulnérabilité est découverte, l'attaquant peut l'exploiter.



ACCESSIBILITÉ NUMÉRIQUE

La WAI (Web Accessibility Initiative, 1996) définit l'accessibilité numérique comme le fait de rendre possible l'utilisation du web par les personnes en situation de fragilité. Plus précisément, qu'elles peuvent percevoir, comprendre, naviguer et interagir avec le web, et qu'elles peuvent contribuer sur le web. L'accessibilité du web bénéficie aux personnes âgées dont les capacités changent avec l'âge, et comprend tous les handicaps qui affectent l'accès au Web, ce qui inclut les handicaps visuels, auditifs, physiques, de parole, cognitifs et neurologiques.

Plus d'infos

AGRANDISSEUR D'ÉCRAN

Loupe virtuelle qui permet d'agrandir tout ou partie de l'écran. Logiciel spécialisé qui permet d'agrandir l'écran de modifier les paramètres du pointeur, du curseur, d'inverser les couleurs et comporte en option un lecteur d'écran. (Zoomtext, supernova).

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD) OU PRIVACY IMPACT ANALYSIS (PIA)

Évaluation, préalablement au traitement, du risque potentiel sur la vie privée de la personne concernée engendré par le traitement de ses données personnelles.

BASE LÉGALE

Il s'agit de l'élément qui légitime le traitement de données personnelles. Cela peut être notamment : une obligation légale (ex : une loi obligeant à recenser certains documents/données personnelles de l'utilisateur) ; un contrat ou mesures précontractuelles ; le consentement de la personne concernée (cette dernière a par exemple coché une case dans un formulaire permettant de traiter ses données personnelles) ; un intérêt légitime (par exemple lorsqu'il existe une relation commerciale ou de service entre le responsable du traitement et la personne concernée, ou lorsque des données sont utilisées uniquement à des fins de lutte contre la fraude) ; ou encore, l'intérêt vital de la personne concernée.

BRUTEFORCE

Attaque informatique dont le but est d'essayer toutes les combinaisons possibles d'une valeur afin d'éventuellement en trouver une qui soit valide. Généralement utilisée pour trouver des mots de passe, cette technique perd en efficacité proportionnellement à la longueur de la valeur à découvrir.

DONNÉE PERSONNELLE

Information permettant d'identifier directement ou indirectement une personne physique. Il peut s'agir d'un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou des informations spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

DONNÉES « SENSIBLES » OU « CATÉGORIE PARTICULIÈRE DE DONNÉE »

Les données dites « sensibles » sont des informations qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci, ou qui sont relatives à des condamnations ou infractions relatives à celles-ci.

HIÉRARCHIE DE L'INFORMATION

C'est le classement des informations effectué par un journal ou média (journal papier/radio/TV ou Internet) en ordonnant ces informations de la plus importante à la moins importante. C'est choisir l'information mise en avant, mais aussi éliminer les informations jugées secondaires. L'accès facilité aux médias (via internet), le flux croissant d'informations et les préoccupations propres à nos sociétés ont un impact sur le classement de l'information.

IDENTITÉ GRAPHIQUE

L'identité visuelle ou identité graphique exprime grâce à un style graphique propre à la structure, les valeurs, l'activité et les ambitions de celle-ci et se traduit par des signes, des couleurs, des formes, des textes ainsi que des mises en forme. L'identité graphique se décline sur les sites web ou applications mobiles. Lorsqu'elle est formalisée, elle s'exprime dans une charte graphique, qui précise par exemple les modalités de représentation du logo ou de l'insigne de l'entité.

Plus d'infos

JOURNALISATION

Enregistrement séquentiel dans un fichier (le «journal» ou «log») ou une base de données de tous les événements affectant un processus particulier. La journalisation permet de garder une trace des actions effectuées sur le système et l'analyse du journal permet de détecter les comportements anormaux des utilisateurs ou processus.

GLOSSAIRE

LECTEUR D'ÉCRAN, REVUE D'ÉCRAN

Logiciel d'assistance technique destiné aux personnes « empêchées de lire » : il retranscrit par synthèse vocale et/ou sur un afficheur braille ce qui est affiché sur l'écran d'un ordinateur tant en termes de contenu que de structure et permet d'interagir avec le système d'exploitation et les logiciels applications (Job Access With Speech, Non Visual Desktop Access).

NAVIGATION

Action de passer d'une information à une autre dans un document hypertexte ou hypermédia.

Plus d'infos

PERSONNE CONCERNÉE

Une personne concernée est la personne physique dont les données personnelles sont collectées.

RESPONSABLE DU TRAITEMENT

Désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités (pourquoi la donnée est-elle traitée ?) et les moyens (comment la donnée est-elle traitée?) du traitement de données personnelles.

SOUS-TRAITANT

Désigne l'entité ou la personne physique qui traite des données personnelles pour le compte du responsable du traitement. Exemple : prestataire Cloud, agence marketing, éditeur de logiciel.

SYNTHÈSE VOCALE

Permet de créer une alternative sonore avec une voix de synthèse à partir d'un texte (Text2speech)

TECHNOLOGIES D'ASSISTANCE

Matériel ou logiciel qui agit afin de fournir des fonctionnalités répondant aux besoins des utilisateurs ayant des limitations fonctionnelles.

TÉLÉVERSER

A l'inverse du téléchargement, qui consiste à récupérer un fichier depuis une source distante, le téléversement désigne l'envoi par le client d'un fichier vers une source distante (en anglais, to upload).

TRAITEMENT

Un traitement de données personnelle consiste en toute opération, informatique ou non, appliquées à des données ou des ensembles de données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

TYPOGRAPHIE

Procédé de composition et d'impression sur formes en relief (caractères mobiles, gravures, clichés). C'est également l'art d'utiliser les différents types de caractères dans un but esthétique et pratique.

Plus d'infos

UUID-4

Les UUID, ou Universally Unique Identifier, sont des suites de 128 caractères dont le mode de génération dépend de leur version et servant d'identificateurs qui sont soit garantis mondialement uniques ou sont mondialement uniques avec une haute probabilité. La version 4 est générée de manière totalement aléatoire et permet donc d'automatiser facilement la création d'objets identifiés de façon unique et dont l'identifiant est impossible à découvrir par bruteforce.

VOCALISATION DES AIDES TECHNOLOGIQUES

Complément naturel de la synthèse vocale, la vocalisation des aides technologiques permet d'obtenir des actions à partir de la commande vocale en langage naturel. Des exemples, SIRI pour la gestion vocale de l'IPHONE, Alexa, Google home, Cortana pour obtenir des services ou des renseignements à partir d'une interface d'intelligence artificielle.

Le présent guide, qui ne présente pas un caractère exhaustif, est un recueil de bonnes pratiques fournissant des pistes de réflexions et d'actions dont l'analyse et la mise en œuvre relèvent de la responsabilité des éditeurs de services numériques. L'actualité et la validité de son contenu peuvent évoluer postérieurement à sa publication.

Nos remerciements à Clémence Le Marrec, Responsable des actions collectives de prévention (Direction de l'action sociale CNAV Ile-de-France), aux experts Jacques Bermont, Gaël Guilloux, Guillaume Pezzali, Morgane Morey, Camille Gaffiot, Raphaël Walter, Johann Fallourd qui ont contribué à la rédaction du guide ainsi qu'à Yves Moly, Directeur technique et développement (DEKRA Certification France) et Frédéric Duvignaud, Responsable développement (DEKRA Certification France) pour leur relecture.

Edité le 18 juin 2020 par MEDAPPCARE (DEKRA) : 5 avenue Garlande, 92220 Bagneux
Responsable de la publication : Yvan Mainguy, Directeur général DEKRA Certification France
Graphisme, illustrations et maquette : Nicolas Martin
Imprimé en France par EXAPRINT : Business Plaza bât 2, 159 Rue de Thor, 34000 Montpellier

CE QU'EN DISENT LES ÉDITEURS

« Cette évaluation nous a permis de progresser de manière qualitative sur différents aspects et notamment sur le volet juridique »

« C'est logique car on veut être pertinent et conforme sinon on est dans le gadget »

« Normal que l'Assurance retraite Ile-de-France veuille évaluer les services qu'elle soutient »

« Point de vue très positif surtout dans le cadre de notre prochaîne levée de fond avec les résultats de l'évaluation à présenter »

« Suite aux résultats de l'audit, nous avons entamé des actions correctives notamment sur la vulnérabilité permettant l'exécution de code indésirable »

« Concernant le RGPD, c'est un sujet sur lequel nous avons à cœur de nous mettre en conformité rapidement »

« Nous allons qualifier la politique de mot de passe sécurisé qu'il faudra adapter »

MEDAPPCARE DEKRA

avec le soutien de Sécurité sociale l'Assurance Retraite Ile-de-France