fair & smart

PERSONAL DATA SOLUTIONS

Avec la participation de :

HAAS AVOCATS

Guide pratique de mise en oeuvre d'une solution de gestion des consentements

1ère édition - 2022

Nous contacter : contact@fairandsmart.com

SOMMAIRE

La gouvernance des données personnelles
au coeur d'une relation de confiance

Depuis 2016, Fair&Smart met en œuvre les technologies les plus innovantes au service d'une gestion éthique et transparente des données personnelles.
Nos solutions SaaS permettent aux organisations publiques et privées de gérer les aspects de la conformité RGPD et ePrivacy qui sont les plus visibles pour la personne concernée (Privacy UX) :

- gestion des demandes de droits RGPD : Right Requests ;
- acquisition et transferts de données personnelles : Right Data ;
- gestion des consentements et préférences : Right Consents.

Régulièrement plébiscitées par les analystes spécialisés comme Gartner ou Wavestone, nos solutions sont également labellisées PrivacyTech (AFNOR Certification). Toutefois, elles ne sont que des outils, dont la bonne mise en œuvre est cruciale et s'inscrit dans une démarche plus globale.

La gestion des consentements et préférences implique des interactions régulières avec la personne concernée. Au-delà des aspects liés à la conformité, elle peut être une bonne expérience, génératrice de confiance et d'engagement, ou une moins bonne expérience, génératrice de frustration ou de parcours utilisateur dégradé.

Forts de l'expérience acquise dans la mise en œuvre de solutions de collecte et de gestion du consentement (explicite et cookies), nous avons souhaité partager avec vous quelques bonnes pratiques et leçons apprises avec nos clients.

Ce guide s'adresse aux organisations de toute taille et de tout secteur d'activité, à tous les acteurs concernés, et se veut aussi concret que possible. Nous espérons que vous y trouverez toutes les clés pour sélectionner puis implémenter efficacement une solution de gestion du consentement adaptée à vos besoins.

Je remercie chaleureusement Me Gérard Haas, notre DPO, pour sa mise en avant éclairée des principaux points de vigilance juridiques à prendre en compte

N'hésitez pas à nous faire part de vos retours ou à nous contacter directement si vous avez des questions que nous n'avons pas abordées.

A la frontière entre obligations légales, contraintes techniques et parcours utilisateur, la gestion des consentements est le visage d'une gestion éthique et transparente des données personnelles, condition essentielle du succès des services numériques de demain.

Xavier Lefevre
CEO Fair&Smart

Le consentement
armure numérique de la donnée personnelle

« M'avez-vous, avant le mariage, demandé mon consentement, et si je voulais bien de vous ? Vous n'avez consulté, pour cela, que mon père et ma mère ; ce sont eux proprement qui vous ont épousé. »

Molière (George Dandin ou le Mari confondu)

Gérard HAAS

Le consentement a un rôle central dans le règlement général de la protection des données.
Il constitue, en effet, l'un des fondements possibles pour traiter des données à caractère personnel applicable notamment lorsqu'aucun fondement n'est envisageable. Lorsqu'il ne sert pas de fondement au traitement, il constitue une protection pour la personne concernée.

Selon les dispositions du règlement, lorsque le traitement repose sur le consentement, le responsable de traitement (RT) doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement des données personnelles le concernant (RGPD, art. 7).

Le règlement précise clairement que le consentement nécessite alors une déclaration de la part de la personne concernée ou un acte positif clair, c'est-à-dire un acte délibéré de la personne afin de donner son consentement au traitement spécifique (RGPD, cons. 32).

Si le consentement peut ainsi être recueilli au moyen d'une déclaration écrite ou orale (enregistrée), y compris par voie électronique, le RT doit documenter les conditions de recueil du consentement afin de démontrer :

- la mise en place de mécanismes permettant de ne pas lier le recueil du consentement à la réalisation d'un contrat (consentement « libre »);
- la séparation claire et intelligible des différentes finalités du traitement (granularité du consentement ou consentement « spécifique »);
- la bonne information des personnes (consentement « éclairé »);
- le caractère positif de l'expression du choix de la personne (consentement « univoque »).

Le RT peut également tenir un registre des consentements qui sera un sous-registre du registre des activités de traitements afin de conserver une trace que le traitement repose sur le consentement explicite de la personne concernée.

Ce guide nous donne en quatre étapes les moyens de valoriser les données personnelles de ses utilisateurs en étant un acteur digne de confiance. Bien utilisé, les données d'un utilisateur permettront de lui apporter une réponse à son besoin et une expérience qui lui donnera envie de rester ou de revenir.

En effet, c'est la durée du consentement donné qui fera la richesse de l'entreprise (Etape 4). C'est pourquoi, il est nécessaire de bien évaluer ses besoins (Etape1) pour organiser la collecte des données via un formulaire, méthode très efficace pour recueillir un consentement actif et volontaire (Etape 2). Il suffit ensuite de les intégrer dans les CRM pour ensuite les exploiter (Etape 3).

En définitive, le consentement contribue à la maîtrise par la personne concernée de ses données à caractère personnel. Il permet également au responsable du traitement de traiter les données qu'il n'aurait certainement pas pu traiter sur un autre fondement.

Finalement, le consentement s'apparente à une véritable armure de la donnée personnelle.

Gérard HAAS
Avocat au barreau de Paris, spécialiste en propriété intellectuelle, Droit du numérique et de la protection des données

Me Gérard Haas conseille, protège à l'ère numérique, l'humain et ses créations. Il assure une défense dynamique des intérêts de ses clients devant les juridictions civiles, commerciales, pénales, arbitraires tant en première instance que devant la Cour d'Appel.

Il est l'auteur notamment des ouvrages : *Le RGPD expliqué à mon Boss* ; *Le Guide juridique du RGPD* ; *Le guide juridique de l'Intelligence Artificielle*.

Introduction - Les enjeux

Le Règlement Général relatif à la Protection des Données à caractère personnel (RGPD) est entré en vigueur le 25 Mai 2018 et inspire de plus en plus de réglementations similaires partout dans le Monde.

La mise en conformité de votre organisation, au même titre que toutes celles qui traitent des données à caractère personnel (DCP) de citoyens européens, a exigé de nombreux efforts et parfois de lourds investissements. Pourtant, la majeure partie de ce travail reste invisible (registre de traitement, analyses d'impact, mesures de sécurité appropriées, sensibilisation des équipes...etc).

En revanche, il y a un volet de la conformité de votre organisation qui est visible par tous à l'extérieur (clients, adhérents, citoyens, patients, ou encore autorités de contrôle) : votre gestion des consentements.

Les enjeux se situent à 4 niveaux :

1. Validité du consentement

En tant que base légale sur laquelle s'appuie certains de vos traitements informatiques, un des premiers enjeux est d'assurer la validité des consentements collectés.
Le RGPD, la directive ePrivacy, les Guidelines de l'edpb (European Data Protection Board) entre autres en fixent les conditions :

- le consentement doit être libre ;
- le consentement doit être spécifique ;
- le consentement doit être éclairé ;
- le consentement doit être univoque ;
- le consentement doit être révocable.

[Avis de Me Gérard HAAS]

« La notion de révocabilité est importante car le responsable de donnée doit être en mesure de démontrer qu'il est possible pour chaque utilisateur de retirer son consentement. (Considérant 42 du RGPD). Si le retrait doit être libre, il ne saurait entraîner aucun surcoût ni effet préjudiciable pour la personne concernée. »

2. Auditabilité

La validité du consentement doit pouvoir être démontrée par votre organisation à tout moment. Il s'agit donc d'en conserver des preuves qui seront utiles :

- en cas de contrôle par une autorité de contrôle comme la CNIL ;
- en cas de contestation par un utilisateur ou un partenaire.

Attention : si un consentement est déclaré non-valide, la conséquence est l'effacement immédiat des données personnelles et l'impossibilité de se prévaloir d'une autre base légale pour les traitements envisagés. Au-delà de l'amende potentielle encourue, les préjudices en terme d'image peuvent s'avérer la plus lourde sanction.

[Avis de Me Gérard HAAS]

« L'information préalable au recueil du consument obéit aux mêmes principes que ceux visés au titre de l'obligation de transparence des articles 13 et 14 du RGPD. Ainsi, un consentement faiblement éclairé ou spécifique, non univoque est de nature à invalider l'accord obtenu et emporte violation de l'article 6 du RGPD. »

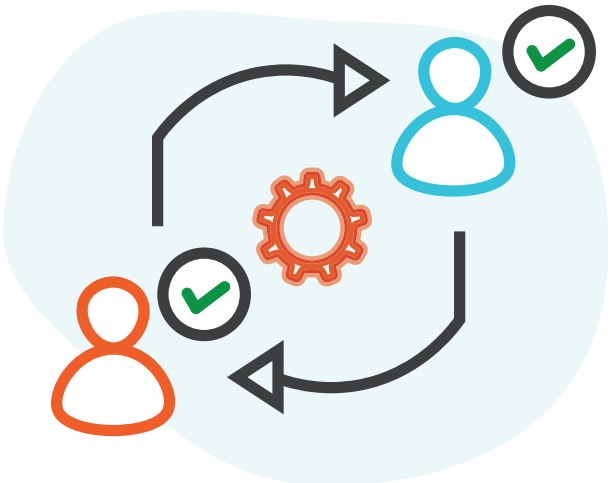
3. Exploitation

La gestion des consentements ne se limite pas à une action ponctuelle de collecte. Il convient d'anticiper :

- La gestion du cycle de vie (révocation, conservation, renouvellement...) ;
- La propagation/consommation des consentements dans les applicatifs métier.

4. L'expérience utilisateur

La gestion des consentements implique des interactions régulières avec vos clients, adhérents, citoyens, patients. A ce titre, c'est une composante à part entière de la qualité de la relation, et de la confiance envers votre organisation.



ETAPE 1 : Recenser vos besoins

Faire l'état des lieux de la gestion du consentement dans votre organisation

Quelles opérations (traitements) s'appuient sur le consentement comme base légale ?

Vous avez probablement finalisé l'élaboration de votre Registre de Traitements.
Dans ce Registre de Traitements, en collaboration avec votre DPO, il vous faudra tout d'abord identifier les traitements dont la basaazacéité est le consentement. L'objectif ici est de bien comprendre quels traitements sont concernés et quels services de votre organisation ils impactent car cela sera primordial pour la suite.

[Avis de Me Gérard HAAS]

« Le consentement peut couvrir différentes activités de traitement dès lors que ces traitements servent une même finalité. Toutefois, autant de consentements que de finalités doivent être obtenus. »

Quels sont les outils existants ?

Si cela était nécessaire, votre organisation a certainement déjà mis en place des modules de collecte du consentement. La plupart du temps, la fonctionnalité de collecte du consentement a été développée dans les applicatifs métier ou marketing qui en avaient besoin ou y est intégrée. Il est probable que plusieurs "solutions" de gestion du consentement coexistent au sein de votre organisation (au minimum, vous avez sûrement un gestionnaire de cookies sur votre site internet).
Pour chaque solution, vous pourrez évaluer les avantages de celle-ci et les points de frustration des utilisateurs liés à son utilisation à l'aide de questionnaires quantitatifs ou d'entretiens qualitatifs par exemple.

Il vous faudra :

- évaluer la volumétrie pour chaque applicatif ;
- étudier le format des consentements collectés ;
- étudier les systèmes d'ID/Auth associés ;
- recenser les bases de données de stockage et/ou de réplication.

Enfin, il pourra être nécessaire d'approfondir le sujet de l'identification d'un utilisateur au sein de vos différents outils. On observe souvent par exemple que le système d'identification utilisé pour gérer les prospects est différent de celui utilisé pour gérer les clients. Le suivi des consentements d'un prospect qui devient client peut ainsi s'avérer compliqué.
Rapprochez-vous de votre département informatique pour savoir si une réconciliation autour d'une fédération d'identités existe ou pas.

Qualifier le besoin

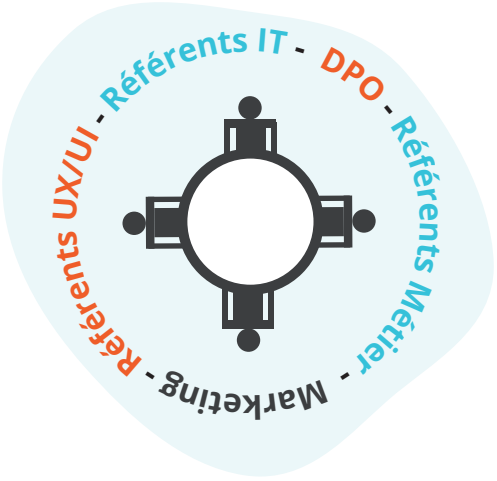
S'inscrire dans une vision stratégique à moyen terme

Les besoins de gestion des consentements doivent être envisagés dans une perspective plus générale de gestion de la relation client/adhérent/patient/citoyen/usager pour la collecte et la modification, et s'inscrire dans la stratégie IT en ce qui concerne l'exploitation et la maintenance évolutive.
Il est donc nécessaire de dialoguer de manière régulière avec le métier et les décideurs stratégiques afin de bien s'assurer que les mises en œuvre opérationnelles des besoins sont toujours bien en ligne avec les objectifs stratégiques fixés par l'organisation.

Organiser des ateliers avec les parties prenantes

Un atelier par traitement ou si les interlocuteurs sont les mêmes, possibilité de regrouper plusieurs ateliers.
En fonction des canaux de collecte, des parcours utilisateurs, des applicatifs métier concernés, ces ateliers sont destinés à qualifier précisément le besoin en prenant en compte les attentes et contraintes des différents services.
Ces ateliers réunissent le plus souvent :

- le DPO ou un membre de son équipe ;
- un ou plusieurs référents métier ou marketing ;
- un référent UX/UI ou expérience utilisateur ;
- un ou plusieurs référents IT (front - back - intégration).



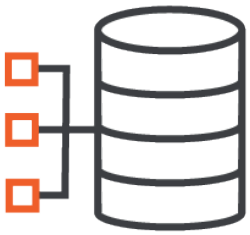
A l'issue de ces ateliers, vous devriez pouvoir compléter pour chaque traitement nécessitant un consentement une fiche du type suivant :

Responsable de traitement	
Finalité(s) de traitement	
Type de personnes concernées	
DCP concernées	
Mesures de sécurité particulières	
Durée de conservation des DCP	
Y'a-t-il collecte de DCP simultanée ?	
Y'a-t-il collecte pour le compte d'un tiers ?	
Canaux de collecte (online/offline) / volumétrie	
Système ID/Auth utilisé	
Applicatifs amont concernés	
Applicatifs aval concernés	

[Avis de Me Gérard HAAS]

« D'une manière générale le responsable de traitement est soumis à une obligation générale de sécurité. Autrement dit, il doit mettre en œuvre des mesures techniques et organisationnelles de sécurité adaptées et appropriées. Pour évaluer, si le niveau de sécurité est adéquate, il faut tenir des risques encourus pour les données elles-mêmes et en particulier : la destruction, la perte, l'altération, la divulgation, l'accès non autorisé.»

ETAPE 2 : Préparer la collecte



Une fois vos besoins bien définis et grâce aux informations rassemblées dans les fiches traitement, vous allez pouvoir concevoir vos formulaires de collecte de consentement et les tester dans chaque parcours utilisateur.

Concevoir vos premiers formulaires de collecte de consentement

Le formulaire de collecte va être exposé à l'utilisateur final à un moment précis de son parcours. Un seul formulaire peut concerner plusieurs traitements ou un seul. C'est en grande partie de ce formulaire que va dépendre la validité des consentements collectés (informé, spécifique, univoque...). Le plus grand soin doit donc y être apporté.

Le socle des exigences réglementaires

Pour se conformer au RGPD et aux guidelines de l'edpb, votre formulaire doit contenir obligatoirement les champs suivants :

- identité du responsable de traitement ;
- (types de) données concernées ;
- finalité de chacun des traitements ;
- mention du droit de retirer son consentement ;
- existence éventuelle de prise de décision automatisée ;
- existence éventuelle de transfert à des tiers (si oui leur identité) ;
- les boutons «accepter» et «refuser» pour chaque traitement de votre formulaire.

D'autres informations peuvent être fournies sans être obligatoires, par exemple un lien vers votre politique de confidentialité ou encore la durée de conservation des DCP concernées (cette dernière information augmente sensiblement le taux d'acceptation des utilisateurs).

[Avis de Me Gérard HAAS]

« En pratique, la politique de confidentialité renforce la confiance entre l'utilisateur et l'organisation qui collecte et traite ses données personnelles. En faisant preuve de transparence et de clarté, l'organisation garantit à ses utilisateurs qu'elle veille à la protection de leurs données. »

Un travail collaboratif

Assurer la validité des consentements sans dégrader la fluidité du parcours utilisateur et en maximisant le taux d'acceptation. Voici ce qui est le plus souvent attendu d'un formulaire efficace.

Pour atteindre cet objectif, plusieurs compétences sont nécessaires et des boucles itératives peuvent être mises en oeuvre entre :

- le DPO ou un membre de son équipe ;
- un ou plusieurs référents métier ou marketing ;
- un référent UX/UI ou expérience utilisateur.

La rédaction est particulièrement importante, pour permettre une information fidèle de l'utilisateur dans un langage simple, clair et compréhensible.

[Avis de Me Gérard HAAS]

« Le RGPD ne définit pas le terme de transparence. Il indique néanmoins que le principe de transparence sollicite que toute information et communication sur un item soit aisément accessible et facile à comprendre, et qu'un langage clair et simple soit utilisé. »

Il est donc important que l'outil de gestion des consentements que vous utilisez permette une édition collaborative des formulaires, permettant plusieurs cycles d'amélioration avant leur mise en ligne.

Gérer le multilingue est également indispensable si vous êtes amené à exposer vos formulaires à des utilisateurs de langues différentes.
On pourra également être attentif au respect de certains critères d'accessibilité, en particulier dans un contexte de collecte de consentement multi-canal (web et mobile par exemple, grâce à des formulaires Responsive Design).

Pour conserver une certaine fluidité dans le parcours utilisateur, préférez un outil qui vous permet de personnaliser les formulaires selon votre charte graphique (style CSS) et ses évolutions futures probables.

En fonction de l'outil sélectionné, il se peut qu'il y ait plus ou moins de choses à personnaliser lors de la construction de vos formulaires. Il est important de s'entourer, pour la construction de votre prototype, de profils UX par exemple qui sauront vous aider pour faire passer vos messages à vos utilisateurs, en s'appuyant sur votre charte graphique et en la déclinant dans vos formulaires par exemple.
La première étape consiste à mettre en place une maquette ou un prototype, qui, sur un premier traitement, vous permettra de tester ce formulaire (ou de faire de l'A/B testing par exemple en créant 2 prototypes différents) auprès de vos futurs utilisateurs.

Tester vos formulaires auprès d'utilisateurs test

Sélectionner un panel de testeurs

Il est utile de tester vos prototypes de formulaires avant de les diffuser largement, notamment pour valider leur design et leur bonne compréhension par l'utilisateur (est-ce que c'est assez explicite, clair…). Pour ce faire, vous pouvez constituer un panel de testeurs représentatifs de vos utilisateurs cibles (tranche d'âge, culture numérique…).

Ces testeurs peuvent être recrutés au sein de votre organisation mais on évitera autant que possible les biais potentiels (ne choisissez pas une personne qui a contribué à ma conception du formulaire par exemple).

Elaborez ensuite un questionnaire qualitatif pour vous permettre de collecter les réactions des utilisateurs et d'identifier les points d'amélioration.

Tester votre prototype auprès de vos utilisateurs

Il est fortement conseillé d'être présent (physiquement ou virtuellement) lorsque les personnes choisies effectuent les tests. Vous pourrez ainsi capter les signaux non verbaux (expressions du visage par exemple) qui vous donneront des indications sur la compréhension du formulaire par l'utilisateur, sur la fluidité perçue du parcours…

Bien sûr, aucune assistance ou explication ne doit être fournie à vos testeurs. Vos utilisateurs finaux seront en totale autonomie. Si des indications sur la marche à suivre sont nécessaires, c'est que le formulaire n'est pas bon.

Ensuite, en faisant la synthèse des retours collectés, vous pourrez déterminer quels formulaires ont été les mieux compris et appréciés, quelles choses peuvent être modifiées ou améliorées en classant les retours par ordre de priorité (par exemple on peut attribuer une note de frustration pour chacune des remarques effectuées, et prioriser les modifications à apporter selon cet indicateur).

ETAPE 3 : Intégrer et exploiter les consentements

Nous avons vu les premières étapes qui permettent de mettre au point une collecte des consentements conforme et efficace. Mais la collecte des consentements n'a de sens que si on est en mesure de les exploiter fidèlement en aval.

La mise en œuvre de cette exploitation peut s'avérer plus ou moins complexe en fonction du nombre d'applicatifs avals concernés, de la volumétrie de consentements ou de l'architecture informatique existante. En tous les cas, vos équipes IT sont indispensables à la bonne mise en œuvre de cette étape.

Déployer la collecte des consentements sur les différents canaux

Après avoir conçu et éventuellement testé les formulaires de collecte de consentements adaptés à vos cas d'usage, il s'agit maintenant de les déployer en production. Concrètement, il s'agit de les intégrer aux applicatifs frontaux exposés à vos utilisateurs finaux aux moments voulus du parcours utilisateur.
Cette intégration peut prendre plus ou moins de temps en fonction du nombre d'applications concernées. Elle peut aussi impliquer différents intervenants de vos équipes informatiques.

Idéalement, un environnement de test vous permettra de valider le bon affichage des formulaires, le bon enregistrement des réponses, et le bon déroulement de la suite du parcours utilisateur.

Pensez à anticiper les évolutions probables de vos formulaires dans le temps, et favorisez quand c'est possible des modalités d'intégrations qui vous permettent de déployer facilement de nouvelles versions de vos formulaires sans devoir intervenir à nouveau sur chaque application front concernée.

Enfin, certaines plateformes permettent également la collecte de consentement par un opérateur depuis un centre d'appel ou un guichet physique. Dans ce cas, une intégration sur-mesure sur les postes/applications utilisées par les opérateurs peut être nécessaire.
Un cycle de vie spécifique peut aussi être mis en œuvre dans le cas de collecte de consentement au format papier (impression du formulaire, soumission à la personne concernée, numérisation du formulaire rempli et réinjection dans le système).

Construire votre base de stockage des consentements

La prise en compte en temps réel des consentements et préférences collectés est indispensable pour assurer votre conformité réglementaire comme la satisfaction de vos utilisateurs. Ces derniers attendent en effet que leurs derniers choix soient respectés, quel que soit leur dernier canal d'interaction avec votre organisation (web, mobile, centre d'appel, agence, point de vente...). Le moyen le plus efficace pour y parvenir est de construire une "base unique de vérité".

De quoi s'agit-il ?

Il s'agit d'une base de données centrale où sont stockés en temps réel tous les consentements et préférences de tous vos utilisateurs, au fur-et-à-mesure de leur collecte. Un registre unique des consentements et préférences.

Ils doivent y être stockés dans des formats lisibles par ordinateur (machine readable) pour faciliter leur utilisation ultérieure.

C'est cette base unique de vérité qui fait foi. Elle doit donc être parfaitement sécurisée. Des copies de sauvegarde régulières peuvent être effectuées selon votre politique RSSI, associées à des procédures de restauration en cas d'incident régulièrement testées.

Des niveaux de performance adaptés à votre volumétrie doivent être anticipés, tant en lecture qu'en écriture.

Connecter votre base unique de vérité à votre SI

Votre base unique de vérité doit être connectée à votre SI existant.

L'objectif est de garantir qu'à tout moment, tous les applicatifs susceptibles d'effectuer des traitements de DCP dont la base légale est le consentement, puissent vérifier s'ils sont autorisés ou pas à le faire pour tel utilisateur, dans tel cas d'usage ou pour telle finalité, et le cas échéant, en prenant bien en compte les préférences exprimées par l'utilisateur final.

Dans une implémentation optimale, chaque applicatif aval concerné (CRM, emailing...) interroge directement en temps réel la base unique de vérité.

Parfois, des applications propriétaires peu ouvertes ne permettent pas cette interrogation directe temps réel et une réplication de la base des consentements peut être nécessaire.
Dans ce cas, des mécanismes de transfert (type batch) ou de synchronisation peuvent être implémentés via des connecteurs spécifiques ou génériques (type API REST). Il s'agit alors de bien identifier quelles données doivent être répliquées (en respectant le principe de minimisation) et à quelle fréquence.

Si les applicatifs avals concernés sont des solutions SaaS éditées par des tiers, une vérification des clauses contractuelles peut être nécessaire (mesures de sécurité, transferts hors UE...).

Avis de Me Gérard HAAS

« Avec la globalisation des échanges et l'utilisation croissante des nouvelles technologies, le nombre de transferts de données hors de France ne cesse de croître. Or, le transfert de données hors de l'Union européenne et de l'Espace Economique Européen est possible, à condition d'assurer un niveau de protection des données suffisant et approprié. Ces transferts doivent être encadrés en utilisant différents outils juridiques.. »

Générer et stocker des reçus de consentement à forte valeur probante

Il appartient au responsable de traitement (c'est-à-dire à votre organisation) de démontrer l'existence et la validité des consentements collectés.
Stocker les consentements dans un format exploitable par machine à grande échelle est nécessaire, en particulier quand les volumétries sont importantes et que des niveaux de performance élevés sont requis (en écriture et en lecture).
Néanmoins, cela peut s'avérer insuffisant pour prouver la validité et l'authenticité des consentements collectés.

Des mécanismes de renforcement de la valeur probante peuvent alors être mis en place. Certains reposent sur l'utilisation de la blockchain, d'autres sur la génération de reçus de consentement respectant un certain formalisme.

La génération et la conservation d'un reçu de consentement dans un format lisible par un humain permet :

- d'améliorer l'expérience utilisateur ;
- de simplifier leur exploitation par des opérateurs (centre d'appels, magasins...) ;
- de faciliter le traitement de demandes particulières par le DPO ;
- d'éviter les litiges et de minimiser les risques ;
- de faciliter les vérifications des autorités de contrôle (CNIL).

Certains standards ont été développés (Kantara, ISO27560) pour permettre une interopérabilité de ces consentements et leur bonne exploitation par un écosystème de partenaires.
Ces reçus de consentement peuvent également être horodatés en utilisant une source de temps fiable (RFC3161), ou encore signés pour en garantir l'intégrité (calcul d'une empreinte numérique ou hash).

L'enjeu est bien d'être en mesure de démontrer que le consentement est authentique et que la manière dont il a été collecté lui permet de remplir tous les critères de validité.

ETAPE 4 : Gérer les consentements dans le temps

Mettre en place des mécanismes permettant de gérer le cycle de vie des consentements

Les consentements ont une durée de validité déterminée. Passée cette durée, il peut être nécessaire de les renouveler (rafraîchir) ou de considérer qu'ils ne sont plus valables.
Les preuves de consentement (registre et reçus) ne doivent pas non plus être conservées sans limitation de durée. Chaque fois que des consentements atteignent la date de suppression fixée en collaboration avec le DPO, des mécanismes paramétrables d'effacement automatique doivent être mis en oeuvre.

[Avis de Me Gérard HAAS]

« Il s'agit d'un principe général énoncé à l'article 5 du RGPD qui impose à chaque responsable de traitement de déterminer une durée de conservation des données personnelles cohérentes et justifiée au regard de l'objectif de leur traitement. En conséquence, un organisme ne peut conserver des données personnelles de manière illimitée, sauf dans certains cas spécifiques et limités à ce qui est strictement nécessaire. Par principe, les données doivent être effacées à l'issue de l'utilisation courante, qui correspond à la durée nécessaire à l'objectif du traitement. Néanmoins, cette règle n'implique pas de supprimer les données systématiquement et en toutes circonstances. En effet, une donnée personnelle obéit à un cycle de vie durant lequel une même donnée peut avoir plusieurs utilités successives. Cela signifie que, pour chacune de ces utilités, une durée différente peut s'appliquer. »

Le cas échéant, il convient de mettre en place des procédures ou des modalités d'information de la personne concernée : pour lui proposer de re-donner son consentement pour une nouvelle période, ou pour l'informer des conséquences du non-renouvellement de ce consentement (arrêt des traitements en question, suppression de certaines données...etc).

Suivre les statistiques et analyser les données de collecte

Le suivi de certains indicateurs peut être précieux pour mesurer l'efficacité de votre collecte de consentement et la maintenir dans le temps.
On peut citer par ex :

- le nombre de consentements collectés (total, par jour, par semaine, par canal...) ;
- les traitements les plus couramment acceptés par les utilisateurs ;
- les taux d'acceptation d'un même traitement via des formulaires différents ;
- les préférences les plus fréquentes et leur évolution.

D'autres indicateurs spécifiques peuvent être pertinents pour votre activité.
Si la solution que vous choisissez ne les propose pas nativement, assurez-vous de pouvoir les générer vous-même depuis d'autres outils (type BI) en privilégiant des solutions sans data lock-in.

Améliorer les modalités de collecte en continu

Une fois les formulaires de collecte mis en production, n'hésitez pas à les améliorer de façon continue suivant les retours utilisateurs.

Les formulaires peuvent évoluer sans automatiquement rendre caduques les consentements collectés en utilisant une version antérieure. De même, il est important de mettre en place dès la mise en ligne de vos formulaires des indicateurs (ou KPIs) qui vous aideront à déterminer les priorités dans l'amélioration de vos formulaires.
Selon l'outil sélectionné, des dashboards plus ou moins configurables vous permettront d'avoir une visibilité en temps réel sur vos collectes de consentements.

Pour aller plus loin : offrir la meilleure expérience utilisateur (Privacy UX)

Contrairement aux idées reçues, plus on donne la possibilité aux individus de changer d'avis plus tard, plus ils ont tendance à dire "oui".

C'est tout l'enjeu d'un Preference Center ou Privacy Center.

Le Preference Center peut être mis à disposition de l'utilisateur depuis son espace personnel authentifié (espace client, espace adhérent, portail citoyen...). Il lui permet à tout moment de consulter l'historique des consentements qu'il a donnés, avec toutes les informations attachées (finalités de traitement, politiques de confidentialité...).

Il peut aussi modifier ses préférences, renouveler son consentement, ou en donner un nouveau pour de nouvelles finalités (marketing direct ou offres de partenaires par exemple sont des cas d'usage fréquents).

Cet espace doit être accessible à l'utilisateur quand il le souhaite, lui présenter une vue fidèle et transparente de ses consentements et préférences avec votre organisation et ses partenaires, et enfin lui offrir une réelle capacité de contrôle et d'action.

Nous contacter : contact@fairandsmart.com