Consultation juridique : le logiciel PageLife au regard du RGPD

- Analyse juridique, au regard du RGPD, du logiciel « PageLife » et propositions en vue de minimiser les risques de non conformité (note rédigée),
- Rédaction des mentions d'information des utilisateurs et de recueil du consentement.

Dans le cadre de la présente note :

« PageLife » désigne aussi bien le nom du logiciel que la société qui pourrait être créée pour exploiter ce logiciel.
« Client » désigne un client de PageLife (sauf dans les clauses relatives au transfert hors UE).
« Visiteur », désigne un client du client, visiteur du site internet de ce dernier.

Contexte

PageLife se définit comme un logiciel de preuve sociale présenté sur le site internet https://www.pagelifemarketing.com.

PageLife s'adresse à des clients, pour lesquels il s'agit d'un moyen de promotion de leur activité en direction de visiteurs de leur site internet.

L'idée est qu'à chaque fois qu'un visiteur d'un site remplit un formulaire ou achète un produit, cela crée une petite "bulle" (comme un petit *pop-up*) qui s'affiche sur la page de ce site pour montrer aux « prochains » visiteurs les inscrits/acheteurs.

Par exemple : "Jean de Rennes, FRA, vient d'acheter le produit P, il y a 2 heures".

Du point de vue technique, les données collectées sont :
-l'email du visiteur,
-le prénom du visiteur,
-la date de l'achat ou de l'inscription sur le site internet du visiteur,
-l'adresse IP permettant de localiser grossièrement le visiteur (ville, département, région, pays). Il ne s'agit pas de la localisation exacte.

Deux données supplémentaires sont récupérées sur Internet via des interfaces publiques ou services :
- une petite photo de profil du visiteur, si on la trouve (car il n'en existe pas toujours). Cette photo est dite "publique" c'est-à-dire accessible via Internet.

-une petite carte Google Map trouvée grâce aux informations ville + département + région + pays, informations obtenues grâce à un service privé américain permettant de retrouver ces éléments à partir de l'adresse IP.

Il semble également que dans certains cas, l'adresse IP soit parfois récupérée auprès d'un site tiers offrant gratuitement cette prestation.

Toutes ces données sont stockées sur une base de données Google (Google Firebase) ainsi que sur les serveurs d'Amazon (AWS) parfois situés à Paris, Londres, en Irlande ou en Virginie aux USA.

L'email est stocké de manière chiffrée "avec perte", donc irrécupérable (pas d'opération inverse possible pour le retrouver). Cet élément constitue un identifiant de la bulle qui a été publiée sur le site de manière fugace.

Il convient d'identifier les mesures à mettre en place et de prévoir la rédaction de certaines mentions, étant précisé que l'avocat ne dispose pas des contrats passés par son client avec AWS, Google ou d'autres prestataires.

I – Analyse juridique, au regard du RGPD, du logiciel *« PageLife »* et propositions en vue de minimiser les risques de non conformité

Critère territorial

Le RGPD est applicable (article 3) aux traitements de données effectués dans le cadre d'activités réalisées par un responsable de traitement ou un sous-traitant dans l'Union européenne, que le traitement lui-même ait lieu ou non dans l'Union. Un autre critère alternatif est celui de la situation géographique des personnes concernées. Dans le cas de PageLife, si l'activité est réalisée dans l'Union ou vise des personnes dans l'Union, le RGPD est applicable.

Qui est responsable de traitement ?

L'article 4 du RGPD définit comme responsable de traitement comme *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».*

Le même article définit le sous-traitant comme *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».*

Le client de PageLife ayant communiqué ses traitements de données à PageLife, ce client sera vraisemblablement qualifié de responsable de traitement. La collecte et la transmission

de données personnelles, telles qu'adresses IP, constituent en effet un traitement de données et en choisissant les finalités de ces traitements (preuve sociale) et les moyens de traitement (recours à un prestataire), il se comporte comme responsable de traitement. De plus, le client est plus généralement responsable des traitements de ses données de clientèle, qui peuvent être plus précises et plus complètes, et qu'il recueille pour son propre compte, ce qui constitue une autre finalité, qui lui est propre.

Concernant PageLife, la question est d'une appréciation plus délicate. En effet, PageLife est l'entité *« qui traite des données à caractère personnel pour le compte du responsable du traitement »,* ce qui correspond à la définition du sous-traitant.

Dans son guide du sous-traitant paru en septembre 2017, la CNIL, indique toutefois que l'on est sous-traitant si l'on traite des données pour le compte, sur instruction et sous l'autorité d'un responsable de traitement. Selon la CNIL, sont notamment des sous-traitants *« les prestataires de services informatiques (hébergement, maintenance,...), les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux donnée ».*

Elle précise également que lorsqu'un organisme sous-traitant détermine la finalité et les moyens d'un traitement, il ne peut pas être qualifié de sous-traitant : un tel organisme doit être considéré comme étant également un responsable de ce traitement (en application de l'article 28.10 du RGPD, qui dispose que lorsqu'un sous-traitant *« détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement »*).

La CNIL reprend dans ce guide réalisé en vue de l'application du RGPD l'avis 1/200 du groupe des CNIL européennes (G29) du 16 février 2010 qui précise le faisceau d'indices à utiliser dans le cadre d'une analyse au cas par cas :

- *« niveau d'instruction donné par le client au prestataire : quelle est l'autonomie du prestataire dans la réalisation de sa prestation ?*
- *degré de contrôle de l'exécution de la prestation : quel est le degré de « surveillance » du client sur la prestation ?*
- *valeur ajoutée fournie par le prestataire: le prestataire dispose-t-il d'une expertise approfondie dans le domaine ?*
- *degré de transparence sur le recours à un prestataire : l'identité du prestataire est-elle connue des personnes concernées qui utilisent les services du client ? ».*

Ces notions avaient d'ailleurs été reprises et explicitées dans une synthèse des réponses à la consultation publique sur le *cloud computing* lancée par la CNIL en 2011. Concernant le niveau d'instruction, cela signifie que si le client laisse une grande autonomie au prestataire dans la réalisation de sa prestation, ce dernier agit plutôt en qualité de responsable de traitement. Il en va de même concernant le niveau de surveillance du prestataire. Concernant la valeur ajoutée, plus le prestataire dispose d'une expertise approfondie, plus il est à même de décider des moyens de traitement à mettre en place et donc susceptible d'être qualifié de responsable de traitement. Concernant le fait que l'identité du prestataire est connue des clients, c'est un indice de ce que le prestataire agit comme responsable de traitement. Bien que ce critère ne figure pas dans la liste, le fait que l'offre (à propos du

cloud) soit standard et que le client n'ait pas de marge de manœuvre semble également militer dans le sens d'une qualification comme responsable de traitement (Voir DEBET, MASSOT, METALLINOS, Informatique et libertés, Lextenso, 2015, p. 278).

Dans le cas de PageLife, l'entité est autonome pour réaliser la prestation, celle-ci n'étant pas surveillée par le client. PageLife apporte une expertise dont ne dispose probablement pas le client. Bien que la qualification comme sous-traitant soit envisageable, la qualification comme responsable de traitement semble donc plus juste et plus prudente.

Alors que le client est responsable de traitement et que PageLife l'est également, comment s'organisent les responsabilités ? Cela st prévu par l'article 26 du RGPD selon lequel :
« 1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14 [information et accès des personnes concernés à leurs données à caractère personnel], par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.
2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée. [Ici, le visiteur].
3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement. ».

Il sera donc nécessaire de prévoir un contrat organisant ces partages de responsabilités entre PageLife et chacun de ses clients, d'autant que l'article 82 § 4 prévoit que *« Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective. »* La répartition définitive de cette indemnisation entre les différents acteurs est un élément qui doit être anticipé contractuellement.

Mais cette responsabilité ne s'applique que pour les données qui sont partagées entre le client et PageLife, c'est-à-dire l'adresse IP, l'email, le prénom. Pour le reste du traitement, PageLife assume seul la responsabilité de responsable du traitement des données de géolocalisation et des photographies. Inversement, PageLife n'est pas responsable des données que le client ne lui communique pas.

Si l'on applique les mêmes critères aux sociétés auxquelles PageLife aura recours telles que Google et Amazon Web Services afin de déterminer si ces dernières sont sous-traitantes ou

responsables de traitements (cf. article 28.10 relatif au sous-traitant qui devient responsable de traitement car il en détermine les finalités et les moyens), il est assez probable que ces dernières se verront qualifier comme responsables de traitements. Dans un tel cas, la responsabilité conjointe semble possible mais plus difficile à admettre, certains moyens du traitement étant peut-être partagés mais non les finalités.

Google LLC fait d'ailleurs une telle analyse en tant que prestataire du service FireBase : *« Firebase customers typically act as the "data controller" for any personal data about their end-users they provide to Google in connection with their use of Firebase, and Google is, generally, a "data processor" ».* (https://firebase.google.com/support/privacy/).

Quelles données ?

Des données telles que l'e-mail, la photographie, la géolocalisation, l'adresse IP sont des données à caractère personnel.

Rappelons que le Conseil d'Etat ne conteste pas qu'une adresse IP constitue une donnée personnelle (CE, 23 mai 2007, n° 288149, inédit, SACEM) et que le G 29 a étendu la notion de donnée à caractère personnel à l'adresse MAC enregistrée sur des composants matériels informatiques (Avis 13/2011 du G29, WP 185, relatif aux services de géolocalisation des dispositifs mobiles intelligents, adopté le 4 avril 2011), aux données de localisation, aux métadonnées se rapportant à la configuration d'un compteur intelligent et que la CNIL considère comme donnée personnelle un identifiant *bluetooth* de téléphone mobile (CNIL, 29ème rapport annuel)…

Le prénom et la date d'achat ou de l'inscription ne sont pas nécessairement des données à caractère personnel. Mais en réalité, ces données peuvent être considérées comme indirectement personnelles dans la mesure où leur croisement permettrait de réidentifier une personne (identité déduite d'un faisceau de données, cf. DEBET, MASSOT, METALLINOS, Informatique et libertés, Lextenso, 2015, p. 251.)

Quels traitements ?

Est considéré comme traitement *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, 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 ».* (article 4).

Dans le cas présent, la collecte de données (adresses IP, e-mail, notamment) obtenues via les visiteurs, leur enregistrement, leur utilisation pour collecter d'autres données (géolocalisation, photographie voire adresse IP si elle n'est pas fournie) ainsi que leur communication sur le site internet du client par les moyens techniques de ce dernier, sont constitutifs de traitements de données à caractère personnel.

La liceité du traitement

La liceité du traitement ne peut dans le cas présent se rattacher qu'à un seul critère : le consentement du visiteur (éventuellement sur le site du client). On ne peut en effet rattacher la liceité du traitement à sa nécessité pour l'exécution d'un contrat auquel le visiteur est partie, au respect d'une obligation légale, à la sauvegarde d'intérêts vitaux, à une mission d'intérêt public ou aux intérêts légitimes du responsable de traitement ou d'un tiers, cette dernière notion étant, imprécise et ayant été appréciée strictement par la CNIL (le seul intérêt commercial ayant été caractérisé comme insuffisant, cf. DEBET, MASSOT, METALLINOS, Informatique et libertés, Lextenso, 2015, p. 394 s.).

Il convient donc d'organiser les modalités du recueil de ce consentement. Il est probablement plus simple que le client de PageLife accepte de collecter sur son site un tel consentement, lequel devra être obtenu à partir de termes clairs et simples.

Le transfert à l'étranger : consentement

En cas de transfert de données à caractère personnel vers un pays tiers, il est nécessaire qu'un fondement juridique permette un tel transfert. Le transfert peut notamment être fondé sur une décision dite d'adéquation de la Commission européenne. Notons, en ce qui concerne les transferts de données vers les Etats-Unis, que le *Privacy Shield* vise à reconnaître un mécanisme de protection « essentiellement équivalent » aux exigences européennes (mais ce dispositif est fragile car il fait l'objet de deux recours judiciaires).

Google LLC y figure :
https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI
AWS y figure également :
https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4&status=Active

Si le mécanisme du *Privacy Shield* est invalidé, le recours immédiat à des clauses contractuelles types de la Commission européenne (ou de la CNIL lorsqu'elles seront adoptées) sera nécessaire.

Toutefois, ces clauses contractuelles types n'ont pas encore été renouvelées et ne tiennent pas encore compte des dispositions du RGPD, d'où la nécessité de les compléter (voir à la fin du présent document).

Il est par ailleurs conseillé d'identifier les applications informatiques, les bases de données, les lieux de stockage (notamment serveurs concernés), les organismes ayant accès aux données concernées et de sécuriser au maximum ces transferts, et ce de bout en bout à partir des installations du client. Le registre des traitements doit mentionner ces transferts (article 49 *in fine*).

Registre

La qualité de responsable des traitements (comme celle de sous-traitant) oblige à tenir un registre des traitements dans la mesure où les traitements ne sont pas occasionnels (article 30, *in fine*).

Le contenu du registre est le suivant : nom du responsable de traitement et ses coordonnées, finalités, catégories de personnes, catégories de destinataires, transferts, délais de conservation. Il en va de même pour le sous-traitant sauf en ce qui concerne les délais de conservation.

Un modèle figure sur le site de la CNIL : https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

DPO

L'article 37 du RGPD dispose que la désignation d'un délégué à la protection des données interne ou externe est obligatoire lorsque :

« a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

L'organisme n'est pas public, les activités n'exigent pas un suivi régulier et systématique et les données concernées ne sont pas des données dites sensibles. »

Les critères de désignation du délégué à la protection des données ne paraissent donc pas remplis pour PageLife en l'état des informations communiquées.

Analyse d'impact

Une analyse d'impact (article 35, § 3 du RGPD) du traitement de données mis en œuvre est nécessaires lorsque les risques sont élevés : évaluation systématique et approfondie d'aspects personnels fondés sur un traitement automatisé, y compris le profilage, et sur la base desquels sont prises des décisions produisant des effets juridiques, traitement à grande échelle de données dites sensibles, surveillance systématique à grande échelle d'une zone accessible au public.

Le G29 a développé une liste de critères : évaluation et notation, prise de décision ayant des effets juridiques, surveillance systématique, données sensibles, traitement à grande échelle, séries de données assemblées et combinées, données concernant des personnes

vulnérables, recours à de nouvelles technologies, transfert de données hors UE, traitement privant d'un droit, d'un service ou d'un contrat, deux critères justifiant une telle étude d'impact.

Les critères susceptibles d'êtres remplis sont soulignés ci-dessus. Un traitement à grande échelle s'apprécie au cas par cas selon plusieurs critères : le nombre de personnes concernées en valeur absolue ou relative par rapport à une population donnée, le volume de données et/ou les différents items traités, la durée ou la permanence de l'activité, l'étendue géographique. Dans la perspective d'un développement du produit en France et compte tenu du fait que les données ne sont pas conservées si ce n'est pour générer un identifiant du *pop-up* conservé peu de temps, il ne semble pas que le risque soit présent actuellement.

La notion d'assemblage et de combinaison implique que ceux-ci dépassent les attentes raisonnables de la personne considérée concernant l'usage ultérieur des données. Dans le cas où le fondement juridique du traitement est le consentement des personnes sur la base d'informations claires, cela ne semble pas poser de difficulté particulière puisque les attentes raisonnables seront fonction des informations communiquées.

Le recours à une technologie nouvelle (ex. internet des objets, système permettant de combiner différentes sources de données comme la reconnaissance faciale et les empreintes digitales pour organiser l'accès à des locaux) ou l'utilisation innovante de solutions technologique ou organisationnelles, qui semble bien être mise en œuvre ici, pourrait en revanche constater un fondement d'une telle étude d'impact.

Il en va de même du transfert de données en dehors de l'Union européenne. On se situe donc dans les conditions susceptibles de justifier une étude d'impact, deux critères ou plus étant remplis.

Par ailleurs, tant que l'activité de PageLife est encore en démarrage, le risque réel de contrôle de la CNIL est plutôt faible, mais théoriquement, cet étude (qui peut être assez longue et coûteuse) apparaît nécessaire avant mise en œuvre du traitement. La question se posera dès lors que l'activité se développera avec une augmentation massive du nombre de données traitées.
https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Information

Des mentions d'information spécifiques des personnes concernées (visiteurs) sont prévues aux articles 13 et 14 du RGPD selon que les informations sont collectées directement (adresse IP, e-mail, prénom) ou non (adresse IP, géolocalisation, photographie) auprès d'elles. (Voir plus bas).

Gestion des droits des personnes

Les personnes concernées ont sur leurs données à caractère personnel, outre un droit à l'information : un droit d'accès, un droit de rectification et d'effacement, un droit à la

limitation du traitement, un droit à la portabilité des données, un droit d'opposition, un droit à ne pas faire l'objet d'une décision individuelle automatisée.

Il sera nécessaire d'organiser avec le client les modalités selon lesquelles ces droits seront exercés, ce qui peut s'effectuer de manière contractuelle. Cela étant, presque tous ces droits à l'exception du droit à l'information, n'auront, en pratique, plus lieu pour les personnes concernées de s'exercer auprès de PageLife dès lors que PageLife aura supprimé leurs données.

Mise en œuvre de mesures techniques et organisationnelles

Ces mesures dépendent de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement, et enfin des risques et de leur degré de probabilité. Le RGPD évoque notamment la pseudonymisation et le chiffrement mais aussi des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des données, des moyens permettant de rétablir leur disponibilité et leur accès, une procédure visant à tester, analyser et tester régulièrement l'efficacité des mesures techniques et organisationnelles.

Pseudonymisation et chiffrement

Sur ce sujet plus technique, il est préférable de se reporter à la doctrine de la CNIL.
Notons toutefois que la CNIL préconise le chiffrement plutôt que la pseudonymisation qui permet la réidentification (CNIL , 37ème rapport d'activité).

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

La CNIL recommande notamment ce qui suit (fiche 17):

Utiliser un algorithme reconnu et sûr, par exemple, les algorithmes suivants :
« - SHA-256, SHA-512 ou SHA-341 comme fonction de hachage ;
- HMAC utilisant SHA-256, bcrypt, scrypt ou PBKDF2 pour stocker les mots de passe; - AES ou AES-CBC pour le chiffrement symétrique ;
- RSA-OAEP comme défini dans PKCS#1 v2.1 pour le chiffrement asymétrique ;
- enfin, pour les signatures, RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1.
• Utiliser les tailles de clés suffisantes42, pour AES il est recommandé d'utiliser des clés de 128 bits et, pour les algorithmes bases sur RSA, des modules et exposants secrets d'au moins 2048 bits ou 3072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65536.
• Protéger les clés secrètes, au minimum par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sur.
• Rédiger une procédures indiquant la manière dont les clés et certificats vont être gérées en prenant en compte les cas d'oubli de mot de passe de déverrouillage.

CE QU'IL NE FAUT PAS FAIRE
Utiliser des algorithmes obsolètes, comme les chiffrements DES et 3DES ou les fonctions de hachage MD5 et SHA1.

Confondre fonction de hachage et chiffrement et considérer qu'une fonction de hachage seule est suffisante pour assurer la confidentialité d'une donnée. Bien que les fonctions de hachages soient des fonctions « à sens unique », c'est à dire des fonctions difficiles à inverser, une donnée peut être retrouvée à partir de son empreinte. Ces fonctions entant rapides à utiliser, il est souvent possible de tester automatiquement toutes les possibilités et ainsi de reconnaitre l'empreinte. »

Sur la sécurisation du système d'information, on se reportera au guide d'hygiène informatique de l'ANSSI.
https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

En tout état de cause, il apparaît nécessaire de sensibiliser et former les personnels, de connaître le système, d'authentifier et contrôler les accès, de sécuriser les postes de travail et le réseau, gérer le nomadisme, maintenir le système à jour, auditer, superviser…

Sécurisation des données

L'article 32 § 2 du RGPD impose au responsable de traitement (comme au sous-traitant) de mesurer les risques inhérents au traitement et de prendre les mesures propres à les atténuer. Les principaux risques sont la destruction, la perte ou l'altération, la divulgation non autorisée à de telles données de manière accidentelle ou illicite, étant rappelé que le code pénal sanctionne le non respect de l'obligation de sécurité et de confidentialité des données par une peine de 5 ans d'emprisonnement et 300000 euros d'amende (peine encourue, cf. article 226-17 du code pénal).

A ce titre, chaque responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

La proportionnalité

Selon l'article 5, les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Si la finalité est ici d'apporter la preuve qu'un site est visité par des clients, éventuellement distincts et d'origines géographiques diverses, il ne devrait pas être utile de donner d'autres informations que le minimum nécessaire.

L'email du visiteur n'est pas diffusé et serait assurément considéré comme une information fournie de manière disproportionnée par rapport aux finalités poursuivies.

Le prénom peut-être envisagé dans la mesure où il ne permet pas de distinguer une personne d'une autre. Le prénom renseigne toutefois généralement sur le sexe. Cela présente-t-il un intérêt ? L'utilisation des seules initiales est également possible.

La photographie est quant à elle très fortement identifiante et inutile par rapport à l'objectif poursuivi. Elle devrait *a minima* être floutée. Une autre option, plus sûre, serait de communiquer une sorte d'« avatar ».

La géolocalisation peut contribuer, en particulier avec d'autres éléments, à identifier des personnes surtout dans les zones à faible densité de population. Le maillage devrait donc être suffisamment large pour ne pas permettre d'identifier des personnes sur des zones à faible densité. Par ailleurs, quel est l'objectif poursuivi par la géolocalisation ? S'il s'agit d'être en mesure d'expliquer que l'on s'adresse à une clientèle internationale, éventuellement diversifiée, le pays (et à l'extrême limite la région), devrait suffire.

Le recours à des services de géolocalisation proposés par Google est probablement de nature à augmenter le risque de contrôle : la CNIL a notamment imposé 100000 euros de sanctions pécuniaires à propos de Google Street View et Google Latitude. Des condamnations au moins équivalentes ont été prononcées par les « CNIL » belge, allemande et italienne (Voir la délibération CNIL 2011-035 du 17 mars 2011 et le rapport de M.P. Gosselin, rapporteur). Google a fait également l'objet de beaucoup d'attention de la CNIL et de la CJUE sur la question du droit à l'oubli (CJUE, Google Spain et Google, 13 mai 2014, C-131/12)…

La géolocalisation doit nécessairement être proportionnée au but recherché. Une utilisation est proportionnée lorsque le but recherché peut être atteint par d'autres moyens (moins intrusifs).

La date d'achat ou de l'inscription ne semble pas constituer des données directement identifiantes. En revanche le type de produits ou services achetés pourrait, croisé avec d'autres données, révéler des préférences et centres d'intérêt personnels. Il est donc préférable de ne pas identifier de tels produits ou services.

Privacy by Design / by Default

Le principe de privacy by design est posé par l'article 25 § 1 du RGPD selon lequel : *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. »*

En pratique, cela implique pour le responsable de traitement (comme pour le sous-traitant), de minimiser la collecte des données (ex. pas besoin de la date de naissance d'une personne pour lui demander si elle est majeure, pas besoin de l'année de naissance pour souhaiter un anniversaire, etc.), de dissimuler de la vue de tous les données et leur interdépendance (ex.

nom et salaire), de séparer physiquement les données traitées pour quelles ne soient pas conservées au même endroit ni dans la même base le but étant d'empêcher la constitution de profils (pas besoin de l'adresse exacte d'une personne pour une publicité ciblée), d'informer les personnes concernées du niveau de sécurité et des mesures prises pour assurer une protection adéquate (sans entrer dans le détail naturellement), de permettre à la personne concernée de contrôler ses propres données, de mettre en œuvre une politique de confidentialité, d'être en mesure de démontrer la conformité des traitements.

Le principe de privacy by default est par alleurs posé par l'article 25 § 2 du RGPD selon lequel : *« Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ».*

Ces principes de Privacy by Design / by Default rejoignent le principe de proportionnalité.

Durée de conservation et archivage

L'article 5, e, prévoit que les données conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Les données étant utilisées « à la volée », il semble difficile de les conserver longtemps. Une durée comprise entre un mois (pour la base active) et six mois maximum (pour les archives intermédiaires) apparaît raisonnable. En tout état de cause, la nécessité de conservation des données doit pouvoir être justifiée.

La CNIL préconise l'archivage des données dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaitre en raison de leurs fonctions (par exemple, le service du contentieux) ou dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter, mais il semble que la séparation physique ait néanmoins sa faveur. Elle préconise également le traçage de la consultation des données d'archive. https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

Par ailleurs, il serait inconcevable de pouvoir conserver ces données plus longtemps que le client de PageLife. En matière de fichier clients/prospects, la doctrine de la CNIL prévoit une durée de 3 ans à compter de la fin de la relation commerciale. https://www.cnil.fr/sites/default/files/typo/document/20120719-REF-DUREE_CONSERVATION-VD.pdf

Violation des données

La violation de données c'est-à-dire toute faille de sécurité entrainant la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel de données faisant l'objet d'un traitement, doit être notifiée par le responsable de traitement à la CNIL dans les meilleurs délais et si possible dans les 72 heures. (Une telle obligation s'applique également à l'égard des personnes concernées et doit en outre être mise en œuvre par le sous-traitant à l'égard du responsable de traitement selon des modalités précisées aux articles 33 et 34 du RGPD). Il est certainement utile pour PageLife d'anticiper un tel cas de figure, par exemple en prévoyant une procédure adaptée. Cela étant, un contractualisation avec les clients peut permettre de mieux organiser la gestion des incidents.

Préconisations, en l'état des informations transmises :

- **minimisation et proportionnalité des données (prénom ou initiales, photo supprimée mais avatar, maillage géographique large par pays,**
- **mise en place d'un registre des traitements,**
- **recueil du consentement auprès du visiteur et transfert à PageLife selon une procédure permettant leur traçabilité et avec un procédé technique fiable,**
- **archivage de ces consentements selon un procédé technique fiable,**
- **localisation des données des visiteurs, en particulier hors UE si cette option ne peut vraiment pas être évitée,**
- **analyse des contrats de service, notamment avec Google ou tout autre prestataire traitant des données utilisées par PageLife,**
- **cryptage de bout en bout (y compris à partir du client) pour sécuriser les flux de données des visiteurs (personnes concernées),**
- **organisation de la sécurité via des mesures techniques et organisationnelles appropriées,**
- **organisation de l'archivage des données dans des bases séparées,**
- **recours à des prestataires traitant des données du client sur le territoire de l'Union européenne uniquement,**
- **mise en place de mentions d'information des visiteurs,**
- **préparation d'un contrat avec le client de PageLife, définissant notamment les responsabilités de chacun, les procédures de gestion des droits des personnes, la conduite à tenir en cas incident (violations de données)…**
- **une analyse d'impact semble également nécessaire mais le risque d'un contrôle sera beaucoup plus évident en cas de transfert de données hors UE et de traitement de données à grande échelle.**

II – Mentions d'information des utilisateurs et de recueil du consentement. [Attention, en aucun cas l'apposition de ces mentions d'information par le client de PageLife ne lui assure une conformité par rapport à ses traitements de données à caractère personnel]

Informations à fournir au visiteur du site (données à caractère personnel collectées sur le site XXX afin de permettre un traitement de ces données à des fins de « preuve sociale »)

- identité et coordonnées de XXX [client de PageLife], responsable de traitement, et celles de son représentant ;

- les coordonnées du délégué à la protection des données sont : ---;

- les finalités du traitement des données à caractère personnel sont la réalisation par PageLife d'une « preuve sociale » de l'activité de XXX en utilisant les informations du visiteur ci-après : prénom, Pays, inscription sur le site de XXX. Ces données sont destinées à permettre l'apparition de pop-ups quelques minutes à quelques heures après cet événement sur le site de XXX, l'objectif étant de montrer aux autres visiteurs que le site est actif et remporte un certain succès ;

- les informations communiquées dans ces pop-ups sont du type : Jean, FRA, vient de s'inscrire sur le site XXX, il y a 2 heures" ;

- la base juridique du traitement est le consentement du visiteur ;

- les destinataires ou les catégories de destinataires des données à caractère personnel sont la société PageLife ainsi que les prestataires auxquels celle-ci a recours à savoir Amazon Web Services [intitulé exact de la personne morale concernée] et Google LLC [intitulé exact de la personne morale concernée] ;

- XXX effectue via son prestataire PageLife, un transfert de données à caractère personnel notamment vers le Royaume-Uni, l'Irlande et les Etats-Unis [liste précise des pays concernés]. Lorsque les données sont exportées en dehors de l'Union européenne ou en dehors pays que la Commission européenne reconnaît comme offrant des garanties équivalentes (en vertu d'une décision d'adéquation) en matière de protection des données personnelles, soit le mécanisme de protection dit du Privacy Shield est applicable (Etats-Unis), soit les transferts reposent sur des clauses contractuelles types de la Commission européenne assurant également une protection des données personnelles ;

- le visiteur peut obtenir une copie de ses données en s'adressant à XXX [coordonnées complètes avec adresse physique, email et téléphone / délégué à la protection des données de XXX s'il existe] ;

- la durée de conservation des données à caractère personnel par PageLife est de [1/6] mois à compter de leur collecte ;

- le visiteur peut demander auprès de XXX l'accès à ses données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement de données, et dispose du droit de s'opposer au traitement et du droit à la portabilité de ses données, étant précisé que XXX s'engage à en informer aussitôt PageLife si celle-ci conserve des données du visiteur ;

- le visiteur a le droit d'introduire une réclamation auprès d'une autorité de contrôle (CNIL, en France);

- la fourniture de ses données le visiteur, facultative, présente un caractère contractuel et ne conditionne pas conclusion d'un contrat, la conséquence de la non-fourniture de ces données étant la non utilisation par XXX du service proposé par PageLife ;

- le visiteur peut retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant ce retrait, étant précisé que XXX s'engage à en informer aussitôt PageLife si celle-ci conserve des données du visiteur ;

Informations liées à la collecte de données à caractère personnel collectées auprès de tiers

- identité et coordonnées de PageLife, responsable de traitement, et celles de son représentant ;

- les finalités du traitement des données à caractère personnel sont la réalisation par PageLife d'une « preuve sociale » de l'activité de XXX en utilisant les informations du visiteur ci-après : prénom, Pays, inscription sur le site de XXX. Ces données sont destinées à permettre l'apparition de pop-ups quelques minutes à quelques heures après cet événement sur le site de XXX, l'objectif étant de montrer aux autres visiteurs que le site est actif et remporte un certain succès ;

- les catégories de données à caractère personnel recueillies auprès de tiers à partir des données communiquées à PageLife par XXX sont la géolocalisation du visiteur (Pays), et le cas échéant son adresse IP recueillie à partir de son adresse e-mail [éventuellement : sa photographie qui sera floutée pour rendre le visiteur non identifiable] ;

- PageLife effectue pour son client XXX, un transfert de données à caractère personnel notamment vers le Royaume-Uni, l'Irlande et les Etats-Unis [liste précise des pays concernés]. Lorsque les données sont exportées en dehors de l'Union européenne ou en dehors pays que la Commission européenne reconnaît comme offrant des garanties équivalentes (en vertu d'une décision d'adéquation) en matière de protection des données personnelles, soit le mécanisme de protection dit du Privacy Shield est applicable (Etats-Unis), soit les transferts reposent sur des clauses contractuelles types de la Commission européenne assurant également une protection des données personnelles ;

- Seuls le prénom, l'adresse e-mail et le cas échéant l'adresse IP du visiteur sont communiqués par XXX à PageLife, qui obtient alors auprès de Google LLC et d'Amazon Web Services la géolocalisation sommaire (Pays) [éventuellement : une photographie qui sera floutée pour rendre le visiteur non identifiable] ; le cas échéant, l'adresse IP est obtenue auprès de [---] à partir de l'adresse e-mail du visiteur ;

- la durée de conservation des données à caractère personnel par PageLife est de 1/6 mois à compter de leur collecte ;

- le visiteur peut demander auprès de XXX l'accès à ses données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement de données, et dispose du droit de s'opposer au traitement et du droit à la portabilité de ses données, étant précisé que XXX s'engage à en informer aussitôt PageLife si celle-ci conserve des données du visiteur ;

- le visiteur a le droit d'introduire une réclamation auprès d'une autorité de contrôle (CNIL, en France);

- les données à caractère personnel recueillies auprès de tiers à partir des données transmises à PageLife par XXX le sont auprès de Google LLC [intitulé exact de la personne morale concernée et source plus précise] et d'Amazon Web Services [intitulé exact de la personne morale concernée et source plus précise]. Elles sont issues [ou non] de sources accessibles au public;

- le visiteur peut retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant ce retrait ;

Consentement spécifique PageLife : case à cocher par le visiteur [non précochée]

« Visiteur du site XXX, j'accepte le traitement de mes données personnelles par XXX, PageLife et ses partenaires dans les conditions mentionnées ci-dessus. Je suis informé(e) de mon droit de retirer ce consentement à tout moment. »

Consentement spécifique transfert hors UE [si ne peut être évité] pour le fonctionnement de PageLife : case à cocher par le visiteur [non précochée]

« Visiteur du site XXX, j'accepte le transfert de mes données personnelles en dehors de l'Union européenne dans les conditions mentionnées ci-dessus. Je suis informé(e) de mon droit de retirer ce consentement à tout moment. »

Remarque : En cas de transfert de données à caractère personnelle en dehors de l'Union européenne vers un pays n'ayant pas fait l'objet d'une décision d'adéquation, il sera nécessaire d'avoir recours à un mécanisme tel que les clauses contractuelles types de la Commission européenne, qui n'ont pas encore été mises à jour pour tenir compte du RGPD, (ou encore de la CNIL, non encore élaborées). Elles sont disponibles ci-après : https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne

Elles doivent toutefois être complétées par ce qui suit dans la mesure du possible, ou par d'autres dispositions équivalentes.

Clauses à faire signer avec tout prestataire lorsque les données sont exportées en dehors de l'Union européenne ou en dehors de pays que la Commission européenne reconnaît comme offrant des garanties équivalentes (en vertu d'une décision d'adéquation). [**L'approbation préalable de ces clauses par la CNIL sera nécessaire].**

« Outre la signature des clauses contractuelles types figurant en annexe du présent contrat, le prestataire s'engage à effectuer les traitements des données personnelles en dehors du territoire de l'Union européenne dans le strict cadre de l'exécution du présent contrat et des finalités ci-après : recueil de photographies / de données de localisation de personnes physiques via par l'utilisation de données fournies par PageLife, en vue pour PageLife, d'être en mesure d'offrir certaines prestations à ses clients. Le prestataire s'engage à mettre en œuvre l'ensemble des engagements listés ci-après, sur l'ensemble du périmètre des traitements qu'il exécute sur l'ensemble des données à caractère personnel collecté ou traitées dans le cadre du présent contrat. A cet égard et outre les engagements qui lui incombent au sens des clauses contractuelles types figurant en annexe, le prestataire, entendu comme l'importateur des données, s'engage à ce qui suit.

Article un : droits des personnes concernées
Les personnes concernées, au sens des clauses contractuelles types figurant en annexe du contrat, sont susceptibles de faire valoir directement auprès du prestataire les droits dont elle bénéficie au sens du règlement européen (UE) 2016/79 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci après le « RGPD »), à l'égard du traitement des données à caractère personnel, en ce compris leur droit d'accès, de rectification, d'effacement, d'opposition, de limitation, de portabilité et de révocation du consentement, à charge pour le

prestataire d'en avertir le client PageLife, entendu comme l'exportateur des données, et de mettre en œuvre toute action visant à répondre à la demande formulée.

Article deux : sécurité et confidentialité

Le prestataire met en œuvre, dans la collecte, le traitement et la conservation des données personnelles dans le cadre du contrat, les mesures techniques et organisationnelles appropriées permettant d'assurer la protection optimale des données à caractère personnel des personnes concernées et la conformité des traitements aux exigences du RGPD, en ce compris la protection structurelle des données à caractère personnel au sein des outils logiciels, infrastructures virtuelles ou matérielles et plus généralement l'ensemble des éléments techniques mis en œuvre pour exécuter les traitements, sur l'entier périmètre sous la responsabilité du prestataire.

Article trois : formation et gouvernance interne

Le prestataire met en œuvre :

–toutes mesures de formation et de sensibilisation de ses préposés aux obligations du RGPD et notamment au caractère spécial de l'utilisation des données personnelles qui peut être fait dans la stricte limite des finalités convenues et de l'exécution du présent contrat ;

–et la gouvernance et les procédures internes de nature à assurer le respect des engagements et le contrôle de la confidentialité des données à caractère personnel conformément au présent article.

Article quatre : analyse d'impact préalable

Le prestataire s'engage auprès des personnes concernées à traiter les données à caractère personnel les concernant, conformément aux finalités stipulées au contrat et aux instructions du client, dans le cadre des mesures de sécurité convenue avec le client et conformes aux exigences de la réglementation susmentionnée, notamment en ce qui concerne l'éventuelle exécution de toute analyse préalable d'impact nécessaire au regard des catégories de données collectées ou de la typologie des traitements effectués.

Article cinq : réparation du préjudice subi

Conformément aux clauses contractuelles types, si une personne concernée subit un dommage du fait d'un manquement au présent article par le prestataire ou par tout sous-traitant ultérieur auquel le prestataire aurait confié tout ou partie de ses prestations et qui aurait collecté, traité ou conservé les données à caractère personnel de ce fait, et est empêché d'agir directement contre le client notamment parce que celui-ci aurait juridiquement disparu sans que ses droits et obligations n'aient été repris par un tiers, la personne concernée sera en mesure d'agir directement rn compensation de ses préjudices contre le prestataire, ce que celui-ci reconnaît.

Il appartient également aux prestataires de stipuler dans ses accords avec ses sous-traitants ultérieurs que les personnes concernées seront susceptibles d'agir directement contre lesdits sous-traitants ultérieurs pour manquement aux obligations du présent article, dans le cas où le client et le prestataire aurait disparu sans reprise de leurs droits et obligations par un tiers.

Article six : autorité de contrôle

Le cas échéant, le prestataire reconnaît d'ores et déjà la compétence de l'autorité de contrôle et/ou des juridictions retenues par la personne concernée pour faire valoir ses droits.

L'autorité de contrôle compétente pour les personnes concernées pourra effectuer toutes vérifications directement chez le prestataire ainsi que ses éventuelles sous-traitants ultérieurs.

Article sept : primauté des clauses contractuelles types
En cas de contradiction entre le présent article et les clauses contractuelles types figurant en annexe du présent contrat, ces dernières prévalent en toute hypothèse.

Article huit : garanties à fournir
Par ailleurs, le prestataire s'engage vis-à-vis du client à fournir les garanties suivantes pour veiller à l'effectivité de la protection des données à caractère personnel et des droits reconnus ci-dessus au bénéfice des personnes concernées :
–établissement et fourniture à première demande de la documentation décrivant la confidentialité mise en œuvre par lui pour protéger les données personnelles ;
–conclusion des clauses contractuelles types encadrant tout éventuel transfert des données à tout sous-traitant secondaire qui ne serait pas situé sur le territoire de l'union européenne, ou de tout dispositif équivalent dûment reconnu par les autorités de contrôle ;
–contrôles et audits internes réguliers de nature à vérifier la permanence des dispositifs et procédures de protections internes des données personnelles, pendant tout le temps de leur conservation par le prestataire, tous traitements confondus ;
–mise en œuvre et maintien d'une procédure de signalement de toute faille ou accès non autorisé aux données, avérée ou suspectée, conduisant à l'alerte dans les meilleurs délais du client et le cas échéant de la personne physique concernée ;
–mise en œuvre et maintien d'une procédure de réception et d'exécution des demandes d'accès, de rectification ou de suppression émanant des personnes physiques concernées, et permettant l'information corrélative du client desdites demandes ;
–mise en œuvre et maintien d'un mécanisme de portabilité des données personnelles permettant de manière simple et sécurisée d'identifier l'ensemble des données personnelles correspondant à une personne physique, aux fins de suppression aux fins de portabilité vers un tiers prestataire, à la demande de la personne concernée, sans surcoût. En cas de demande de portabilité, le prestataire extrait et transmet les données personnelles vers le destinataire qui sera indiqué par le client en format structuré, courant et lisible par les services du marché.

Article neuf : limitation de l'utilisation des données
Le prestataire s'engage s'abstenir d'exploiter ou utiliser, faire des copies ou créer des fichiers des données personnelles au sein du système d'information du client à ses propres fins ou pour le compte d'un tiers. Le traitement d'une donnée personnelle correspondra strictement l'exécution des finalités stipulées ci-avant, dans le seul cadre de l'exploitation des services fournis par le prestataire.

Article dix : restriction d'accès protection réseau
Le prestataire mettra en place des restrictions d'accès logique et physique ainsi que les protections réseaux nécessaires et conformes à l'exposé des dispositifs de sécurité déployée, ainsi que tous dispositifs nécessaires de traçabilité des actions. Une annexe au contrat expose les dispositifs et procédures mis en œuvre pendant toute la durée du contrat.

Article onze : expiration ou résiliation du contrat
A l'expiration contractuellement déterminée du présent contrat, ou en cas de résiliation de ce dernier pour tout motif, le prestataire s'engage à retourner ou détruire les données personnelles en sa possession sous son contrôle, dans le cadre de la fourniture des services. »

Conclusion

Le concept proposé est original mais se heurte frontalement avec le principe de proportionnalité, ce qui amène à devoir minimiser au maximum le recueil de données compte tenu de l'objectif poursuivi. Eventuellement, il faudrait être en capacité de démontrer en quoi la communication de données telles que la photographie, la géolocalisation (notamment au niveau de la région) voire l'acquisition spécifique de tel ou tel produit par un client est déterminante pour augmenter ses ventes. A défaut, il est préférable de ne pas prévoir de géolocalisation au niveau régional, de photographie dans toute la mesure du possible, ni de précision quant à l'achat de tel ou tel produit ou service. Ensuite, le recours à des prestataires tels que Google (plusieurs fois sanctionnée par la CNIL), et Amazon Web Services, qui proposent des services innovants, est susceptible d'être problématique. Google LLC et Amazon Web Services adhèrent certes au *privacy shield* ce qui sécurise les transferts, pour l'instant. Mais compte tenu de l'historique de Google notamment, l'entreprise ayant été plusieurs fois sanctionnée par le CNIL, cette adhésion n'est pas une garantie juridique absolue. Surtout, le *privacy shield* fait l'objet de procédures judiciaires et une invalidation de ce mécanisme conduira à recourir logiquement au mécanisme des clauses contractuelles types de la Commission européenne (ou de la CNIL lorsqu'elles seront adoptées). Or Google LLC et Amazon Web Services ne feront pas nécessairement, compte tenu de leur importance, preuve de souplesse pour signer de tels documents. Enfin, et c'est l'une des difficultés importantes, le traitement va en pratique reposer essentiellement sur le consentement du visiteur du client via ce dernier alors que les données sont traitées dans l'intérêt exclusif du client, ce qui peut rendre difficile la collecte auprès du visiteur. Cela amène à une réflexion plus globale sur le modèle économique susceptible de permettre le meilleur développement du projet. Naturellement, ces contraintes seront moins importantes si l'activité se développe en dehors de l'Union européenne, étant rappelé que des dispositions relatives à la protection des données existent toutefois dans plusieurs pays (https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde). Il convient également de noter que le conformité du dispositif ne pourra s'apprécier parfaitement que lorsque la loi CNIL adaptant certaines dispositions du RGPD, actuellement en discussion au parlement, aura été promulguée.

Pour rappel, les sanctions liées à la violation des données personnelles sont les suivantes :
- administratives (de 3 millions aujourd'hui à 20 millions et 4 % du CA mondial à partir du 25 mai prochain). Avant cela, il y a habituellement des étapes préalables : avertissement, mise en demeure, limitation du traitement, suspension du flux, injonctions…
- pénales (droit à la vie privée, infraction CNIL 226-16 et suivants CP),
- civiles (dommages et intérêts pour les personnes concernées),
- risque d'image majeur.

Nantes, le 19 avril 2018