Mathias
Avocats

Sites internet et RGPD : Quels points d'attention ?

Me Garance Mathias

Avocat Associé – MATHIAS AVOCAT

AFUJ
Association Francophone
des Utilisateurs de Joomla!®

JDF
JOOMLADAY FR

#JD19FR

PARIS 8 & 9 MARS 2019

Quelques rappels utiles …

Qu’est-ce qu’une donnée à caractère personnel ?

« *Toute information se rapportant à une* ***personne physique identifiée ou identifiable****, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Que retenir ?

- ✓ La notion de « données à caractère personnel » est large.
- ✓ Une personne peut être directement identifiée par exemple par son nom et son prénom.
- ✓ Une personne peut être identifiable par exemple au moyen d’un identifiant, d’un numéro, de ses habitudes de vie, de ses préférences ou encore de caractéristiques qui lui sont propres (adresse mail, adresse IP, numéro d’adhérent/de client, numéro de téléphone, image, activités sportives/loisirs, etc.).

Quelques rappels utiles …

Qu’est-ce qu’un 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* ».

Que retenir ?

- ✓ La notion de traitement est large.
- ✓ Un traitement de données à caractère personnel n’est pas nécessairement automatisé : les fichiers au format papier sont également concernés.
- ✓ Un fichier ne contenant que des coordonnées relatives à des personnes morales de droit privé ou de droit public (dénomination sociale, adresse de l’établissement, numéro de téléphone du standard, adresse électronique générique de contact de type « entité@email.fr ») ne constitue pas un traitement de données à caractère personnel.

Quelques rappels utiles …

Qui est le responsable du traitement ?

> « *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*** ».

Que retenir ?

- ✓ Le responsable du traitement détermine les finalités **et** les moyens du traitement des données à caractère personnel.
- ✓ **Finalité(s)** : objectif(s) poursuivi(s) par l'utilisation des données à caractère personnel (prestation de service à un client final, prospection commerciale, établissement de statistiques sur les produits, etc.).
- ✓ **Moyens** : moyens techniques et organisationnels du traitement des données (matériels informatiques, logiciels, type de données collectées, définition de la durée de conservation, modalités de collecte des données, choix d'une solution proposée par un éditeur, etc.).

Quelques rappels utiles …

Qui est le sous-traitant ?

« *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* ».

Que retenir ?

- ✓ Le sous-traitant traite les données à caractère personnel uniquement **pour le compte** du responsable du traitement, et **sur ses instructions documentées**.
- ✓ Le RGPD **impose directement des obligations au sous-traitant** (désignation d'un DPO dans certains cas, obligation d'assurer la sécurité et la confidentialité des données, tenue de registres).
- ✓ Les **obligations du sous-traitant** et le **traitement qui lui est confié** doivent être **définis dans le contrat** qui le lie au responsable du traitement.

➔ Penser, si ce n'est pas déjà fait, à **mettre à jour les modèles de contrat** pour y intégrer un article ou une annexe dédiée à l'encadrement de la sous-traitance de données.

Quelques rappels utiles …

Principe de licéité, loyauté et transparence

Principe de limitation des finalités

Principe de minimisation des données

Principe d’exactitude des données

Principe de limitation de la conservation des données

Principe d’intégrité et de confidentialité

Quelques rappels utiles …

Consentement

Exécution d’un contrat auquel la personne est partie

Respect d’une obligation légale à laquelle le responsable de traitement est soumis

Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique

Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement

Intérêt légitime poursuivi par le responsable de traitement ou par un tiers

Tout traitement de données à caractère personnel doit avoir une base juridique.

Le consentement n’est pas systématiquement la base juridique du traitement !

Site web : les enjeux de la conformité

Les réflexes de la conformité d’un site web

- Respecter les normes relatives aux cookies et autres traceurs ;
- Intégrer des mentions d’information aux formulaires de collecte ;
- S’assurer de la conformité des campagnes de prospection ;
- S’assurer de la sécurisation du site.

Client, prestataire : qui est responsable de quoi ?

Le prestataire à qui est confié la réalisation du site du client n’en devient pas pour autant responsable des traitements opérés sur le site.

Il revient au responsable du traitement, en l’espèce le client, de déterminer les moyens et les finalités du traitement.

En pratique, cela signifie notamment qu’il doit trancher sur les caractéristiques du traitement, fixer les durées de conservation, déterminer les modalités de traitement des demandes d’exercice des droits par les personnes, fournir les mentions d’information, et plus généralement, donner toutes les instructions à son sous-traitant concernant la mise en œuvre du traitement.

Client, prestataire : qui est responsable de quoi ?

Le prestataire reste tenu d’un devoir de conseil.

Il doit notamment assister le client quand à la durée de conservation des données, aux modalités de délivrance de l’information, etc.

Il doit également signaler au client, dès qu’il en a connaissance, si l’une de ses instructions constitue une violation des règles en matière de protection des données.

De plus, le prestataire doit assurer la mise en œuvre des mesures fixées par le client responsable du traitement.

Par exemple, le prestataire doit implémenter les durées de conservation des données communiquées par le client,

Cookies et autres traceurs : que retenir ?

Par « cookies », il est entendu **tout mécanisme visant à inscrire ou à accéder à des informations dans le terminal d’un utilisateur par voie électronique**.

Sont ainsi visées les classiques cookies HTTP, mais également les *local shared objects* ou cookies flash, pixels invisibles ou web bugs , les techniques de fingerprinting, ou encore les identificateurs cachés.

Par principe, il est **interdit de déposer des cookies sur le terminal d’un utilisateur sans l’en avoir préalablement informé, lui avoir fourni des moyens de s’opposer au dépôt de cookies et avoir recueilli son consentement**. La Cnil a identifié des cookies qui, par exception, peuvent être déposés et lus sans le consentement des personnes.

Cookies et autres traceurs : que retenir ?

Cookies devant faire l’objet d’une information et d’un consentement préalable

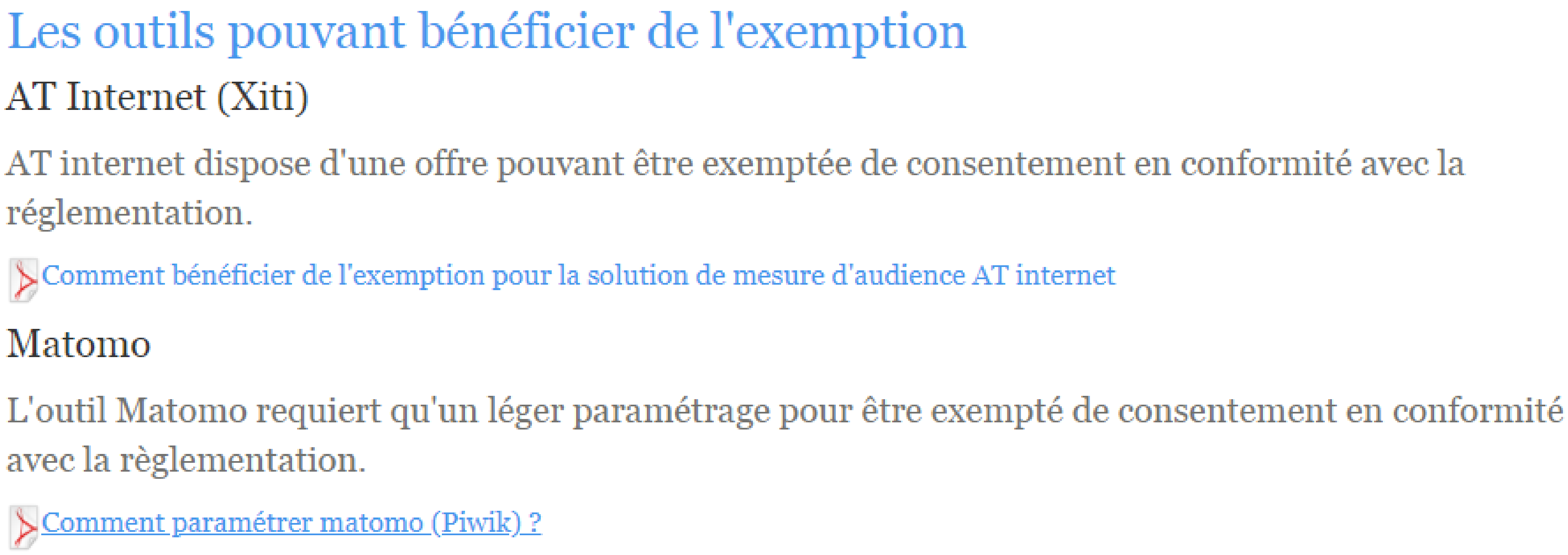
- Cookies de ciblage publicitaire ;
- Cookies de mesures d’audience (type « Google Analytics »), à l’exception de ceux respectant les conditions posées par la Cnil ;
- Cookies de réseaux sociaux générés notamment par les boutons de partage et fonctionnalités intégrées (bouton « J’aime », fil d’actualité Twitter, lecteur vidéo, etc.) .

Cookies pouvant être lus et déposés sans consentement

- Cookies « techniques » c’est-à-dire ayant pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- Cookies strictement nécessaires à la fourniture d’un service expressément demandé par l’utilisateur ;
- Cookies de mesure d’audience respectant les conditions posées par la Cnil.

Focus sur le cookie de mesure d’audience

La Cnil préconise deux cookies pour mettre en place des cookies de mesure d’audience ne nécessitant pas le recueil préalable du consentement.



Les outils pouvant bénéficier de l'exemption

AT Internet (Xiti)

AT internet dispose d'une offre pouvant être exemptée de consentement en conformité avec la réglementation.

Comment bénéficier de l'exemption pour la solution de mesure d'audience AT internet

Matomo

L'outil Matomo requiert qu'un léger paramétrage pour être exempté de consentement en conformité avec la règlementation.

Comment paramétrer matomo (Piwik) ?

Focus sur le cookie de mesure d’audience

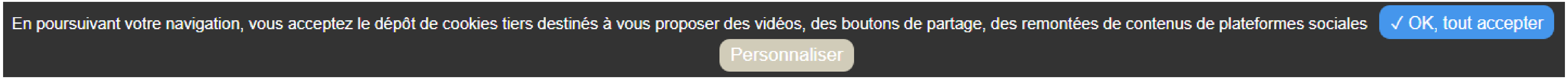
Il reste possible d’avoir recours à une autre solution de mesure d’audience, comme Google Analytics. Dans cette hypothèse :

Soit elle est paramétrée pour correspondre aux exigences de la Cnil. Elle pourra alors être déposée sans que le consentement de l’internaute ne doivent être recueilli

Soit il sera nécessaire de recueillir le consentement de l’internaute avant de déposer le cookie.

Un exemple de « bandeau cookies » conforme

Exemple de « bandeau cookies » conforme : celui de la Cnil.


En poursuivant votre navigation, vous acceptez le dépôt de cookies tiers destinés à vous proposer des vidéos, des boutons de partage, des remontées de contenus de plateformes sociales

Par le bouton « Personnaliser », le bandeau indique à l'internaute qu'il peut effectuer des choix.

Il apparait à première visite, et liste clairement les finalités poursuivies par l'utilisation des cookies.

Solution de gestion des consentements aux cookies

Voici la solution utilisée par la Cnil, qui apparaît lorsque l'on clique sur le bouton « personnaliser »

Gestion de vos préférences sur les cookies

Certaines fonctionnalités de ce site (partage de contenus sur les réseaux sociaux, lecture directe de vidéos) s'appuient sur des services proposés par des sites tiers. Ces fonctionnalités déposent des cookies permettant notamment à ces sites de tracer votre navigation. Ces cookies ne sont déposés que si vous donnez votre accord. Vous pouvez vous informer sur la nature des cookies déposés, les accepter ou les refuser soit globalement pour l'ensemble du site et l'ensemble des services, soit service par service.

Préférences pour tous les services

Réseaux sociaux

Les réseaux sociaux permettent d'améliorer la convivialité du site et aident à sa promotion via les partages.

Facebook

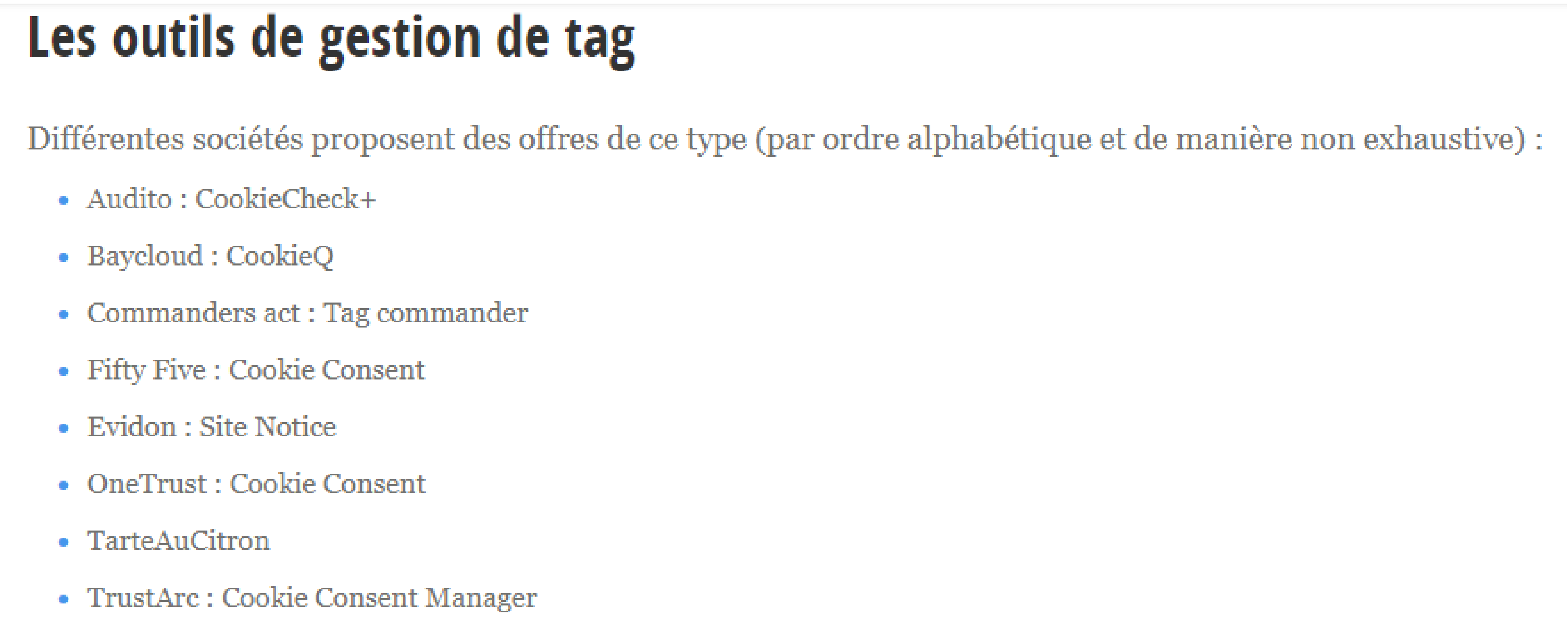
Twitter

L'internaute peut choisir par type de cookies ceux qu'il accepte et ceux qu'il refuse.

Solution de gestion des consentements aux cookies

La Cnil préconise le recours à des gestionnaires de tag pour gérer le consentement de l'internaute et le dépôt des cookies.

La Cnil indique également comment paramétrer la solution open source TarteAuCitron.



Les outils de gestion de tag

Différentes sociétés proposent des offres de ce type (par ordre alphabétique et de manière non exhaustive) :

- Audito : CookieCheck+
- Baycloud : CookieQ
- Commanders act : Tag commander
- Fifty Five : Cookie Consent
- Evidon : Site Notice
- OneTrust : Cookie Consent
- TarteAuCitron
- TrustArc : Cookie Consent Manager

Et les formulaires de collecte ?

- Le responsable du traitement doit informer les personnes dont les données à caractère personnel sont traitées.

  ➔ Sur un site internet, cela se traduit principalement par **l’intégration de mentions d’information sur les pages contenant des formulaires de collecte** (formulaire de contact, inscription à la newsletter, création de compte, etc.).

  ➔ Une bonne pratique consiste également à rédiger, en complément des mentions d’information, une **politique relative à la protection des données** à caractère personnel permettant de centraliser l’information et d’avoir une vue d’ensemble sur tous les traitements réalisés sur le site.

Et les formulaires de collecte ?

Contenu d’une mention d’information pour un formulaire de collecte

- ✓ Identification du responsable du traitement ;
- ✓ Finalité(s) du traitement et base juridique de celui-ci ; le cas échéant, description de l’intérêt légitime poursuivi ; le cas échéant, existence du droit de retirer le consentement donné à tout moment ;
- ✓ Coordonnées du délégué à la protection des données (si désigné) ;
- ✓ Caractère obligatoire ou facultatif du recueil des données ;
- ✓ Destinataires des données (internes et externes) ;
- ✓ Droits reconnus aux personnes par la réglementation et modalités d’exercice ;
- ✓ Droit de saisir la CNIL d’une réclamation ;
- ✓ Durée de conservation des données ;
- ✓ Dans certains cas : l’existence d’un transfert des données hors UE et les modalités d’accès aux garanties encadrant le transfert ; l’existence d’une prise de décision automatisée ou d’un profilage, les informations permettant de comprendre la logique de ces mécanismes et les conséquences pour les personnes.

Emailing commercial : comment se conformer ?

DOIS-JE RECUEILLIR LE CONSENTEMENT ?		
BtoC	**Principe : OPT-IN** Information préalable + recueil du consentement **(Prospects)**	**Exception : OPT-OUT** Information préalable + droit d'opposition <u>Si les trois conditions sont remplies</u> : ➔ La personne prospectée est déjà cliente ➔ La prospection émane de la société qui a collecté les données ➔ La prospection concerne un produit ou service analogue à celui commandé **(Clients)**
BtoB	**OPT-OUT** Information préalable + Droit d'opposition (au moment de la collecte des données et à chaque envoi) Uniquement si la prospection commerciale adressée a un lien avec la fonction occupée par la personne dans son entité	

Le point sur le consentement

Le consentement est une manifestation de volonté **libre, éclairée, spécifique** et **univoque**.

- L'usage de cases pré-cochées est à proscrire.
- La personne doit être informée clairement de chaque finalité auquel elle consent.
- Le consentement doit être matérialisé dans la base de données.
- Le consentement doit pouvoir être retiré à tout moment par la personne.

Exemple : une newsletter commerciale

- Au regard de tous les éléments que l’on vient d’aborder, un exemple : une newsletter nécessitant le recueil du consentement (opt-in) de l’abonné.

  ➔ **Intégrer une case ou une option permettant de recueillir le consentement**. La case ne doit pas être précochée, l’option ne doit pas être pré-selectionnée.

  ➔ **Indiquer en des termes clairs à la personne concernée ce à quoi elle consent**. Par exemple, s’il est envisagé de transmettre les données à des partenaires commerciaux, cela doit faire l’objet d’une case distincte, et la personne doit pouvoir consentir uniquement à l’un ou à l’autre.

  ➔ Attention : **le consentement doit pouvoir être retiré aussi facilement qu’il a été donné**. La personne doit pouvoir retirer son consentement à tout moment. En pratique, penser à **insérer un lien de désinscription** effectif en bas de chaque envoi.

  ➔ S’assurer de la **traçabilité/matérialisation du consentement** dans la base de données.

  ➔ **Penser à intégrer au formulaire une mention d’information adéquate.**

Assurer la sécurité du site

- Le responsable du traitement et le sous-traitant doivent mettre en œuvre des mesures appropriées afin de garantir la sécurité des données. **Ces mesures doivent être régulièrement réévaluées et adaptées au besoin**.
- **Les textes ne prescrivent pas de mesures techniques obligatoires**. Certaines mesures sont toutefois préconisées, notamment :
  - ➔ La Cnil recommande régulièrement l'usage du protocole HTTPS, avec la version la plus à jour de TLS.
  - ➔ La Cnil préconise également le chiffrement et/ou la pseudonymisation des données conservées.
  - ➔ La Cnil a adopté le 19 janvier 2017 une recommandation relative aux mots de passe : préconisations relatives à la taille minimale, la complexité, le nombre de tentatives de connexion autorisées avant la suspension de l'accès au compte, etc.

Les bons réflexes sur le plan technique

S’assurer de la sécurisation du site (protocoles à jour, accès restreint au *back office*, etc.)

Vérifier la conformité en matière de cookies (durée de vie des cookies déposés, recueil du consentement, etc.)

S’assurer que les données sont effectivement supprimées à l’expiration des durées fixées par le client responsable du traitement, ou lorsqu’il est fait droit à une demande de suppression par une personne concernée

S’assurer de la traçabilité du consentement des personnes concernées en base de données

Pour suivre l’actualité du droit des nouvelles technologies, de la propriété intellectuelle ou encore de la protection des données à caractère personnel :

Abonnez-vous à la newsletter du cabinet sur www.avocats-mathias.com
Suivez-nous sur Twitter : @GaranceMathias

MATHIAS AVOCATS
19 rue Vernier – 75017 PARIS
Tél.: 01 43 80 02 01
E-mail: contact@avocats-mathias.com

AFUJ
Association Francophone
des Utilisateurs de Joomla!®

JOOMLADAY FR

#JD19FR

PARIS 8 & 9 MARS 2019