JustRelate

Bannières de cookies

La check-list pratique de conformité RGPD & LIL

Votre bannière de cookies est-elle vraiment conforme ? Seule une infime minorité respecte strictement les critères des autorités de contrôle. Le verdict est sans appel : si un seul critère fait défaut, l'ensemble des consentements collectés devient invalide. C'est pourquoi nous avons condensé les exigences des autorités de contrôle dans un guide pratique et compact.

- Les exigences de la **Commission Nationale de l'Informatique et des Libertés** (CNIL) et du **Comité Européen de la Protection des Données** (CEPD)
- Les obligations légales du **Règlement Général sur la Protection des Données** (RGPD) et de la **Loi Informatique et Libertés** (LIL)

Conception du choix (caractère facultatif et clarté)

- ☐ **Équivalence entre accepter et refuser :** refuser les traceurs doit être aussi simple que les accepter. Si un simple clic suffit pour tout accepter, un seul clic doit également suffire pour tout refuser.
- ☐ **Pas de designs manipulateurs (dark patterns) :** la bannière ne doit pas recourir à des pratiques de conception trompeuses. Les boutons et les polices de caractères pour l'acceptation et le refus doivent présenter la même taille, la même lisibilité et le même niveau de mise en évidence visuelle.
- ☐ **Permettre une sélection granulaire :** les utilisateurs doivent avoir la possibilité de donner leur consentement de manière spécifique et indépendante pour chaque finalité. Cela peut être réalisé via un bouton tel que « Personnaliser mes choix » au premier niveau, qui mène à un aperçu détaillé.
- ☐ **Préréglages clairs (opt-in) :** les cases à cocher (checkboxes) ou les curseurs (sliders) doivent être désactivés par défaut (opt-in).

Enregistrement et retrait du consentement

- ☐ **Enregistrement du choix (bonne pratique: 6 mois) :** la décision de l'utilisateur (qu'il s'agisse d'un consentement ou d'un refus) doit être enregistrée afin que la bannière ne s'affiche pas à chaque nouvelle visite de la page, ce qui porterait atteinte à la liberté de choix. À l'expiration de 6 mois ou en cas de modification des finalités ou des services, le consentement doit être renouvelé.
- ☐ **Permettre une révocation simple et à tout moment :** les utilisateurs doivent pouvoir révoquer un consentement donné aussi facilement qu'ils l'ont donné. À cette fin, un lien facilement accessible ou une icône statique (par exemple en bas à gauche de l'écran) doit être disponible en permanence.

JustRelate

Information et transparence

- [ ] **Indiquer clairement les finalités :** les finalités précises des traceurs (par exemple, publicité personnalisée, mesure d'audience, partage sur les réseaux sociaux) doivent être présentées de manière compréhensible et dans un langage clair dès le premier écran. Chaque finalité doit être accompagnée d'un titre court et mis en évidence, ainsi que d'une brève description.

- [ ] **Informations légales et informations relatives aux données personnelles :** une bannière de consentement ne doit pas faire office de « barrière » devant ces contenus, de sorte que l'utilisateur soit contraint d'accepter ou de refuser les cookies avant de pouvoir consulter les mentions légales ou la politique de confidentialité. Il est préférable de désactiver l'affichage de la bannière sur les pages contenant les mentions légales obligatoires.

- [ ] **Le nombre et l'identité des responsables du ou des traitements impliqués :**

  Le nombre de responsables du ou des traitements concernés devrait être indiqué dans la première phase d'information.

- [ ] Une liste complète et à jour des responsables du traitement doit être mise à disposition lors de la demande de consentement, par exemple via un lien hypertexte accessible dans une deuxième fenêtre d'information.

- [ ] Pour les services et les cookies ne nécessitant pas de consentement, la CNIL recommande, dans un souci de transparence, de les mentionner dans la politique de confidentialité. Il n'est pas nécessaire de les énumérer dans la fenêtre de consentement.

Catégorisation correcte

- [ ] **Des finalités clairement distinctes :** Les services et les cookies doivent être regroupés en fonction de leurs finalités concrètes et précises. Il ne doit y avoir ni cookies non classés, ni catégorie « Divers »! Voici quelques catégories types reconnues par la CNIL: Publicité personnalisée, Mesure d'audience et Partage sur les réseaux sociaux. L'exception prévue par art. 82 de la LIL s'applique uniquement aux traceurs « strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur ».

- [ ] **Google Analytics et Google Tag Manager** relèvent de la catégorie des services soumis au recueil du consentement. La raison en est notamment le détournement des données ainsi que la possibilité de réidentifier les utilisateurs malgré l'anonymisation de l'adresse IP. Ceci s'applique pleinement et sans réserve au mode appelé « Consent Mode avancé » (**Advanced Consent Mode**) de Google Analytics 4 (GA4). Avec le « Consent Mode avancé », le script Google Analytics (GA4) est chargé immédiatement, avant même que l'utilisateur n'ait fait un choix sur la bannière. Si l'utilisateur refuse les cookies (ou ne réagit pas), GA4 ne dépose certes aucun cookie dans le navigateur, mais il envoie ce que l'on appelle des « pings sans cookies » aux serveurs de Google.

- [ ] Selon la CNIL, **l'A/B testing** sert principalement à l'optimisation commerciale (augmentation du taux de conversion, promotion des ventes). Par conséquent, un consentement (opt-in) est en principe requis. La seule exception : un outil d'A/B testing ne peut être exempté de consentement que s'il est strictement couplé à un outil de mesure d'audience (analyse web) lui-même exempté et reconnu par la CNIL.

JustRelate

Catégorisation correcte (suite)

- [ ] Les traceurs utilisés pour la facturation des activités **d'affiliation** ne sont pas exemptés de consentement.

- [ ] Même les services d'analyse web soi-disant respectueux de la vie privée, tels que **Matomo ou Piwik** PRO, ne peuvent pas être utilisés par défaut sans consentement, car ils lisent activement, entre autres, la résolution de l'écran. En revanche, une configuration centralisée d'**etracker Analytics** facilite le respect des exigences strictes liées à l'exemption de consentement en mode cookie. Dans son mode sans cookie activé par défaut, etracker Analytics peut être utilisé d'emblée sans consentement. L'exemption de consentement pour l'analyse web avec cookies ne s'adresse qu'aux éditeurs de sites web qui n'ont pas besoin de suivi de campagnes, c'est-à-dire qui ne mesurent pas la performance des publicités ou des e-mails.

Nombreux pièges techniques

- [ ] La mise en place d'une configuration juridiquement et techniquement correcte s'avère d'autant plus difficile dans le cadre d'un tracking hybride (avec et sans cookies), de la collecte de conversions avancées intégrant des données de ciblage personnelles, ou d'un double suivi des conversions (à la fois par pixel et côté serveur) nécessitant une déduplication rigoureuse des données de conversion. Les pièges sont extrêmement nombreux et peuvent entraîner aussi bien des violations de la loi que des erreurs de configuration coûteuses dans le pilotage des enchères publicitaires (Ads).

- [ ] De nombreux éditeurs de sites web se fient **aux fonctions de scan et de blocage automatiques** ainsi qu'aux catégorisations automatisées des solutions de Consent Management. Bien que ces outils puissent soutenir les processus de vérification manuelle, ils sont sujets aux erreurs, en particulier avec les services moins courants. De plus, la prudence est de mise car les analyses ne s'effectuent parfois que de manière hebdomadaire, ce qui peut conduire temporairement à une situation de non-conformité. Les solutions intégrées de Tag et de Consent Management rendent les fonctions de scan et de blocage automatiques superflues.

- [ ] Étant donné que **Google Maps et YouTube** transmettent des adresses IP et d'autres données d'appareil à Google et déposent des cookies lors du chargement des scripts et des iFrames, ils ne peuvent pas être chargés par défaut sans consentement. Dans ce cas, il est recommandé d'utiliser ce que l'on appelle le « blocage de contenu » (content blocking): cela permet de s'assurer qu'en l'absence de consentement, seule une mention relative au contenu masqué s'affiche, offrant la possibilité d'une activation ciblée par le biais d'un consentement.