Recommandation

PROPOSANT DES MODALITÉS PRATIQUES DE MISE EN CONFORMITÉ EN CAS DE RECOURS AUX « COOKIES ET AUTRES TRACEURS »

Version consolidée publiée le 16 janvier 2026 à partir des textes suivants :

- *délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs » ; et*
- *délibération n° 2025-131 du 18 décembre 2025 proposant des modalités pratiques de mise en conformité du consentement multi-terminaux et portant modification de la recommandation n° 2020-092 du 17 septembre 2020 dite « cookies et autres traceurs »*

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Périmètre de la recommandation

1.1. Acteurs concernés

La présente recommandation concerne tous les organismes qui recourent à des traceurs, tels que définis dans les lignes directrices du 17 septembre 2020.

1.2. Environnements concernés

Modifié par la délibération n° 2025-131 du 18 décembre 2025

La présente recommandation tient particulièrement compte des configurations propres aux environnements web et aux applications mobiles. La présente recommandation peut cependant inspirer et guider l'élaboration d'interfaces dans d'autres contextes où le consentement prévu par l'article 82 de la loi « Informatique et Libertés » est requis : télévision connectée, console de jeux vidéo, assistant vocal, objets communicants, véhicule connecté, etc.

La recommandation concerne tant les environnements dans lesquels les utilisateurs sont authentifiés à un compte (parfois appelés « univers logués ») que les univers où ils ne le sont pas (« univers non logués »). En effet, le fait que les utilisateurs soient authentifiés ne dispense pas de recueillir leur consentement conformément à l'article 82 de la loi « Informatique et Libertés », dès lors que des traceurs soumis au consentement sont utilisés.

Toutefois, l'article 7 relatif au consentement multi-terminaux concerne uniquement les univers dans lesquels les utilisateurs sont authentifiés et s'applique à l'ensemble des environnements (terminal, navigateur ou application) à partir desquels ils s'authentifient.

2. Information, consentement et refus

Comme rappelé par les lignes directrices du 17 septembre 2020, lorsqu'aucune des exceptions prévues à l'article 82 de la loi « Informatique et Libertés » n'est applicable, les utilisateurs doivent, d'une part, recevoir une information conforme à cet article, complétée, le cas échéant, par les exigences du RGPD, et, d'autre part, se voir indiquer les conséquences de leur choix.

Au sein de la présente recommandation, l'absence de consentement des utilisateurs est désignée par le terme « refus ». Toute inaction ou action des utilisateurs autre qu'un acte positif signifiant son consentement doit être interprétée comme un refus de consentir ; dans ce cas, aucune opération de lecture ou d'écriture soumise au consentement ne peut légalement avoir lieu.

De manière générale, afin d'être compréhensible et de ne pas induire en erreur les utilisateurs, la Commission recommande aux organismes concernés de s'assurer que les utilisateurs prennent la pleine mesure des options qui s'offrent à eux, notamment au travers du design choisi et de l'information délivrée.

Par ailleurs, la Commission encourage le développement d'interfaces standardisées, fonctionnant de la même manière et utilisant un vocabulaire uniformisé, de nature à faciliter la compréhension des utilisateurs dans leur navigation sur les sites ou applications mobiles.

2.1. Information sur les finalités des traceurs

Comme rappelé dans les lignes directrices, les finalités des traceurs doivent être présentées aux utilisateurs avant que ceux-ci ne se voient offrir la possibilité de consentir ou de refuser. Elles doivent être formulées de manière intelligible, dans un langage adapté et suffisamment clair pour permettre aux utilisateurs de comprendre précisément ce à quoi ils consentent.

Afin d'en faciliter la lecture, la Commission recommande que chaque finalité soit mise en exergue dans un intitulé court et mis en évidence, accompagné d'un bref descriptif. Des exemples permettant de se conformer aux règles applicables sont présentés ci-dessous, de manière non exhaustive :

- Si le ou les traceurs sont utilisés afin d'afficher de la publicité personnalisée, cette finalité peut être décrite de la manière suivante : « **Publicité personnalisée** : *[nom du site / de l'application] [et **des***

sociétés tierces / nos partenaires* utilise / utilisent des traceurs afin d'afficher de la publicité personnalisée en fonction de votre navigation et de votre profil ».*

- Si le ou les traceurs ne sont utilisés que pour mesurer l'audience de la publicité affichée, sans la sélectionner sur la base de données à caractère personnel, le responsable du traitement peut utiliser la formulation suivante : « **Publicité non personnalisée** : *[nom du site / de l'application] [et **des sociétés tierces / nos partenaires**] utilise / utilisent des traceurs dans le but de mesurer l'audience de la publicité [sur le site ou l'application], sans vous profiler* ».
- Si la publicité est adaptée en fonction de la géolocalisation précise, cette finalité peut être décrite de la manière suivante : « **Publicité géolocalisée** : *[nom du site / de l'application] [et **des sociétés tierces/ nos partenaires**] utilise / utilisent des traceurs pour vous adresser de la publicité en fonction de votre localisation* ».
- Si les traceurs sont utilisés pour personnaliser le contenu éditorial ou les produits et services fournis affichés par l'éditeur, les formulations suivantes pourraient être affichées : « ***Personnalisation de contenu** : Notre site / application [et des **sociétés tierces**] utilise / utilisons des traceurs pour personnaliser le contenu éditorial [de notre site / application] en fonction de votre utilisation »,* ou *« Notre site / application [et **des sociétés tierces**] utilise / utilisons des traceurs pour personnaliser l'affichage de nos produits et services en fonction de ceux que vous avez précédemment consultés [sur notre site / application]* »).
- Si les traceurs sont utilisés afin de partager des données sur les réseaux sociaux, leur finalité peut être décrite de la manière suivante : *« **Partage sur les réseaux sociaux** : Notre site / application utilise des traceurs pour vous permettre de partager du contenu sur les réseaux sociaux ou plateformes présents [sur notre site / application]* ». Si l'éditeur a choisi de mettre en place un mécanisme permettant de ne déclencher ces traceurs que lorsque les utilisateurs souhaitent effectivement partager des données avec les réseaux sociaux concernés (et qu'ils interagissent avec la fonctionnalité ou le bouton permettant cette interaction), l'information et le recueil du consentement pourraient apparaitre lorsque les utilisateurs décident de déclencher ladite fonctionnalité de partage.

La Commission recommande en outre de faire figurer, en complément de la liste des finalités présentées sur le premier écran, une description plus détaillée de ces finalités, de manière aisément accessible depuis l'interface de recueil du consentement. Cette information peut, par exemple, être affichée sous un bouton de déroulement que l'internaute peut activer directement au premier niveau d'information. Elle peut également être rendue disponible en cliquant sur un lien hypertexte présent au premier niveau d'information.

Le contenu de cette information additionnelle peut, par exemple, venir préciser que l'affichage de la publicité englobe différentes opérations techniques concourant à la même finalité. Celles-ci incluent également le plafonnement de l'affichage (parfois appelé « *capping* publicitaire », consistant à ne pas présenter à un utilisateur une même publicité de manière trop répétitive), la lutte contre la « fraude au clic » (détection d'éditeurs prétendant réaliser une audience publicitaire supérieure à la réalité), la facturation de la prestation d'affichage, la mesure des cibles ayant plus d'appétences à la publicité pour mieux comprendre l'audience, etc.

Figure 1- Le détail des finalités est disponible sous un bouton de déroulement que l'utilisateur peut activer sur le premier niveau d'information

Figure 2 - Le détail des finalités est disponible en cliquant sur un lien hypertexte présent sur le premier niveau d'information

Enfin, afin d'accroître la transparence, un responsable de traitement peut également préciser les catégories de données collectées en les associant aux finalités qu'elles permettent d'atteindre.

2.2 - Information sur la portée du consentement

Lorsque des traceurs soumis au consentement, déposés par d'autres entités que l'éditeur du site ou l'application mobile, permettent un suivi de la navigation de l'utilisateur au-delà du site ou de l'application mobile où ceux-ci sont initialement déposés, la Commission recommande fortement que le consentement soit recueilli sur chacun des sites ou applications concernés par ce suivi de navigation, afin de garantir que l'utilisateur soit pleinement conscient de la portée de son consentement.

2.2. Information concernant l'identité du ou des responsables du traitement

Les utilisateurs doivent pouvoir prendre connaissance de l'identité de l'ensemble des responsables du ou des traitements, y compris les responsables de traitement conjoints, avant de donner leur consentement ou de refuser. Ainsi, comme explicité dans les lignes directrices du 17 septembre 2020, la liste exhaustive et régulièrement mise à jour des responsables du ou des traitements doit être mise à la disposition des utilisateurs au moment du recueil de leur consentement.

En pratique, afin de concilier les exigences de clarté et de concision des informations avec la nécessité d'identifier l'ensemble des responsables du ou des traitements, les informations spécifiques sur ces entités (identité, lien vers leur politique de traitement des données à caractère personnel), régulièrement mises à jour, peuvent par exemple être fournies à un second niveau d'information. Elles peuvent ainsi être mises à disposition depuis le premier niveau *via*, par exemple, un lien hypertexte ou un bouton accessible depuis ce niveau. La Commission recommande en outre d'utiliser une dénomination descriptive et utilisant des termes clairs, telle que « liste des sociétés utilisant des traceurs sur notre site / application ».

Enfin, la Commission recommande qu'une telle liste soit également mise à la disposition des utilisateurs de manière permanente, à un endroit aisément accessible à tout moment sur le site web ou l'application mobile. Ainsi, le mécanisme permettant de prendre connaissance de la liste à jour des responsables de traitement devrait de préférence être placé dans des zones de l'écran qui attirent l'attention des utilisateurs ou dans des zones où ils s'attendent à le trouver, tout au long de leur navigation. A titre d'exemple, l'éditeur d'un site web peut fournir aux utilisateurs un module de paramétrage accessible sur toutes les pages du site au moyen d'une icône statique « *cookie* » toujours visible ou d'un lien hypertexte situé en bas ou en haut de page.

Afin d'accroître la lecture de l'information par les utilisateurs, le nombre de responsables du ou des traitements impliqués pourrait être indiqué au premier niveau d'information. De même, le rôle des responsables du ou des traitements pourrait être mis en évidence en les regroupant par catégories, lesquelles seraient définies en fonction de leur activité et de la finalité des traceurs utilisés.

2.3. L'expression du consentement ou du refus

S'agissant du caractère univoque du consentement

Le consentement doit se manifester par un acte positif clair des utilisateurs, répondant aux conditions fixées par le RGPD, interprétées par la Commission dans ses lignes directrices du 17 septembre 2020.

La Commission estime qu'une demande de consentement effectuée au moyen de cases à cocher, décochées par défaut, est facilement compréhensible par les utilisateurs. Le responsable du ou des traitements peut également avoir recours à des interrupteurs (« *sliders* »), désactivés par défaut, si le choix exprimé par les utilisateurs est aisément identifiable. La Commission recommande d'être attentif à ce que l'information accompagnant chaque élément actionnable permettant d'exprimer un consentement ou un refus soit facilement compréhensible et ne nécessite pas d'efforts de concentration ou d'interprétation de la part de l'utilisateur. Ainsi, il est notamment recommandé de s'assurer qu'elle n'est pas rédigée de telle manière qu'une lecture rapide ou peu attentive pourrait laisser croire que l'option sélectionnée produit l'inverse de ce que les utilisateurs pensaient choisir.

S'agissant du caractère libre du consentement

Le consentement ne peut être valide que si les utilisateurs sont en mesure d'exercer librement leur choix.

Afin de s'assurer du caractère libre du consentement donné, la Commission recommande de demander aux utilisateurs leur consentement de façon indépendante et spécifique pour chaque finalité distincte.

Toutefois, la Commission estime que cela ne fait pas obstacle à la possibilité de proposer aux utilisateurs de consentir de manière globale à un ensemble de finalités, sous réserve de présenter, au préalable, aux utilisateurs l'ensemble des finalités poursuivies.

A ce titre, la Commission souligne qu'il est possible de proposer des boutons d'acceptation et de refus globaux au stade du premier niveau d'information, via par exemple la présentation de boutons intitulés « tout accepter » et « tout refuser », « j'autorise » et « je n'autorise pas », « j'accepte tout » et « je n'accepte rien » et permettant de consentir ou de refuser, en une seule action, à plusieurs finalités.

Pour permettre aux personnes de choisir finalité par finalité, il est possible d'inclure un bouton, sur le même niveau d'information que les liens ou boutons permettant de tout accepter et de tout refuser, permettant d'accéder au choix finalité par finalité. A titre d'exemple, un bouton « personnaliser mes choix » ou « décider par finalité » permettrait d'indiquer clairement cette possibilité. Les utilisateurs pourraient se voir également proposer d'accepter ou de refuser finalité par finalité directement sur le premier niveau d'information. Ils pourraient aussi être invités à cliquer sur chaque finalité afin qu'un menu déroulant leur propose des boutons « accepter » ou « refuser ».

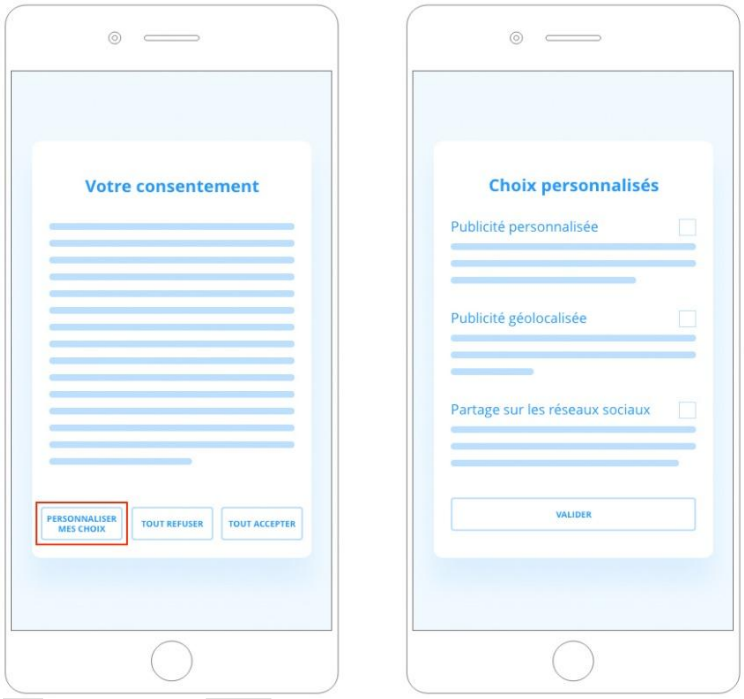

Figure 3 - La possibilité de consentir de manière granulaire peut-être offerte sur un second niveau d'information via un bouton « personnaliser mes choix » inséré sur le même niveau d'information (premier niveau) que les boutons permettant de « tout accepter » et de « tout refuser ».

De manière générale, la Commission recommande d'utiliser une dénomination descriptive et intuitive afin que les utilisateurs puissent avoir pleinement conscience de la possibilité d'exercer un choix par finalité.

S'agissant des modalités du refus

Le responsable de traitement doit offrir aux utilisateurs tant la possibilité d'accepter que de refuser les opérations de lecture et/ou d'écriture avec le même degré de simplicité.

Ainsi, la Commission recommande fortement que le mécanisme permettant d'exprimer un refus de consentir aux opérations de lecture et/ou d'écriture soit accessible sur le même écran et avec la même facilité que le mécanisme permettant d'exprimer un consentement. En effet, elle estime que les interfaces de recueil du consentement qui nécessitent un seul clic pour consentir au traçage tandis que plusieurs actions sont nécessaires pour « paramétrer » un refus de consentir présentent, dans la plupart des cas, le risque de biaiser le choix de l'utilisateur, qui souhaite pouvoir visualiser le site ou utiliser l'application rapidement.

Par exemple, au stade du premier niveau d'information, les utilisateurs peuvent avoir le choix entre deux boutons présentés au même niveau et sur le même format, sur lesquels sont inscrits respectivement « tout accepter » et « tout refuser », « autoriser » et « interdire », ou « consentir » et « ne pas consentir », ou toute autre formulation équivalente et suffisamment claire. La Commission considère que cette modalité constitue un moyen simple et clair pour permettre à l'utilisateur d'exprimer son refus aussi facilement que son consentement.

Figure 4 - L'utilisateur peut avoir le choix entre un bouton « tout accepter » et un bouton « tout refuser » présentés au même niveau et sur le même format.

L'expression du refus de consentir peut toutefois découler d'autres types d'actions que celle consistant à cliquer sur l'un des boutons décrits ci-dessus. En tout état de cause, la Commission rappelle que les modalités permettant aux utilisateurs de consentir ou de refuser doivent être présentées de façon claire et compréhensible. En particulier, lorsque le refus peut être manifesté par la simple fermeture de la fenêtre de recueil du consentement ou encore par l'absence d'interaction avec celle-ci pendant un certain laps de temps, cette possibilité doit être clairement indiquée aux utilisateurs sur cette fenêtre. En effet, à défaut, l'utilisateur serait susceptible de ne pas comprendre que ces actions conduisent à ce qu'aucune opération de lecture ou d'écriture soumise au consentement ne peut avoir légalement lieu. Un design et une information appropriés devraient lui permettre de bien comprendre les options qui s'offrent à lui.

Figure 5 - L'utilisateur peut cliquer sur « continuer sans accepter » pour exprimer son refus au dépôt et à la lecture de traceurs.

Afin de ne pas induire en erreur les utilisateurs, la Commission recommande que les responsables de traitement s'assurent que les interfaces de recueil des choix n'intègrent pas de pratiques de design potentiellement trompeuses laissant penser aux utilisateurs que leur consentement est obligatoire ou qui mettent visuellement plus en valeur un choix plutôt qu'un autre. Il est recommandé d'utiliser des boutons et une police d'écriture de même taille, offrant la même facilité de lecture, et mis en évidence de manière identique.

S'agissant de la conservation des choix

La Commission observe qu'il est, en principe, nécessaire de conserver les choix exprimés par les utilisateurs durant leur navigation sur le site. En effet, à défaut de la conservation de ces choix, les utilisateurs se verraient afficher une nouvelle fenêtre de demande de consentement à chaque page consultée, ce qui pourrait porter atteinte à la liberté de leur choix.

De plus, la Commission recommande que, lorsque le refus peut être manifesté par la poursuite de la navigation, le message sollicitant le consentement (par exemple, la fenêtre ou le bandeau) disparaisse au bout d'un laps de temps court, de manière à ne pas gêner l'utilisation du site ou de l'application et à ne pas, ainsi, conditionner le confort de navigation de l'utilisateur à l'expression de son consentement au traceur.

De manière générale, la Commission recommande que le choix exprimé par les utilisateurs, qu'il s'agisse d'un consentement ou d'un refus, soit enregistré de manière à ne pas les solliciter à nouveau pendant un certain laps de temps. La durée de conservation de ces choix sera appréciée au cas par cas, au regard de la nature du site ou de l'application concernée et des spécificités de son audience.

Par ailleurs, dans la mesure où le consentement peut être oublié par les personnes qui l'ont manifesté à un instant donné, la Commission recommande aux responsables de traitement de renouveler son recueil à des intervalles appropriés. Dans ce cas, la durée de validité du consentement choisi par le responsable du traitement doit tenir compte du contexte, de la portée du consentement initial et des attentes des utilisateurs.

Au regard de ces éléments, la Commission considère, de manière générale, que conserver ces choix (tant le consentement que le refus) pendant une durée de 6 mois constitue une bonne pratique de la part des éditeurs.

3. Retrait et gestion du consentement

Les utilisateurs ayant donné leur consentement à l'utilisation de traceurs doivent être en mesure de le retirer à tout moment. La Commission rappelle qu'il doit être aussi simple de retirer son consentement que de le donner.

Les utilisateurs doivent être informés de manière simple et intelligible, avant même de donner leur consentement, des solutions mises à leur disposition pour le retirer.

En pratique, la Commission recommande que les solutions permettant aux utilisateurs de retirer leur consentement soient aisément accessibles à tout moment. La simplicité de l'accès peut notamment se mesurer au temps passé et au nombre d'actions nécessaires pour effectivement retirer le consentement.

La possibilité de retirer son consentement peut par exemple être offerte *via* un lien accessible à tout moment depuis le service concerné. Il est recommandé d'utiliser une dénomination descriptive et intuitive telle que « module de gestion des *cookies* » ou « gérer mes *cookies* » ou bien « *cookies* », etc. L'éditeur d'un site web peut également fournir aux utilisateurs un module de paramétrage accessible sur toutes les pages du site au moyen d'une icône « *cookie* », située par exemple en bas à gauche de l'écran, leur permettant d'accéder au mécanisme de gestion et de retrait de leur consentement.

Figure 6 – Le mécanisme de gestion et de retrait du consentement peut être offert via une icône « gérer mes cookies », située en bas à gauche de l'écran.

En tout état de cause, la Commission recommande que le mécanisme permettant de gérer et de retirer son consentement soit placé dans une zone qui attire l'attention des utilisateurs ou dans des zones où ils s'attendent à le trouver, et que les visuels utilisés soient les plus explicites possibles.

Enfin, pour que le retrait du consentement soit effectif, il peut être nécessaire de mettre en place des solutions spécifiques pour garantir l'absence de lecture ou d'écriture des traceurs précédemment utilisés.

4. Preuve du consentement

Les responsables du ou des traitements doivent être en mesure de démontrer, à tout moment, que les utilisateurs ont donné leur consentement. Pour ce faire, des mécanismes permettant de démontrer que le consentement des utilisateurs a été valablement recueilli doivent être mis en place.

Dans le cas où ces organismes ne collectent pas eux-mêmes le consentement des utilisateurs (notamment pour les traceurs dits « *cookies* tiers »), la Commission estime qu'une telle obligation ne saurait être remplie par la seule présence d'une clause contractuelle engageant l'une des parties à recueillir un consentement valable pour le compte de l'autre partie, dans la mesure où une telle clause ne permet pas de garantir, en toutes circonstances, l'existence d'un consentement valide. A cet égard, la Commission recommande qu'une telle clause soit complétée pour préciser que l'organisme qui recueille le consentement doit également mettre à disposition des autres parties la preuve du consentement, afin que chaque responsable de traitement souhaitant s'en prévaloir puisse en faire effectivement état.

S'agissant de la preuve de validité du consentement, la Commission recommande notamment les modalités suivantes, non exclusives :

- Les différentes versions du code informatique utilisé par l'organisme recueillant le consentement peuvent être mises sous séquestre auprès d'un tiers, ou, plus simplement, un condensat (ou « *hash* ») de ce code peut être publié de façon horodatée sur une plate-forme publique, pour pouvoir prouver son authenticité *a posteriori* ;
- Une capture d'écran du rendu visuel affiché sur un terminal mobile ou fixe peut être conservée, de façon horodatée, pour chaque version du site ou de l'application ;
- Des audits réguliers des mécanismes de recueil du consentement mis en œuvre par les sites ou applications depuis lesquels il est recueilli peuvent être mis en œuvre par des tiers mandatés à cette fin ;
- Les informations relatives aux outils mis en œuvre et à leurs configurations successives (tels que les solutions de recueil du consentement, également connues sous l'appellation CMP, pour « *Consent Management Plateform* ») peuvent être conservées, de façon horodatée, par les tiers éditant ces solutions.

5. Traceurs exemptés du recueil du consentement

La Commission relève que l'article 82 de la loi « Informatique et Libertés » n'impose pas d'informer les utilisateurs sur l'existence d'opérations de lecture et écriture non soumises au consentement préalable. Par exemple, l'usage par un site web d'un *cookie* de préférence linguistique stockant uniquement une valeur indiquant la langue préférée de l'utilisateur est susceptible d'être couvert par l'exemption et ne constitue pas un traitement de données à caractère personnel soumis au RGPD. Toutefois, afin d'assurer une transparence pleine et entière sur ces opérations, la Commission recommande que les utilisateurs soient également informés de l'existence de ces traceurs et de leurs finalités en intégrant, par exemple, une mention les concernant dans la politique de confidentialité.

S'agissant, plus spécifiquement, des traceurs de mesure d'audience exemptés du recueil du consentement tels que décrits à l'article 5 des lignes directrices du 17 septembre 2020, la Commission recommande également que :

- les utilisateurs soient informés de la mise en œuvre de ces traceurs, par exemple *via* la politique de confidentialité du site ou de l'application mobile ;
- la durée de vie des traceurs soit limitée à une durée permettant une comparaison pertinente des audiences dans le temps, comme c'est le cas d'une durée de treize mois, et qu'elle ne soit pas prorogée automatiquement lors des nouvelles visites ;
- les informations collectées par l'intermédiaire de ces traceurs soient conservées pour une durée maximale de vingt-cinq mois ;
- les durées de vie et de conservation ci-dessus mentionnées fassent l'objet d'un examen périodique.

6. Mesures techniques pour accroître la transparence des traceurs

L'utilisation de *cookies* différents pour chaque finalité distincte permettrait aux utilisateurs de les distinguer et de s'assurer du respect de leur consentement, mais également de rendre plus transparentes les opérations de lecture ou d'écriture. Plus particulièrement, la Commission recommande que les traceurs précédemment listés comme étant exemptés du recueil du consentement ne soient utilisés que pour une seule et même finalité, afin que l'absence de consentement des utilisateurs soit sans effet sur l'usage de traceurs nécessaires à leur navigation.

La Commission incite à ne pas avoir recours à des techniques de masquage de l'identité de l'entité utilisant des traceurs, telles que la délégation de sous-domaine.

La Commission recommande également que les noms des traceurs utilisés soient explicites et, dans la mesure du possible, uniformisés quel que soit l'acteur à l'origine de leur émission.

Enfin, la Commission encourage les professionnels à nommer le traceur permettant de stocker le choix des utilisateurs « eu-consent », en attachant à chaque finalité une valeur booléenne « vrai » ou « faux » mémorisant les choix effectués.

7. Conditions nécessaires à la mise en œuvre d'un consentement multi-terminaux dans un univers authentifié

Ajouté par la délibération n° 2025-131 du 18 décembre 2025

La mise en œuvre d'un dispositif de consentement multi-terminaux est facultative et ne constitue pas une obligation pour le responsable du traitement.

7.1. Définition du consentement multi-terminaux et conditions de légalité

Le consentement multi-terminaux est un mécanisme permettant d'appliquer les choix d'un utilisateur concernant la mise en œuvre d'opérations de lecture ou d'écriture d'informations à l'ensemble des environnements (les terminaux – ordinateur, tablette, ordiphone, télévision connectée, etc. –, le navigateur ou l'interface applicative utilisés) à partir desquels il accède à un site web ou une application mobile donnée, sans qu'il ait besoin de les répéter sur chacun de ces environnements. Dans le contexte des univers authentifiés, ces choix ne sont plus rattachés à un terminal mais au compte de l'utilisateur associé à un site web ou à une application mobile. Lorsqu'un utilisateur y accède et exprime ses choix sur un appareil connecté à son compte, ils sont automatiquement appliqués aux autres environnements via lesquels il peut également se connecter (comme sa tablette, son ordinateur ou sa télévision connectée). L'utilisateur peut gérer les choix rattachés à son compte quel que soit le terminal utilisé.

Le consentement multi-terminaux, dans un univers authentifié, ne peut être mis en œuvre que dans les conditions juridiques rappelées dans les lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et aux autres articles de la présente recommandation (notamment l'article 2, paragraphes 2-1, 2-3 et 2-4), ainsi qu'aux conditions suivantes.

En premier lieu, les choix formulés par l'utilisateur doivent avoir une portée identique pour assurer le respect des règles rappelées aux articles 2 et 3 de la recommandation. Ainsi, si le consentement peut être donné en une fois pour plusieurs terminaux, il doit en être de même pour le refus ou le retrait du consentement.

En second lieu, l'utilisateur doit être informé de la portée du consentement avant de pouvoir exercer leurs choix afin que celui-ci soit éclairé : l'information doit notamment préciser que les choix seront appliqués pour tous les terminaux sur lesquels l'utilisateur du compte est authentifié.

7.2. Adapter l'information aux caractéristiques du consentement multi-terminaux

L'information de l'utilisateur peut se faire, par exemple, par le biais de la fenêtre de recueil du consentement (aussi appelée *consent management platform* ou CMP), dès le premier niveau d'information.

L'information relative à la portée des choix effectués et la possibilité de les modifier devrait être rappelée immédiatement après l'authentification lorsqu'il s'agit d'un terminal qui n'a pas encore été relié au compte, à l'aide d'un bandeau éphémère d'information qui indique, le cas échéant, si les choix associés au compte ont été enregistrés ou modifiés.

7.3. Gérer l'éventuelle contradiction entre les choix formulés en univers non authentifié et ceux enregistrés sur le compte

S'agissant des solutions pour gérer cette situation

Lorsque des traceurs sont utilisés dans un univers non authentifié, un terminal sur lequel aucun choix n'est enregistré (lors d'une première visite sur le site via le terminal en question ou quand les traceurs précédemment déposés sur ce terminal ont été effacés) va afficher une fenêtre de recueil du consentement. Or, via cette fenêtre, l'utilisateur est susceptible, avant de s'authentifier, d'exprimer et d'enregistrer sur son terminal des choix différents de ceux enregistrés sur son compte. Il appartient au responsable de traiter cette situation d'une façon qui soit claire et loyale vis-à-vis de l'utilisateur.

La CNIL identifie deux modalités principales qui permettent de résoudre cette contradiction :

- **Modalité 1 :** les choix formulés sur le nouveau terminal avant l'authentification au compte (c'est-à-dire au niveau de la dernière fenêtre de recueil du consentement affichée) écrasent ceux enregistrés précédemment au sein du compte. Les nouveaux choix enregistrés s'appliqueront à l'ensemble des autres terminaux connectés au compte, ce qui présente l'avantage d'assurer que le dernier choix exprimé par l'utilisateur est pris en compte, indépendamment du terminal.
- **Modalité 2 :** les choix enregistrés au sein du compte prévalent sur les choix formulés sur le nouveau terminal avant l'authentification au compte (c'est-à-dire au niveau de la dernière fenêtre de recueil du consentement affichée). Pour être effectif, cette modalité suppose de distinguer le suivi de navigation de l'utilisateur selon qu'il est authentifié ou non (par exemple via deux cookies et/ou identifiants différents).

La CNIL encourage les acteurs concernés à faire émerger une unique modalité afin de faciliter la compréhension par les utilisateurs du dispositif, quel que soit l'application mobile ou le site web visité.

S'agissant de l'information spécifique à la gestion des contradictions

L'information doit être adaptée au contexte dans lequel elle apparaît (utilisateur authentifié ou non, contradiction entre les choix, etc.) afin de limiter les risques de confusion pour l'utilisateur. Une fois authentifié, l'utilisateur doit être informé, de manière claire, de la contradiction entre les choix qui viennent d'être formulés et ceux déjà associés au compte. L'information donnée doit alors indiquer :

- **pour la modalité 1**, si les choix associés au compte ont été enregistrés ou modifiés, comme il est mentionné au 7.2 ;
- **pour la modalité 2,** l'existence d'une contradiction entre les derniers choix exprimés et ceux qui étaient déjà associés au compte, ainsi que le fait que ces derniers continueront de s'appliquer au sein du compte.

Quelle que soit la modalité, l'information doit préciser les moyens à la disposition de l'utilisateur pour modifier ses choix, ce qui peut prendre la forme d'un bandeau éphémère qui peut être le même que celui visé au paragraphe 7.2 de la recommandation sous réserve d'une information adaptée et spécifique à la gestion des contradictions.

7.4. Sur l'interaction avec l'univers non authentifié

Dans le cadre d'un dispositif de consentement multi-terminaux, les choix de l'utilisateur en univers authentifié ne doivent pas avoir d'impact sur les choix préalablement enregistrés en univers non authentifié (par exemple via un cookie déposé au sein d'un navigateur).

Ainsi, dans le cas de terminaux partagés entre plusieurs utilisateurs (par exemple, un ordinateur familial ou une télévision connectée au sein d'un foyer), les choix individuels associés à un compte donné (éventuellement exprimés sur un autre terminal individuel) ne doivent pas impacter l'ensemble des utilisateurs du terminal partagé lorsqu'ils ne sont pas authentifiés par ce même compte (navigation en univers non authentifié).

7.5. Minimiser les données transmises en cas de recours à un sous-traitant

Dans le cadre de la mise en place d'un dispositif de consentement multi-terminaux, une attention devrait être portée aux données à caractère personnel échangées avec un prestataire qui pourrait intervenir dans le traitement de données.

En particulier, la CNIL recommande, conformément aux principes de minimisation et de protection des données dès la conception et la protection des données par défaut (article 25 du RGPD), de ne pas transmettre l'identifiant de compte de l'utilisateur dans la mesure où il contient en clair des données à caractère personnel fournies par l'utilisateur (par exemple, un pseudonyme contenant le prénom, voire le nom, ou une adresse de courrier électronique) au prestataire de la plateforme de gestion du consentement. Elle recommande de lui substituer systématiquement un identifiant technique pour lui permettre notamment de réconcilier les différents terminaux de l'utilisateur.

7.6. Évolution vers un mécanisme de consentement multi-terminaux

Lorsque le recueil du consentement se traduit en un mécanisme de consentement multi-terminaux pour un site web ou une application mobile, les responsables de traitement devront recueillir un nouveau consentement libre, spécifique, éclairé et univoque. En effet, le consentement exprimé sur un terminal donné préalablement au passage à une gestion du consentement multi-terminaux ne pourra pas être considéré valide pour d'autres terminaux, l'utilisateur n'ayant pas été informé de la portée multi-terminaux du consentement exprimé.

7.7. Bonne pratique : permettre à l'utilisateur de faire des choix distincts par terminal

A titre de bonne pratique, la CNIL encourage le responsable du traitement à laisser à l'utilisateur la possibilité de revenir sur ses choix, terminal par terminal, afin d'avoir la possibilité de différencier ses usages et la gestion de ses données à caractère personnel en fonction des contextes dans lesquels il accède au service et, donc, des terminaux qu'il utilise.

En pratique, cette possibilité pourrait être accessible, par exemple, au niveau du panneau de configuration qui permet la gestion et le retrait du consentement associé au compte au travers d'un centre de préférences.