RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE AUX FINS DE GESTION DES ACTIVITÉS COMMERCIALES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À QUI S'ADRESSE CE RÉFÉRENTIEL ?

Ce référentiel encadre la mise en œuvre par des organismes de droit privé ou public de leurs fichiers « clients » et « prospects ».

Compte tenu de la nature particulière de leurs activités, ce référentiel ne s'applique pas aux traitements mis en œuvre par :

- les établissements de santé ou d'éducation ;
- les établissements bancaires ou assimilés ;
- les entreprises d'assurances ;
- les opérateurs soumis à l'agrément de l'Autorité de régulation des jeux en ligne.

2. PORTÉE DU RÉFÉRENTIEL

Les traitements mis en œuvre aux fins de gestion des activités commerciales, qu'ils soient mis en œuvre à partir d'outils internes ou externalisés auprès d'un prestataire de service, conduisent à collecter des données relatives à des personnes physiques (clients, prospects, fournisseurs et toute personne susceptible d'être en relation contractuelle avec l'organisme dans le cadre de la gestion de son activité commerciale). À ce titre, ils sont soumis aux dispositions du RGPD, de la loi du 6 janvier 1978 modifiée ainsi qu'aux dispositions spécifiques relatives à la protection de la vie privée dans le secteur des communications électroniques.

Les organismes concernés, en tant que responsables de traitement, doivent mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection des données personnelles dès la conception des traitements et tout au long de la vie de ceux-ci. Ils doivent, en outre, être en mesure de démontrer cette conformité à tout instant. Les traitements mis en œuvre doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir les modèles de registre sur le site cnil.fr).

L'application de ce référentiel permet d'assurer la conformité des traitements de gestion commerciale au regard des principes relatifs à la protection des données.

Il constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD) dans les cas où celle-ci est nécessaire. Les organismes pourront ainsi définir leurs mesures permettant d'assurer la proportionnalité et la nécessité de leur traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) et la maîtrise de leurs risques (point 10). À cette fin, l'organisme pourra se référer aux lignes directrices de la CNIL sur les analyses d'impact relatives à la protection des données.

3. OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITÉS)

Un traitement de gestion des activités commerciales peut être mis en œuvre pour les finalités suivantes :

a) **gestion des contrats** (p. ex. : gestion des commandes, de la livraison, de l'exécution du service ou fourniture du bien, des factures et paiements) ;
b) **gestion de programmes de fidélité ;**
c) **tenue de la comptabilité générale et des comptabilités auxiliaires qui peuvent lui être rattachées ;**
d) **établissement de statistiques financières ;**
e) **réalisation d'enquêtes de satisfaction et d'études clients** comprenant les sondages, les tests produits, les statistiques de vente réalisées par l'organisme concerné ;
f) **gestion des réclamations, du service après-vente et des garanties** ;
g) **réalisation d'actions de prospection commerciale et de marketing** (envoi de messages publicitaires, jeux concours, parrainage, promotion, sondage) ;
h) **sélection de fournisseurs.**

Projet

Les informations recueillies pour une de ces finalités ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec la finalité première. Tout nouvel usage des données doit en effet respecter les principes de protection des données personnelles. Les traitements mis en œuvre ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des finalités ci-dessus énoncées.

Parce que plus sensibles, ce référentiel n'a pas vocation à encadrer les traitements suivants :

- la détection et la prévention de la fraude ;
- l'exclusion temporaire ou permanente des personnes du bénéfice d'une prestation de services ou de la fourniture d'un bien (par exemple, en raison d'impayés, d'incivilités des clients ou de comportements abusifs). Ces finalités sont encadrées par le référentiel XXXX ;
- le profilage des personnes. Pour ce qui concerne le suivi de leur navigation, l'organisme qui veut mettre en œuvre un tel traitement devra se conformer à la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux *cookies* et autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978 et pourra se référer à la rubrique dédiée sur le site de la CNIL ;
- le suivi de la fréquentation et du parcours clients dans les commerces physiques ;
- l'enrichissement de bases de données à partir d'informations collectées par des tiers.

4. BASE(S) LÉGALE(S) DU TRAITEMENT

Chaque finalité du traitement doit reposer sur l'une des bases légales fixées par la réglementation. Les différents fondements autorisant un organisme donné à traiter des données personnelles sont listés ci-dessous.

a) le consentement libre, spécifique, éclairé et univoque de la personne concernée ;

Le consentement, pour être valable, requiert une action positive et spécifique de la personne concernée (p. ex. : une case à cocher dédiée, non pré-cochée). L'acceptation de conditions générales d'utilisation ne peut suffire : l'accord doit être libre et non influencé ou contraint (il ne peut conditionner la souscription à un service ou l'achat d'un bien, la création d'un compte en ligne pour accéder à un service, *etc.*).

b) l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à sa demande. Les données collectées doivent être nécessaires à l'exécution des mesures contractuelles et/ou pré-contractuelles ;

c) le respect d'une obligation légale incombant à l'organisme ;

d) la réalisation de l'intérêt légitime poursuivi par l'organisme ou par le destinataire des données, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Un tableau, ci-après, illustre par des exemples pratiques les cas dans lesquels les bases légales peuvent être retenues en fonction de l'objectif poursuivi par le traitement.

Les bases légales doivent être portées à la connaissance des personnes dont les données sont traitées puisqu'elles permettent, notamment, de déterminer leurs droits.

5. DONNEES PERSONNELLES CONCERNEES

Dans un souci de minimisation des données personnelles traitées, l'organisme doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de gestion des activités commerciales. Il peut s'agir des données relatives :

Projet

a) **à l'identification de la personne concernée** ;

Le code interne utilisé pour l'identifier dans la base de données ne peut pas être son numéro de carte bancaire, de sécurité sociale, ni de titre d'identité.

Si l'organisme doit s'assurer de l'identité d'une personne avant d'entrer en relation commerciale avec elle, la simple présentation d'un justificatif peut suffire. Une copie de ce justificatif peut être conservée pour une durée de 6 ans lorsque la loi le prévoit ou si l'organisme justifie en avoir besoin pour se pré-constituer une preuve en cas de contentieux. Dans ce cas, des mesures de sécurité renforcées, telles que par exemple la limitation de la qualité de l'image numérisée ou l'intégration d'un filigrane comportant la date de collecte et l'identité de l'organisme, doivent être mises en œuvre afin de lutter contre les risques de mésusage de ces informations, en particulier l'utilisation des photographies à des fins de reconnaissance faciale.

b) **à la vie professionnelle** (par exemple, pour la gestion des contrats de fournisseurs) ;

c) **aux moyens de paiement utilisés** (voir également le point 7) ;

d) **à la transaction et aux biens ou services souscrits** (données liées au règlement des factures, au suivi de la relation commerciale, aux avis laissés, à la gestion des réclamations, etc.) ;
e) **à la situation familiale, économique et financière** de la ou des personnes concernées par la transaction lorsque de telles données présentent un lien avec la relation commerciale.

De manière exceptionnelle, par exemple si ces informations sont nécessaires au regard de la finalité du traitement et à condition de disposer d'une base légale appropriée, certaines données dites « sensibles » (susceptibles en particulier de révéler les opinions politiques, philosophiques ou religieuses, l'orientation sexuelle ou des informations sur la santé de la personne concernée) peuvent être collectées.

Un tableau, ci-après, énumère les données pouvant être collectées et traitées selon les finalités du traitement.

Après s'être assuré de la nécessité et de la pertinence des données personnelles qu'il utilise, l'organisme doit par ailleurs s'assurer, tout au long de la durée de vie du traitement, de la qualité des données qu'il traite. Cela signifie en pratique que, conformément à la règlementation, les données soient exactes et mises à jour.

6. DESTINATAIRES DES INFORMATIONS

Les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions.

Les habilitations d'accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité. **Voir point 9 relatif à la sécurité.**

En cas de recours à un sous-traitant, le contrat qui le lie à l'organisme doit faire mention des obligations qui lui incombent en matière de protection des données (article 28 du RGPD). Le Guide du sous-traitant édité par la CNIL précise ces obligations et les clauses à intégrer dans les contrats.

La transmission de données personnelles à des partenaires commerciaux nécessite, en amont :

- d'informer les personnes concernées sur le support de collecte des données (formulaire en ligne ou formulaire papier) de la finalité de cette transmission et des catégories de destinataires concernés. La liste précise des destinataires doit être régulièrement actualisée et mise à la disposition des personnes à partir de ce même support (par exemple, en y faisant figurer un lien hypertexte) ;
- de recueillir le consentement (voir paragraphe 4.a) des personnes lorsque ces partenaires commerciaux ont vocation à procéder à leur propre prospection commerciale par voie électronique (messages textes, courriels, télécopies ou automates d'appel). Le consentement des personnes recueilli à cette fin doit être conservé à titre probatoire ;
- de permettre aux personnes de s'y opposer lorsque la prospection est réalisée par voie postale ou par le biais d'un appel téléphonique.

Projet

Les données dites « sensibles » visées au point 5 ne peuvent être transmises à des tiers.

Pour assurer la continuité de la protection des données à caractère personnel, les transferts de ces dernières en dehors de l'Union européenne sont soumis à des règles particulières. Ainsi, toute transmission de données hors de l'UE doit :

- être fondée sur une décision d'adéquation ; ou
- être encadrée par des règles internes d'entreprise, des clauses types de protection des données, un code de conduite ou un mécanisme de certification approuvé par la CNIL ; ou
- être encadrée par des clauses contractuelles *ad hoc* préalablement autorisées par la CNIL ; ou
- répondre à une des dérogations prévues à l'article 49 du RGPD.

7. DUREES DE CONSERVATION

Une durée de conservation précise doit être fixée en fonction de chaque finalité. **En aucun cas, les données ne doivent être conservées pour une durée indéfinie**.

P. ex. : le cryptogramme visuel de la carte bancaire doit être supprimé dès que le règlement de la prestation ou de l'achat a été réalisé. En revanche, le numéro d'une carte de paiement peut être conservé pour permettre des achats ultérieurs dans les conditions posées par la recommandation relative au traitement de la carte de paiement en matière de vente de biens ou de fourniture de services à distance.

Les données nécessaires à l'exécution d'un contrat sont conservées pendant la durée de la relation contractuelle.

Elles peuvent également être conservées :

- pour une durée de 3 ans à compter du dernier contact que les personnes auxquelles elles se rapportent ont eu avec l'organisme (p. ex., pour les clients, un achat ou la date d'expiration d'une garantie ou, pour les prospects, un clic sur un lien hypertexte contenu dans un courrier électronique) ;
- après l'exécution du contrat, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables ou fiscales) ou s'il souhaite se constituer une preuve en cas de contentieux et dans la limite du délai de prescription applicable.

Pour les activités commerciales qui impliquent la création, par les clients eux-mêmes, d'un compte en ligne (par exemple, les sites de rencontres ou les réseaux sociaux), les données ont vocation à être conservées jusqu'à la suppression du compte par l'utilisateur. Toutefois, il est fréquent que les utilisateurs n'utilisent plus ces comptes sans pour autant les effacer, ce qui les conduit à perdurer indéfiniment. Dans ce cas, un délai raisonnable (p. ex. : 2 ans) doit être déterminé, à l'issue duquel les comptes doivent être considérés comme inactifs. Il convient alors d'avertir les utilisateurs concernés et de supprimer les comptes de ceux qui n'auraient pas réagi dans le délai fixé par l'organisme.

Lorsqu'une personne exerce son droit d'opposition à recevoir de la prospection, afin de garantir son effectivité, les informations permettant de prendre en compte ce droit doivent être conservées au minimum 3 ans. Ces données ne peuvent en aucun cas être utilisées à d'autres fins que la gestion du droit d'opposition et seules les données nécessaires à la prise en compte du droit d'opposition doivent être conservées (p. ex. : l'adresse électronique).

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :

- « Sécurité : Archiver de manière sécurisée » ;
- « Limiter la conservation des données ».

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles auront ont été dûment anonymisées (Voir les lignes directrices du G29 sur l'anonymisation).

Projet

8. INFORMATION DES PERSONNES

Un traitement de données personnelles doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

Dès le stade de la collecte des données personnelles, les personnes doivent être informées des modalités de traitement de leurs données dans les conditions prévues par les articles 13 et 14 du RGPD. Voir les modèles de mention d'information.

Selon la finalité poursuivie et les données collectées, le consentement des personnes (p. ex. : en cas de cession des données électroniques à des fins de prospection commerciale) ou un moyen de s'opposer à certaines opérations de traitement (p. ex. : prospection pour des produits ou services analogues, prospection entre professionnels ou par voie postale) doivent également être prévus sur le formulaire de collecte des données.

Les personnes concernées doivent par ailleurs être informées de la manière d'exercer leurs droits.

9. DROITS DES PERSONNES

Les personnes concernées disposent des droits suivants, qu'ils exercent dans les conditions prévues par le RGPD :

- droit de **retirer leur consentement** ou de s'**opposer** au traitement de leurs données ;
- droit d'**accès, de rectification et d'effacement** des données qui les concernent ;
- droit à la **limitation** du traitement (p. ex. : lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme, le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires) ;
- droit à la **portabilité** : l'organisme doit permettre à toute personne de recevoir, dans un format structuré et couramment utilisé, l'ensemble des données traitées par des moyens automatisés. La personne concernée peut demander à ce que ses données soient directement transmises par l'organisme initial à un autre organisme. Ne sont concernées, que les données fournies par la personne sur la base de son consentement ou d'un contrat. Il est donc recommandé de préciser aux personnes les traitements concernés par ce droit à la portabilité.

Tout organisme voulant mettre en œuvre de la prospection commerciale par voie téléphonique devra retirer de sa liste les personnes inscrites sur la liste d'opposition prévue par les articles L. 223-1 et suivants du code de la consommation (liste dite « BLOCTEL »).

10. SÉCURITÉ

L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.
En particulier, dans le contexte spécifique du présent référentiel, **soit l'organisme adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir** :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes accédant aux données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (*login*) unique à chaque utilisateur
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation

Projet

Catégories	Mesures
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (*firewall*) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des ordiphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant n'est incorporé aux URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les *cookies* non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir des clauses spécifiques dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, *etc.*)
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret par un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer par défaut des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires libres ou les encadrer strictement
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour ce faire, l'organisme pourra utilement se référer au Guide de la sécurité des données personnelles.

PROJET

ILLUSTRATION PRATIQUE DES BASES LEGALES AU REGARD DES FINALITES

FINALITE	BASE LEGALE / ce qui vous autorise à traiter les données	DUREE DE CONSERVATION
Gestion des contrats, y compris programme de fidélité :		
Commandes, livraisons, service après-vente	Exécution du contrat	Durée de la relation contractuelle
Obligations comptables, fiscales, etc.	Respect d'une obligation légale de conservation des données (p. ex. : obligation de s'assurer de l'identité de la personne en demandant la fourniture d'un justificatif d'identité)	Sous la forme d'archive intermédiaire : durée légale de conservation (p. ex. : obligation comptable de 10 ans)
Par exemple la gestion des pré-contentieux et contentieux	Intérêt légitime de l'organisme pour l'établissement de la preuve d'un droit ou d'un contrat (p. ex. : en cas de contentieux)	Durée de la prescription liée (civile, commerciale, etc.)
Opérations de prospection		
Par voie électronique (en vue de l'envoi de courriel, SMS, automate vocal, etc.)	Consentement	Jusqu'au retrait du consentement ou 3 ans à compter du dernier contact
Par voie postale ou intervention humaine	Intérêt légitime de l'organisme sous réserve de permettre aux personnes de s'y opposer préalablement et à tout moment	
À destination de professionnels		
Pour des biens et services analogues		
Gestion d'une liste d'opposition :	Intérêt légitime	Minimum 3 ans à compter de l'exercice du droit
Cession de données		
Données électroniques (en vue de l'envoi d'email, SMS, automate d'appel, etc.)	Consentement	Jusqu'au retrait du consentement
Cession de données uniquement pour contacter les personnes par téléphone ou voie postale	Intérêt légitime de l'organisme sous réserve de l'apposition ou du respect d'un droit d'opposition (*opt-out*).	Jusqu'à l'exercice du droit d'opposition
Traçage / suivi de la navigation des personnes	Voir la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978	
	Consentement spécifique	Jusqu'au retrait du consentement ou date d'expiration de la carte bancaire.

projet

Conservation du numéro de carte bancaire pour faciliter les achats ultérieurs (hors crypto)	Intérêt légitime	Pour les clients qui optent pour un abonnement « premium » / « à volonté » afin de bénéficier, gratuitement ou non, de services annexes visant à faciliter leurs achats (livraison rapide, ventes privées, accès à des contenus supplémentaires, etc.).

DONNEES POUVANT ETRE COLLECTEES ET TRAITEES SELON LES FINALITES DU TRAITEMENT

Identité	Civilité, nom ou raison sociale, prénoms, adresse (y compris siège social, lieu de facturation), n° de téléphone, n° de fax, adresses courriel, date de naissance, code interne de traitement permettant l'identification du client, code d'identification comptable, numéro SIREN.
Situation personnelle	Vie maritale, nombre de personnes composant le foyer, nombre et âge du (ou des) enfant(s) au foyer, profession, domaine d'activité, catégorie socioprofessionnelle, présence d'animaux domestiques.
Vie professionnelle	Profession, catégorie économique, activité.
Règlement / Paiement	Paiement, conditions et modalités de règlement (p. ex. : remises, acomptes, ristournes), RIP/RIB, n° de chèque, n° de carte bancaire, date de fin de validité de la carte bancaire, cryptogramme visuel, conditions de crédit, durée.
	Remises consenties, reçus, soldes et crédits souscrits (montant et durée, nom de l'organisme prêteur) en cas de financement de la commande par crédit.
Transaction	Numéro de la transaction, le détail de l'achat, de l'abonnement, du bien ou du service souscrit.
Suivi de la relation commerciale	Demandes de documentation, demandes d'essai, articles, produits achetés, services ou abonnements souscrits, services faisant l'objet de la commande et de la facture, quantité, montant, périodicité, date et montant de la commande et de la facture, échéance de la facture, conditions et adresse de livraison, historique des achats et des prestations de services, retour des produits, origine de la vente (vendeur, représentant, partenaire, affilié).
	La commande, les factures, correspondances avec le client et service après-vente, échanges et commentaires des clients et prospects, personne(s) en charge de la relation client.
En vue de sollicitations	Données nécessaires à la réalisation des actions de fidélisation, de prospection, d'étude, de sondage, de test produit et de promotion, à l'organisation et au traitement des jeux-concours, de loteries et de toute opération promotionnelle telles que la date de participation, les réponses apportées aux jeux-concours et la nature des lots offerts.
Avis	Données relatives aux contributions des personnes qui déposent des avis sur des produits, services ou contenus, notamment leur pseudonyme.
Informations stockées sur l'équipement terminal	*Cookies* et autres traceurs dans le respect de la recommandation n° 2013 378 du 5 décembre 2013.

Projet