GUIDE RELATIF AUX TRAITEMENTS DES DONNÉES PERSONNELLES POUR LE SECTEUR DES JEUX D'ARGENT ET DE HASARD

ANJ
AUTORITÉ NATIONALE DES JEUX

EN COLLABORATION AVEC LA CNIL

Dans le cadre de leur activité, les opérateurs et établissements de jeux légalement autorisés sont amenés à traiter des données à caractère personnel. Face aux interrogations exprimées quant à l'articulation entre le RGPD et les dispositions spécifiques du droit des jeux, l'ANJ a estimé utile d'éclairer les opérateurs et les établissements de jeux sur les règles applicables afin de les accompagner dans leur mise en conformité.

Ce guide n'a pas de finalité prescriptive, il vise à clarifier le droit applicable et à apporter des recommandations pour aider les acteurs à se mettre en conformité.

Ce guide a été élaboré en collaboration avec la CNIL, autorité chargée de veiller au respect du RGPD, laquelle a contribué de façon active à sa rédaction[1].

SOMMAIRE

1 - Le collège de la CNIL a examiné le guide à deux reprises : d'une part en amont de la consultation des opérateurs et établissements de jeux (séance plénière du 12 février 2026) et d'autre part au moment de la finalisation du guide (séance plénière du 21 mai 2026).

A qui s'adresse ce guide et quels en sont les objectifs principaux ?

1. POURQUOI UN GUIDE PRATIQUE ?

Le règlement général sur la protection des données (RGPD)[2], entré en application le 25 mai 2018, uniformise, en matière de données personnelles, le droit au sein de l'Union européenne.

Ce texte reprend les grands principes déjà prévus, en France, par la loi dite « informatique et libertés »[3] de 1978. Le RGPD n'en a pas moins abandonné la logique précédente, basée sur les déclarations à adresser à la Commission Nationale de l'Informatique et des Libertés (CNIL), pour privilégier une logique de responsabilisation des acteurs utilisant des données personnelles, les entités traitant ces dernières devant s'assurer elles-mêmes de la conformité de leurs fichiers et traitements dès l'origine et en permanence (*privacy by design*). Le RGPD a aussi renforcé sur certains aspects les obligations des responsables de traitement et de leurs sous-traitants, tout en assortissant leur violation de sanctions pécuniaires bien plus importantes et par conséquent dissuasives, les contrevenants s'exposant dans certains cas à des amendes administratives d'un montant maximum de 20 millions d'euros ou 4 % de leur chiffre d'affaires annuel mondial.

La protection des données personnelles est devenue un enjeu crucial pour toutes les entreprises, plus particulièrement les opérateurs de jeux d'argent et de hasard, qu'ils proposent leurs services « en dur » ou en ligne[4], eu égard au volume considérable et croissant de données personnelles qu'ils traitent. Ces traitements ont lieu dans un contexte juridique singulier, qui influe significativement sur la manière dont ils sont réalisés. En effet, les jeux d'argent et de hasard ne sont « *ni un commerce ordinaire, ni un service ordinaire* »[5]. Les opérateurs de ce secteur doivent concourir[6] à trois des quatre objectifs de la politique de l'Etat en ce domaine, à savoir « *prévenir le jeu excessif ou pathologique et protéger les mineurs*», « *assurer l'intégrité, la fiabilité et la transparence des opérations de jeu* » et « *prévenir les activités frauduleuses ou criminelles ainsi que le blanchiment des capitaux et le financement du terrorisme* »[7].

L'importance quantitative et qualitative des données personnelles traitées par les opérateurs de jeux d'argent et de hasard explique que la protection des données constitue un enjeu pour eux et pour les autorités administratives chargées, chacune dans leur domaine de compétence, de les contrôler (CNIL, ANJ, etc.). Ce constat ainsi que le souhait exprimé en ce sens par les opérateurs ont motivé l'élaboration du présent guide qui, il faut cependant le souligner d'emblée, expose des règles qui doivent avoir été mises en œuvre par les opérateurs depuis 2018.

2 - Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
3 - Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.
4 - Avec début 2024, plus de 13 milliards d'euros de chiffre d'affaires, soit plus de 50% de croissance depuis l'ouverture du marché à la concurrence en 2010.
5 - Comme le précise expressément l'article L. 320-2 du code de la sécurité intérieure.
6 - Article L. 320-4 du code de la sécurité intérieure.
7 - Article L. 320-3 du code de la sécurité intérieure.

Ce guide n'a ni pour objet ni pour effet de créer de nouvelles obligations à la charge des opérateurs. Il a été élaboré avec pour objectif de leur apporter une aide pour se mettre en conformité avec les normes déjà en vigueur, celles du RGPD, en tenant compte du cadre spécifique des jeux d'argent et de hasard dans lequel s'inscrit leur activité.

Les exemples donnés le sont à titre illustratif. Le guide ne dispense pas les opérateurs de solliciter, en tant que de besoin, l'assistance d'un conseil juridique, notamment en présence de situations complexes.

2. ACTEURS CONCERNÉS PAR CE GUIDE

Le présent guide s'adresse à l'ensemble des opérateurs de jeux d'argent et de hasard légalement autorisés à proposer leurs services en France, à savoir :

- les opérateurs titulaires de droits exclusifs, parmi lesquels, d'une part, la société La FRANÇAISE DES JEUX (FDJ) pour les jeux de tirage et grattage en points de vente physiques et en ligne, ainsi que les paris sportifs en réseau physique de distribution, et, d'autre part, le GIE PMU pour les paris hippiques en réseau physique de distribution et en hippodromes ;
- les opérateurs en ligne agréés par l'ANJ en paris sportifs, paris hippiques ou en jeux de cercle (poker) ;
- et les casinos et clubs de jeux[8].

Le présent guide peut également intéresser les prestataires de services auxquels les opérateurs de jeux peuvent faire appel dans le cadre de leur activité et qui les assistent dans le traitement des données des joueurs, tels que les sociétés de marketing, les prestataires de paiement, les hébergeurs ainsi que, s'agissant des opérateurs titulaires de droit exclusif, leurs mandataires.

3. PÉRIMÈTRE DU GUIDE DE CONFORMITÉ

S'il couvre l'ensemble des aspects de la conformité RGPD applicables aux opérateurs de jeux d'argent et de hasard s'agissant des données personnelles des joueurs, ce guide n'envisage pas en tant que tels les traitements des données personnelles relatives à d'autres personnes que les joueurs[9]. Ainsi, par exemple, ne sont pas examinés ici les traitements de données personnelles réalisés par les opérateurs en leur qualité d'employeur dans le cadre de la gestion de leurs ressources humaines. Les traitements considérés ne sont donc que ceux qui sont directement liés à l'activité sur le secteur régulé par l'ANJ.

***

8 - S'agissant des casinos et clubs de jeux, la lutte contre le blanchiment et le financement du terrorisme ainsi que les stratégies promotionnelles ne relèvent pas du champ de compétences de l'ANJ et le présent guide n'a pas vocation à traiter ces aspects à leur égard.
9 - Les joueurs étant les clients des opérateurs de jeux mais également les prospects.

Le guide rappelle, dans une première partie, les grands principes généraux du RGPD, auxquels les opérateurs doivent toujours se référer quel que soit le traitement qu'ils envisagent. Sa seconde partie envisage spécifiquement trois thèmes correspondant aux trois finalités susceptibles de susciter le plus d'interrogations en matière de jeux d'argent et de hasard, à savoir i) la gestion et le suivi des clients et la prospection commerciale ; ii) la prévention du jeu excessif ou pathologique et iii) la lutte contre le blanchiment des capitaux et le financement du terrorisme.

PARTIE 1
Rappel des principes généraux du RGPD

1. DÉFINITIONS ET GRANDS PRINCIPES

a. Principales définitions à connaître

i. Données à caractère personnel

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable[10], directement ou indirectement, notamment par référence à un identifiant ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Ainsi, une donnée est dite « à caractère personnel » dès lors que, grâce à elle, une personne physique peut être :

- identifiée (par exemple : son nom et son prénom sont mentionnés dans un fichier) ;
- ou identifiable (par exemple : un numéro de client, un identifiant joueur, un pseudonyme choisi par un joueur, un numéro de téléphone ou de plaque d'immatriculation, le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou la photo d'une personne).

A noter : l'identification d'une personne physique peut être réalisée à partir d'une seule donnée (par exemple un nom), mais également par un croisement de plusieurs données.

ii. Qu'est-ce qu'un traitement de données personnelles ?

Un traitement de données personnelles est 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.

Cette notion est donc très large : tout maniement de données personnelles, en ce compris une simple consultation, est un « traitement de données personnelles ».

Exemples de traitements de données personnelles :

- une base de données regroupant les coordonnées de prospects ou un fichier clients qui regroupe l'ensemble des informations relatives aux joueurs ;
- un fichier de personnes interdites de jeux ;
- un fichier de personnes ayant souscrit une limitation volontaire d'accès (LVA) ;
- un fichier de joueurs identifiés comme ayant un jeu excessif ou pathologique ;
- un fichier des joueurs dits VIPs ;
- la vidéosurveillance à des fins de sécurité des personnes et des biens au sein des locaux de l'opérateur tel un casino ou un club de jeu.

10 - Article 4 paragraphe 1 du RGPD.

A noter
Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers « papier » sont également concernés par le RGPD.

iii. Traitement de données à caractère personnel dites « sensibles » au sens de l'article 9 du RGPD

Les données dites « sensibles » sont celles qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques lorsqu'elles sont traitées aux fins d'identifier une personne physique de manière unique, les données concernant la santé et les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique[11].

Le traitement de ces données est possible dans les cas limitativement prévus par l'article 9.2 du RGPD, notamment si la personne a donné son consentement explicite ou si un motif d'intérêt public important (tel que la prévention du jeu excessif ou pathologique) le justifie.

Exemples de traitements de données sensibles :

- l'identification d'une personne en tant que « joueur excessif ou pathologique » peut être considérée comme le traitement d'une donnée de santé (dès lors que cela pourrait révéler une assuétude aux jeux d'argent) ;
- la mise en place par un opérateur de jeu d'un moyen d'identification biométrique (empreintes digitales, reconnaissance vocale, faciale, etc.) pour vérifier l'identité d'un joueur en vue de l'ouverture de son compte.

Pour aller plus loin concernant les données sensibles : https://www.cnil.fr/fr/definition/donnee-sensible.

iv. Les finalités de traitement[12]

Un traitement de données poursuit toujours un objectif : c'est sa « finalité ». Celle-ci doit être déterminée, explicite, légitime et préalable au recueil des données et à leur utilisation. Autrement dit, il n'est pas permis de collecter des données dans l'ignorance de l'usage qui va en être fait.

Exemples de finalités :

- la prospection commerciale ;
- l'identification des joueurs à des fins de prévention du jeu excessif et pathologique ;
- la lutte contre le blanchiment et le financement du terrorisme.

11 - Article 4 paragraphe 15 et article 9.1 du RGPD.
12 - Pour en savoir plus : https://www.cnil.fr/fr/passer-laction/definir-une-finalite.

L'opérateur ne peut collecter des données personnelles que pour un objectif bien déterminé et légitime et ne peut les traiter ultérieurement de façon incompatible avec cet objectif initial. Ce principe de finalité limite la manière dont le responsable de traitement peut utiliser ou réutiliser ces données dans le futur. Par exemple, l'opérateur ne peut pas réutiliser le fichier de surveillance des joueurs ayant des pratiques de jeu excessif ou pathologique pour leur proposer des offres commerciales (en revanche il peut l'utiliser pour limiter ou supprimer l'envoi à ces joueurs d'offres commerciales car la finalité reste dans ce cas la prévention du jeu excessif ou pathologique).

v. Le responsable du traitement

Le responsable de traitement est la personne morale (par exemple la société) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. Par hypothèse dans le présent guide, l'opérateur de jeu sera considéré responsable du traitement (à comparer avec le sous-traitant tel que défini ci-dessous).

En pratique, il s'agit de la personne morale incarnée par son représentant légal. C'est ce dernier qui doit s'assurer que le traitement mis en œuvre respecte les règles du RGPD.

vi. Le sous-traitant[13]

Un sous-traitant, qui est une catégorie de destinataires de données, est l'entreprise ou l'organisation qui traite des données pour le compte d'un responsable de traitement dans le cadre d'un service ou d'une prestation.

Un sous-traitant a des obligations concernant les données personnelles[14], qui doivent être précisées dans le contrat qui le lie à son donneur d'ordre, à savoir l'opérateur dans le domaine des jeux d'argent et de hasard. Les obligations à faire apparaître dans les contrats de sous-traitance sont les suivantes (liste non exhaustive) :

- **respect des principes de protection des données dès la conception et par défaut** : le sous-traitant doit mettre en œuvre des mesures techniques et organisationnelles adéquates afin que le traitement réponde aux exigences du RGPD et protège les droits des personnes concernées. Ces mesures doivent être prises dès la conception du traitement et intégrées par défaut au système d'information ;

- **sécurité des données** : le sous-traitant doit mettre en place des mesures de sécurité adéquates pour protéger les données personnelles contre le vol, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé. Ces mesures doivent être proportionnées aux risques présentés par le traitement et à la nature des données traitées ;

- **assistance et conseil** : le sous-traitant doit assister le responsable du traitement dans l'accomplissement de ses obligations en matière de protection des données et lui fournir des conseils sur les moyens de se conformer au RGPD ;

13 - Pour en savoir plus : https://www.cnil.fr/fr/sous-traitant.
14 - Pour en savoir plus : https://www.cnil.fr/fr/responsable-de-traitement-et-sous-traitant-6-bonnes-pratiques-pour-respecter-les-donnees.

- **notification des violations de données** : le sous-traitant doit informer le responsable du traitement, dans les meilleurs délais possibles, de toute violation de données dont il a connaissance ;

- **respect des droits des personnes concernées** : le sous-traitant doit aider le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits ;

- **sous-traitance ultérieure** : le sous-traitant ne peut pas sous-traiter un traitement de données à un autre sous-traitant sans l'autorisation écrite préalable du responsable du traitement ;

- **mise à disposition pour les contrôles** : le sous-traitant doit faciliter les contrôles du responsable du traitement et de l'autorité de contrôle compétente et coopérer avec eux en cas de contrôle.

Illustrations :

- les prestataires de services informatiques (par exemple : hébergement, maintenance, etc.) ;
- les prestataires de services de vérification de l'identité pour les traitements mis en œuvre pour le compte de l'opérateur de jeu.

b. Les premières étapes de la mise en conformité

Rappel des étapes fondamentales à mettre en place si cela n'est pas déjà fait :

- Désigner un responsable de la protection des données (DPO)
- Recenser vos fichiers comportant des données personnelles
- Informer les joueurs de la collecte et du traitement de leurs données
- Mettre en place des mesures de sécurité adéquates

En application du principe de protection de la vie privée dès la conception (privacy by design), les opérateurs de jeux d'argent et de hasard doivent prendre en compte la protection des données personnelles dès la conception des jeux, des plateformes et des processus de collecte et de traitement des données.

1) Désigner un délégué à la protection des données (DPO)

Le DPO est un rouage important de la mise en œuvre de la stratégie de protection des données de l'opérateur et veille au respect du RGPD.

Le DPO peut être un salarié de l'opérateur ou un prestataire externe. Il doit être choisi et désigné sur la base de ses compétences professionnelles et, en particulier, de ses connaissances et de son expertise en matière de protection des données, ainsi que de sa capacité à accomplir en toute indépendance les missions visées à l'article 39 du RGPD. Il doit enfin disposer de moyens suffisants pour exercer sa mission.

Exemples de missions du DPO :

- mettre en place et piloter la politique de protection des données de l'opérateur ;
- former et sensibiliser les employés aux enjeux de la protection des données ;
- réaliser des audits de conformité ;
- gérer les demandes d'exercice des droits des joueurs (droits d'accès, de rectification, etc.) ;
- répondre aux questions des autorités de régulation.

Un opérateur de jeux d'argent et de hasard doit-il désigner un DPO ?

Rappel du texte : Article 37 du RGPD – Désignation du délégué à la protection des données :

« Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données 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 c**onsistent 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 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »

S'agissant des opérateurs de jeux d'argent et de hasard, la désignation d'un DPO paraît en principe s'imposer, dans la mesure où ces derniers sont amenés à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données sensibles.

Même en l'absence de traitement à grande échelle (par exemple dans de petits établissements de jeu), la désignation d'un DPO est vivement encouragée.

Pour en savoir plus : Comment choisir et désigner un DPO ?

2) Réaliser une cartographie des données et des traitements (le registre)

La cartographie des données permet d'identifier et de documenter l'ensemble des données personnelles traitées par l'opérateur[15]. Le registre du responsable du traitement doit recenser l'ensemble des traitements mis en œuvre par votre organisme et doit comporter :

- le nom et les coordonnées du responsable du traitement et du DPO ;
- les finalités du traitement (vérification de l'identité, lutte contre la fraude, marketing, etc.) ;
- les catégories de personnes concernées (clients/joueurs, prospects etc.) ;
- les catégories de données concernées (nom, adresse postale, adresse électronique, données financières, etc.) ;
- les catégories de destinataires des données (services internes de l'opérateur, prestataires externes, etc.) ;
- les éventuels transferts de données à caractère personnel vers un pays tiers et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;
- les durées de conservation ;
- les mesures de sécurité mises en place (chiffrement, contrôle d'accès, etc.).

15 - L'article 30.5 du RGPD prévoit que les entreprises de moins de 250 salariés ne doivent pas tenir un registre, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées (exemple : système de reconnaissance biométrique), s'il n'est pas occasionnel ou s'il porte sur des données sensibles (exemple : données de santé) ou sur des données de condamnation.

Cette cartographie permet à l'opérateur :

- de se poser les bonnes questions, avec les différents métiers de l'organisme, sur les objectifs des fichiers mis en place, la minimisation des données recueillies, leur sensibilité, leurs conditions de conservation, leurs destinataires, et d'évaluer les risques ;
- de mettre en place des mesures de protection adéquates ;
- de démontrer sa conformité au RGPD.

Concrètement, l'opérateur peut décider de réaliser cette cartographie manuellement ou se doter d'une solution informatique pour l'assister dans cette tâche.

Pour en savoir plus : https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement.

3) Prévoir une politique de données personnelles transparente, précise et claire

Il est recommandé de centraliser les différentes informations sur la politique en matière de données personnelles dans un document unique ou un espace dédié de votre site internet, pour que les personnes puissent prendre facilement connaissance de l'ensemble de l'information. Le document doit être lisible et compréhensible de tous.

La politique de données personnelles doit être portée à la connaissance des joueurs pour les informer de manière transparente sur le traitement de leurs données personnelles. Par exemple, sur un site internet, l'opérateur peut utiliser un lien renvoyant directement vers la politique de protection des données, clairement visible sur chaque page du site, intitulé de manière claire (« Données personnelles » ou « Politique de Confidentialité », par exemple).

Cette politique de confidentialité doit être distincte des règlements de jeu et des conditions générales d'utilisation (CGU) du site internet.

4) Mettre en place des procédures internes et regrouper la documentation nécessaire

Il est important de mettre en place des procédures internes pour garantir le respect du RGPD en prenant en compte l'ensemble des évènements qui peuvent survenir au cours de la vie d'un traitement :

- les modalités de traitement des données personnelles (consentement, information des joueurs, sécurité du traitement et AIPD, gestion des accès et habilitations, etc.) ;
- la gestion des demandes d'exercice des droits ;
- la gestion des incidents de sécurité ;
- un changement de prestataire ;
- la communication avec les autorités de régulation, etc.

La documentation relative à la protection des données doit être conservée de manière sécurisée et accessible aux seules personnes désignées ou habilitées.

5) Réaliser une étude d'impact lorsque cela est nécessaire

L'analyse d'impact sur la protection des données (AIPD) a pour objet de cartographier et d'évaluer les risques d'un traitement sur la protection des données personnelles et d'établir un plan d'action pour les réduire à un niveau acceptable.

La réalisation d'une AIPD est obligatoire si le traitement envisagé est susceptible d'engendrer un risque élevé pour les droits et libertés des individus (article 35 du RGPD).

Dans ses lignes directrices concernant l'AIPD[16], le Comité européen de la protection des données (CEPD) a identifié neuf critères permettant d'aider les responsables de traitement à déterminer si une AIPD est requise : tout traitement de données personnelles remplissant au moins deux critères de cette liste sera présumé soumis à l'obligation de réaliser une AIPD. Certains de ces critères sont particulièrement pertinents pour les opérateurs de jeux :

- la collecte de données sensibles (données de santé, données biométriques, etc.) ou de données à caractère hautement personnel (catégories de données qui peuvent être considérées comme augmentant le risque d'atteinte aux droits et libertés des personnes, telles que des données financières) ;
- le traitement de données à grande échelle ;
- le traitement de données impliquant un profilage (par exemple lorsqu'un joueur est classé comme un joueur excessif ou pathologique ou lorsqu'un opérateur analyse les usages ou la navigation sur son site Web pour créer des profils comportementaux ou marketing) ;
- la collecte de données de personnes vulnérables, (par exemple pour les joueurs souffrant d'addiction au jeu) ;
- le croisement ou la combinaison d'ensembles de données (par exemple, lorsque l'opérateur de jeu se fonde sur plusieurs indicateurs pour en déduire qu'un joueur est excessif ou pathologique) ;
- le traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat, tels que les traitements pouvant conduire à l'exclusion d'un joueur ou à la limitation de ses mises.

En pratique : Les opérateurs de jeux doivent réaliser une AIPD pour les traitements à des fins d'identification du joueur pathologique ou excessif et des traitements à des fins de lutte contre le blanchiment et le financement du terrorisme.

Pour en savoir plus : https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd.

2. LES PRINCIPALES EXIGENCES DU RGPD

Le RGPD impose aux opérateurs de jeux d'argent et de hasard un ensemble d'obligations qui visent à garantir que les données des joueurs sont traitées de manière licite, sécurisée et respectueuse de leurs droits et libertés.

a. Principe de licéité du traitement (base légale)

La base légale est ce qui donne le droit à un organisme de traiter des données personnelles. La collecte et plus généralement tout traitement de données personnelles ne peuvent être effectués qu'à la condition de reposer sur l'une, et une seule, des six bases légales prévues par le RGPD pour chacune des finalités identifiées (voir ci-après le b. sur les finalités).

Selon celle qui sera retenue, les obligations de l'organisme et les droits des personnes pourront varier.

16 - Accessible ici : https://www.cnil.fr/sites/cnil/files/atoms/files/wp248_rev.01_fr.pdf.

i. Exécution d'un contrat

La base légale du contrat peut être mobilisée si d'une part, un contrat valide est conclu entre le responsable et le joueur et, d'autre part, si le traitement est objectivement nécessaire à son exécution.

Exemple : Le traitement des données personnelles dont un opérateur a besoin pour exécuter un contrat de limitation volontaire d'accès (LVA).

ii. Obligation légale

Le traitement est nécessaire au respect d'une obligation légale à laquelle l'opérateur est soumis. L'obligation légale doit être impérative, suffisamment claire et précise pour fonder valablement un traitement. Les textes créant cette obligation doivent au moins définir la finalité de ce traitement.

Exemples : Les traitements des données personnelles que l'opérateur réalise afin de se conformer à ses obligations de vérification de l'identité des joueurs, d'identification et d'accompagnement des joueurs excessifs ou pathologiques ou de lutte contre le blanchiment et le financement du terrorisme.

iii. Protection des intérêts vitaux

Le traitement est nécessaire à la protection des intérêts vitaux de la personne concernée ou d'une autre personne physique.

iv. Intérêts légitimes

Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par l'opérateur ou par un tiers, à condition que l'intérêt de l'opérateur ne l'emporte pas sur les droits et libertés des personnes concernées[17].

Exemples :

- En cas de mise à niveau d'un système informatique, l'opérateur peut être amené, sur le fondement de l'intérêt légitime, à traiter les données pour les migrer d'un système à un autre.
- Certains modes de prospection commerciale « traditionnels » (qui sont moins utilisés de nos jours, tels que la prospection par voie postale ou téléphonique non automatisée) à l'égard de prospects (qui n'ont donc pas encore de compte joueur), peuvent relever du fondement de l'intérêt légitime.

v. Consentement

Le joueur donne son consentement explicite au traitement de ses données personnelles. Le consentement doit être libre, univoque, éclairé et spécifique. Il doit être donné par un acte positif clair, par exemple par une case à cocher (opt-in) et non par une case pré-cochée devant être décochée (opt-out). Le consentement doit pouvoir être retiré à tout moment par le biais d'une modalité simple et équivalente à celle utilisée pour recueillir le consentement (par exemple, si le recueil s'est fait en ligne, il doit pouvoir être retiré en ligne également).

17 - Voir sur ce point https://www.cnil.fr/fr/les-bases-legales/interet-legitime.

Exemple : la cession de fichier à des tiers, les prospections commerciales par courriel, sms et automates d'appel pour les prospects, les prospections commerciales quelle que soit leur forme à l'égard des joueurs qui ont un compte[18].

vi. Mission d'intérêt public

Pour se fonder sur la base légale de la « mission d'intérêt public » le traitement doit être nécessaire à l'accomplissement d'une mission d'intérêt public. Cette base légale concerne en premier lieu les traitements mis en œuvre par les autorités publiques. Elle peut néanmoins autoriser la mise en œuvre de traitements par des organismes privés, dès lors qu'ils poursuivent une mission d'intérêt public. En l'espèce, les opérateurs de jeux ne peuvent pas mobiliser cette base légale dans la mesure où ils ne poursuivent pas de mission d'intérêt public.

Pour en savoir plus sur les bases légales : https://www.cnil.fr/fr/les-bases-legales.

b. Traitement basé sur des finalités bien établies

L'opérateur doit définir des finalités qui s'attachent au traitement de données personnelles qu'il entend réaliser et ce, avant même que ne débute ce traitement. Ces finalités doivent être :

- déterminées, c'est-à-dire établi dès la définition du projet ;
- explicites, c'est-à-dire communiquées de manière compréhensible aux joueurs avant la collecte des données ;
- légitimes, c'est-à-dire compatibles avec les missions de l'organisme et conformes au RGPD et à la réglementation applicable aux jeux d'argent et de hasard.

Ce but initial poursuivi par votre organisme doit être respecté. Les opérateurs ne peuvent pas traiter des données personnelles pour des finalités autres que celles qui ont été déterminées au préalable et portées à la connaissance des joueurs.

Exemple : Un opérateur ne pourrait pas utiliser des données émanant du fichier des interdits de jeux pour faire de la prospection commerciale.

Pour en savoir plus : définir une finalité.

c. Minimisation des données traitées

Le principe de minimisation des données impose aux opérateurs de ne collecter et de traiter que les données personnelles qui sont strictement nécessaires aux finalités poursuivies. Il s'ensuit que les opérateurs doivent :

18 - Le 3° de l'article 2 du décret n° 2010-518 du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux dispose à cet égard que l'opérateur doit demander à la personne qui souhaite ouvrir un compte joueur « *si elle consent à ce que les données personnelles qu'elle confie à l'opérateur fassent l'objet d'utilisations à des fins de prospection commerciale* », l'alinéa 6 de ce même article 2 prévoyant que ce consentement doit être recueilli distinctement de celui portant sur le règlement de l'opérateur.

- identifier les finalités précises du traitement des données avant de collecter les données ;
- collecter uniquement les données qui sont indispensables pour atteindre ces finalités ;
- ne pas collecter de données superflues ou non pertinentes ;
- supprimer les données qui ne sont plus nécessaires dès que possible.

Autrement dit, vous devez limiter autant que possible la quantité des données traitées.

Exemple : Dans le cadre de la collecte des données de joueurs pour assurer le suivi client, les informations concernant son précédent emploi ne semblent pas nécessaires à cette finalité. Ainsi il convient de ne pas les collecter[19].

d. Principe d'une durée de conservation limitée

Les données personnelles des joueurs doivent être conservées pendant une durée limitée définie en fonction de l'objectif poursuivi par le traitement. Le droit à l'effacement est écarté dans certains cas, notamment lorsque le traitement est fondé sur la base légale « obligation légale ».

Les données personnelles poursuivent des phases successives (aussi appelées cycle de vie des données) sont les suivantes :

1) Base active : il s'agit de l'ensemble des données personnelles nécessaires à la gestion courante des comptes joueurs, telles que les données d'identité, les données d'activité, les données de transactions, etc. Ces données doivent être accessibles aux services opérationnels de l'opérateur afin de permettre la fourniture des services de jeux d'argent et de hasard.

Concrètement, les données restent en base active tant que le compte joueur est ouvert.

2) Archivage intermédiaire : cette phase correspond à la conservation de données qui ne sont plus nécessaires à la gestion courante des comptes joueurs mais qui présentent encore un intérêt pour l'opérateur, notamment pour des besoins administratifs tels que la gestion de contentieux. L'accès à ces données doit être strictement encadré et davantage limité aux personnes habilitées afin qu'elles puissent uniquement être consultées de manière ponctuelle et par des personnes dont la mission le justifie. Cette durée doit être définie en amont et respectée afin qu'à expiration de celle-ci, l'opérateur procède à la suppression.

Concrètement, dès lors que le compte joueur est clôturé, les données passent en archivage intermédiaire et sont conservées par l'opérateur jusqu'à expiration de ses obligations légales de conservation conformément à l'article 31 du décret n° 2010-518 du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux (à savoir pendant 6 ans à compter de la clôture du compte joueur correspondant).

3) Suppression : cette phase ultime correspond à la destruction définitive des données personnelles qui ne sont plus nécessaires pour aucune finalité légitime. Cette suppression doit intervenir en principe 6 ans après la clôture du compte joueur correspondant, conformément à l'article 31 du décret n° 2010 518 du 19 mai 2010 susmentionné.

19 - Se référer aux pages 7 et 8 du document : https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_traitements-donnees-caractere-personnel_gestion-activites-commerciales.pdf

Le respect du principe de limitation de la durée de conservation permet de protéger la vie privée des joueurs et de limiter, dans une certaine mesure, les conséquences de fuites de données.

Ainsi, la gestion du cycle de vie des données impose :

- aux opérateurs de jeux d'argent et de hasard de mettre en place une gestion rigoureuse du cycle de vie des données des joueurs afin de garantir le respect de leurs obligations légales et réglementaires, notamment en matière de protection des données personnelles ;
- une gestion impliquant de définir des durées de conservation adaptées aux données traitées ainsi qu'aux finalités du traitement en vue de mettre en œuvre des procédures adéquates pour l'archivage ou la destruction des données arrivées à terme.

Pour en savoir plus : https://www.cnil.fr/fr/passer-laction/les-durees-de-conservation-des-donnees.

e. Des données sécurisées

Les opérateurs de jeux d'argent et de hasard doivent garantir la sécurité des données personnelles des joueurs en mettant en œuvre des mesures techniques et organisationnelles adéquates et proportionnées aux risques encourus par les données concernées.

i. Sécurisation des données

Il est recommandé de mettre en place les mesures suivantes (liste non limitative) :

- sensibilisation et formation des employés : programme de sensibilisation à la sécurité des données pour tous les employés, formations régulières sur les bonnes pratiques de sécurité, procédures de signalement des incidents de sécurité claires et accessibles ;
- mise en place de contrôles d'accès stricts : comptes nominatifs pour chacun des employés et intervenants, système de gestion des accès basé sur les rôles (RBAC[20]) définis en fonction des profils de mission, audit régulier des droits d'accès ;
- authentification des accédants et politique de gestion des mots de passe, conformes aux recommandations et communications de la CNIL, notamment :
  - https://www.cnil.fr/fr/mots-de-passe-recommandations-pour-maitriser-sa-securite ;
  - https://www.cnil.fr/fr/recommandation-mfa ;
  - https://www.cnil.fr/fr/consignes-pour-renforcer-la-securite-des-grandes-bases-de-donnees ;
- chiffrement des données : chiffrement des postes de travail (notamment les postes nomades), chiffrement des données en transit (chiffrement de flux (HTTPS) et chiffrement des supports de sauvegardes externes) et plus généralement chiffrement au repos des données sensibles (fichiers chiffrés), utilisation de clés de chiffrement fortes et régulièrement mises à jour, processus sécurisé de gestion des clés de chiffrement ;
- journalisation : mise en place d'une traçabilité sur l'accès et la modification des données. Au-delà de la mise en place d'une journalisation, le déploiement d'une mesure technique de surveillance active des journaux applicatifs, en vue de permettre la détection immédiate d'actions malveillantes au sein du traitement est recommandée. ;
- mise en place de procédures de sauvegarde et de restauration : sauvegardes régulières des

20 - Acronyme du terme anglais *Role-Based Access Control* (contrôle basé sur les rôles).

données, tests de restauration réguliers, plans de reprise d'activité en cas de sinistre ;
- réalisation d'audits de sécurité réguliers : audits internes et externes de la sécurité (tests d'intrusion, analyse des vulnérabilités) des traitements de données ;
- mise en place d'un antivirus sur les environnements de travail et les serveurs ;
- déploiement régulier des mises à jour de sécurité.

Exemple : Les fichiers ou les traitements comportant des données sensibles doivent faire l'objet d'une politique d'accès stricte. Seules les personnes pour lesquelles la consultation est strictement nécessaire doivent avoir accès à ces dossiers. Par ailleurs, ces fichiers doivent nécessairement se trouver dans des armoires fermées à clef pour les documents papier ou dans des coffres forts numériques (avec des mots de passe robustes dans le cas d'un fichier ou dans le cas d'un accès à un traitement, à l'aide d'une authentification multifacteur pour limiter les risques d'usurpation).

Pour d'autres exemples concrets de mesures : sécurisation des données.

ii. Cas de violation des données

En cas de violation des données personnelles, les opérateurs doivent :

- identifier et qualifier la violation (nature des données compromises, nombre de personnes concernées, etc.) ;
- notifier l'autorité de contrôle compétente (la CNIL en France) dans les 72 heures suivant la prise de connaissance de la violation, même sur le fondement d'une caractérisation incomplète de l'incident ;
- informer les personnes concernées si la violation est susceptible de présenter un risque élevé pour leurs droits et libertés ;
- mettre en œuvre des mesures pour limiter les conséquences de la violation (modification des mots de passe, gel des comptes, restauration de données, etc.) ;
- tirer les leçons de la violation et mettre en place des mesures correctives pour prévenir de nouvelles violations.

Les opérateurs doivent également documenter toutes les étapes de la gestion d'une violation des données.

Exemples de violation :

- un salarié d'un opérateur perd une clé USB contenant des fichiers répertoriant les clients les plus fidèles de ce même opérateur ;
- un individu malveillant parvient à pénétrer la sécurité informatique grâce à une campagne d'hameçonnage (phishing) et modifie les comptes de joueurs.

f. Des droits des personnes respectés

Le RGPD confère aux personnes un certain nombre de droits concernant leurs données personnelles. Les opérateurs de jeux d'argent et de hasard doivent respecter ces droits et mettre en place les procédures nécessaires pour les exercer.

i. Droit d'information

Les joueurs ont le droit d'être informés de la manière dont leurs données personnelles sont collectées, traitées et utilisées. Cette information doit être claire, concise et accessible.

Les opérateurs doivent notamment fournir aux joueurs les informations suivantes en cas de collecte directe auprès des joueurs :

- l'identité et les coordonnées du responsable du traitement ;
- les finalités du traitement des données ;
- la base légale du traitement ;
- le caractère obligatoire ou facultatif du recueil des données ;
- les destinataires ou catégories de destinataires des données ;
- les droits des personnes ;
- la durée de conservation des données ;
- l'existence ou non d'un transfert de données hors de l'Union européenne (en indiquant le pays et l'outil juridique permettant de protéger les données) ;
- les moyens de contacter le DPO ;
- le droit d'introduire une réclamation auprès de la CNIL.

En cas de collecte indirecte des données auprès d'un tiers (par exemple : données récupérées auprès de partenaires commerciaux, de *data brokers* ou de sources accessibles au public), les organismes doivent fournir, en complément :

- les catégories de données personnelles ;
- la ou les sources des données (en indiquant notamment s'il s'agit ou non de sources accessibles au public).

Concrètement, s'agissant des opérateurs de jeux, ces informations doivent figurer sur leur site internet de la manière la plus visible possible et dans une rubrique dédiée.
S'agissant plus spécifiquement des casinos et des personnes exploitant des postes d'enregistrement au nom et pour le compte de la société FDJ ou du GIE PMU, il est recommandé à titre de bonnes pratiques que l'information soit diffusée également sur un support matériel adapté à l'environnement physique. Il peut s'agir d'un panneau d'information et/ou d'une fiche d'information complète disponible dans un lieu facilement accessible.

Pour en savoir plus : https://www.cnil.fr/fr/respecter-les-droits-des-personnes.

ii. Droit d'accès, de rectification, de limitation, d'opposition et à l'effacement

Les joueurs ont des droits sur leurs données. Un joueur peut ainsi :

- **accéder** à ses données personnelles et en obtenir la copie.
- **rectifier** les données inexactes ou incomplètes le concernant, et ce à tout moment.
- **faire effacer** ses données lorsque :
    - leur traitement n'est plus nécessaire au regard des finalités pour lesquelles elles ont été collectées. En principe, compte tenu des obligations légales de conservation des données des joueurs durant 6 ans, la demande d'effacement d'un joueur relative à son compte-joueur n'est

pas possible tant que ce délai n'est pas expiré ;
- le traitement ne dispose plus de base légale. Par exemple, la base légale était le consentement, il a été retiré (c'est le cas si un prospect ou un joueur retire son consentement pour recevoir la newsletter de l'opérateur. L'opérateur n'a plus le droit de conserver l'adresse email du joueur dans la liste d'envoi marketing) ;
- les données ont été traitées illicitement.

- **demander la limitation ou le « gel » des données** (par exemple, 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) ;
- **récupérer ses données pour les réutiliser (droit à la portabilité)** : ce droit ne s'applique que si les trois conditions suivantes sont réunies : limitation aux seules données personnelles fournies par la personne concernée ; si les données sont traitées de manière automatisée (exclusion des fichiers par voie papier) sur la base légale du consentement de la personne concernée ou de l'exécution d'un contrat conclu avec la personne concernée ; respecter les droits et libertés de tiers. Lorsque les données sont fournies sur la base d'une obligation légale, il n'y a pas de droit à la portabilité.
- **s'opposer au traitement** à condition d'invoquer des raisons particulières et seulement si le traitement est mis en œuvre sur la base légale de l'intérêt légitime de l'opérateur. Ainsi, le responsable de traitement peut refuser à la personne concernée l'exercice de son droit d'opposition si le traitement des informations la concernant repose sur l'obligation légale.

Les opérateurs doivent mettre en place des procédures simples et accessibles pour que les joueurs puissent exercer leurs droits. Par exemple, les opérateurs peuvent mettre en place un tableau de bord (*dashboard*) au sein du compte, un formulaire en ligne ou un service téléphonique dédié.

Pour faciliter l'exercice des droits, l'opérateur doit mettre à la disposition des personnes concernées une adresse de courriel dédiée et/ou le cas échéant les coordonnées du délégué à la protection des données (DPD/DPO). La mise en place d'un canal dédié à la réception des demandes d'exercice de droits n'exonère pas l'opérateur de son obligation de traiter les demandes qui lui sont adressées par d'autres canaux.

g. Règles spécifiques au transfert de données hors UE [21]

Le RGPD impose des restrictions strictes au transfert de données personnelles vers des pays tiers, c'est-à-dire des pays situés en dehors de l'Union européenne et de l'Espace économique européen (EEE).

Les opérateurs de jeux d'argent et de hasard doivent respecter ces restrictions s'ils souhaitent transférer des données personnelles de joueurs vers un pays tiers.

En principe, les transferts de données vers des pays tiers ne sont autorisés que dans les cas suivants :

- le pays tiers offre un niveau de protection des données adéquat reconnu par la Commission européenne;
- des garanties appropriées sont mises en place pour protéger les données personnelles, telles que des clauses contractuelles types approuvées par la Commission européenne ou des règles d'entreprises contraignantes (cf. sur ce point le site de la Commission européenne) ;

21 - Pour en savoir plus : https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue.

- si l'Etat tiers n'est pas reconnu comme offrant un niveau de protection adéquat et en l'absence de garanties appropriées, il existe des dérogations soumises à des conditions particulières, d'interprétation stricte, détaillées à l'article 49 du RGPD. Par exemple, le joueur a donné son consentement au transfert ponctuel après avoir été informée des risques que ce transfert pouvait comporter pour elle.

Pour savoir si un pays est jugé adéquat ou s'il nécessite la mise en œuvre de mesures particulières telles que celles citées ci-dessus, la CNIL a mis à disposition une carte des pays en fonction de leur niveau de sécurité.

Les opérateurs de jeux d'argent et de hasard doivent veiller à ce que les transferts de données vers des pays tiers soient effectués dans le strict respect des exigences du RGPD. En cas de non-respect, les opérateurs s'exposent à des sanctions importantes.

Voici quelques exemples de situations où des transferts de données personnelles de joueurs vers un pays tiers peuvent être nécessaires :

- hébergement des données sur des serveurs situés dans un pays tiers : l'opérateur doit s'assurer que le prestataire d'hébergement offre un niveau de protection des données adéquat ;
- assistance technique fournie par un prestataire situé dans un pays tiers : l'opérateur doit s'assurer que le prestataire d'assistance technique respecte les exigences du RGPD. Par exemple, lorsque l'entreprise qui assure la maintenance de l'ERP[22] ou du CRM[23] de l'opérateur est implantée dans un pays autre que la France.

22 - Un système ERP (*Enterprise resource planning*) est un type de logiciel que les entreprises utilisent pour gérer leurs activités quotidiennes telles que la comptabilité, les achats, la gestion de projets, la gestion des risques et la conformité.

23 - Un CRM (*Customer Relationship Management*) est un système informatisé conçu pour gérer et améliorer les relations avec les clients d'une entreprise.

PARTIE 2
Etudes de trois finalités particulières

1. GESTION DES CLIENTS ET PROSPECTION COMMERCIALE

Les recommandations contenues dans la présente section sont destinées aux opérateurs agréés de jeux en ligne ainsi qu'aux opérateurs titulaires de droits exclusifs et ne portent pas sur l'activité des casinos et clubs de jeux.

Dans le cadre de la gestion de ses activités commerciales et promotionnelles, toute entreprise de jeux est amenée à traiter des données relatives à des personnes physiques (clients ou prospects) collectées en des occasions diverses (collecte lors de l'ouverture d'un compte, du paiement d'un gain, de la souscription à un programme de fidélité ou de l'obtention d'une gratification financière) ou de différentes manières (collecte en ligne, suivi de navigation par le biais de cookies ou d'autres traceurs, formulaires papier).

A. BASE LÉGALE DES TRAITEMENTS ET CATÉGORIES DE DONNÉES TRAITÉES SELON LA FINALITÉ CONCERNÉE

a. La gestion des comptes clients

Les opérateurs agréés de jeux en ligne et les opérateurs titulaires de droits exclusifs sont nécessairement amenés à traiter des données personnelles à des fins de gestion des comptes clients, que ce soit à l'occasion de l'ouverture des comptes joueurs, de leur fonctionnement, de leur clôture, de réclamations ou de contentieux.

i. Finalités d'ouverture du compte et de vérification de l'identité

⟶ **Base légale : respect d'une obligation légale (article 6.1.c du RGPD)**

S'agissant du jeu sur compte, au moment où celui-ci est ouvert, l'opérateur doit demander au joueur la communication de certaines données qu'il lui appartient de vérifier. C'est ainsi que l'article 2 du décret n° 2010-518 du 19 mai 2010 modifié mentionne les données suivantes :

- nom de naissance ;
- prénoms ;
- date et lieu de naissance ;
- adresse postale, qui est celle de son domicile[24] ;
- le cas échéant, une adresse électronique.

24 - La communication de l'adresse postale du domicile du joueur n'est pas exigée lors de l'ouverture d'un compte joueur en réseau physique de distribution auprès d'un opérateur titulaire de droits exclusifs, sous réserve des dispositions de l'article R. 561-5-3 du code monétaire et financier.

L'article 4 du décret n°2010-518 du 19 mai 2010 modifié exige en outre que la personne sollicitant l'ouverture d'un compte communique à l'opérateur[25], dans le délai de 30 jours à compter de la demande d'ouverture du compte les éléments suivants pour justifier de son identité, sa date et lieu de naissance et de son domicile :

- une copie de sa carte nationale d'identité, de son passeport, de son permis de conduire, de son titre de séjour ou de sa carte de résident en cours de validité justifiant de son identité et de sa date de naissance ;
- un document portant justification de l'adresse postale de son domicile, qui peut être une quittance de loyer, une facture d'eau, de gaz, d'électricité, d'internet ou de téléphone ou son dernier avis d'imposition ou de non-imposition[26], cette liste n'étant pas limitative.

L'article 5 du même décret exige également la communication d'un document comportant les références du compte de paiement ouvert au nom du joueur, à défaut duquel le reversement des avoirs du compte du joueur en ligne ou en réseau physique de distribution sur le compte de paiement de son titulaire ne peut avoir lieu.

Par ailleurs, le deuxième alinéa de l'article 24 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne prévoit que «*toutes les connexions établies, par l'intermédiaire d'un service de communication au public en ligne, à une adresse d'un site de l'opérateur ou de l'une de ses filiales et qui soit proviennent d'un terminal de consultation situé sur le territoire français, soit sont réalisées, après identification du joueur, au moyen d'un compte de joueur résidant en France, sont redirigées par l'opérateur vers ce site dédié* ». Il en résulte la possibilité de faire un traitement de l'adresse IP de la personne concernée. La collecte de cette donnée permet à l'opérateur de s'assurer que la personne qui participe à ses jeux ne le fait pas depuis un pays où elle y est prohibée.

Il convient de préciser que l'opérateur qui souhaite mettre en place une vérification supplémentaire de l'identité par un traitement de données biométriques (par exemple la reconnaissance faciale), devrait être en mesure de justifier de la proportionnalité du dispositif. Ces dispositifs doivent, selon la CNIL, intégrer des garanties fortes en matière de protection des données personnelle : l'opérateur doit recueillir le **consentement explicite** du joueur s'agissant du traitement d'une donnée sensible conformément à l'article 9.2.a du RGPD, veiller au respect des droits de la personne et prendre les mesures techniques et organisationnelles garantissant la sécurité des données ainsi traitées.

En outre, eu égard aux enjeux de protection des données et aux risques d'atteintes aux libertés individuelles qu'un tel dispositif est susceptible de créer, tout projet d'y recourir devra à tout le moins faire l'objet d'une analyse d'impact relative à la protection des données (AIPD). Il est renvoyé à la fiche de la CNIL sur ce sujet : https://www.cnil.fr/fr/biometrie-disposition-de-particuliers-quels-sont-les-principes-respecter[27].

25 - A défaut de mise en œuvre des moyens d'identification électronique définis aux 1° et 2° de l'article R. 561-5-1 du code monétaire et financier.
26 - Ou la saisie d'un code d'activation que l'opérateur lui a notifié à l'adresse postale de son domicile.
27 - Voir également : https://www.cnil.fr/fr/biometrie et https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees.

ii. Finalités de fonctionnement du compte-joueur, de traçage des opérations et de mise à disposition des données du joueur

⟶ **Base légale : respect d'une obligation légale (article 6.1.c du RGPD)**

Une fois le compte joueur ouvert, l'article 13 du décret n° 2010-518 du 19 mai 2010 modifié prévoit le traitement de données personnelles. En effet, en vertu des dispositions de cet article, le compte joueur doit retracer :

1. Les données personnelles du joueur : nom de naissance, prénoms, sexe, date et lieu de naissance, le cas échéant adresse postale du domicile et adresse de courrier électronique ;
2. L'identifiant permettant au joueur d'accéder à son compte ;
3. La date la plus récente à laquelle le joueur a accepté les clauses du règlement portant conditions générales de l'offre de jeux et de paris ;
4. Les références du compte de paiement du joueur ;
5. La date de création du compte ;
6. Les montants retenus par le joueur en application des articles 16 et 17 ;
7. Le solde des avoirs du joueur, en distinguant les sommes versées par le joueur, les sommes versées par l'opérateur sous forme de gains, y compris les abondements de gains, et les sommes versées par ce dernier à titre d'offre promotionnelle et pouvant être misées par le joueur ;
8. L'historique, sur un an, des mises, des gains et des pertes du joueur, pour chaque course hippique, compétition sportive, partie de jeux de cercle ou jeu de loterie ;
9. L'historique, sur un an, des offres promotionnelles attribuées par l'opérateur sous quelque forme que ce soit, y compris les lots en nature ;
10. L'historique, sur un an, du déroulement des parties de jeux de cercle auxquelles le joueur a participé ;
11. L'historique, sur un an, des mouvements financiers affectant le compte.

Le même article prévoit *in fine* que ces données sont mises à la disposition du joueur, de manière permanente et aisément accessible, au sein de son compte après authentification, sur le site de l'opérateur, par exemple dans un tableau de bord (*dashboard*) au sein du compte.

iii. Finalités de gestion des contrats de jeu et des réclamations

⟶ **Base légale : exécution de mesures précontractuelles ou d'un contrat (article 6.1.b du RGPD)**

Les traitements qui ont pour finalité la gestion des contrats de jeu et des réclamations ont pour base légale l'exécution d'un contrat.

Ces traitements peuvent concerner des données dont la collecte est prévue par le décret du 19 mai 2010, telles que :

- les références du compte de paiement permettent de verser au joueur ses gains conformément au contrat de jeu ;
- l'historique des mises peut être utilisé dans le cadre d'une réclamation.

D'autres données peuvent également être collectées et traitées pour les finalités de gestion des contrats de jeu et des réclamations, parmi lesquelles :

- le numéro de téléphone de la personne concernée.

Toutefois, seules les données strictement nécessaires à la finalité peuvent être collectées conformément au principe de minimisation.

iv. Finalités de gestion des contentieux

⟶ **Base légale : intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 6.1.f du RGPD)**

Dans le cadre d'un contentieux avec un client, l'opérateur peut être amené à traiter, sur la base légale de l'intérêt légitime, des données personnelles de ce dernier, toutes celles qui peuvent être utiles à sa défense.

Concernant le cas particulier des enregistrements d'appel avec le service client, ces derniers ne peuvent être, **sauf dispositions légales le prévoyant expressément, ni permanents ni systématiques**. A cet égard, la formation restreinte de la CNIL a rappelé que « *si la conservation de certaines données collectées dans le cadre de finalités déterminées et légitimes peut se justifier à des fins contentieuses ou précontentieuses, un tel objectif ne saurait justifier en tant que tel l'enregistrement de tous les appels téléphoniques, dans leur intégralité* »[28].

v. Finalités de gestion des programmes de fidélité

⟶ **Base légale : exécution de mesures précontractuelles ou d'un contrat (article 6.1.b du RGPD)**

Lorsqu'un opérateur met en place un programme de fidélité, les joueurs qui y adhèrent acceptent que certaines de leurs données de jeux soient traitées dans le cadre de cette finalité.

La base légale est ainsi l'exécution du contrat (en l'espèce un contrat d'adhésion au programme de fidélité), étant immédiatement rappelé que les opérateurs doivent faire preuve d'une particulière vigilance à l'égard des adhérents à ces programmes en raison des risques que, par nature, ceux-ci peuvent alimenter sur le terrain du jeu excessif ou pathologique.

vi. Finalité d'établissement de statistiques

⟶ **Base légale : intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 6.1.f du RGPD)**

Les traitements de données personnelles pertinentes à des fins statistiques peuvent être réalisés sur le fondement de l'intérêt légitime de l'opérateur, lequel peut en effet avoir intérêt à pouvoir analyser et évaluer les besoins d'amélioration de son offre et de la relation client sur la base de statistiques.

A noter : Afin que le traitement soit considéré comme étant de nature statistique, son résultat doit correspondre à des données agrégées. Le résultat ne devra pas être utilisé pour prendre des mesures ou des décisions concernant une personne physique en particulier.

28 - Délibération de la formation restreinte de la CNIL n°SAN-2024-014 du 26 septembre 2024 concernant la société COSMOSPACE.

b. La prospection commerciale

Si la prospection commerciale est un outil stratégique usuel et naturel dans une démarche de recrutement ou de fidélisation de consommateurs, les jeux d'argent et de hasard « *ne sont ni un commerce ni un service ordinaire* »[29]. Les risques que les jeux d'argent et de hasard présentent, notamment, du point de vue du jeu excessif ou pathologique, ont nécessairement une incidence sur le contenu et les modalités de cette prospection. En matière de données personnelles, les règles applicables en matière de prospection commerciale diffèrent selon le canal de diffusion utilisé :

- **la prospection non automatisée effectuée par voie postale et par téléphone** (hors automate d'appel, SMS ou MMS) relève en principe du RGPD ;
- **la prospection par voie électronique (courrier électronique, SMS, MMS) et automate d'appel** relève quant à elle principalement des règles spécifiques relatives à la protection de la vie privée dans le secteur des communications électroniques issues de l'article 13 de la directive *ePrivacy*[30] dont les dispositions ont été transposées à l'article L. 34-5 du code des postes et des communications électroniques. Certaines règles du RGPD s'appliquent également, notamment celles relatives à la définition du consentement et aux droits des personnes.

Toutefois, s'agissant des jeux d'argent et de hasard, doivent également être prises en compte **les dispositions spéciales du décret n° 2010-518 du 19 mai 2010 modifié.**

i. Le consentement, base légale de toute prospection commerciale à l'attention des clients

Le 3° de l'article 2 du décret susvisé n° 2010-518 du 19 mai 2010 prévoit expressément que lorsqu'une personne sollicite l'ouverture d'un compte joueur auprès d'un opérateur agréé de jeux ou de paris en ligne ou d'un opérateur titulaire de droits exclusifs, celui-ci, avant l'ouverture de ce compte, lui demande de façon distincte « ***si elle consent à ce que les données personnelles qu'elle confie à l'opérateur fassent l'objet d'utilisations à des fins de prospection commerciale*** » en l'ayant informée préalablement de la finalité de ces utilisations.

La CNIL considère ainsi que la base légale pour les traitements à des fins de prospection commerciale quel que soit leur vecteur (par téléphone, voie postale, courrier électronique, SMS, MMS et automate d'appel) est en principe, en matière de jeu d'argent et de hasard, le **consentement**.

Ainsi, la prospection commerciale n'est possible qu'à la condition que les personnes aient explicitement donné leur consentement avant tout démarchage.

Exemple de mention à faire figurer pour recueillir le consentement :

> ☐ J'accepte que mes données personnelles soient utilisées pour de la prospection commerciale par courrier électronique [*préciser les autres vecteurs concernés le cas échéant*] de la part de la société [*dénomination de l'opérateur*]. Je suis informé que je pourrai retirer mon consentement à tout moment. En savoir plus au sein de la politique de confidentialité [*ajouter le lien hypertexte*].

29 - Article L. 320-2 du code de la sécurité intérieure.
30 - Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

La CNIL considère que le principe est le même s'agissant de la **transmission**, à titre onéreux ou non, de données à caractère personnel à des partenaires commerciaux souhaitant les réutiliser à des fins commerciales. En effet, le 3° de l'article 2 du décret susvisé n° 2010-518 du 19 mai 2010 modifié exigeant le recueil du consentement pour toute prospection commerciale, toute transmission de données personnelles à des partenaires à des fins de prospections commerciales par ces derniers nécessite également un consentement.

Pour ce faire, il convient d'informer les personnes concernées de l'identité des partenaires responsables de traitement qui utiliseraient leurs données à des fins de prospection, par le biais d'une liste exhaustive mise à disposition directement sur ou depuis le support de collecte (par exemple, en y faisant figurer un lien hypertexte), ainsi que de la finalité spécifique de la transmission.

Dans un tel cas, l'opérateur peut utiliser une seule et même case à cocher pour recueillir le consentement à la transmission des données et celui lié à l'utilisation future des données à des fins de prospection commerciale, sous réserve de fournir une information préalable complète telle que décrite plus haut, notamment l'indication de toutes les personnes auxquelles les données seront communiquées. A cet égard, il est recommandé que l'opérateur permette toutefois aux joueurs d'écarter la transmission de ces données à certains partenaires de l'opérateur.

Exemple :

> ☐ J'accepte que mes coordonnées soient transmises aux partenaires suivants [*lien vers la liste des partenaires*] à des fins de prospection commerciale par courrier électronique [*préciser les autres vecteurs concernés le cas échéant*].

Par ailleurs, il convient de préciser que :

- les partenaires rendus destinataires des données doivent, lors de la première communication avec les personnes concernées, leur communiquer toutes les informations mentionnées à l'article 14 du RGPD, telles que celles relatives à la manière d'exercer leurs droits, notamment l'existence du droit de retirer le consentement à tout moment, ainsi que la source des données utilisées ;
- l'opérateur est tenu de notifier aux partenaires, auxquels les données à caractère personnel ont été communiquées, toute demande d'effacement ou de limitation du traitement exprimée par les personnes concernées.

S'agissant du transfert de données à des partenaires situés en dehors de l'Union européenne, il est renvoyé sur ce sujet au g) « Règles spécifiques au transfert de données hors UE » de la partie I.2. du présent guide ainsi qu'aux fiches de la CNIL regroupées sous ce lien : https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue.

ii. Le consentement, également base légale pour la prospection commerciale à l'attention des prospects

Pour la prospection commerciale dirigée vers les personnes qui ne sont pas clientes de l'opérateur, à savoir les prospects, la base légale est, selon la CNIL, le consentement, étant précisé que :

- **Conformément au droit commun**, la base légale est le consentement pour la prospection par voie électronique (courrier électronique, SMS, MMS) et par automate d'appel (article L. 34-5 du CPCE).

Il convient de préciser que l'exception concernant les « services analogues » prévu par l'article visé ci-dessus n'est pas applicable en l'espèce. En effet, il est prévu que le recueil du consentement n'est pas nécessaire pour adresser à ses clients des sollicitations sur des produits et services analogues à ceux déjà acquis ou souscrits par le consommateur concerné. Or, cette exception ne s'applique que dans une relation fournisseur / client, soumise à des dispositions spécifiques. Cette exception ne peut pas être mobilisée lorsqu'aucune vente ou prestation de service n'a été effectuée, y compris lorsque le client a créé un compte en ligne (par exemple sur un site de commerce en ligne). En effet, la simple création d'un compte ne signifie pas qu'il y aura une commande éventuelle de produits ou de services auprès de la société.

- **Conformément au droit commun**, la base légale est le consentement pour la prospection par téléphone à compter du 11 août 2026[31].
- **En raison des risques liés au jeu excessif ou pathologique[32] à prendre en compte lors de la balance des droits et des intérêts en cause**, la base légale de l'intérêt légitime apparait difficile à mobiliser pour la prospection non automatisée effectuée par voie postale. Le consentement constitue la base légale la plus appropriée.

c. Le cas particulier des cookies et autres traceurs

L'utilisation de **cookies** et autres traceurs relève essentiellement de l'article 82 de la loi « *Informatique et libertés* »[33] dont les dispositions garantissent aux personnes la protection de leurs terminaux contre tout accès ou stockage d'information non désiré.

Les internautes doivent ainsi être informés et donner leur consentement préalablement au dépôt et à la lecture de traceurs ou cookies (sauf dans certains cas spécifiques).

i. Quelles sont les technologies concernées ?

Sont concernées toutes les technologies ayant pour effet de lire ou écrire des données dans le terminal de l'utilisateur et ce, quel que soit le type de terminal utilisé (ordinateurs, téléphones portables, tablettes numériques et consoles de jeux vidéo connectées à Internet ainsi que tout autre équipement terminal connecté à un réseau de télécommunication ouvert au public).

C'est par exemple le cas des cookies, à savoir de petites quantités de données stockées dans le navigateur d'une personne pour permettre la remontée d'informations sur sa navigation et permettre ou faciliter celle-ci[34].

Au-delà des cookies, sont notamment concernés tous les autres identifiants générés par un logiciel ou un système d'exploitation (numéro de série, adresse MAC, identifiant unique de terminal (IDFV), ou tout ensemble de données qui servent à calculer une empreinte unique du terminal (par exemple avec une méthode de « *fingerprinting* »).

31 - La loi n° 2025-594 du 30 juin 2025 contre toutes les fraudes aux aides publiques prévoit, à compter du 11 août 2026, que le consentement explicite des consommateurs doit être requis pour tout démarchage téléphonique (article 13 modifiant notamment l'article L.223-1 du code de la consommation).
32 - CJUE, 9ème chambre, arrêt du 4 octobre 2024 dans l'affaire C-621-22.
33 - qui transpose l'article 5.3 de la directive « *ePrivacy* ».
34 - Sur ce point, il est renvoyé à la fiche de la CNIL : https://www.cnil.fr/fr/definition/cookie.

ii. Cadre juridique applicable

L'article 82 de la loi « *Informatique et libertés* » pose le principe d'un **consentement préalable** de l'utilisateur avant le stockage d'informations sur son terminal ou l'accès à des informations déjà stockées sur celui-ci.

Exemples :

- les cookies liés aux opérations relatives à la **publicité personnalisée** ;
- les cookies de partage sur les réseaux sociaux.

Par exception, sont exemptés de consentement préalable les cookies ou autres traceurs strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur ou ceux permettant ou facilitant une communication par voie électronique, par exemple :

- les traceurs destinés à l'authentification auprès d'un service, y compris ceux visant à assurer la sécurité du mécanisme d'authentification, par exemple en limitant les tentatives d'accès robotisées ou inattendues ;
- les traceurs de personnalisation de l'interface utilisateur (par exemple, pour le choix de la langue ou de la présentation d'un service), lorsqu'une telle personnalisation constitue un élément intrinsèque et attendu du service ;
- les traceurs d'audience à condition qu'ils aient une finalité strictement limitée à la seule mesure de l'audience pour produire des données statistiques anonymes uniquement. Ces traceurs ne doivent pas :
  - > conduire à un recoupement des données avec d'autres traitements ou à ce que les données soient transmises à des tiers ;
  - > permettre le suivi global de la navigation de la personne utilisant différentes applications ou naviguant sur différents sites web. Toute solution utilisant un même identifiant à travers plusieurs sites (via par exemple des cookies déposés sur un domaine tiers chargé par plusieurs sites) pour croiser, dédoubler ou mesurer un taux de couverture (« *reach* ») unifié d'un contenu est exclue[35].

iii. Comment recueillir un consentement valide lorsqu'il est requis ?

Le consentement requis en la matière doit répondre à la définition et aux conditions prévues aux articles 4.11 et 7 du RGPD. Il doit donc être, selon la CNIL, **libre, spécifique, éclairé, univoque** et l'utilisateur doit être en mesure de le retirer, à tout moment, avec la même simplicité qu'il l'a accordé.

Afin de rappeler et d'expliciter le droit applicable au dépôt et à la lecture de traceurs dans le terminal de l'utilisateur, la CNIL a adopté le 17 septembre 2020 des lignes directrices[36], complétées par une recommandation visant notamment à proposer des exemples de modalités pratiques de recueil du consentement[37].

35 - Voir sur ce point l'article 5 de la recommandation cookies et la page du site de la CNIL https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience

36 - Délibération n° 2020-091 du 17 septembre 2020 de la CNIL portant adoption de 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 abrogeant la délibération n° 2019-093 du 4 juillet 2019.

37 - Délibération n° 2020-092 du 17 septembre 2020 de la CNIL portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ».

En particulier, la CNIL considère que les bandeaux d'information doivent offrir à l'utilisateur un moyen de refuser les cookies avec le même degré de simplicité que celui prévu pour les accepter.

Les opérateurs sont invités à se référer à ces lignes directrices et à cette recommandation, ainsi qu'aux différentes fiches de la CNIL sur ce sujet, notamment https://www.cnil.fr/fr/cookies-et-autres-traceurs.

B. ACCÉDANTS, DESTINATAIRES ET TIERS AUTORISÉS

i. Accédants

Pour mémoire, le terme « accédant », qui n'est employé ni par le RGPD ni par la loi « *Informatique et libertés* », est utilisé par la CNIL pour désigner les personnes qui, chez le responsable de traitement, sont appelées à effectuer les diverses opérations de traitement.

Afin de respecter l'obligation de sécurité des données, les données à caractère personnel doivent être rendues accessibles uniquement aux personnes habilitées à en connaitre au regard de leurs attributions.

Exemples pour la finalité prospection commerciale : les personnes autorisées du département commercial et du service client.

ii. Destinataires

La finalité de gestion des clients peut justifier de transmettre des données à des prestataires de services sous-traitants de l'opérateur.

Exemples :

- expert-comptable ;
- les prestataire de service de vérification de l'identité pour les traitements mis en œuvre pour le compte de l'opérateur de jeu ;
- prestataires de services informatiques, dont hébergeurs ;
- prestataires de service client.

Il importe de souligner que les sous-traitants doivent être informés des obligations spécifiques qui pèsent sur les opérateurs de jeux d'argent et de hasard, notamment en ce qui concerne l'encadrement des communications commerciales, y compris celui des gratifications financières, la lutte contre le jeu excessif ou pathologique et sur celui de la protection des mineurs. Une manière de sensibiliser ces sous-traitants peut consister en un renvoi détaillé et précis dans le contrat à la législation applicable dans ce secteur ou en la reproduction de certaines des dispositions légales pertinentes. Un tel renvoi ou une telle reproduction peut également être réalisé, le cas échéant, vers la décision d'approbation, éventuellement sous conditions, des stratégies promotionnelles ou du plan d'action de l'opérateur pour la lutte contre le jeu excessif ou pathologique et la protection des mineurs.

Il est renvoyé à ce titre à la fiche de la CNIL relative aux sous-traitants https://www.cnil.fr/fr/sous-traitant.

iii. Données mises à disposition de l'ANJ

L'article 38 de la loi n°2010-476 du 12 mai 2010 prévoit un contrôle permanent par l'ANJ de l'activité des opérateurs de jeux ou de paris en ligne agréés et de l'activité de l'opérateur titulaire de droits exclusifs pour son activité de jeux de loterie en ligne aux fins d'assurer le respect des objectifs définis à l'article L. 320-3 du code de la sécurité intérieure. A cet effet, les opérateurs mettent des données à la disposition permanente dans un coffre-fort électronique, accessible à tout moment à l'ANJ. L'article 30 du décret 2010-518 du 19 mai 2010 modifié précise quelles sont les données devant ainsi être mis à disposition et en particulier les données personnelles suivantes :

- toute information détenue par l'opérateur concernant chaque joueur, et notamment les informations suivantes : nom de naissance, prénoms, sexe, date et lieu de naissance, adresse de courrier électronique, date d'ouverture du compte joueur et, le cas échéant, adresse postale du domicile, identifiant permettant l'accès au compte joueur, référence du compte de paiement tel que mentionné au dernier alinéa de l'article 17 de la loi du 12 mai 2010, sur lequel l'opérateur reversera, le cas échéant, les avoirs du joueur ;
- les opérations de compte réalisées par les joueurs ;
- les opérations de jeu réalisées par les joueurs ainsi que toute donnée concourant à la formation du solde du compte joueur ;
- les profils des joueurs et leurs comportements de jeu ;
- les offres promotionnelles attribuées par l'opérateur sous quelque forme que ce soit, y compris les lots en nature et leur utilisation par les joueurs ;
- les contrôles menés et leurs résultats, ainsi que les incidents de jeu et les opérations frauduleuses détectées.

En outre, l'article 42 de la loi n°2010-476 susvisée prévoit que pour l'accomplissement des missions qui lui sont confiées, l'ANJ peut recueillir « *toutes les informations nécessaires* » notamment des opérateurs de jeux ou de paris en ligne et des opérateurs titulaires de droits exclusifs et se faire communiquer tout document en la possession de ces opérateurs.

C. DURÉE DE CONSERVATION

Une durée de conservation doit être fixée en fonction de chaque finalité. De manière générale, les durées de conservation ne doivent pas dépasser les durées de prescriptions légales. A l'issue de ce délai, l'opérateur doit supprimer ces données.

L'article 31 du décret n°2010-518 du 19 mai 2010 susvisé prévoit que, pour les données personnelles concernant chaque joueur et énumérées à l'article 30 susvisé, le délai de conservation est de **6 ans à compter de la clôture du compte joueur correspondant**. Cette durée de conservation a vocation à s'appliquer aux finalités ayant pour base légale le respect des dispositions dudit décret.

S'agissant des autres finalités, le présent guide suggère les durées de conservation mentionnées dans le tableau ci-dessous. Un opérateur peut néanmoins choisir des durées différentes, à condition que cette durée respecte les textes applicables et n'excède pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5.1 du RGPD).

Finalité	Base légale	**Durée de conservation**
Ouverture du compte et de vérification de l'identité	Respect d'une obligation légale	6 ans à compter de la clôture du compte joueur correspondant
Fonctionnement du compte-joueur, de traçage des opérations et de mise à disposition du joueur	Respect d'une obligation légale	6 ans à compter de la clôture du compte joueur correspondant
Gestion des contrats de jeu et des réclamations	Exécution d'un contrat	6 ans à compter de la clôture du compte joueur correspondant
Gestion des contentieux	Intérêt légitime	Pendant toute la durée du contentieux et jusqu'à l'expiration de l'ensemble des voies de recours
Gestion des offres promotionnelles (y compris dans le cadre des programmes de fidélité)	Exécution d'un contrat	Durée de la participation au programme de fidélité (A noter : si la durée est plus courte que l'obligation de conservation prévue à l'article 31 du décret n°2010-518 du 19 mai 2010 susvisé (6 ans à compter de la clôture du compte joueur correspondant), cela n'implique pas une suppression automatique de données mais simplement un arrêt d'utilisation des données pour la finalité précisée)
Statistiques	Intérêt légitime	Durée nécessaire pour la réalisation de l'objectif visé par les statistiques ou jusqu'à l'exercice du droit d'opposition
Prospection commerciale à l'attention des clients et des prospects	Consentement	Jusqu'au retrait du consentement ou 3 ans à compter du dernier contact des personnes avec l'opérateur (A noter : si la durée est plus courte que l'obligation de conservation prévue à l'article 31 du décret n°2010-518 du 19 mai 2010 susvisé (6 ans à compter de la clôture du compte joueur correspondant), cela n'implique pas une suppression automatique de données mais simplement un arrêt d'utilisation des données pour la finalité précisée)

D. INFORMATION DES PERSONNES CONCERNÉES

Les traitements de données à caractère personnel doivent être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

Conformément aux dispositions des articles 12 à 14 du RGPD, les personnes doivent être informées des modalités de traitement de leurs données, la base légale, les finalités, la durée de conservation, ainsi que de la manière d'exercer leurs droits.

En outre, l'article 2 du décret n°2010-518 modifié prévoit que l'opérateur informe la personne que :

- la demande d'ouverture d'un compte joueur emporte renonciation à l'exercice du droit prévu au premier alinéa de l'article 56 de la loi « *Informatique et libertés* », à savoir le droit d'opposition ;
- elle dispose, pour les données personnelles la concernant, d'un droit d'accès et de rectification, conformément aux dispositions des articles 49 et 50 de la même loi.
- l'ANJ peut être destinataire des données personnelles qu'il lui a confiées, ainsi que de celles relatives à son activité de jeu ou de pari.

En pratique, il convient donc de mentionner ces précisions dans la politique de protection des données personnelles de l'opérateur.

E. DROITS DES PERSONNES

Conformément aux dispositions du RGPD, les personnes disposent de droits s'agissant de leurs données personnelles (il est renvoyé au f) « Des droits des personnes respectés » de la partie I.2. du présent guide).
Il n'y a pas de droit à l'opposition, la création d'un compte de jeu emportant renonciation à ce droit[38], à l'exception des traitements dont la base légale est l'intérêt légitime (par exemple : les statistiques). Ainsi, le responsable de traitement peut refuser à la personne concernée l'exercice de son droit d'opposition si le traitement de données la concernant repose sur la base légale de l'obligation légale. S'agissant des traitements fondés sur le consentement, les personnes ont la possibilité de retirer leur consentement.

2. PRÉVENTION DU JEU EXCESSIF OU PATHOLOGIQUE

Les jeux d'argent et de hasard autorisés en application de l'article L. 320 6 du code de la sécurité intérieure ne sont « *ni un commerce ordinaire, ni un service ordinaire* » et font l'objet d'un encadrement strict aux fins de prévenir les risques d'atteinte à l'ordre public et à l'ordre social, notamment en matière de protection de la santé et des mineurs[39]. La dangerosité potentielle des jeux d'argent et de hasard explique pourquoi le premier objectif de la politique de l'Etat en matière de jeux d'argent et de hasard est de limiter et d'encadrer l'offre et la consommation des jeux et d'en contrôler l'exploitation afin de prévenir le jeu excessif ou pathologique et de protéger les mineurs[40]. La lutte contre le jeu excessif ou pathologique constitue l'une des raisons impérieuses d'intérêt général justifiant les restrictions que l'Etat apporte en matière de jeux d'argent et de hasard à la liberté d'établissement et la libre prestation de services protégées respectivement aux articles 49 et 56 du Traité sur le fonctionnement de l'Union européenne.

Ce principe directeur de lutte contre le jeu excessif ou pathologique irrigue largement le droit des jeux d'argent et de hasard. C'est ainsi que l'article L. 320-4 du code de la sécurité intérieure exige des opérateurs qu'ils concourent à la réalisation de l'objectif général de prévention du jeu excessif ou pathologique énoncé au 1° de l'article L. 320-3 du même code. Ce concours des opérateurs se concrétise notamment à l'occasion de l'exécution des obligations légales pesant sur eux :

- mise en place de dispositifs de modération, d'auto-exclusion et d'autolimitation des dépôts et des mises,
- prise en compte des interdictions de jeux,
- encadrement de la promotion de l'offre de jeux sous ses différents aspects (stratégie promotionnelle des opérateurs, communications commerciales et gratifications financières),
- identification des personnes dont le jeu est excessif ou pathologique
- accompagnement de celles-ci en vue de modérer leur pratique[42].

38 - Ainsi que le précise l'article 2 du décret n°2010-518 du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux.
39 - Article L. 320-2 du code de la sécurité intérieure.
40 - Article L. 320-3, 1° du code de la sécurité intérieure.
41 - Ces obligations trouvent leur source dans le code de la sécurité intérieure, la loi n° 2010-476 du 12 mai 2010 modifiée, le décret n° 2010-518, le décret n° 2010-1349, l'arrêté du 9 avril 2021 définissant le cadre de référence pour la prévention du jeu excessif ou pathologique et la protection des mineurs, ainsi que dans l'arrêté du 14 mai 2007 relatif à la réglementation des jeux dans les casinos.
42 - C'est une obligation cardinale issue de l'ordonnance du 2 octobre 2019 réformant la régulation des jeux d'argent et de hasard mise à la charge de tous les opérateurs (opérateurs agréés, opérateurs titulaires de droits exclusifs, casinos et clubs de jeux).
43 - Accessible ici : https://anj.fr/lautorite-nationale-des-jeux-publie-le-cadre-de-reference-pour-la-prevention-du-jeu-excessif.
44 - Accessibles ici : https://anj.fr/identification-et-accompagnement-des-joueurs-excessifs-deux-nouveaux-guides-pratiques-pour-les.

Un arrêté du 9 avril 2021[43] définissant le cadre de référence pour la prévention du jeu excessif ou pathologique et la protection des mineurs a précisé le contenu de ces cinq obligations et déterminé certaines bonnes pratiques pour leur exécution. En outre, deux guides[44], l'un concernant les casinos et clubs de jeux, l'autre les opérateurs agréés ou titulaires de droits exclusifs, ont été adoptés en 2024 par l'ANJ pour aider ces derniers en vue de la mise en œuvre des obligations spécifiques que sont l'identification et l'accompagnement des joueurs excessifs ou pathologiques.
A l'évidence, le respect des règles relatives à la lutte contre le jeu excessif ou pathologique suppose que les opérateurs traitent des données à caractère personnel. Mais, parce qu'ils conduisent à une immixtion dans la vie privée des joueurs, ces traitements doivent être réalisés avec précaution, dans le respect du RGPD.

A. FINALITÉS CONCERNÉES, BASES LÉGALES DES TRAITEMENTS ET CATÉGORIES DES DONNÉES TRAITÉES

a. Vue d'ensemble

i. Finalités

Si les traitements examinés ici tendent tous à la réalisation d'un même objectif, à savoir celui de la prévention du jeu excessif ou pathologique, **cet objectif peut lui-même être décliné en plusieurs finalités** qui se rapportent plus particulièrement à :

- l'identification des personnes dont le jeu est excessif ou pathologique ;
- l'accompagnement des personnes dont le jeu est excessif ou pathologique, en vue de modérer leur pratique[45] ;
- le respect des décisions d'interdiction de jeux par les opérateurs agréés, les opérateurs titulaires de droits exclusifs pour le jeu sur compte, les casinos et les clubs de jeux[46] ;
- la mise en œuvre des mécanismes de modération et d'autolimitation : modérateurs de dépôts, de mises et de temps de jeux déterminés par les joueurs au moment de l'inscription et pouvant être modifiés ultérieurement[47] ;
- l'exécution des demandes d'auto-exclusion formulées par les joueurs s'agissant du jeu sur compte, en ligne et en réseau physique de distribution[48], et
- l'exécution des contrats de limitation volontaire d'accès (LVA) s'agissant des casinos et clubs de jeux[49].

ii. Base légale des traitements

Les traitements de données à caractère personnel servant à la réalisation de ces finalités sont nécessaires pour l'exécution par les opérateurs d'une obligation légale[50].

45 - Loi du 12 mai 2010 modifiée, art. 34, IX, al. 3.
46 - Voir notamment sur ce point, pour les opérateurs de jeu sur compte, l'article 22 du décret 2010-518 modifié et, pour les casinos et clubs de jeux, les articles R.321-27 du code de la sécurité intérieure et 23 de l'arrêté du 14 mai 2007 relatif à la réglementation des jeux dans les casinos.
47 - CSI, art. L. 320-11 – décret n° 2010-518 du 19 mai 2010 modifié, art. 16 à 17.
48 - Idem 6 du décret n° 2010-518 du 19 mai 2010 modifié, art. 18.
49 - Arrêté du 14 mai 2007 relatif à la réglementation des jeux dans les casinos, art. 23, al. 2.
50 - Le IX de l'article 34 de la loi du 12 mai 2010 prévoit expressément cette obligation. Le cadre de référence issu de l'arrêté du 9 avril 2021 précise le contenu de cette obligation et impose l'obligation impérative de traiter les données à caractère personnel de joueurs afin de satisfaire aux exigences du IX de l'article 34 susvisé.

iii. Catégories de données

Les dispositions législatives et règlementaires[51] déterminent la plupart des catégories de données que les **opérateurs agréés**, d'une part, et les **opérateurs titulaires de droits exclusifs** pour le jeu sur compte, d'autre part, doivent traiter pour respecter leurs différentes obligations relatives à la mise en œuvre des mécanismes de modération et d'autolimitation et à l'exécution des demandes d'auto-exclusion.

.

De même, les textes règlementaires prévoient les données que les **casinos et clubs de jeux** doivent recueillir afin d'identifier et de refuser l'admission des mineurs et des personnes interdites de jeux[52]. Il est renvoyé à ces textes pour le détail des données concernées pour l'ensemble des finalités susvisées.

b. S'agissant en particulier de la finalité d'identification des joueurs excessifs ou pathologiques

Les finalités d'identification et d'accompagnement des personnes dont le jeu est excessif ou pathologique impliquent le traitement de données particulières, lesquelles diffèrent selon les opérateurs concernés.

En tout état de cause et quel que soit l'opérateur concerné, les données traitées doivent toujours l'être dans le respect des « grands principes » de la protection des données énoncés par le RGPD, notamment les principes de limitation des finalités, de minimisation, de proportionnalité et d'exactitude des données.

i. Les données traitées par les opérateurs agréés et les opérateurs titulaires de droits exclusifs pour le jeu sur compte

Les textes susvisés[53] et le guide *Identification et accompagnement des joueurs excessifs ou pathologiques – jeu en ligne*[54] mentionnent plusieurs indicateurs susceptibles d'être pris en compte dans le cadre des finalités d'identification et d'accompagnement des personnes dont le jeu est excessif ou pathologique selon les opérateurs concernés. Ces indicateurs s'articulent autour de deux catégories de données :

- Les données devant être collectées en tout état de cause (liste limitative) :
  - les données relatives à l'identité du joueur ;
  - les données de contact, dont l'obtention est nécessaire pour échanger avec lui, l'informer et le cas échéant accompagner le joueur qui souffrirait d'une assuétude aux jeux d'argent : adresse postale, numéro de téléphone, et, le cas échéant, adresse électronique ;
  - les données relatives aux opérations de jeux, les prises de jeu étant, eu égard à leur fréquence ou à leur objet, susceptibles de traduire un jeu excessif ou pathologique : nombre de parties de jeu, durée des sessions de jeu, caractéristiques des jeux auxquels participe la personne ;

51 - La loi du 12 mai 2010 modifiée, le décret n° 2010-518 du 19 mai 2010 modifié ainsi que le cadre de référence issu de l'arrêté du 9 avril 2021.
52 - Voir l'arrêté du 14 mai 2007 modifié relatif à la réglementation des jeux dans les casinos.
53 - La loi du 12 mai 2010 modifiée, le décret n° 2010-518 du 19 mai 2010 modifié ainsi que le cadre de référence issu de l'arrêté du 9 avril 2021.
54 - Voir sur ce point le guide « Identification et accompagnement des joueurs excessifs ou pathologiques - jeu en ligne » publié en 2024 par l'ANJ.

- les données financières, qui sont essentielles pour déterminer et mesurer l'addiction du joueur : nombre et montant des mises, approvisionnement, pertes, gains, reversement, coordonnées du compte de paiement et document permettant de vérifier que le joueur en est titulaire (IBAN), moyens de paiement utilisés s'agissant du jeu sur compte[55] ;
- les données relatives à l'historique des dispositifs de modération, d'auto-exclusion et présence passée sur le fichier des interdictions de jeux ;

• Les données collectées selon les évènements significatifs qui surviennent au cours de la pratique de jeu[56] (cette catégorie correspond aux données collectées lorsque se produit un fait générateur) :
- les données relatives à l'attitude du joueur lorsqu'elle est manifestement atypique, notamment ses échanges avec le service client : demandes répétées de gratifications financières, manifestation d'agressivité, de frustration ou de détresse ;
- les données émanant de l'entourage du joueur qui peut contacter l'opérateur pour l'alerter sur un comportement du joueur : lien (par exemple : « famille », « amis », « travail ») de cette personne avec le joueur, nom de naissance et prénom(s) du joueur concerné. Il est recommandé que les opérateurs ne retranscrivent pas les échanges avec les proches dans le dossier du joueur mais consignent l'existence de l'alerte et, si nécessaire, la nature générique de l'alerte (par exemple : « difficultés financières » ; « conflits familiaux » ; « isolement » ; « vulnérabilité particulière »)[57]. L'opérateur ne peut transmettre à l'entourage la moindre donnée sur le joueur concerné, pas même lui confirmer que le joueur est son client.

ii. Les données traitées par les casinos et clubs de jeux

Les dispositions législatives et règlementaires[58] ne déterminent pas expressément les données que les **casinos et clubs de jeux** traitent pour l'identification et l'accompagnement des personnes dont le jeu est excessif ou pathologique. En revanche, le cadre de référence issu de l'arrêté du 9 avril 2021 mentionne plusieurs types de données sur lesquels ils peuvent s'appuyer à cette fin. En outre, le guide *Identification et accompagnement des joueurs excessifs ou pathologiques dans les casinos et clubs de jeux* de 2024 dresse une liste d'indicateurs sur lesquels les opérateurs peuvent se fonder pour réaliser cette identification et cet accompagnement. Il est renvoyé sur ce point à ce guide[59], lequel met en avant différents indicateurs, étant précisé que leurs collectes ne sauraient impliquer la mise en place de dispositifs de recueil d'identité systématique de tous les joueurs. Ces indicateurs s'articulent autour de trois catégories de données :

• Les données susceptibles d'être collectées au cours de la pratique de jeu :
- Les données relatives à l'identité du joueur ;
- Les données relatives aux comportements de jeu, telles que le nombre et la fréquence des entrées dans l'établissement, le montant et la fréquence des mises, l'intensité de jeu et les tentatives de compensation des pertes ;
- Les données relatives à l'utilisation des mesures de protection, telles que la demande d'une LVA ou une demande de renseignement sur l'interdiction volontaire de jeu ;

55 - Le joueur peut utiliser les moyens de paiement de la société à laquelle il appartient pour alimenter un jeu que ses propres ressources ne lui permettent pas de financer. En ce qui concerne les traitements des données relatives à la carte de paiement en matière de fourniture de services à distance, v. la recommandation adoptées par la CNIL dans sa délibération n° 2018-303 du 6 septembre 2018.
56 - Cette liste n'est pas limitative. Si l'opérateur de jeux souhaite collecter des **données collectées qui ne sont pas expressément visées** dans le présent guide ou dans les guides pratiques sur l'identification et l'accompagnement des joueurs excessifs ou pathologiques, il doit **documenter la nécessité pour lui de collecter cette donnée** notamment en **se fondant sur de la littérature scientifique**.
57 - Aucune donnée sensible concernant le joueur ne peut être collectée dans le cadre de cette consignation.
58 - En ce compris l'arrêté du 14 mai 2007 modifié relatif à la réglementation des jeux dans les casinos.
59 - cf. les indicateurs définis aux pages 10 à 14 du guide.

- Les données collectées selon les évènements significatifs qui surviennent au cours de la pratique de jeu[60] (cette catégorie correspond aux données collectées lorsque se produit un fait générateur) :
  - Les données émanant de l'entourage du joueur qui peut contacter l'établissement pour l'alerter sur un comportement du joueur : lien (par exemple : « famille », « amis », « travail ») de cette personne avec le joueur, nom de naissance et prénom(s) du joueur concerné. Il est recommandé que les opérateurs ne retranscrivent pas les échanges avec les proches dans le dossier du joueur mais consignent l'existence de l'alerte et, si nécessaire, la nature générique de l'alerte (par exemple : « difficultés financières » ; « conflits familiaux » ; « isolement » ; « vulnérabilité particulière »)[61]. L'opérateur ne peut transmettre à l'entourage la moindre donnée sur le joueur concerné, pas même lui confirmer que le joueur est son client.
  - Par ailleurs, et **uniquement lorsqu'elles sont manifestement atypiques**, doivent être également prises en compte certaines données relatives à l'attitude du joueur pouvant révéler un risque de jeu excessif ou pathologique telles que la nature de certains de ses échanges avec l'établissement de jeux faisant état de difficultés, l'expression de signes de colère envers la direction, d'autres joueurs ou le personnel de l'établissement, de forts signes d'anxiété ou la dégradation manifeste de l'apparence physique.

- Les données que, le cas échéant, l'opérateur prend en compte ou demande au joueur après une première analyse le conduisant à considérer que ce dernier pourrait avoir une pratique de jeu excessive ou pathologique :
  - Présence passée sur le fichier des personnes interdites de jeux, utilisation actuelle ou passée d'un dispositif étranger équivalent ;
  - Historique des mesures d'accompagnement mise en place par l'établissement, ou par un autre établissement ou opérateur de jeu (par exemple, l'existence d'une LVA révolue, ou en cours dans un autre casino de la région ou membre du même groupe) ;
  - Comptes rendus d'entretien avec le référent « prévention jeu excessif », étant précisé que les opérateurs ne retranscrivent pas en intégralité les échanges avec le joueur mais uniquement les informations strictement nécessaires à son accompagnement et à son suivi (informations communiquées au joueur par l'établissement, degré d'acceptation du joueur du constat de jeu excessif, informations complémentaires apportées par le joueur sur ses pratiques de jeu ou signaux de jeu excessif rencontrés, modalités d'accompagnement et de suivi proposées par l'établissement, préférences du joueur en matière de modalités d'accompagnement et de suivi, conclusion de l'entretien). Si le joueur fait état de facteurs particuliers de vulnérabilité au jeu excessif, il est recommandé de les consigner de façon générique (par exemple : « difficultés financières » ; « conflits familiaux » ; « isolement » ; « vulnérabilité particulière »)[62].
  - Résultats du test Indice Canadien du Jeu Excessif (ICJE) fait avec l'établissement.

iii. Les données traitées par les opérateurs titulaires de droits exclusifs pour leur activité en réseau physique de distribution

La situation des **opérateurs titulaires de droits exclusifs** se rapproche de celle des casinos et clubs de jeux pour leur activité en réseau physique de distribution s'agissant des joueurs qui ne jouent pas sur compte[63]. Il est renvoyé à cet égard au point précédent relatif aux casinos et clubs de jeux.

60 - Cette liste n'est pas limitative. Si l'opérateur de jeux souhaite collecter des **données collectées qui ne sont pas expressément visées** dans le présent guide ou dans les guides pratiques sur l'identification et l'accompagnement des joueurs excessifs ou pathologiques, il doit **documenter la nécessité pour lui de collecter cette donnée** notamment en **se fondant sur de la littérature scientifique**.

61 - Aucune donnée sensible concernant le joueur ne peut être collectée dans le cadre de cette consignation.

62 - Aucune donnée sensible concernant le joueur ne peut être collectée dans le cadre de cette consignation.

63 - Le cadre de référence issu de l'arrêté du 9 avril 2021 indique à cet égard que « *la détection s'opère par le repérage de signaux forts aisément identifiables du jeu excessif* ».

B. TRAITEMENTS DE DONNÉES DE SANTÉ

Cette partie ne concerne que le traitement à des fins d'identification des joueurs excessifs ou pathologiques.

a. Qualification de données de santé

Rappel : qu'est-ce qu'une « *donnée concernant la santé* » (ci-après « d*onnées de santé* ») au sens du RGPD ?

Le considérant 35 du RGPD énonce : « *Les données de santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée* ».

L'article 4.15 du RGPD définit les données de santé comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

La CNIL précise qu'entrent dans cette notion trois catégories de données[64] :

- celles qui sont des données de santé par nature : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc. ;
- **celles qui, après le croisement d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne** ;
- celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite sur le plan médical.

L'alinéa 3 du IX de l'article 34 de la loi du 12 mai 2010 modifiée susvisée prévoit que « *Les opérateurs, casinos et clubs de jeux **identifient les personnes dont le jeu est excessif ou pathologique** et les accompagnent en vue de modérer leur pratique, dans le respect du cadre de référence* ».

L'arrêté du 9 avril 2021 évoqué plus haut définissant le cadre de référence pour la prévention du jeu excessif ou pathologique et la protection des mineurs précise notamment que : « *cette obligation d'identification s'entend comme la détection et l'évaluation d'une perte de contrôle manifeste ou d'un niveau caractérisé de risque de jeu excessif ou pathologique.*

- *Pour mettre en œuvre cette obligation, l'opérateur déploie une approche et des outils d'identification et d'analyse adaptés en fonction du canal de distribution de son offre de jeu et des types de signaux relevés.*
- *Les opérateurs s'efforcent d'identifier aussi tôt que possible les joueurs dont les pratiques de jeu commencent à basculer vers des comportements excessifs ou pathologiques. Ils adaptent leurs interventions en fonction du niveau de risque identifié.*

64 - Voir sur ce point : https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante.

- L'identification doit être strictement distinguée d'un diagnostic médical caractérisant une pathologie, qui relève de la compétence exclusive des professionnels du soin. Il n'appartient donc pas à l'opérateur ou à ses préposés d'effectuer ce diagnostic ».

Le traitement d'identification d'une personne comme joueur excessif ou pathologique (en particulier celles pour lesquels le niveau de risque est identifié comme « modéré » ou « risque de jeu excessif ou pathologique ») est, selon la CNIL, un traitement de données de santé. L'article L.1111-8 du code de la santé publique ne devrait en principe pas s'appliquer, les opérateurs ne devant pas avoir en principe l'obligation de recourir à un prestataire agrée ou certifié « HDS ».

En effet, si l'identification des personnes dont le jeu est excessif ou pathologique ne consiste pas pour les opérateurs en l'établissement d'un diagnostic médical – que seul un professionnel du soin peut poser – ces derniers n'en sont pas moins amenés à croiser certaines données leur permettant de tirer une conclusion sur une pratique de jeu que la loi et l'arrêté qualifient d'excessive ou pathologique. La caractérisation d'une telle pratique est ainsi susceptible de révéler une addiction comportementale reconnue comme une maladie[65].

Une précision s'impose à cet égard : les données à caractère personnel que les opérateurs traitent ne constituent pas en elles-mêmes, sauf circonstances exceptionnelles[66], des données de santé[67]. Seule revêt cette nature la donnée issue du traitement combiné de l'ensemble de ces données, donnée qui révèlerait l'existence d'une pratique de jeu excessive ou pathologique d'un joueur déterminé.

b. Conséquences de la qualification de données de santé

Les données concernant la santé sont considérées comme des données sensibles dont le traitement n'est autorisé que par exception, notamment en présence d'un « *motif d'intérêt public important sur la base du droit de l'Union ou du droit d'un État membre* » (ce qui est le cas s'agissant de la lutte contre le jeu excessif et pathologique), à la condition que le traitement :

- soit proportionné à l'objectif poursuivi,
- respecte l'essence du droit à la protection des données,
- et prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. A cet égard, de telles garanties sont prévues par le cadre de référence[68]. Il prévoit notamment qu'une AIPD doit être réalisée, qu'une procédure interne écrite formalise et définit les signaux d'alerte et que le dispositif de détection et les indicateurs de suivi retenus soient formalisés par l'opérateur dans le cadre du plan d'actions annuel qu'il soumet à l'ANJ pour validation.

65 - Le « jeu pathologique » est reconnu comme une maladie psychiatrique dans le Manuel diagnostique et statistique des troubles mentaux (DSM-5).

67 - Par exemple, lorsque le joueur décide de sa propre initiative de communiquer une donnée de santé le concernant (par exemple, un joueur qui décide d'adresser à un opérateur un courrier ou un certificat d'un psychiatre faisant état du caractère pathologique des pratiques de son jeu). En revanche, aucune donnée de santé concernant le joueur ne peut être collectée lorsque l'information émane de l'entourage.

67 - Les signaux émotionnels peuvent être collectés dès lors qu'ils ne relèvent pas de la définition de l'article 9 du RGPD. Il s'agit des signaux émotionnels tels qu'ils sont décrits dans le « guide identification et accompagnement des joueurs excessifs ou pathologiques dans les casinos et clubs de jeux » : le joueur tremble ou transpire abondamment en jouant ; le joueur semble anxieux, agite nerveusement la jambe en jouant ; le joueur est en colère, jure ou grogne en jouant, frappe les machines ; apparence triste, déprimée, pleurs après une perte ; changements d'humeur.

68 - Issu de l'arrêté du 9 avril 2021.

La qualification de donnée de santé fait peser des obligations particulières sur les opérateurs :

- **mesures de sécurité organisationnelles et techniques plus strictes** pour prévenir les risques graves d'atteintes à la vie privée qui pourraient résulter de la fuite d'une telle donnée (voir sur ce point le e) « Des données sécurisées » de la partie I.2. du présent guide) ; à cet égard, il est recommandé en particulier de renforcer la sécurité des accès par des mesures telles qu'une authentification multifacteur, combinée à une gestion stricte des droits d'accès, qui doivent être limités aux profils pour lesquels l'accès à ces données est nécessaire en raison de leurs missions.
- tenue d'un **registre** des traitements des données personnelles par le responsable de traitement et les sous-traitants (voir sur ce point le 2) « Réaliser une cartographie des données et des traitements (le registre) » de la partie I.1.b) du présent guide)[69] ;
- réalisation d'une **analyse d'impact** (voir sur ce point le 5) « Réaliser une étude d'impact lorsque cela est nécessaire » de la partie I.1.b) du présent guide et les développements ci-dessous).

C. LES OUTILS D'IDENTIFICATION DES JOUEURS PATHOLOGIQUES POUR LES JEUX PROPOSÉS EN LIGNE

Cette partie ne concerne que le traitement à des fins d'identification des joueurs excessifs ou pathologiques.

a. L'intervention humaine

Le cadre de référence prévoit que : « *les données informatisées relatives à l'activité de jeu [sont] analysées par les opérateurs de jeux en ligne pour l'ensemble de leur clientèle, par les opérateurs sous droits exclusifs pour le jeu sur compte.* ***Les analyses automatisées des données quantitatives donnent obligatoirement lieu à une vérification manuelle humaine*** ».

Il en résulte que toutes les décisions entrainant une restriction unilatérale de la possibilité de jouer de la personne concernée devront faire l'objet d'une supervision humaine par l'opérateur de jeu conformément au cadre de référence[70]. Cette vérification humaine peut prendre plusieurs formes. Dans le cas d'une alerte générée par un dispositif informatique d'un opérateur, un agent du service en charge de la prévention du jeu excessif procède à une analyse manuelle pour caractériser précisément le niveau de risque du joueur afin de lui faire part de mesures d'accompagnement les plus adaptées. Des comités de pilotage inter-service sont aussi mis en place afin d'identifier le niveau de risque des joueurs, souvent en raison d'atypismes de jeu pouvant faire soupçonner une addiction (ou un cas de blanchiment)[71].

69 - L'exception relative aux entités comportant moins de 250 employés ne s'applique pas si les traitements qu'elles effectuent portent notamment sur des données de santé (article 30 § 5 du RGPD).

70 - L'article VII du cadre de référence issu de l'arrêté du 9 avril 2021 prévoit notamment que l'identification d'un joueur en tant que joueur excessif peut entrainer la mise en œuvre de mesures d'accompagnement pouvant « *le cas échéant, limiter ou neutraliser la capacité de jeu du joueur* »

71 - Des appels téléphoniques sont également mis en place par les services clients afin de s'assurer, dans le cadre de la prévention du jeu des mineurs, que le propriétaire du compte est majeur.

Deux situations sont à distinguer :

- Pour les joueurs classés « sans risque ou risque faible », il n'y a aucune intervention humaine (décision entièrement automatisées) seuls des **messages automatiques d'information et/ou de prévention sont envoyés**.
- Pour les joueurs classés « risque fort », et pour lesquels il y a donc une décision entrainant une limitation de jeux, alors il y a une intervention humaine en amont de la décision.

b. L'application de l'article 22 du RGPD

Le profilage se définit comme toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique (art. 4.4 du RGPD).

Afin de respecter leur **obligation d'identifier les personnes dont le jeu est excessif ou pathologique**, les opérateurs de jeux proposant l'ouverture d'un compte client peuvent développer des outils algorithmiques qui permettent d'attribuer un niveau de risque au joueur sur la base de plusieurs critères. L'opérateur qui vise à attribuer un niveau de risque spécifique au joueur en évaluant sa pratique et son comportement de jeu, met ainsi en œuvre, selon la CNIL, un **traitement de profilage**.

Or, l'article 22 du RGPD souligne le droit pour toute personne de ne pas faire l'objet d'une décision fondée **exclusivement** sur un traitement automatisé, **y compris le profilage**, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

- **Pour les joueurs pour lesquels** l'analyse est entièrement automatisée et ne donnant lieu à **aucune intervention humaine (joueurs classés « sans risque ou risque faible »)** :

L'article 22 du RGPD n'a pas vocation à s'appliquer lorsque la classification n'affecte pas le joueur ce qui est le cas si seuls des messages de prévention ne comportant pas de décisions « produisant des effets juridiques » ou « affectant de manière significative » le joueur sont envoyés.

- **Pour les joueurs pour lesquels il y a une intervention humaine (joueurs classés « risque fort »)** :

L'article 22 du RGPD n'est pas applicable si l'intervention humaine est prévue en amont d'une éventuelle prise de décision « ***produisant des effets juridiques pour la personne concernée ou l'affectant de manière significative de façon similaire*** ».

Lorsque l'opérateur souhaite mettre en place une mesure de restriction unilatérale d'accès au service permanente ou temporaire, une intervention humaine est nécessaire conformément au cadre de référence, l'article 22 ne devrait donc pas s'appliquer. Cette intervention devrait dépasser une simple validation pour éviter une influence excessive de l'algorithme, comme l'a précisé la Cour de justice de l'Union européenne (CJUE) notamment dans le cadre du *scoring* bancaire[72].

72 - CJUE, 1ère chambre, arrêt du 7 décembre 2023, dans l'affaire C-634/21.

D. TRAITEMENTS DEVANT DONNER LIEU À UNE ANALYSE D'IMPACT (AIPD)

Comme indiqué au point le 5) « Réaliser une étude d'impact lorsque cela est nécessaire » de la partie I.1.b) du présent guide auquel il est renvoyé, la réalisation d'une AIPD est requise lorsqu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* ». En outre, le Groupe de travail « Article 29 » sur la protection des données (G29) a défini neuf critères permettant de regarder un traitement comme susceptible d'engendrer un risque élevé, lesquels ont été repris par le Comité européen à la protection des données (CEPD) et par la CNIL. Lorsqu'un traitement **présente au moins deux de ces critères**, l'opérateur doit mener une analyse d'impact.

Or, en matière de prévention du jeu excessif ou pathologique, plusieurs de ces critères paraissent, selon la CNIL, systématiquement réunis, parmi lesquels le traitement de données de santé, la combinaison de plusieurs données, le traitement à large échelle pour certains opérateurs et, parfois, l'usage de techniques innovantes (telles qu'un outil algorithmique pour les opérateurs agréés en ligne).

En conséquence, il apparaît que tous les opérateurs de jeux d'argent et de hasard peuvent effectuer une AIPD s'agissant des traitements de données qu'ils mettent en œuvre pour la lutte contre le jeu excessif ou pathologique. C'est d'ailleurs ce que prévoit expressément l'article VII du cadre de référence[73].

E. ACCÉDANTS, DESTINATAIRES ET TIERS AUTORISÉS

La transmission des données traitées au titre de la prévention du jeu excessif ou pathologique est soumise au régime de droit commun des transmissions de données et il est renvoyé sur ce point au B) « Accédants, destinataires et tiers autorisés » de la partie II.1. du présent guide.

A ces règles, s'ajoute la mise en place d'une **vigilance renforcée** eu égard au caractère sensible des données traitées, en particulier les données de santé. La protection des données personnelles nécessite en effet de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques eu égard à la nature des données concernées.

En particulier, concernant les **accédants**, le fichier doit être accessible aux seules personnes (qu'elles soient salariées ou prestataires) en charge de la prévention du jeu excessif ou pathologique (par exemple le référent « prévention jeu excessif »). Les données pertinentes doivent être en outre communiquées aux personnes qui ont un intérêt légitime à en connaître, par exemple au service juridique et au responsable du service client de l'opérateur afin que celui-ci puisse en tirer les conséquences (par exemple en excluant de l'envoi de communications commerciales les personnes identifiées comme joueur excessif).

Il s'ensuit, en pratique, que ce fichier, sous un format numérique, doit être sécurisé et son accès protégé (par exemple, par un mot de passe robuste). Sous un format papier, les données sensibles doivent être gardées dans un endroit sécurisé et accessible uniquement par les personnes habilitées (par exemple, dans une armoire fermée à clé). Un journal des accès à ce fichier doit être tenu, pour permettre d'identifier les personnes qui l'ont consulté ainsi que le moment auquel cette consultation a eu lieu. S'agissant des accès administrateur (compte technique à haut privilège), il est recommandé que les opérateurs s'assurent

73 - Issu de l'arrêté du 9 avril 2021.

de l'utilisation de comptes nominatifs soumis à la journalisation des accès, ainsi que de la signature d'un accord de confidentialité spécifique du fait des données traitées. Du fait de la nature des accès, il est recommandé que les opérateurs s'assurent également de la mise en œuvre d'une authentification multifacteur dans le cas des comptes à privilèges afin de limiter les risques d'usurpation de ces accès.

Seuls les prestataires impliqués en matière de prévention du jeu excessif ou pathologique peuvent être rendus destinataires des données personnelles y afférentes. Selon la CNIL, il ne saurait y avoir de transmission des données à des partenaires commerciaux à des fins de prospection, cette finalité n'étant pas compatible avec la prévention du jeu excessif ou pathologique. Pour répondre à leur obligation générale de prévention du jeu excessif ou pathologique, les opérateurs doivent veiller à ce que les personnes qui participent à la promotion de leur offre ne puissent recevoir les données personnelles de joueurs bénéficiant d'une mesure d'auto-exclusion, d'une mesure d'interdiction de jeu ou qu'ils ont identifiées comme ayant un jeu excessif ou pathologique (l'accompagnement étant incompatible avec l'envoi de communications commerciales).

F. DURÉE DE CONSERVATION

Une durée de conservation doit être fixée en fonction de chaque finalité. De manière générale, les durées de conservation ne doivent, en principe, pas dépasser les durées de prescriptions légales. A l'issue de ce délai, l'opérateur doit supprimer ces données.

La conservation des données à caractère personnel est indispensable : en effet, **les opérateurs doivent être en mesure de prouver qu'ils ont respecté leurs obligations au titre de la prévention du jeu excessif ou pathologique** et ce, tant à l'égard de l'ANJ, qui les contrôle, que des joueurs qui pourraient essayer de rechercher leur responsabilité à raison d'un manquement à ces obligations. **Les opérateurs doivent donc s'organiser pour conserver cette preuve.**

S'agissant des joueurs sur compte, l'article 31 du décret n°2010-518 du 19 mai 2010 modifié prévoit expressément un délai de conservation des données personnelles des joueurs de **6 ans à compter de la clôture du compte joueur correspondant** qui a vocation à s'appliquer aux finalités en lien avec la prévention du jeu excessif ou pathologique.

Finalité	Base légale	**Durée de conservation**
Prévention du jeu excessif ou pathologique	Respect d'une obligation légale	6 ans à compter de la clôture du compte joueur correspondant

S'agissant des opérateurs titulaires de droits exclusifs, pour les jeux proposés en réseau physique de distribution hors jeu sur compte, et des casinos et clubs de jeux, la CNIL recommande de retenir une durée de conservation des données personnelles de **6 ans à compter de leur collecte**.

Finalité	Base légale	**Durée de conservation**
Prévention du jeu excessif ou pathologique	Respect d'une obligation légale	6 ans à compter de la collecte de la donnée

G. INFORMATIONS DES PERSONNES CONCERNÉES

L'information à délivrer aux personnes concernées par un traitement relatif à la prévention du jeu excessif ou pathologique, y compris concernant des données de santé, est soumise au régime de droit commun de l'information des personnes, prévu aux articles 12, 13[74] et 14[75] du RGPD.

S'agissant du détail des **modalités de l'information** des joueurs sur les traitements, il est renvoyé au f) « Des droits des personnes respectés » de la partie I.2. du présent guide.

Focus relatif au profilage

La CNIL considère que les opérateurs de jeux qui ont recours à des outils algorithmiques pour permettre d'attribuer un niveau de risque au joueur en évaluant sa pratique et son comportement de jeu, mettent en œuvre un **traitement de profilage.**

Les opérateurs doivent fournir aux joueurs une information complète relative au profilage[76]. Sur ce point, les responsables du traitement doivent veiller à expliquer clairement et simplement aux personnes concernées la manière dont fonctionne le profilage ou le processus décisionnel automatisé. En particulier, lorsque le traitement implique une prise de décision fondée sur le profilage (et ce même s'il ne relève pas des dispositions de l'article 22), les personnes doivent être clairement informées que le traitement vise à la fois a) le profilage et b) la prise de décision fondée sur le profil généré[77].
A cet égard la CNIL recommande que l'opérateur mette en œuvre des mesures spécifiques de transparence, concernant le profilage des joueurs, notamment :

- Les différentes catégories de classification (joueurs à faible risque, risque modéré ou fort risque de jeu excessif ou pathologique) et à quoi correspond chaque classification.
- La manière dont les joueurs sont classés (recours à un outil algorithmique, les critères retenus etc.).
- Les effets générés par la classification du joueur et les conséquences de la prise de décision fondée sur le profilage (messages de prévention automatiques, l'intégration de l'outil de modération dans le parcours du joueur, les appels sortants etc.).

S'agissant du **support de l'information** relative aux traitements des données personnelles, il convient de distinguer selon que le jeu intervient en ligne ou non.

Pour les opérateurs agréés en ligne - ainsi que pour les opérateurs en monopole s'agissant du jeu sur compte – la CNIL recommande que le site internet des opérateurs soit le support d'information à privilégier. L'information doit être la plus visible possible et pourrait figurer dans une rubrique dédiée.

74 - S'agissant de la collecte directe des données.
75 - S'agissant de la collecte indirecte (auprès d'un tiers).
76 - Le considérant 60 du RGPD prévoit notamment que « *(…) la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci (…)* ».
77 - Ainsi que cela ressort des lignes directrices du « G29 » du 6 février 2018 relatives à la prise de décision individuelle automatisée et au profilage (https://www.cnil.fr/sites/default/files/atoms/files/wp251_profilage-fr.pdf).

Pour les casinos et clubs de jeux, il est recommandé par la CNIL, à titre de bonnes pratiques, que l'information soit diffusée sur un support matériel adapté à l'environnement physique. Il peut s'agir d'un panneau d'information et/ou d'une fiche d'information disponible dans un lieu facilement accessible, par exemple dans le hall d'entrée du casino ou club de jeux ou au niveau de l'accueil. Si le casino ou club de jeux a un site internet, il est recommandé également de réitérer l'information relative aux traitements des données personnelles sur une page dédiée dudit site. De même, si le casino ou club de jeux a mis en place un « programme de fidélité », il pourrait faire figurer les informations relatives aux traitements des données personnelles sur les supports (prospectus, site dédié etc.) présentant ce programme.

S'agissant des personnes privées exploitant des postes d'enregistrement au nom et pour le compte de la société LA FRANCAISE DES JEUX ou du GIE PARI MUTUEL URBAIN, il est recommandé par la CNIL, à titre de bonnes pratiques, que l'information soit diffusée sur un support matériel adapté à l'environnement physique. Cette information peut prendre la forme, par exemple, d'affichettes apposées sur le comptoir de jeu de manière à garantir l'accessibilité des informations.

H. DROITS DES PERSONNES

Conformément aux dispositions du RGPD, les personnes disposent des droits suivants s'agissant de leurs données personnelles :

- droit d'accès : l'opérateur doit fournir une copie des données personnelles qu'il détient sur le joueur. Le joueur est notamment informé de la qualification de sa pratique de jeu (c'est-à-dire le niveau de risque associé) lorsqu'il exerce son droit d'accès auprès d'un opérateur ;
- droit de rectification[78] : les dispositions de l'article 16 du RGPD prévoient que « *la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes* » ;
- droit à la limitation du traitement (par exemple : lorsque la personne conteste l'exactitude de ses données, elle peut demander la limitation temporaire du traitement de ses données le temps qu'il soit procédé aux vérifications nécessaires).

Le droit à l'effacement ne s'applique pas, le traitement étant nécessaire pour respecter une obligation légale auquel le responsable du traitement est soumis[79].

Les données étant fournies sur la base d'une obligation légale, il n'y a pas de droit à opposition[80], ni à portabilité.

78 - rectification ne s'applique donc qu'aux données inexactes ou incomplètes, le joueur peut contester son classement mais il devra motiver sa contestation en pointant l'inexactitude des données ou encore leur caractère incomplet. Cette rectification peut cependant intervenir sur « les données d'entrée » ou « de sortie ». Comme rappelé dans les lignes directrices du « G29 » du 6 février 2018 relatives à la prise de décision individuelle automatisée et au profilage : « *Les droits de rectification et à l'effacement s'appliquent à la fois aux «données à caractère personnel saisies» (les données à caractère personnel utilisées pour créer le profil) et aux «données de sortie» (le profil lui-même ou la «note» attribuée à la personne)* » (p. 19).

79 - Le b) de l'article 17.3 du RGPD prévoit l'absence de droit à l'effacement « *pour respecter une obligation légale qui requiert le traitement prévu par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis (…)* ».

80 - 6 En matière de jeu sur compte, l'absence du droit d'opposition est également rappelé par l'article 2 du décret n°2010-518 du 19 mai 2010 modifié relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux.

3. LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME (LCB-FT)[81]

Les recommandations contenues dans la présente section sont destinées aux opérateurs agréés de jeux en ligne ainsi qu'aux opérateurs titulaires de droits exclusifs et ne portent pas sur l'activité des casinos et clubs de jeux.

L'article L. 561-2 du CMF range les opérateurs de jeux d'argent et de hasard parmi les personnes assujetties aux obligations relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme. Cet assujettissement fait écho à l'obligation qui pèse sur eux en vertu de l'article L. 320-4 du code de la sécurité intérieure de concourir à la réalisation des objectifs de la politique de l'Etat en matière de jeux d'argent et de hasard, objectifs au nombre desquels figure celui énoncé au 3° de l'article L. 320-3 du même code de : « Prévenir les activités frauduleuses ou criminelles ainsi que le blanchiment des capitaux et le financement du terrorisme ». Les principales règles qui s'imposent aux opérateurs de jeux d'argent et de hasard en matière de lutte contre le blanchiment ont été rappelées et précisées dans l'arrêté du 9 septembre 2021 définissant le cadre de référence pour la lutte contre la fraude et contre le blanchiment des capitaux et le financement du terrorisme (ci-après le « Cadre de référence LCB-FT »[82]).

Les objectifs du RGPD et ceux de la règlementation relative à la lutte contre le blanchiment et le financement du terrorisme (LCB-FT) peuvent se coordonner harmonieusement autour d'une logique commune d'analyse des risques et de proportionnalité. La directive (UE) 2024/1640 du 31 mai 2024 (dite 6ème directive anti-blanchiment) et le règlement 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (qui entrera en vigueur le 10 juillet 2027) comportent d'ailleurs des règles sur la protection des données à caractère personnel assurant l'articulation entre ces deux corps de règles[83].

Concernant plus précisément l'articulation entre les obligations des opérateurs de jeux en matière de LCB-FT et les règles en matière de protection des données personnelles, les opérateurs doivent s'assurer de la proportionnalité de leurs traitements, au regard du risque de blanchiment et de financement du terrorisme propre à chaque joueur, et avoir conscience du caractère intrusif des demandes d'informations qu'ils peuvent être amenés à formuler. Pour autant, les exigences du RGPD ne sauraient, à l'évidence, être invoquées par un opérateur pour justifier un manquement à ses obligations relatives à la lutte contre le blanchiment et le financement du terrorisme.

81 - Cette partie du guide relative aux traitements à des fins de lutte contre le blanchiment des capitaux et le financement du terrorisme concerne essentiellement les opérateurs agréés en ligne et les opérateurs titulaires de droits exclusifs, étant précisé que les mandataires de ces derniers n'ont pas la qualité d'assujetti au sens de l'article L. 561-2 du CMF.

82 - Consultable en suivant ce lien.

83 - Le règlement comporte ainsi un Chapitre VII relatif à la protection des données et la conservation des informations assurant l'articulation de ses règles avec celles du RGPD. A cet égard, le droit à l'information des personnes est rappelé, tout comme l'obligation pour les assujettis de s'assurer que les données qu'ils traitent proviennent de sources fiables, exactes et à jour.

A. FINALITÉS CONCERNÉES

Plusieurs finalités peuvent être distinguées ici, qui se rattachent toutes à la LCB-FT :

- **la mise en œuvre des obligations de vigilance à l'égard de la clientèle conformément à l'approche par les risques**

Il s'agit des traitements de données qui permettent de déterminer le profil de risque des clients avec lequel l'opérateur est en relation d'affaires. Cette finalité implique la vérification de l'identité des joueurs (voir les points a. « Concernant les opérateurs de jeu en ligne » et b. « Concernant les opérateurs de jeux en réseau physique de distribution (hors jeu sur compte) » de la partie II.3.C)) sur les catégories de données traitées pour satisfaire à l'obligation d'identification).

- **le déclenchement des alertes et la réalisation de déclarations de soupçon**

Ces traitements rendent possible l'identification d'opérations ou tentatives d'opérations portant sur des sommes qui sont susceptibles de provenir d'une fraude fiscale, d'une infraction passible d'une peine privative de liberté supérieure à un an, de participer au financement du terrorisme. En particulier, ces traitements conduisent à la génération d'alertes susceptibles de faire apparaître un atypisme sur une période donnée au regard de la connaissance actualisée du joueur. Ces alertes, qui donnent lieu à une analyse complémentaire non automatisée, peuvent conduire à une déclaration de soupçon à la cellule de renseignement Tracfin, déclaration qui doit être étayée et, le cas échéant, complétée au regard des informations que l'opérateur recueille par la suite.

- **la recherche des personnes qui doivent faire l'objet de mesures de vigilance complémentaires, telles que les personnes politiquement exposées (PPE) au sens de l'article R. 561-18 du CMF et de celles qui sont susceptibles de faire l'objet de mesures de vigilance renforcées lorsqu'une opération de jeux présente un caractère particulièrement atypique ou s'avère d'un montant inhabituellement élevé**

Le fichier des relations d'affaires (base client) peut être rapproché d'un fichier documentaire fiabilisé utilisé comme base de référence par l'opérateur pour identifier les personnes qualifiées de PPE et celles susceptibles de faire l'objet de mesures de vigilance complémentaires ou renforcées.

- **la mise en œuvre de mesures de gel des avoirs en application de sanctions financières**

Ces traitements, nécessaires afin de détecter les personnes concernées par une mesure de gel des avoirs, permettent l'identification et la déclaration de joueurs qui figurent sur les listes de mesures de gel des avoirs, si besoin après collecte d'informations complémentaires auprès de la Direction générale du Trésor.

L'utilisation de bases de données fournies par des acteurs privés

Le traitement de catégories particulières de données personnelles et de données relatives à des condamnations pénales et à des infractions fait l'objet d'un régime particulier : celui d'une interdiction assortie d'exemptions précisément énumérées en fonction des données concernées (il est renvoyé sur ce point au C) « Les catégories de données traitées » de la partie II.3. du présent guide).

Le recours à un dispositif automatisé d'identification de la présence de personnes sur des listes consolidées (communément appelé « *watchlist* »), bien qu'opérationnellement très utile et souvent très répandu en pratique, ne doit pas occulter le fait qu'il s'agit d'un outil qui peut être sollicité parmi un ensemble d'autres mesures et outils, en fonction de chaque contexte pertinent. L'intérêt que présente ce type de base de données doit être mis en perspective avec le fait qu'elle contient généralement des données à caractère personnel soumises à l'application des articles 9 et 10 du RGPD.

En conséquence, lorsqu'un opérateur envisage d'utiliser un service qui permet d'accéder au contenu d'une telle base de données pour utiliser les données qu'elle contient, il doit s'assurer de le faire conformément aux exigences de la réglementation relative à la protection des données personnelles, en s'assurant notamment du fait qu'elle n'a pas été constituée de manière illicite.

B. BASE LÉGALE DES TRAITEMENTS

Les traitements visés ci-dessous ont tous pour base légale le respect d'une obligation légale (article 6.1.c du RGPD).

Les traitements qui concernent exclusivement la lutte contre la fraude sans relever de la lutte contre le blanchiment (certaines fraudes sont étrangères au blanchiment telles que, par exemple, la tentative de contournement d'une mesure d'interdiction de jeu) reposent sur une base légale différente, qui peut être celle de l'intérêt légitime.

- **Finalité de mise en œuvre des obligations de vigilance à l'égard de la clientèle conformément à l'approche par les risques**

L'obligation de vigilance qui pèse sur les opérateurs est prévue et décrite quant à ses modalités aux articles L. 561-4-1 et suivants du CMF. A cet égard, il résulte des dispositions de l'article

L. 561-10-1 du CMF que, lorsque le risque de blanchiment des capitaux et de financement du terrorisme présenté par une relation d'affaires, une offre ou une opération apparaît élevé, les opérateurs mettent en place des mesures de vigilance renforcées, qui consistent principalement à améliorer la connaissance de la clientèle et exercer une surveillance accrue des opérations de jeu.

- **Finalité de recherche des personnes qui doivent faire l'objet de mesures de vigilance complémentaires telles que les PPE au sens de l'article R. 561-18 du CMF**

Selon l'article L. 561-10 du CMF, les opérateurs appliquent des mesures de vigilance complémentaires notamment lorsqu'ils sont en présence d'une PPE ou d'une personne domiciliée dans un pays tiers

à haut risque ou encore lorsque l'offre ou l'opération présente, par sa nature, un risque particulier de blanchiment des capitaux ou de financement du terrorisme, notamment lorsqu'elles favorisent l'anonymat.

- **Finalité de mise en œuvre de mesures de gel des avoirs en application de sanctions financières**

Les opérateurs qui détiennent ou reçoivent des fonds d'un joueur sont tenus d'appliquer sans délai les mesures de gel prévues aux articles L. 562-4, R. 562-1 et R. 562-3 du CMF.

- **Finalité de réalisation de déclarations de soupçon**

Il est rappelé que, selon l'article L. 561-15 du CMF, les opérateurs sont tenus de déclarer au service TRACFIN les sommes ou les opérations portant sur des sommes dont ils savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an, d'une fraude fiscale ou sont liées au financement du terrorisme dans les conditions prévues aux articles L. 561-15, L. 561-30 2, R. 561-23, R. 561-24, R. 561-31 et D. 561-32-1 du CMF.

C. LES CATÉGORIES DE DONNÉES TRAITÉES

A titre préliminaire, il convient de rappeler que le « principe de minimisation » s'applique (il est renvoyé au point c) « Minimisation des données traitées » de la partie I.2.) aux données traitées en matière de LCB-FT et que, par conséquent, la collecte des informations ne peut être systématique et indifférenciée pour l'ensemble des personnes concernées.

Toutefois, la collecte de certaines informations (telles que les données relatives à l'identification et au justificatif de domicile et, en ce qui concerne les PPE et les personnes concernées au titre de mesures de vigilance renforcées, des informations sur l'origine des revenus et du patrimoine) est obligatoire.

En matière de LCB-FT, les données « non pertinentes » telles que le numéro de Sécurité sociale et le numéro fiscal ne doivent faire l'objet d'aucun traitement. Cependant, le traitement de ces informations peut, dans certaines hypothèses, être justifié par l'application d'un texte qui s'impose aux opérateurs. Elles ne sont alors plus considérées comme « non pertinentes » dans ce contexte (par exemple, en matière de gel des avoirs et d'interdiction de mise à disposition prévues par le CMF).

NB : Dans l'hypothèse où les entités assujetties peuvent traiter des données à caractère personnel visées aux articles 9 et 10 du RGPD (cf. art. 76 du Règlement (UE) 2024/1624), des conditions, présentées ci-dessous, devraient être remplies.

- article 9 du RGPD (catégories particulières de données à caractère personnel, telles que les données concernant la santé)
  - les entités assujetties doivent informer leurs clients ou clients potentiels que ces catégories de données peuvent être traitées aux fins du respect des exigences prévues dans le Règlement (UE) 2024/1624) ;
  - les données doivent provenir de sources fiables, exactes et à jour ;
  - les entités assujetties ne doivent pas prendre de décisions susceptibles de conduire à des résultats biaisés et discriminatoires sur la base de ces données ;
  - les entités assujetties doivent adopter des mesures pour garantir un niveau élevé de sécurité conformément à l'article 32 du règlement (UE) 2016/679, en particulier en ce qui concerne la confidentialité.

- article 10 du RGPD (données à caractère personnel relatives aux condamnations pénales et aux infractions)

En plus des conditions énoncées ci-dessus pour l'article 9 du RGPD, il convient que :

- ces données à caractère personnel concernent le blanchiment des capitaux, les infractions sous-jacentes associées ou le financement du terrorisme ;
- les entités assujetties aient mis en place des procédures permettant de distinguer, dans le traitement de ces données, les allégations, les enquêtes, les procédures et les condamnations, en tenant compte du droit fondamental à accéder à un tribunal impartial, des droits de la défense et de la présomption d'innocence.

a. Concernant les opérateurs de jeu en ligne :

Les opérateurs en ligne sont amenés à collecter des données intéressant la LCB-FT **dès l'entrée en relation d'affaires**, c'est-à-dire dès que le joueur ouvre un compte auprès d'eux (il est renvoyé au point i) « Le consentement, base légale de toute prospection commerciale à l'attention des clients » de la partie II.1.A.b)). Cette obligation d'identification des joueurs est prévue tant par la législation sur les jeux d'argent que par celle du code monétaire et financier. L'opérateur collectera ainsi les données suivantes : nom, prénom(s), sexe, pseudonyme(s) le cas échéant, date et lieu de naissance, adresse postale du joueur. La vérification de l'identité et du domicile (il est renvoyé au point i) « Le consentement, base légale de toute prospection commerciale à l'attention des clients » de la partie II.1.A.b)) sera réalisée au regard des documents que le joueur lui aura remis et dont la liste figure au II de l'article 4 du décret n° 2010 518 du 19 mai 2010 modifié (à défaut de vérification de l'identité effectuée en recourant aux moyens d'identification électronique définis aux 1° et 2° de l'article R. 561-5-1 du code monétaire et financier). C'est ainsi que l'identité du joueur sera vérifiée au moyen des pièces suivantes : copie de la carte nationale d'identité, passeport, permis de conduire, titre de séjour ou de sa carte de résident en cours de validité justifiant de son identité et de sa date de naissance. L'adresse postale sera établie, soit au regard du justificatif que le joueur lui aura transmis (qui peut être une quittance de loyer, une facture d'eau, de gaz, d'électricité, d'internet ou de téléphone ou son dernier avis d'imposition ou de non-imposition, cette liste n'étant pas limitative), soit à partir d'un code communiqué par l'opérateur au joueur à l'adresse postale renseignée par celui-ci.

L'opérateur collecte ensuite, **durant la vie du compte joueur**, certaines informations qui vont lui permettre d'apprécier l'existence d'un risque de blanchiment des capitaux. Sont visées ici toutes les données que l'opérateur est tenu de mettre à disposition de l'ANJ en application des articles 38 de la loi du 12 mai 2010 modifiée et 30 du décret n°2010-518 du 19 mai 2010 modifié ainsi que celles que l'opérateur doit nécessairement traiter en pratique pour la formation et l'exécution du contrat de jeux. Il s'agit notamment des données suivantes portant, d'une part, sur l'identité du joueur et l'activité « transactionnelle » du compte joueur (identifiant joueur, date d'ouverture du compte joueur et d'entrée en relation d'affaires, évaluation et composition du solde du compte, adresse IP du joueur, montant et nature des opérations, références du compte de paiement du joueur, modalité d'approvisionnement du compte) et, d'autre part, sur l'activité de jeu à proprement parler (prises de jeux effectuées et atypismes relevés (sure bet etc.), collusion dans les parties de jeux de cercle, utilisation de robots informatiques ou d'autres moyens susceptibles d'affecter la transparence et l'intégrité du jeu).

Au cours de la relation d'affaires, lors de la vie du compte, dans l'hypothèse où un **examen renforcé** est rendu nécessaire par la caractérisation d'une opération de jeux anormale, notamment parce qu'elle

est d'un montant inhabituel, l'opérateur doit ainsi que le prévoit l'article L. 561-10-2 du CMF, interroger le joueur sur l'origine des fonds qui lui ont servi à approvisionner son compte (joueur). Le joueur doit alors pouvoir justifier par tout moyen de cette origine, l'opérateur devant de son côté s'assurer que les justificatifs fournis sont probants. L'opérateur pourra recueillir les informations suivantes, en fonction de la situation du joueur :

- catégorie socioprofessionnelle, profession, nom de l'employeur, nature et niveau des revenus ;
- fiches de paie ;
- déclaration de revenus pour les professions libérales ;
- relevé de pension de retraite, d'invalidité ou alimentaire ;
- attestation notariée établissant l'attribution d'un héritage ;
- un document attestant de la mise en location de biens immobiliers appartenant au joueur (bail commercial, rural ou d'habitation) ;
- avis d'imposition dans le cas où les autres éléments collectés ne permettent pas d'attester de l'origine des fonds et sous réserve que le numéro de sécurité sociale et le numéro fiscal soient préalablement occultés.

En revanche, les opérateurs ne sont pas fondés à demander aux joueurs la copie d'un relevé bancaire ni celle de leur carte bancaire.

Concernant la collecte de ces informations, il convient de rappeler que les principes suivants doivent être respectés par les opérateurs :

- la collecte de ces documents ne pourrait intervenir qu'en cas de déclenchement d'une alerte et lorsque cela est nécessaire à la levée ou au renforcement du soupçon, et non de façon systématique et indifférenciée au moment de l'entrée en relation d'affaires ;
- d'une manière générale et pour respecter le principe de proportionnalité, il convient que les opérateurs limitent leurs demandes de documents les plus intrusifs aux cas dans lesquels des documents moins intrusifs se sont avérés insuffisants pour infirmer ou confirmer un soupçon ;
- la collecte de l'avis d'imposition ne pourrait intervenir que dans le cas où les autres documents pouvant être collectés ne permettraient pas d'attester de l'origine des fonds ;
- les opérateurs doivent s'abstenir de collecter des données non pertinentes. Si des données non pertinentes (telles que le numéro de sécurité sociale et le numéro fiscal dans certains cas) sont susceptibles de figurer sur des justificatifs, le joueur concerné peut s'il le souhaite fournir des documents caviardés. Dans l'hypothèse où il ne serait pas possible d'accepter des documents occultés (impossibilité technique liée à la conception des outils qui ne permettraient pas de les exploiter convenablement ou remise en cause de la validité ou de l'intégrité des documents, par exemple), l'opérateur pourrait, s'il le souhaite, procéder au caviardage ou proposer des méthodes alternatives compatibles avec la volonté des personnes de produire des pièces occultées, et ce en application du principe de minimisation.

Ces informations sur l'origine des fonds constituent des données sensibles (au sens commun du terme et non au sens du RGPD), ce qui implique que l'opérateur prenne les mesures techniques et organisationnelles appropriées pour préserver leur confidentialité et leur sécurité. La collecte de ces informations ne doit en tout cas être ni systématique ni indifférenciée. Elle suppose toujours une alerte préalable.

Les traitements automatisés qui peuvent être faits ici ne sauraient conduire à eux seuls au prononcé d'une décision à l'égard du joueur (il est renvoyé au point G) « Information des personnes concernées

» de la partie II.3.). Une intervention humaine est toujours requise, par exemple pour décider de mettre fin à la relation d'affaires avec le joueur.

Les opérateurs doivent mettre à jour les informations ainsi recueillies, et requérir du joueur toute pièce utile à cette fin, ceci pour avoir une connaissance appropriée et actualisée de la relation d'affaires, comme le prévoit le 2° de l'article R. 561-12 du CMF.

Enfin, la CNIL rappelle que les données collectées pour une finalité liée à la LCB-FT par les opérateurs ne peuvent faire l'objet de réutilisations, sauf si une telle réutilisation est expressément prévue par la loi.

b. Concernant les opérateurs de jeux en réseau physique de distribution (hors jeu sur compte) :

En réseau physique de distribution (hors jeu sur compte), la situation est différente en raison de l'anonymat des joueurs, ce qui constitue d'ailleurs une vulnérabilité du secteur.

Néanmoins, les opérateurs titulaires de droits exclusifs sont tenus de vérifier l'identité des joueurs en cas de mise ou de gain supérieur à 2 000 euros par transaction[84]. A cette fin, ils recueillent et vérifient, à l'instar des opérateurs en ligne, les nom, prénoms, date et lieu de naissance au regard de documents d'identité dont ils conservent la copie. Ce recueil et cette vérification s'imposent, en réseau physique de distribution et à la société La Française des Jeux uniquement, en cas de demande de paiement unique portant sur plusieurs lots ou gains dont le montant cumulé atteint ou dépasse 300 euros[85]. Les justificatifs que les opérateurs titulaires de droits exclusifs peuvent à ce titre réclamer aux joueurs sont identiques à ceux que les opérateurs en ligne sollicitent.

Les opérateurs titulaires de droits exclusifs sont plus généralement tenus de recueillir et vérifier cette identité lorsqu'ils ont des raisons de soupçonner qu'un joueur cherche à se livrer à une opération de blanchiment ou financer le terrorisme, même dans le cas où ce seuil de 2 000 euros n'est pas atteint. En effet, certaines opérations de jeu peuvent, au regard de leur objet (prise de paris sur des cotes peu élevées), de leur montant ou de leur chronologie (fractionnement de mises), contraindre l'opérateur, directement ou par l'intermédiaire de son mandataire, à vérifier l'identité du joueur et, si les circonstances l'imposent, le conduire à demander au joueur de justifier de l'origine de ses revenus. Les données traitées à cette fin sont identiques à celles qu'un opérateur en ligne pourrait traiter. Cette demande sur l'origine des fonds peut également s'imposer dans le cas où l'opérateur a vérifié l'identité du joueur qui a misé plus de 2 000 euros, cette seule vérification d'identité étant parfois susceptible d'être insuffisante au regard des circonstances.

Lorsque des traitements de données personnelles sont mis en œuvre dans les contextes qui précèdent, il convient de veiller au respect de l'ensemble des obligations prévues par la réglementation applicable, et notamment au respect de l'obligation d'information des personnes concernant les traitements de données personnelles mis en œuvre, au moyen par exemple de mentions d'informations rédigées et communiquées conformément aux exigences des autorités de contrôle[86].

84 - Articles L. 561-13, R. 561-10 et D. 561-10-2 du CMF.
85 - Article 11 du décret n° 2019-1061 du 17 octobre 2019.
86 - https://www.cnil.fr/fr/exemples-de-formulaire-de-collecte-de-donnees-caractere-personnel

En réseau physique de distribution, la collecte des données est le plus souvent réalisée, non par l'opérateur titulaire de droits exclusifs lui-même, mais par son mandataire qui, lorsqu'il agit en son nom et pour son compte, est considéré comme son sous-traitant au sens du RGPD (il est renvoyé au point vi) « Le sous-traitant » de la partie I.1.a)) du présent guide). Le contrat de sous-traitance devra organiser cette collecte et, plus généralement, tous les traitements de données que le mandataire sera amené à accomplir.

D. ACCÉDANTS, DESTINATAIRES ET TIERS AUTORISÉS

La transmission des données traitées au titre de la LCB-FT est soumise au régime de droit commun des transmissions de données et il est renvoyé sur ce point à la partie « Accédants, destinataires et tiers autorisés » du II.B du présent guide, sous réserve des précisions qui suivent.

S'agissant des **accédants, au sein donc du responsable de traitement**, les personnes qui ont accès aux données doivent justifier de l'intérêt qu'elles ont à en connaître. Ces données doivent ainsi être accessibles aux personnes en charge de la LCB-FT chez l'opérateur. Naturellement, les personnes habilitées à prendre la décision de nouer ou de maintenir une relation d'affaires avec une PPE doivent également avoir accès aux informations concernant ces personnes.

Les personnes en charge du service client de l'opérateur ont seulement vocation à être informées de l'existence d'une alerte au titre de la LCB-FT concernant le joueur afin qu'elles fassent preuve de vigilance lorsqu'elles échangent avec lui. L'existence d'une telle alerte peut être portée à la connaissance du service client par l'apposition d'un code particulier (par exemple «<!> LCB-FT») dans le fichier client. Les personnes en charge du service client de l'opérateur peuvent néanmoins être elles-mêmes directement amenées, lors de leurs discussions avec les joueurs, à déceler des signes d'un possible blanchiment, qu'il leur incombe alors de signaler aux équipes dédiées à la LCB-FT. En tout état de cause, elles ne sauraient être informées de l'existence, et encore moins du contenu, d'une déclaration de soupçons[87].

S'agissant des **destinataires**, seuls les acteurs impliqués en matière de LCB-FT peuvent se voir transmettre les données personnelles y afférentes. C'est notamment le cas de l'ANJ et de la cellule de renseignement financier TRACFIN et, s'agissant des joueurs qui font l'objet d'une mesure de gel des avoirs, du ministre chargé de l'économie.

Les sous-traitants des opérateurs au sens du RGPD, c'est-à-dire ceux qui traitent des données pour leur compte sans déterminer les finalités du traitement, peuvent également être destinataires de ces données, sous la condition que cette transmission soit nécessaire à l'exercice de leur mission. Le contrat de sous-traitance doit strictement encadrer le traitement de données qui en résulte[88]. Certaines données pouvant revêtir un caractère sensible, les opérateurs devraient ici être particulièrement vigilants dans la sélection et le contrôle des sous-traitants impliqués en matière de LCB-FT.

Les opérateurs titulaires de droits exclusifs peuvent être amenés à transmettre des données concernant les personnes qui exploitent en leur nom et pour leur compte des postes d'enregistrement, sous les conditions et selon les modalités du contrat qui les lient.

87 - sauf dans l'hypothèse exceptionnelle de l'urgence qui peut conduire à ce qu'elles procèdent elles-mêmes à une déclaration de soupçon.
88 - Sur la sous-traitance, v. https://www.cnil.fr/fr/sous-traitant, notamment sur le Guide pour les sous-traitants.

Enfin, l'article 2.2 du cadre de référence pour la fraude et la LCB-FT adopté par arrêté du 9 septembre 2021 dispose : « *Lorsqu'un opérateur fait partie d'un groupe, l'organisation et les procédures peuvent être mises en œuvre au niveau du groupe mais doivent tenir compte des spécificités propres à l'activité de chaque entité. Ces procédures prévoient également le partage des informations au sein du groupe, la protection des données à caractère personnel ainsi que les mesures de contrôle interne* ». Les opérateurs doivent veiller à ce que les informations qu'ils transmettent aux sociétés de leur groupe (étant précisé que de telles transmissions doivent être exclusivement destinées aux services en charge de la LCB-FT) le soient dans un cadre sécurisé et dans la stricte mesure des besoins de la lutte contre le blanchiment. Les transferts auprès des entreprises du groupe qui se situent dans l'Union européenne et qui sont, par suite, soumises au RGPD, ne posent pas de difficultés spécifiques. En revanche, les transferts réalisés à l'extérieur de l'Union européenne ne peuvent être réalisées qu'à certaines conditions (décision d'adéquation, clauses contractuelles types, règles d'entreprises approuvées par le Comité européen à la protection des données, cette dernière solution étant conçue pour les entreprises qui souhaitent avoir une politique de données intra-groupe en matière de transfert de données personnelles hors de l'Union européenne). Sur ce dernier point, il est renvoyé à la partie introductive du présent guide, relative à la mise en place de procédures internes (voir le point 4) « Mettre en place des procédures internes et regrouper la documentation nécessaire » de la partie I.1. du présent guide).

Pour plus de précisions sur les exigences en matière de traçabilité et des politiques d'accès, il est renvoyé à la première partie du Guide « sécurisation des données » de la CNIL, consultable en suivant ce lien.

E. TRAITEMENTS DEVANT DONNER LIEU À UNE AIPD

Pour mémoire, l'article 35 du RGPD prévoit qu'une analyse d'impact est requise lorsqu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* ». Sur ce point, voir le 5) « Réaliser une étude d'impact lorsque cela est nécessaire » de la partie I.1.b).

En outre, le CEPD a défini neuf critères permettant de regarder un traitement comme susceptible d'engendrer un risque élevé, lesquels ont été repris par le Comité européen à la protection des données (CEPD) et par la CNIL.

En matière de LCB-FT, plusieurs critères sont potentiellement réunis : des profils de joueurs sont définis en fonction de leurs comportements de jeux ; le traitement peut conduire un opérateur à priver un joueur du bénéfice d'un droit ou d'un contrat (suspension, voire clôture du compte joueur ; gels de ses avoirs) ; des données à caractère hautement personnel peuvent être collectées ; des croisements de données peuvent avoir lieu (ce qui est le cas lorsque le fichier des personnes politiquement exposées ou celui des personnes frappées de mesures de gel est croisé avec celui des joueurs ayant un compte chez l'opérateur).

La CNIL considère en conséquence que les opérateurs sont dans l'obligation d'effectuer une analyse d'impact s'agissant des traitements de données dès lors qu'ils mettent en œuvre un traitement pour la LCB-FT.

F. DURÉE ET MODALITÉS DE CONSERVATION

S'agissant du jeu « en ligne » et du jeu sur compte des monopoles, la durée de conservation des données est de :

- **six ans à compter de la clôture du compte joueur concerné**[89] en ce qui concerne les données limitativement énumérées à l'article 30 décret n°2010-518 du 19 mai 2010 ;
- **cinq ans à compter de la clôture de leurs comptes joueurs** ou de la cessation de leurs relations avec eux[90] en ce qui concerne les **documents et informations**, quel qu'en soit le support, relatifs à leurs **relations d'affaires**, ainsi qu'aux mesures de vigilance mises en œuvre (dont font par exemple partie leurs demandes auprès de certains de leurs clients concernant leurs ressources ainsi que les réponses éventuellement obtenues) ;

- **cinq ans à compter de leur exécution**, en ce qui concerne les documents et informations relatifs aux **opérations** faites par leurs clients, ainsi que les documents consignant les caractéristiques des opérations mentionnées à l'article L. 561-10-2 du CMF.

S'agissant du jeu proposé en réseau physique de distribution, à l'exclusion du jeu sur compte, les dispositions de l'article L. 561-12 du CMF fixant une durée de conservation des données pour les opérateurs à **5 ans** trouvent à s'appliquer[91]. Spécialement, l'article R. 561-22-2 du même code prévoit que les opérateurs conservent pendant une durée de 5 ans sur un registre les nom, prénoms, adresse, date et lieu de naissance des joueurs qui ont misé ou gagné plus de 2 000€ par transaction, ainsi que le montant exact des sommes ainsi misées ou gagnées.

Les données traitées pour la finalité LCB-FT doivent être particulièrement protégées (conformément aux dispositions de l'article 32 du RPGD), notamment parce que certaines d'entre elles peuvent être regardées comme des données à caractère hautement personnel. Il s'ensuit, en pratique, que le fichier contenant ces données doit être sécurisé en conséquence et son accès limité au droit d'en connaître.

Un journal des accès à ce fichier doit être tenu, pour permettre d'identifier les personnes qui l'ont consulté ainsi que le moment auquel cette consultation a eu lieu.

Organiser la conservation des données personnelles

Une donnée personnelle peut être utilisée pour plusieurs finalités successives, chacune avec sa propre durée de conservation.

Par ailleurs, une même donnée personnelle peut être utilisée pour des traitements distincts et pour des durées différentes. L'archivage ou la suppression de cette donnée dans l'un des traitements n'interdit pas de continuer à utiliser cette même donnée dans un autre traitement.

Dans ce cas, la CNIL rappelle qu'il est nécessaire de bien distinguer les deux opérations et de leur appliquer à chacune une durée pertinente par rapport à leur objectif. Ainsi, les données liées à la durée la plus longue seront conservées. Pour les autres utilisations (durée plus courte), les données ne pourront plus être utilisées une fois cette durée écoulée.

89 - Article 31 du décret n°2010-518 du 19 mai 2010 modifié.
90 - Article L. 561-12 du CMF.
91 - Articles L. 561-13, R. 561-10 et D. 561-10-2 du CMF.

G. INFORMATION DES PERSONNES CONCERNÉES

L'information à délivrer aux personnes concernées par un traitement relatif à la LCB-FT est soumise au régime de droit commun de l'information des personnes, prévu aux articles 12 à 14 du RGPD. Le fait que les traitements visent à la protection de l'ordre public ne dispense pas l'opérateur de son obligation d'informer les joueurs de ce qu'il procède à des traitements pour les besoins de la LCB-FT. Les personnes dont les données font l'objet d'un traitement doivent être informées de la base légale, des finalités, de la durée de conservation, ainsi que de la manière d'exercer leurs droits. Cette information doit être préalable aux traitements. En pratique, la CNIL recommande que les opérateurs portent cette information à la connaissance des joueurs en même temps qu'ils demanderont à ces derniers d'accepter leur règlement portant conditions générales de leur offre de jeux.

En revanche, l'opérateur n'a pas à exposer aux joueurs la manière dont il traite ces données, dès lors qu'une telle information pourrait compromettre la détection des infractions qu'il s'agit d'identifier.

S'agissant du détail des modalités de l'information des joueurs sur les traitements, il est renvoyé au point f) « Droit des personnes » de la partie I.2. du présent guide. S'agissant du support de l'information, il est rappelé en ce qui concerne les opérateurs de jeux en ligne que la politique de protection des données personnelles doit figurer sur le site internet des opérateurs de la manière la plus visible possible et dans une rubrique dédiée et être accessible via un lien hypertexte dans le formulaire de création de compte. Pour les opérateurs « en dur », la CNIL recommande à titre de bonnes pratiques que l'information soit diffusée également sur un support matériel pour s'adapter à l'environnement physique. Il peut s'agir d'un panneau d'information et/ou d'une fiche d'information complète disponible dans un lieu facilement accessible, par exemple au guichet du point de vente physique. Pour des exemples de mentions d'information à destination des clients, cf. recommandations de la CNIL consultables à l'adresse suivante : https://www.cnil.fr/fr/passer-laction/rgpd-exemples-de-mentions-dinformation.

H. DROIT DES PERSONNES

Les droits des personnes sur leurs données personnelles sont restreints en matière de LCB-FT.

Ainsi, selon l'article L. 561-45 du CMF, le droit d'accès aux traitements mis en œuvre aux seules fins de l'application des dispositions relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme s'exerce auprès de la CNIL selon une procédure de droit d'accès indirect. En tout état de cause, le joueur ne saurait, directement ou indirectement, avoir accès à la déclaration de soupçon dont il a pu faire l'objet, la divulgation de cette déclaration exposant son auteur aux peines prévues à l'article L. 574-1 du CMF.

Le droit à l'effacement ne s'applique pas, le traitement étant nécessaire pour respecter une obligation légale à laquelle le responsable du traitement est soumis.

Le droit d'opposition des traitements est également inapplicable puisque les traitements en question sont fondés sur une obligation légale. S'agissant du jeu sur compte, l'article 2 du décret n° 2010-518 du 19 mai 2010 modifié écarte expressément ce droit d'opposition. La portabilité des données est ici écartée, le traitement répondant à une obligation légale.

En revanche, les personnes dont les données sont traitées peuvent exercer leurs droits à rectification et à la limitation des traitements.

Autorité nationale des jeux
11 boulevard Gallieni
92130 Issy-les-moulineaux

www.anj.fr