Apps de rencontre & données sensibles : « Le match de trop ? »

5 février 2026 - Université AFCDP des DPO

Mathias | Avocats

Notre empreinte numérique au quotidien

Stache Passions

tinder

Meetup

bumble

MOBILE POTESPORT APP

Les sites de rencontre sont **de plus en plus nombreux et diversifiés** (en fonction de l'orientation politique, sexuelle, religieuse etc.). Ainsi, ils font désormais **partie intégrante de notre quotidien**.

En mars 2020, l'application de rencontre Tinder a connu un pic à 3 milliards de swipe par jour.

LINC - Apps de rencontre et données personnelles : « c'est un match ! »

Notre empreinte numérique au quotidien

Couleur des yeux

Signe astrologique

Jours et heures de connexion

Photos

Taille

Âge

Numéro de téléphone

Nombre de swipe

Nom

Orientation sexuelle

Vidéos

Convictions religieuses

E-mail

Opinions politiques

Traits de personnalité

Statut professionnel

Temps passé sur l'application

Prénom

Couleur des cheveux

Poids

Centres d'intérêts

Origines ethniques

Goûts musicaux

Souvenons-nous …

Affaire Maximilian Schrems contre Meta Platforms Ireland Limited

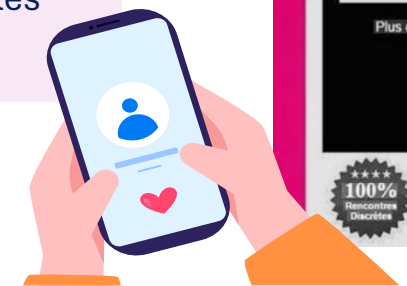
«*La circonstance qu'une personne se soit exprimée sur son orientation sexuelle lors d'une table ronde, dont la participation est ouverte au public,* ***n'autorise pas l'exploitant d'une plateforme de réseau social en ligne à traiter d'autres données relatives à l'orientation sexuelle de cette personne, obtenues, le cas échéant, en dehors de cette plateforme*** ***à partir d'applications et de sites Internet de tiers partenaires,*** ***en vue de l'agrégation et l'analyse de celles-ci, afin de lui proposer de la publicité personnalisée****.* »

« *Le principe de la «* ***minimisation des données*** *», prévu à cette disposition****, s'oppose à ce que l'ensemble des données à caractère personnel*** *qui* ***ont été obtenues par un responsable du traitement****, tel que l'exploitant d'une plateforme de réseau social en ligne,* ***auprès de la personne concernée ou de tiers*** *et qui ont été* ***collectées tant sur cette plateforme qu'en dehors de celle-ci****, soient* ***agrégées, analysées et traitées à des fins de publicité ciblée, sans limitation dans le temps et sans distinction en fonction de la nature de ces données*****. »**

CJUE, 4 octobre 2024, affaire C-446/21, *Maximilian Schrems contre Meta Platforms Ireland Limited*

Affaire Ashley Madison, de la violation de données personnelles au drame humain (2015)

Les données personnelles de 32 millions de comptes ont été exfiltrées (violation de données), provoquant notamment des suicides chez les personnes concernées, ainsi que des contentieux.



Rappel - Quelques définitions (1/2)

Données à caractère personnel

«données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

Article 4§1 du règlement général sur la protection des données (RGPD)

Dans un **arrêt CRU en date du 4 septembre 2025 (affaire C-413/23), la Cour de justice de l'Union européenne** a considéré que :

« des données pseudonymisées ne doivent pas être considérées comme constituant, en toute hypothèse et pour toute personne, des données à caractère personnel aux fins de l'application du règlement 2018/1725, dans la mesure où la pseudonymisation peut, selon les circonstances de l'espèce, effectivement empêcher des personnes autres que le responsable du traitement d'identifier la personne concernée de telle manière que, pour elles, celle-ci n'est pas ou n'est plus identifiable ».

«Les informations relatives à une personne physique ne sont pas nécessairement des données à caractère personnel pour toute autre personne ou entité du simple fait qu'une autre entité peut identifier cette personne physique. Les informations ne revêtent pas de caractère personnel pour une entité donnée lorsque ladite entité ne peut identifier la personne physique à laquelle elles se rapportent, compte tenu des moyens raisonnablement susceptibles d'être utilisés par cette entité. Ces informations ne se muent pas en informations à caractère personnel pour cette entité du simple fait qu'un destinataire ultérieur éventuel dispose de moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique à laquelle les informations se rapportent.»;

La **proposition de règlement « omnibus numérique » publiée le 19 novembre 2025 par la Commission européenne** prévoit, en son **article 3**, une modification de la définition de la donnée à caractère personnel.

Rappel - Quelques définitions (2/2)

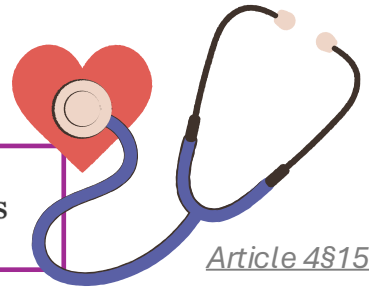
Catégorie particulière de données personnelles

Selon la CNIL :

> Les données sensibles forment une catégorie particulière des données personnelles.
>
> Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Données de santé

> 15. «données concernant la santé», 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;



Article 4§15 du RGPD

Personnes Vulnérables

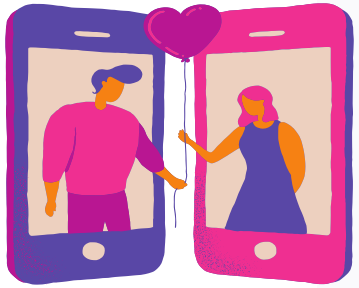
*« Peuvent être considérés comme des personnes concernées vulnérables, **les enfants** (qui peuvent être vus comme incapables de s'opposer ou de consentir sciemment et de manière réfléchie au traitement de leurs données**), les employés**, les segments les plus vulnérables de la population nécessitant une protection particulière **(personnes souffrant de maladie mentale, demandeurs d'asile et personnes âgées, patients, etc.)** et, en tout état de cause, **toutes autres personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié.** »*

Lignes directrices du CEPD

Quid des applications de rencontre utilisant de l'IA ?

Certaines applications de rencontre **utilisent de l'intelligence artificielle,** par exemple pour prédire la réussite de la relation : C'est le cas de Keez.

L'usage de l'IA par les applications de rencontre doit respecter les principes posés par le RGPD.



L'amour est une science

Keez n'est pas un jeu de hasard. Notre IA (LLM & Machine Learning) analyse votre profil à travers les grands modèles de la psychologie moderne pour prédire la réussite de la relation :

- **Modèle du Big Five** (Traits de personnalité)
- **Théorie de l'attachement** (Votre façon d'aimer)
- **Théorie des filtres** (Valeurs, mode de vie, projets)

Source : site de Keez

IA - Comment se mettre en conformité ?

IA : les grands principes pour se mettre en conformité

Phase de développement et de déploiement

Comme tout traitement de données personnelles, la collecte et l'utilisation de données via un système d'IA doit respecter le RGPD et les droits des personnes.

Développement des systèmes d'IA : les recommandations spécifiques

Retrouvez les recommandations de la CNIL sur l'application du RGPD au développement des systèmes d'intelligence artificielle et à la constitution de bases de données d'apprentissage.

Consulter les articles de la CNIL

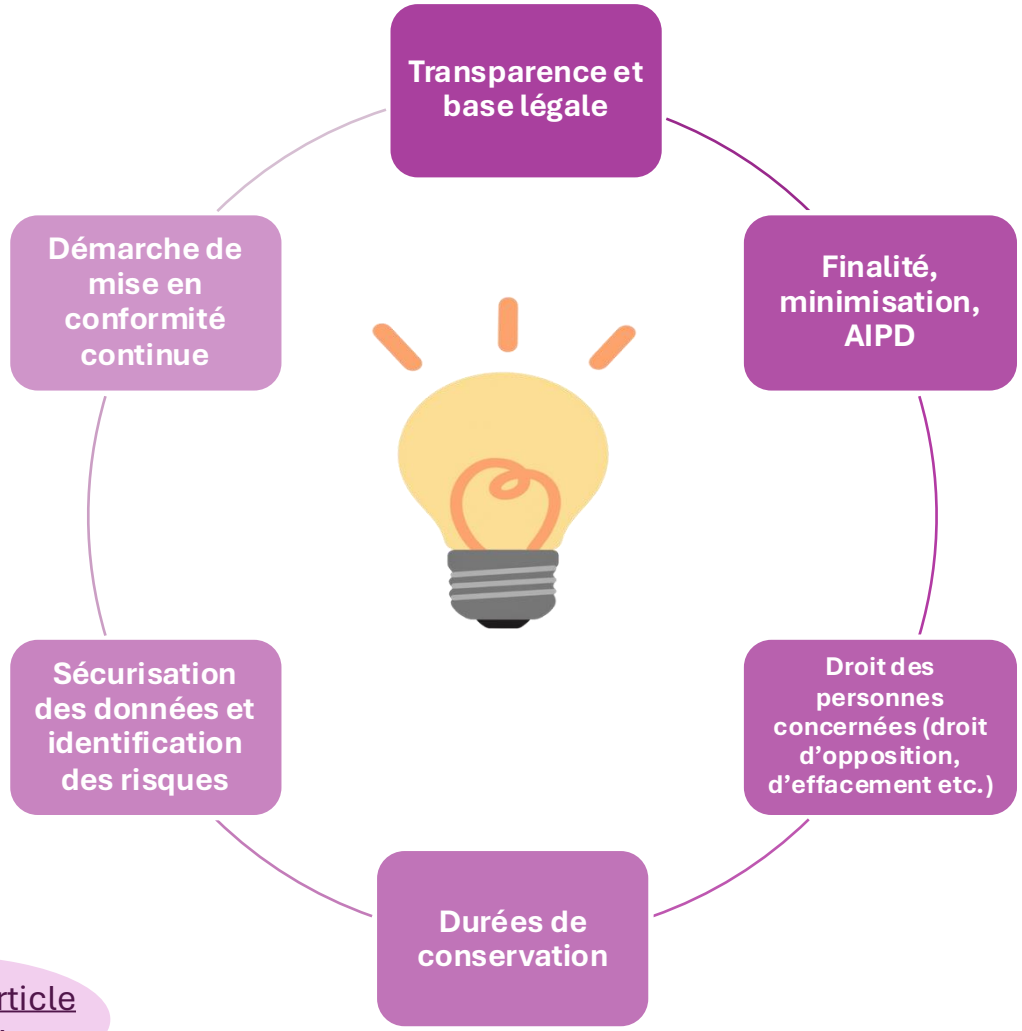
IA : comment être en conformité avec le RGPD ?

05 avril 2022

L'intelligence artificielle pose des questions cruciales et nouvelles, tout particulièrement au regard de la protection des données. La CNIL rappelle les grands principes de la loi Informatique et Libertés et du RGPD à suivre, ainsi que ses positions sur certains aspects plus spécifiques.

Consulter l'article de la CNIL

Rappel - Les grands principes du RGPD



Focus – Respect du principe d'information – Caméras piétons.
Arrêt de la CJUE en date du 18 décembre 2025, affaire C-422/24

« Seule la source des données à caractère personnel collectées constitue le critère pertinent aux fins de la délimitation des champs d'application respectifs des articles 13 et 14 du RGPD ».

« Les informations les plus importantes à destination de la personne concernée peuvent être indiquées, dans le cadre d'un premier niveau, sur un panneau d'avertissement, et les autres informations obligatoires peuvent être fournies à celle-ci, au titre d'un second niveau, de manière appropriée et complète, dans un lieu facilement accessible ».

Rappel : Principe d'interdiction de la reconnaissance faciale

Consulter l'article de la CNIL

les applications de rencontre doivent respecter ces principes

Rappel - Les grands principes du RGPD : l'analyse d'impact sur la protection des données (AIPD)

Une analyse d'impact sur la protection des données, ou AIPD (en anglais *Privacy Impact Assessment*, ou PIA) doit obligatoirement être menée par l'organisme quand **le traitement est *« susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées »* (RGPD, article 35, 1.).**

Comment déterminer si une AIPD est nécessaire ?

→ **Les autorités européennes ont défini 9 critères, notamment :**

- ✓ Prise de décision automatisée avec effet juridique ou effet similaire significatif ;
- ✓ Surveillance systématique ;
- ✓ Données traitées à large échelle ;
- ✓ Données concernant des personnes vulnérables (patients, personnes âgées, enfants, salariés, etc.) ;
- ✓ Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- ✓ Traitements de nature à empêcher les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat (exclusion du bénéfice d'un droit/contrat).
- ✓ Évaluation/notation/*scoring* (y compris le profilage).

→ **Pour la CNIL, la réunion de deux critères justifie qu'une AIPD soit menée.**

DPO : quelques recommandations

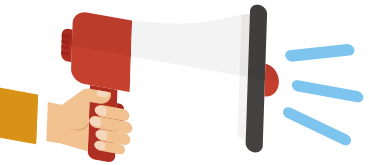
Respecter le principe de minimisation et de conservation limitée.

Adopter des politiques de protection des données et des conditions générales d'utilisation (CGU) transparentes, renforçant la confiance des utilisateurs.

Veiller à adopter des mesures de sécurité adaptées au risque (authentification à double facteur, etc.)

Protection de la vie privée : désactiver par défaut les pixels de suivi avant le recueil du consentement. Refuser les cookies.

Veiller à déterminer les finalités explicites, et recueillir le consentement <u>exprès</u> des personnes pour le traitement des données sensibles (orientation sexuelle, politique, religieuse etc.).



Quelques sanctions prononcées par la CNIL

Dans le cadre d'une procédure de sanction simplifiée en date du 30 avril 2025, la CNIL a sanctionné une société éditant un site web de rencontres destine aux personnes partageant des convictions politiques similaires **en raison de manquements concernant notamment le consentement des personnes (données sensibles), ainsi que le défaut de sécurité des données.**

Le 15 décembre 2016, la CNIL a prononcé une sanction à l'égard d'un site de rencontre, en raison notamment du **manquement a l'obligation de recueillir le consentement exprès des personnes pour le traitement de données sensibles (données relatives à la vie sexuelle).** Le site de rencontre avait fait l'objet en 2015 d'une mise en demeure, au même titre que 7 autres sites de rencontre.

Focus sur les Data Brockers

Le 30 décembre 2025, la CNIL a prononcé une sanction de 3,5 millions à l'encontre d'une société **pour avoir transmis les données des membres de son programme de fidélité à un réseau social, et ce, à des fins publicitaires.**

Dans une décision en date du 27 novembre, l'autorité Belge de protection des données a sanctionné un courtier en données d'une amende de 40 000 euros **pour avoir vendu des données à des fins de marketing sans consentement préalable.**

Utilisateurs : quelques recommandations

Au moment de votre inscription

- ✓ **Privilégier les sites et applications fiables et sécurisés** (applications d'éditeurs de confiance etc.)
- ✓ **Regarder la politique de confidentialité**
- ✓ **Créer un compte avec prudence** (utilisation d'un mot de passe robuste, utilisation d'un pseudonyme etc.)
- ✓ **Veiller à limiter les informations personnelles que vous communiquez** (données sensibles)
- ✓ **Faites attention aux permissions que vous accordez sur votre téléphone** (permissions excessives etc.)

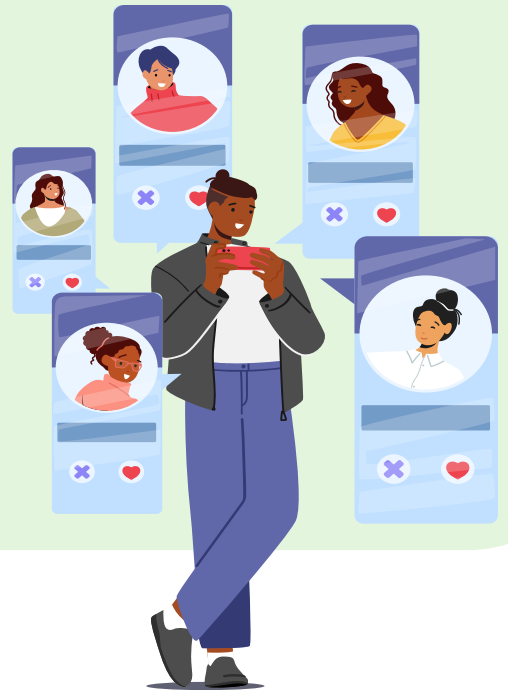
Pendant l'utilisation de l'application

- ✓ **Conserver la maîtrise de votre image** (photos intimes, republication de vos photos etc.)
- ✓ **Limiter la géolocalisation de votre application mobile**
- ✓ **Exercer vos droits quand vous le souhaitez** (droit d'accès, droit à la portabilité etc.)

Consulter les recommandations de la CNIL

Lorsque vous cessez d'utiliser l'application

- ✓ **Demander la suppression de vos données personnelles, et assurez vous que l'application supprime vos informations** (match, profil, etc.) et ne se borne pas à désactiver le compte



Mathias | Avocats

Pour aller plus loin

IA, cybersécurité, data : le livre qu'il vous faut pour garantir votre conformité numérique !

Cet ouvrage contient les clés pour saisir ces nouveaux enjeux juridiques : Gouverner, concevoir, contractualiser, Gérer les crises, et anticiper.

Vivant et actuel, cet ouvrage rassemble les retours d'expérience de professionnels reconnus du monde numérique.

Disponible dès maintenant chez votre libraire !

Notre expertise à votre service

Une newsletter gratuite

L'actualité décryptée pour vous

Utilisation des caméras augmentées dans l'espace public (vidéoprotection algorithmique) : actualités et cadre juridique

10 Fév, 2026 | Conformité, Données personnelles / DPO, Intelligence artificielle

De nombreux acteurs s'interrogent sur la possibilité de recourir aux caméras « augmentées », notamment dans le contexte des élections municipales en 2026. Objectifs de sécurité, respect des libertés et droits fondamentaux, du Règlement général sur la...

lire plus

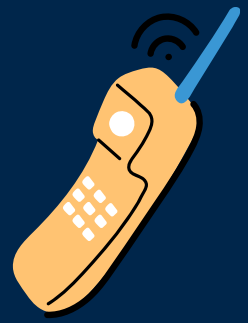
Droit de rectification : comment le mettre en œuvre ?

23 Jan, 2026 | Conformité, Données personnelles / DPO

L'article 16 du Règlement général sur la protection des données (RGPD) précise les conditions et les modalités selon lesquelles « La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification...

lire plus

CONTACTEZ-NOUS !



Mathias Avocats
19 rue Vernier, 75017 Paris
+33 (0)1 43 80 02 01
contact@avocats-mathias.com
www.avocats-mathias.com

Abonnez-vous à notre Newsletter
pour retrouvez toute l'actualité juridique.

Suivez-nous sur les réseaux sociaux