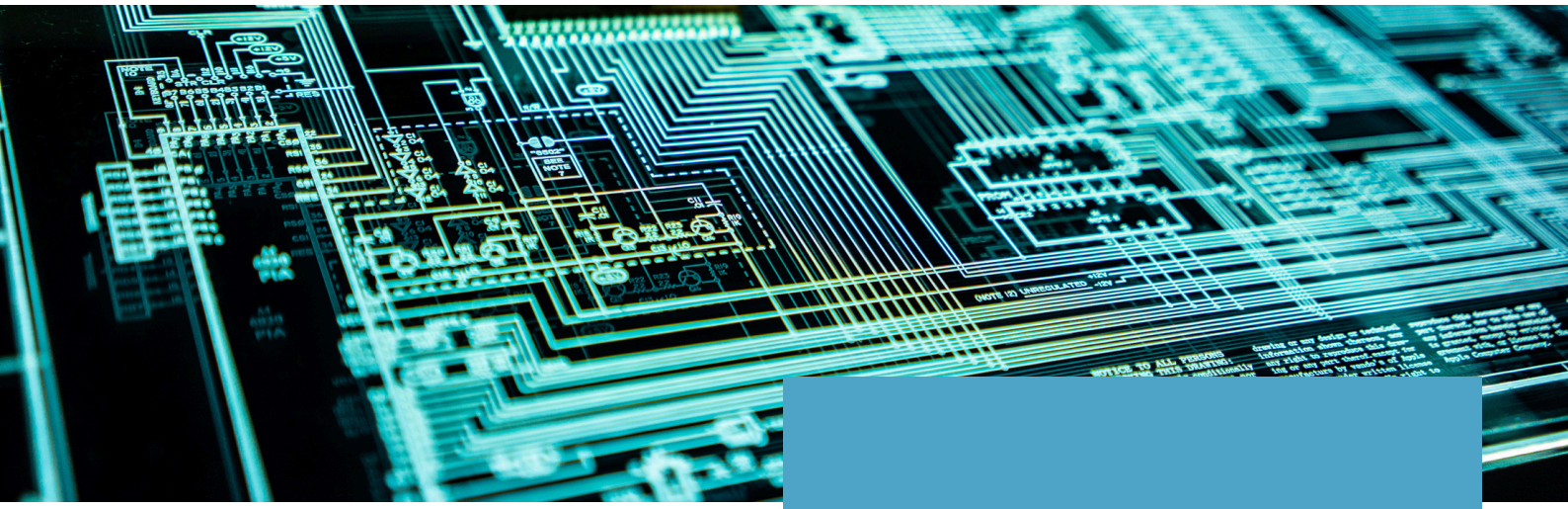
NEWSLETTER

TECH / DATA



DANS CE NUMÉRO

X n'est pas un "contrôleur d'accès"

Après analyse, la Commission européenne a conclu que le réseau social X (ex-Twitter) ne remplit pas les critères du DMA pour être désigné comme "contrôleur d'accès"

ACTUALITÉS NOUVELLES TECHNOLOGIES

Abritel gagne contre la Ville de Paris

Cour d'appel de Paris, Pôle 1 – Ch. 3, 22 octobre 2024, Ville de Paris / Homeaway UK Limited & EG Vacation Rentals Ireland Limited

La Cour d'appel a statué sur le différend entre la Ville de Paris et les sociétés Homeaway UK Limited et EG Vacation Rentals Ireland Limited, exploitant la plateforme Abritel, accusées de ne pas avoir transmis certaines données de locations de meublés de tourisme pour 2018 et 2019, en violation du code du tourisme. La Ville de Paris, réclamant une amende de 93,75 millions d'euros, avait vu ses demandes rejetées en première instance, décision qu'elle avait contestée en appel.

Dans ce litige, la Ville de Paris s'appuyait sur plusieurs dispositions du code du tourisme français. Selon l'article L. 324-2-1, toute plateforme d'intermédiation en ligne doit transmettre aux communes, lorsqu'elles le demandent, les informations sur le nombre de jours pendant lesquels les meublés de tourisme ont été loués par son intermédiaire. Cette obligation s'inscrit dans le cadre d'une réglementation visant à contrôler les locations de courte durée pour éviter la transformation des logements en locations exclusivement touristiques. En vertu des articles R. 324-2 et R. 324-3, les communes peuvent exiger la transmission d'informations une fois par an, avec un délai d'un mois pour leur transmission par voie électronique. La Ville de Paris reprochait à Homeaway UK Limited de ne pas avoir transmis ces informations, ce qui, selon elle, constituait un manquement à ces dispositions réglementaires et législatives.

Dans son analyse, la Cour a d'abord considéré que les services de mise en relation en ligne fournis par Homeaway relèvent des « services de la société de l'information » et sont ainsi couverts par la directive européenne 2000/31/CE. Selon cette directive, les services en ligne sont soumis aux règles du pays d'établissement de la société, en l'occurrence le Royaume-Uni pour Homeaway UK Limited avant 2021, ce qui signifie que les obligations supplémentaires imposées par le code du tourisme français ne peuvent s'appliquer.

La Cour a ensuite étudié les dérogations possibles au principe de libre circulation des services prévues par la directive. Elle a rappelé que les États membres peuvent imposer des obligations supplémentaires pour des raisons d'ordre public ou de protection des consommateurs, mais que ces mesures doivent être proportionnées, spécifiques et ciblées. La Cour a conclu que les articles du code du tourisme susvisés ne répondaient pas à ces critères, étant généraux et s'appliquant indistinctement à toutes les plateformes de location en ligne. Ces dispositions étaient donc inapplicables aux défenderesses.

De plus, la directive exige que tout État membre notifiant des mesures restrictives en informe préalablement la Commission européenne, ce qui n'avait pas été fait par la France pour ces dispositions du code du tourisme. Ce manquement procédural a renforcé la position de la Cour quant à l'inapplicabilité de ces obligations aux entreprises établies dans un autre État membre de l'UE.

La Cour a également constaté que les exigences françaises de transmission de données imposaient une charge administrative importante aux deux sociétés, entraînant des adaptations techniques et organisationnelles incompatibles avec le cadre légal du pays d'origine de Homeaway. Ces contraintes supplémentaires, non prévues dans le pays d'établissement, venaient contredire le principe de libre prestation de services établi par la directive.

En conclusion, la Cour d'appel a confirmé la décision de première instance en rejetant les demandes de la Ville de Paris, au motif que les obligations du code du tourisme n'étaient pas opposables aux sociétés défenderesses en vertu de la directive européenne. Elle a ainsi condamné la Ville de Paris à payer les dépens et une somme de 20 000 euros à Homeaway UK Limited.

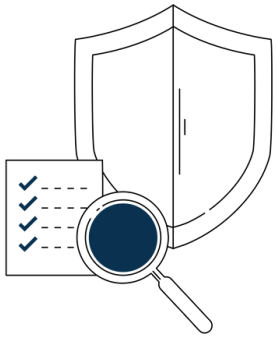
ACTUALITÉS NOUVELLES TECHNOLOGIES

Le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité déposé au Sénat

Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécuritéei_prmd2412608l_cm_15.10.2024.pdf

Le 15 octobre 2024, le Conseil des ministres a présenté un projet de loi sur la résilience des infrastructures critiques et le renforcement de la cybersécurité, visant à transposer trois directives européennes pour renforcer la sécurité nationale et la lutte contre les cybermenaces. Une étude d'impact accompagne ce projet.

Directive - 2022/2557 - EN - EUR-Lex
Directive - 2022/2557 - EN - CER - EUR-Lex

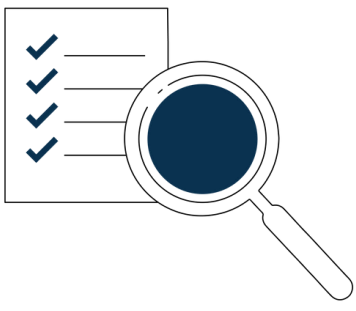


Ce texte transpose notamment la directive (UE) 2022/2557 sur la résilience des entités critiques (REC), qui impose aux États membres de garantir une protection minimale de leurs infrastructures essentielles, couvrant des secteurs tels que l'énergie, la santé, et les infrastructures numériques.

Directive - 2022/2555 - FR - EUR-Lex

La deuxième directive transposée est la directive (UE) 2022/2555, dite NIS2. Celle-ci élargit les obligations de cybersécurité aux entités qualifiées d'essentielles et importantes, pour faire face à l'augmentation des cyberattaques visant des PME, des collectivités locales et des hôpitaux. Ce cadre étendu couvrira en France environ 15 000 entités dans 18 secteurs.

Règlement - 2022/2554 - FR - EUR-Lex
Directive - 2022/2556 - FR - EUR-Lex



Enfin, le projet inclut le Règlement Digital Operational Resilience Act (DORA) et la directive associée (UE) 2022/2556, qui imposent des normes de cybersécurité spécifiques aux entités financières, avec une application prévue pour janvier 2025. Ensemble, ces mesures précisent les obligations de résilience numérique et de gestion des risques pour le secteur financier, assurant ainsi une harmonisation des règles de cybersécurité dans toute l'UE.

ACTUALITÉS NOUVELLES TECHNOLOGIES

Règlement sur la cyberrésilience : le Conseil adopte une nouvelle loi sur les exigences en matière de sécurité pour les produits numériques

Règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques (règlement sur la cyberrésilience), 10 octobre 2024

Le Conseil de l'UE a adopté le 10 octobre 2024 un nouveau règlement sur les exigences de cybersécurité pour les produits comportant des éléments numériques, comme les caméras, réfrigérateurs et jouets connectés, afin de garantir leur sécurité avant leur mise sur le marché (« Règlement sur la cyberrésilience »). Ce règlement vise à combler les lacunes du cadre législatif existant, en sécurisant les produits numériques tout au long de leur cycle de vie et dans toute la chaîne d'approvisionnement. Il instaure des normes de cybersécurité à l'échelle de l'UE pour la conception, le développement et la mise à disposition sur le marché de produits matériels et logiciels, en limitant le chevauchement des réglementations dans différents États membres. Les produits conformes porteront le marquage "CE", indiquant leur conformité aux exigences de sécurité, de santé et d'environnement.

Le règlement s'applique aux produits connectés directement ou indirectement à un réseau, avec des exceptions pour ceux déjà soumis à des exigences de cybersécurité (dispositifs médicaux, aéronautiques, automobiles). Il vise également à informer les consommateurs sur les caractéristiques de cybersécurité des produits qu'ils achètent.

Le Règlement sur la cyberrésilience entrera en vigueur 20 jours après sa publication au Journal officiel de l'UE, avec une application prévue sous 36 mois, certaines dispositions devant s'appliquer plus tôt.

La Commission conclut que le service de réseau social en ligne de X ne doit pas être désigné comme un contrôleur d'accès au sens du Règlement sur les marchés numériques (Digital Markets Act ou DMA)

Le 16 octobre 2024, la Commission a décidé que le service de réseau social en ligne de X ne serait pas désigné comme « contrôleur d'accès » au sens du Règlement sur les marchés numériques (Digital Markets Act ou DMA). Cette décision intervient après une enquête lancée le 13 mai 2024, à la suite de la déclaration de X réfutant ce statut de « contrôleur d'accès ». X avait fait valoir que le réseau social ne constituait pas une passerelle clé entre entreprises et consommateurs, bien qu'il atteigne apparemment les seuils quantitatifs stipulés par la DMA. X soutenait que son service ne joue pas un rôle central permettant aux utilisateurs professionnels de se connecter directement aux utilisateurs finaux, exclusif donc du statut de « contrôleur d'accès » selon le DMA.

Après examen des arguments et contributions des parties prenantes concernées et consultation **du comité consultatif sur les marchés numériques**, la Commission a conclu que le service de réseau social fourni par X ne remplissait pas le rôle de « contrôleur d'accès », X ne représentant pas une passerelle importante permettant aux entreprises d'atteindre directement les utilisateurs finaux.

La Commission continuera de surveiller l'évolution de ce marché concernant ce service, dans l'éventualité de changements significatifs. **La version non confidentielle de la décision sera disponible sur le site internet de l'autorité de régulation des marchés de la Commission.**

ACTUALITÉS DONNÉES PERSONNELLES

1er rapport de la Commission européenne sur l'examen du fonctionnement de la décision d'adéquation du cadre UE-US pour la protection des données à caractère personnel

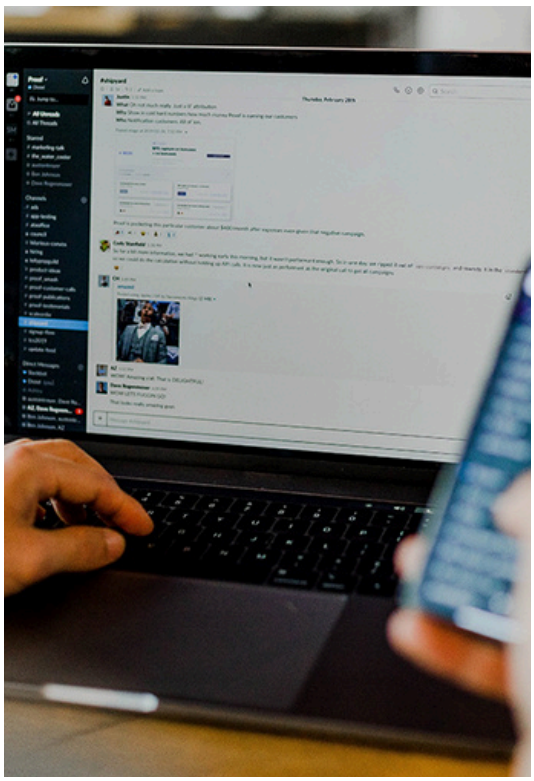
eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0451

La Commission européenne a publié un rapport le 9 octobre 2024 indiquant que le cadre américain de protection de la vie privée (« EU-US Data Privacy Framework ») garantit désormais que les données des Européens ne sont pas utilisées à mauvais escient lorsqu'elles sont transférées vers les Etats-Unis. Ce cadre avait été mis en place en 2023 après que la CJUE avait invalidé deux accords antérieurs de transfert de données, connus sous le nom de « Privacy Shield » et de « Safe harbor ».

La Commission considère que les autorités américaines ont mis en place les structures et les procédures nécessaires pour garantir le bon fonctionnement de ce cadre et salue notamment la mise en place d'une autorité de contrôle américaine. Plus de 2 800 entreprises américaines sont actuellement certifiées dans le cadre de l'accord, ce qui leur permet d'échanger des données plus facilement et à moindre coût, selon le rapport.

Les défenseurs de la vie privée expriment cependant encore des craintes que le cadre de ne comporte toujours de nombreuses lacunes.

CNIL : sanctions de 250K€ et 150K€ de deux services de voyance pour conservation excessive de données personnelles et collecte de données sensibles sans consentement



https://www.cnil.fr/fr/voyance-en-ligne-sanctions-de-250-000-et-150-000-euros-cosmospace-telemaque

Le 26 septembre 2024, la CNIL a sanctionné les sociétés COSMOSPACE et TELEMAQUE, notamment pour avoir conservé des données personnelles de manière excessive, collecté des données sensibles sans consentement valable, et pour avoir manqué aux règles encadrant les opérations de prospection commerciale.

En conséquence, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a prononcé une amende de 250 000 euros à l'encontre de COSMOSPACE et de 150 000 euros à l'encontre de la société TELEMAQUE. Ces amendes ont été adoptées en coopération avec une quinzaine d'homologues européens de la CNIL dans les deux cas.

Le montant de ces amendes a notamment été décidé au regard de la gravité des manquements retenus, du nombre de personnes concernées – la base de données commune aux deux sociétés contenant les données de plus d'1,5 million de personnes – ainsi que de la sensibilité des données traitées. La situation financière des sociétés, et leur structure, ont également été prises en compte, pour retenir des amendes dissuasives mais proportionnées.

ACTUALITÉS DONNÉES PERSONNELLES

CEPD : Lignes directrice Directive ePrivacy

Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, EDPB

L'émergence de nouvelles méthodes de suivi visant à remplacer les outils de suivi existants (par exemple, les cookies, en raison de l'arrêt de la prise en charge des cookies de tiers par certains fournisseurs de navigateurs) et à créer de nouveaux business models est devenue un enjeu majeur pour la protection des données.

Le 16 octobre 2024, le CEPD a publié les lignes directrices 2/2023 sur le champ d'application technique de l'art. 5(3) de la directive vie privée et communications électroniques (Directive ePrivacy), clarifiant ce qui est couvert par « le stockage ou l'accès aux informations » dans des cas tels que :

- Suivi des URL et des pixels
- Traitement local
- le suivi basé sur l'IP
- Rapports IoT
- les identifiants uniques.

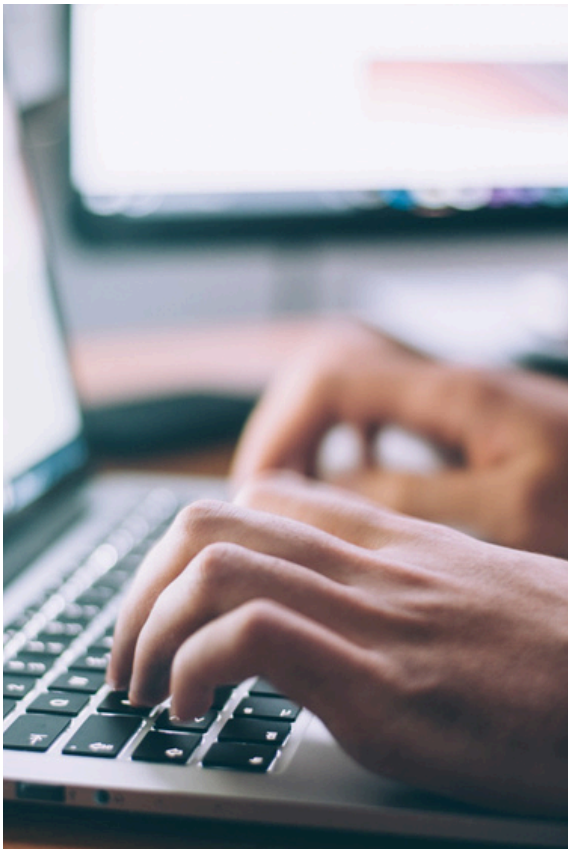
Même si ces opérations relèvent de l'article 5, paragraphe 3, on ne sait toujours pas si un consentement ou une exemption est nécessaire. L'EDPB n'a pas encore répondu à cette question.

Publication par le CEPD des thématiques 2025

CEF 2025: EDPB selects topic for next year's Coordinated Action | European Data Protection Board

Lors de sa plénière d'octobre 2024, le Comité européen de la protection des données (CEPD) a choisi le thème de sa quatrième action coordonnée d'exécution (ACE), qui portera sur la mise en œuvre du droit à l'oubli par les responsables du traitement. Les autorités de protection des données (APD) se joindront à cette action sur une base volontaire dans les semaines à venir et l'action elle-même sera lancée au cours du premier semestre 2025.

Le droit à l'oubli (article 17 du RGPD) est l'un des droits à la protection des données les plus fréquemment exercés et au sujet duquel les autorités de protection des données reçoivent souvent des plaintes. Le but de cette action coordonnée sera, entre autres, d'évaluer la mise en œuvre de ce droit dans la pratique.



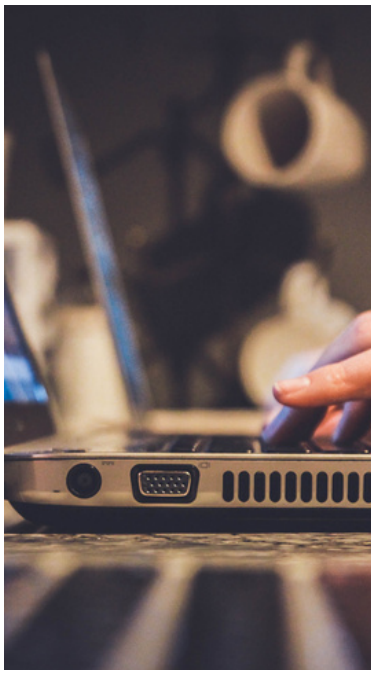
ACTUALITÉS DONNÉES PERSONNELLES

Le CEPD adopte un avis sur les sous-traitants

Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s) | European Data Protection Board

Le CEPD a adopté un avis sur certaines obligations découlant du recours au(x) sous-traitant(s) et sous-sous-traitant(s). Il vise les situations dans lesquelles les responsables du traitement s'appuient sur un ou plusieurs sous-traitants et sous-sous-traitants. En particulier, il aborde des questions relatives à l'interprétation de certaines obligations des responsables de traitement s'appuyant sur des sous-traitants et des sous-sous-traitants ultérieurs, ainsi que le contenu des contrats entre responsables de traitement et sous-traitants ultérieurs, posé par l'article 28 du RGPD.

L'avis explique que les responsables de traitement devraient disposer à tout moment des informations sur l'identité (i.e. nom, adresse, personne de contact) de tous les sous-traitants, sous-sous-traitants ultérieurs, etc., afin de pouvoir s'acquitter au mieux de leurs obligations au titre de l'article 28 du RGPD. En outre, l'obligation du responsable de traitement de vérifier si les sous-sous-traitants présentent des « garanties suffisantes » devrait s'appliquer indépendamment du risque pour les droits et libertés des personnes concernées, bien que l'étendue de cette vérification puisse varier, notamment en fonction des risques associés au traitement. En outre, si le sous-traitant initial doit s'assurer qu'il propose lui-même des sous-traitants avec des garanties suffisantes, la décision finale et la responsabilité d'engager un sous-traitant spécifique restent du ressort du responsable du traitement.



Le CEPD considère qu'en vertu du RGPD, le responsable de traitement n'a pas l'obligation de demander systématiquement aux contrats de sous-traitance de prévoir que les obligations en matière de protection des données soient transmises tout au long de la chaîne de traitement. Mais il appartient au e responsable de traitement d'évaluer s'il est nécessaire de demander une copie de ces contrats ou de les examiner pour pouvoir démontrer la conformité au RGPD.

En outre, lorsque des transferts de données à caractère personnel en dehors de l'Espace économique européen ont lieu entre deux (sous-)sous-traitants, le sous-traitant en tant qu'exportateur de données devrait préparer la documentation pertinente, notamment en ce qui concerne le motif du transfert utilisé, l'analyse d'impact du transfert et les éventuelles mesures supplémentaires. Toutefois, le responsable de traitement restant tenu de justifier de « garanties suffisantes », il devrait évaluer cette documentation et être en mesure de la présenter à l'autorité compétente en matière de protection des données.

ACTUALITÉS DONNÉES PERSONNELLES

Le CEPD adopte des lignes directrices sur l'intérêt légitime

Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Les responsables du traitement ont besoin d'une base juridique pour traiter légalement les données à caractère personnel. L'intérêt légitime est l'une des six bases juridiques possibles.

Les lignes directrices du CEPD analysent les critères énoncés à l'article 6, paragraphe 1, point f), du RGPD que les responsables du traitement doivent remplir pour traiter légalement des données à caractère personnel sur la base d'un intérêt légitime. Elle tient également compte de l'arrêt récent de la Cour de justice de l'Union européenne sur cette question (C-621/22, 4 octobre 2024).
Pour pouvoir invoquer un intérêt légitime, le responsable du traitement doit remplir trois conditions cumulatives:

1. la poursuite d'un intérêt légitime par le responsable du traitement ou par un tiers;
2. la nécessité de traiter des données à caractère personnel aux fins de la poursuite de l'intérêt légitime;
3. Les intérêts ou les libertés et droits fondamentaux des personnes ne prévalent pas sur les intérêts légitimes du responsable du traitement ou d'un tiers (exercice d'équilibrage).

Tout d'abord, seuls les intérêts licites, clairement et précisément articulés, réels et présents peuvent être considérés comme légitimes. Par exemple, de tels intérêts légitimes pourraient exister dans une situation où la personne est un client ou au service du responsable du traitement.

Deuxièmement, s'il existe des alternatives raisonnables, tout aussi efficaces, mais moins intrusives pour atteindre les intérêts poursuivis, le traitement peut ne pas être considéré comme nécessaire. La nécessité d'un traitement devrait également être examinée dans le cadre du principe de minimisation des données.

Troisièmement, le responsable du traitement doit veiller à ce que son intérêt légitime ne l'emporte pas sur les intérêts individuels, les droits fondamentaux des libertés. Dans cet exercice de mise en balance, le responsable du traitement doit tenir compte des intérêts des personnes, de l'incidence du traitement et de leurs attentes raisonnables, ainsi que de l'existence de garanties supplémentaires qui pourraient limiter l'incidence sur la personne.

En outre, les présentes lignes directrices expliquent comment cette évaluation devrait être réalisée dans la pratique, y compris dans un certain nombre de contextes spécifiques tels que la prévention de la fraude, le marketing direct et la sécurité de l'information. Le document explique également la relation entre cette base juridique et un certain nombre de droits des personnes concernées en vertu du RGPD.

La CNIL publie la liste des entités contrôlées en 2023

Contrôles réalisés par la CNIL - data.gouv.fr

NOUS CONTACTER

Stéphanie BERLAND
Avocate - Associée
s.berland@dwf.law
+33 1 40 69 26 63

Emmanuel DURAND
Avocat - Associé
e.durand@dwf.law
+33 1 40 69 26 83

Florence KARILA
Avocate - Associée
f.karila@dwf.law
+33 1 40 69 26 57

Anne-Sylvie VASSENAIX-PAXTON
Avocate - Associée
as.vassenaix-paxton@dwf.law
+33 1 40 69 26 51

DWF est un fournisseur mondial de services juridiques et commerciaux intégrés. Le cabinet emploie environ 4 500 personnes et est présent dans 35 villes à travers le monde. DWF a enregistré un chiffre d'affaires net de 435 millions de livres sterling au cours de l'exercice clos le 30 avril 2024. Pour en savoir plus : **dwfgroup.com**