L'obligation d'information RGPD, règle n°1 du jeu des données personnelles. Par Jean Mindaa, Juriste.

Parution : jeudi 10 juillet 2025

Adresse de l'article original :
https://www.village-justice.com/articles/obligation-information-rgpd-regle-no1-jeu-des-donnees-personnelles,53902.html

Avant toute collecte ou utilisation de données, une règle s'impose : informer. Dans le jeu du RGPD, l'information est la première carte à abattre. Elle rend le traitement lisible, légitime et compréhensible. Sans elle, pas de transparence, pas de confiance, et souvent, pas de base légale valable. Et si l'information, en tant que règle du jeu, fait défaut, alors certains joueurs peuvent tricher et violer les droits des autres participants. Informer dans le cadre du RGPD, c'est permettre à chacun de jouer en connaissance de cause.

Introduction : L'information comme premier acte de tout traitement.

Si le RGPD [1] se veut un pilier de la protection des libertés individuelles, c'est d'abord parce qu'il exige de rendre les traitements de données lisibles, intelligibles et légitimes. L'**obligation d'information** n'est donc pas un simple devoir de communication, elle est la clé de voûte de la transparence. Et cette transparence fonde la confiance.

Informer, au sens du RGPD, implique une capacité à transmettre des messages compréhensibles. Il s'agit d'aller au-delà de la simple transmission d'un document juridique : l'objectif est **d'éclairer, d'expliquer, de rendre accessible**. À toutes les étapes du traitement - avant, pendant, après - les personnes concernées doivent pouvoir identifier les finalités poursuivies, les données traitées, les mesures de protection appliquées etc...

Illustrons :

Avant même que mes données soient collectées, par exemple lorsque je m'apprête à acheter un produit en ligne, je dois pouvoir consulter une politique de confidentialité exhaustive. Celle-ci m'indique entre autres : qui est responsable de traitement ? Quelles données seront collectées (*numéro de carte bancaire, adresse email, nom et prénom, etc.*) ? Dans quel but ? Pour combien de temps ? Cette information n'est donc pas accessoire, elle précède et conditionne l'acte de traitement.

Au cours d'un traitement - imaginons une participation à un essai clinique - un portail de transparence peut me permettre de prendre connaissance de l'utilisation qui est faite de mes données de santé. Je ne suis pas spectateur passif, je reste informé.

Et même **lorsque le traitement prend fin**, le droit à l'information ne s'éteint pas. Si j'exerce mon droit d'accès, le responsable de traitement doit me dire ce qu'il reste de mes données : sont-elles encore stockées ? Sont-elles effacées ? Réutilisées à d'autres fins ? Ce prolongement de la transparence après la clôture du traitement incarne pleinement l'esprit du RGPD.

I. Transparence et information : un principe fondamental, aux contours très concrets.

Le RGPD impose que toute collecte ou utilisation de données personnelles repose sur trois exigences : la **légalité, la loyauté et la transparence**. Cette dernière oblige à rendre les traitements de données compréhensibles pour tous.

Concrètement, cela signifie que les personnes concernées doivent recevoir un ensemble d'informations précises, telles que : pourquoi leurs données sont utilisées (*la finalité*), sur quelle base juridique (*la base légale*), pendant combien de temps elles seront conservées, et quels sont leurs droits (*accès, rectification, effacement, etc.*).

Ces éléments sont encadrés et consacrés par les articles **12, 13 et 14 du RGPD**. Et le texte ne laisse rien au hasard, l'information doit être claire, concise, compréhensible et facilement accessible. Ce niveau d'exigence augmente encore lorsque les données sont sensibles (*comme les données de santé*), mais aussi quand le public est plus vulnérable (*ex. enfants, patients*).

Le RGPD distingue aussi deux cas de figure :

Lorsque les données sont collectées **directement** auprès des personnes, l'article 13 prévoit que l'information doit être donnée au moment même de la collecte.
Lorsqu'elles sont collectées **indirectement**, l'article 14 impose un délai d'un mois maximum pour transmettre l'information.
Cette distinction vise un objectif simple : peu importe comment les données sont obtenues, l'information doit toujours être transmise clairement et au bon moment.

II. L'information comme condition de validité du consentement explicite.

L'obligation d'informer n'est pas seulement un pilier fondamental du RGPD : elle est aussi indissociable de certaines bases légales, à commencer par celle du **consentement explicite** (*Article 9(1)(a) RGPD*). C'est notamment le cas lorsque des données dites "*sensibles*" - comme les données de santé - sont traitées.

Mais ce consentement ne peut être valable que s'il est **éclairé**. Autrement dit, il ne suffit pas qu'une personne accepte ; encore faut-il qu'elle sache précisément à quoi elle dit oui. C'est là que l'information joue un rôle clé, elle précède le consentement et le fonde. Sans elle, le consentement est vide de sens et n'est pas valable.

Le **CEPD/EDPB** a d'ailleurs posé des exigences minimales sur ce point dans ses lignes directrices portant sur le consentement. Avant de recueillir un consentement explicite, plusieurs informations doivent être fournies à la personne concernée [2] :

l'identité du responsable de traitement (*celui qui décide du pourquoi les données sont traitées et du comment elles le sont*) ;
la finalité de chaque opération de traitement (*l'objectif*) ;
les types de données collectées ;
l'existence du droit de retirer son consentement ;
et, le cas échéant, des précisions sur les décisions automatisées ou sur les transferts hors de l'Union européenne.

C'est une nécessité que l'EDPB formule sans ambiguïté :

"Fournir des informations aux personnes concernées avant d'obtenir leur consentement est indispensable afin de leur permettre de prendre des décisions en toute connaissance de cause (...). Si le responsable du traitement ne fournit pas d'informations accessibles, le contrôle utilisateur devient illusoire et le consentement ne constituera pas une base valable pour le traitement."

En clair, le consentement explicite n'est pas un acte isolé, c'est un processus, qui commence par une information claire. Sans cela, l'utilisateur ne consent pas, il subit [3].

III. Quels supports pour informer efficacement les personnes concernées ?

L'obligation d'information se traduit par des **supports** concrets, utilisés au quotidien par les organisations pour rendre leurs traitements transparents. Ces supports sont la vitrine de la conformité et rendent visible ce qui, sans eux, resterait opaque.

Parmi les supports les plus courants, on retrouve :

Les **politiques de confidentialité**, véritables piliers de l'information générale, qui expliquent comment les données personnelles sont collectées, utilisées, sécurisées et quels droits peuvent être exercés par les personnes concernées ;
Les **notes d'information**, souvent plus ciblées, qui détaillent des traitements spécifiques. Elles sont particulièrement utiles dans des contextes sensibles comme la recherche en santé ou les essais cliniques ;
Les **portails de transparence en santé**, conçus pour permettre aux personnes d'accéder facilement à des explications sur l'usage de leurs données de santé. Ces plateformes rendent la transparence continue et accessible ;
Les **panneaux d'information liés à la vidéosurveillance**, qui rappellent la présence de caméras, précisent les zones surveillées, les finalités du dispositif et les droits associés à ce traitement.

Mais l'information ne concerne pas seulement les utilisateurs, patients, usagers. Les salariés aussi sont directement concernés. Et là encore, les supports jouent un rôle clé. Dans l'environnement professionnel, ces vecteurs d'information accompagnent chaque étape de la vie du salarié dans l'entreprise. Dès le recrutement, le contrat de travail intègre des mentions et clauses RGPD. À l'arrivée, une **notice d'information** peut être remise, résumant les traitements opérés en interne. L'accès aux outils numériques s'accompagne généralement d'une **charte informatique**, qui encadre les usages du matériel informatique et rappelle les bonnes pratiques de sécurité. Enfin, une **politique de confidentialité interne**, souvent consultable en ligne ou sur l'intranet, offre une information continue sur la manière dont l'entreprise gère les données personnelles de ses collaborateurs.

Ce dispositif crée une information en cascade, pensée pour suivre les grandes étapes du parcours salarié. Ce n'est pas une obligation formelle du RGPD, mais c'est une **bonne pratique**, qui favorise une meilleure compréhension et une meilleure appropriation de la culture RGPD.

IV. Rendre l'information vraiment accessible est un défi plus complexe qu'il n'y paraît.

Informer, ce n'est pas seulement publier un document juridique sur un site web. C'est permettre à une personne - quelle que soit sa maîtrise du langage juridique ou du numérique - de comprendre ce qu'on fait de ses données. Et en pratique, cet objectif reste souvent difficile à atteindre.

Les exemples sont nombreux. Beaucoup d'organisations diffusent encore des politiques de confidentialité **longues, techniques et rédigées dans un langage juridique peu lisible**. Le résultat est sans appel, les personnes concernées ne les lisent pas, ou n'en comprennent qu'une partie. Ce double échec - manque de lisibilité et d'engagement - compromet l'effectivité de l'information.

Une étude internationale pilotée par la CNIL l'a d'ailleurs mis en lumière : **89 %** des politiques de confidentialité analysées utilisent un langage jugé **trop complexe de niveau universitaire** [4].
Face à ce constat, des pistes concrètes ont été proposées. Dès 2022, la CNIL a rappelé que le RGPD impose des critères essentiels : les informations doivent être *"**concises, transparentes, compréhensibles et aisément accessibles, en des termes clairs et simples**"* (*Art. 12 RGPD*). En réponse, elle a publié une recommandation visant à simplifier le langage employé, en particulier dans les communications destinées au grand public [5].

Quelques exemples de cette simplification :

Remplacer *"finalité"* par *"objectif"* ou *"données à caractère personnel"* par *"information qui vous concerne"*

Préférer *"utilisation de données"* à *"traitement de données"*.

Ces ajustements ne sont pas anecdotiques. Ils participent à rendre l'information plus directe, plus intelligible et surtout plus digeste.
Une information accessible est une information utile. À l'inverse, un texte trop technique, même conforme sur le papier, ne permet pas aux personnes concernées d'exercer leurs droits de manière effective.

Cette exigence de lisibilité ne reste pas théorique. La CNIL elle-même applique ces principes dans sa propre communication. Depuis 2021, elle a amorcé un virage vers un langage plus accessible dans ses supports grand public. Qu'il s'agisse de fiches pratiques, d'actualités, ou de contenus pédagogiques, la CNIL s'efforce désormais de recourir à des termes simples, concrets et immédiatement compréhensibles pour viser une appropriation réelle par le plus grand nombre.
Cela dit, cette simplification ne s'étend pas à l'ensemble de ses publications puisque certains documents conservent un langage plus technique. C'est une nécessité juridique, liée à leur nature et à leur portée. En fin de compte, il existe des espaces où la clarté prime et d'autres où la rigueur formelle prévaut.

V. Interfaces trompeuses qui sapent la transparence.

L'un des défis majeurs de la mise en œuvre de l'information tient aux **interfaces trompeuses**, plus connues sous le nom de *"**dark patterns**"*. Derrière ce terme se cachent des pratiques de design numérique conçues pour **influencer, manipuler ou orienter les choix** des utilisateurs, souvent à leur détriment [6].

Ces mécanismes sont parfois utilisés pour rendre plus difficile l'exercice de droits - par exemple, refuser les cookies - ou pour favoriser la collecte de données personnelles sans véritable consentement, tout en prétendant respecter les obligations du RGPD.

Un exemple classique : sur certains sites, l'option par défaut consiste à accepter la collecte des données. En revanche, l'option de refus est moins visible, dissimulée dans une interface complexe, ou nécessite plusieurs clics pour être activée. Visuellement, les boutons *"Accepter"* sont souvent surdimensionnés, colorés, placés en évidence tandis que les boutons *"Refuser"* sont relégués au second plan, en bas de page, en plus petits, grisés, ou perdus dans un menu secondaire.

Mais la manipulation ne se limite pas à l'esthétique et au visuel. Elle peut aussi concerner l'information textuelle. Certaines formulations floues ou ambiguës nuisent à la compréhension.

Par exemple :
"En cliquant sur valider, vous acceptez de rester connecté avec nous."
Une telle phrase manque de clarté et de précision. À l'inverse, une formulation plus conforme serait : *"en cochant la case "valider", vous confirmez avoir lu et accepté notre politique de confidentialité et consentez à l'utilisation de vos données personnelles pour répondre à votre demande."*

Ces dérives ne sont pas simplement contraires au RGPD ; elles sont effectivement **sanctionnées**. La CNIL a infligé plusieurs amendes à des acteurs ayant utilisé de telles pratiques :

Délibération SAN-2023-025 du 29 décembre 2023 (*Tagadamedia*) ;
Délibération SAN-2024-003 du 31 janvier 2024 (*Foriu*) ;
Délibération SAN-2024-004 du 4 avril 2024 (*Hubside Store*) ;
Délibération SAN-2025-001 du 15 mai 2025 (*Solocal Marketing services*) ;
Délibération SAN-2025-002 du 15 mai 2025 (*Caloga*).

Dans ce contexte, certaines bonnes pratiques s'imposent pour restaurer la transparence. Il s'agit notamment de :

Maintenir une neutralité visuelle entre les différentes options (*ex. : accepter/refuser*) ;
Uniformiser la typographie et la taille des boutons pour éviter les biais de perception ;
Équilibrer la disposition/ emplacement des choix sur l'interface ;
Et surtout, accompagner chaque action (*acceptation, refus*) d'une information claire, concise et explicite qui ne doit pas porter à interprétation.

Un bouton, une case à cocher, une option à valider impliquent que l'utilisateur n'ai pas à deviner les conséquences de ses choix et doit les comprendre immédiatement.

C'est dans cette optique que le **LINC**, le Laboratoire d'innovation numérique de la CNIL, a mené une vaste étude [7] sur les pratiques de design dans le secteur du e-commerce. L'analyse a porté sur 53 000 pages issues de plus de 11 000 sites. Résultat : 1 841 occurrences de dark patterns ont été identifiées, réparties en 15 types de pratiques, regroupées en **7 catégories** :

duper l'utilisateur (sneaking) ;
instaurer un sentiment d'urgence (urgency) ;
détourner l'attention / mal indiquer (misdirection) ;
exercer une pression sociale (social proof) ;
donner une impression de rarete (scarcity) ;
obstruer (obstruction) ;
forcer une action (forced action).

VI. Le portail de transparence en santé : une interface clé pour informer les patients.

Parmi les secteurs où la transparence prend une dimension cruciale, le **domaine de la santé** occupe une place à part entière. Le traitement de données médicales exige un niveau d'information particulièrement élevé. C'est dans ce contexte qu'ont émergé des outils dédiés comme les **portails de transparence**, conçus pour offrir aux patients un accès direct, centralisé et continu aux informations sur l'usage de leurs données de santé.

La CNIL en donne une définition claire [8] : un portail de transparence est un espace en ligne, accessible sur le site du responsable de traitement (*ou de ses partenaires*), qui regroupe l'ensemble des informations relatives :

aux traitements de données de santé en cours ;
aux projets de réutilisation de ces données, présents ou à venir.

Ce type de dispositif répond à une exigence simple qui est de permettre aux personnes concernées de **rester informées dans la durée**, sans avoir à solliciter une nouvelle note d'information à chaque évolution du traitement.

Sa mise en œuvre devient d'autant plus indispensable dans certains contextes spécifiques :

Les **entrepôts de données de santé** (*EDS*), qui centralisent des volumes importants de données à des fins de recherche, de santé publique ou d'évaluation.
Le **référentiel sur l'accès précoce** (CNIL, Délibération n° 2022-107 du 22 septembre 2022 portant adoption d'un référentiel (accès précoce)), dans lequel la CNIL précise que toute réutilisation envisagée des données personnelles doit être signalée au patient, via une note d'information initiale renvoyant explicitement vers un portail de transparence.

Le portail de transparence est un mécanisme, présenté comme une **mesure de transparence complémentaire**, évite d'avoir à renouveler systématiquement l'information individuelle à chaque nouvelle phase de traitement. Il s'agit d'un équilibre entre efficacité opérationnelle et respect des droits des personnes.

La même logique est reprise dans le **référentiel sur l'accès compassionnel** (CNIL, Délibération n° 2022-106 du 22 septembre 2022 portant adoption d'un référentiel (autorisation d'accès compassionnel)), qui concerne l'usage de médicaments en dehors de leur autorisation de mise sur le marché. Ici encore, la CNIL admet que l'information sur les traitements ultérieurs peut être assurée soit de manière individuelle, soit via un portail de transparence mentionné dès la première note d'information.

En définitive, le portail de transparence montre comment, dans des contextes complexes et évolutifs, l'exigence de transparence peut être pensée comme un dispositif vivant, structuré et adapté aux réalités du terrain.

VII. L'exemple Amazon France Logistique : quand l'information est présente mais insuffisante.

Le cas d'Amazon France Logistique illustre avec force que l'existence d'un document d'information ne suffit pas, en soi, à satisfaire à l'obligation d'information du RGPD. En 2024, la CNIL a sanctionné la société pour **manquement à son obligation d'information**, en lien notamment avec les travailleurs intérimaires employés dans ses entrepôts. Concrètement, Amazon avait mis à disposition une politique de confidentialité sur son intranet. Mais cette modalité n'a pas été considérée comme suffisante. La CNIL a estimé que rien ne garantissait que les intérimaires aient effectivement eu connaissance de cette information avant que leurs données ne soient collectées.

La formation restreinte de la CNIL l'a exprimé sans détour : "*L'information doit être faite selon les modalités les plus appropriées en fonction de l'organisation et du fonctionnement de l'entreprise*" (CNIL, Délibération SAN-2023-021 du 27 décembre 2023 (Amazon France Logistique).

En l'occurrence, proposer un document sur l'intranet à des intérimaires qui travaillent physiquement dans des entrepôts, sans accès régulier à un poste informatique et sans qu'aucune incitation ne les oriente vers ce support, ne constitue pas une modalité satisfaisante d'information. Cela revient à placer l'information dans un espace théoriquement accessible mais pratiquement invisible.

Le cas Amazon comporte un second volet : la **vidéosurveillance** mise en place sur les sites. Là encore, l'information délivrée aux salariés et aux visiteurs était incomplète. Les panneaux d'affichage ne mentionnaient ni l'identité du DPO, ni la durée de conservation des images, ni la possibilité d'introduire une réclamation auprès de la CNIL. Ces omissions ont conduit à une non-conformité à l'article 13 du RGPD, qui impose une information complète, fournie au moment de la collecte des données.

Ce type de situation rappelle que l'obligation d'information n'est pas qu'un contenu à rédiger, mais une stratégie à penser. Elle implique de choisir des **canaux et modalités adaptés, de contextualiser la diffusion et de s'assurer que le message parvient effectivement à la personne concernée**. Une approche trop formelle, trop distante des usages concrets, expose à des risques juridiques réels.

VIII. Tableau de recommandations et de bonnes pratiques pour la mise en œuvre de l'obligation d'information.

IX. L'information se joue aussi - et se jouera - dans la transparence des algorithmes, des décisions automatisées et de l'IA.

Dans son arrêt du 27 février 2025 [9], la CJUE précise la portée de l'obligation d'information en cas de décision fondée sur un traitement automatisé, notamment en matière de profilage. Elle reconnaît à la personne concernée un véritable **droit à l'explication** de la logique sous-jacente d'une décision automatisée, telle que prévu à l'article 15(1)(h) du RGPD.

Communiquer des informations :	Explications et exemples
"concises"	+ L'information est délivrée sous une forme brève, claire et immédiatement compréhensible pour tous
"transparentes"	+ Les informations à fournir sont celles qui se rapportent au traitement de données personnelles concerné. Elles correspondent aux éléments listés aux articles 13 ou 14 du RGPD Par exemple : qui est responsable de traitement ? Pourquoi les données sont collectées ? Quelles données sont utilisées ? Combien de temps elles sont conservées ? Etc.
"compréhensibles"	+ Les informations doivent être communiquées dans un langage clair et accessible au grand public. Il convient d'éviter les formulations complexes, le jargon juridique ou technique. Par exemple, dans le cas d'un formulaire en ligne, la personne concernée doit pouvoir exprimer son consentement ou son refus sans effort particulier de concentration ou d'interprétation. Les instructions doivent être explicites, tout comme les conséquences associées à chaque choix, afin de garantir une prise de décision véritablement libre et éclairée. + Les supports d'information, comme les politiques de confidentialité, doivent être structurés de manière logique. Des titres clairs, des repères visuels et une organisation cohérente du contenu permettent de rendre l'information plus digeste et compréhensible pour l'utilisateur.
"aisément accessibles"	+ Les modalités et moyens de communication choisies doivent être adaptées à l'organisation et au fonctionnement de votre structure. Il s'agit de sélectionner les moyens les plus pertinents pour que l'information parvienne effectivement aux personnes concernées. Par exemple, informer via l'intranet de l'entreprise, des salariés qui travaillent quotidiennement sur le terrain et qui n'ont pas vocation à travailler sur un ordinateur, sans aucune incitation à s'y rendre, ne constitue pas un moyen d'information satisfaisant selon la CNIL. Dans ce cas, un support plus direct, comme l'envoi d'un e-mail individuel, serait préférable. + L'accès à l'information doit être simple, direct et immédiat. Par exemple, un utilisateur doit pouvoir consulter la politique de confidentialité en quelques clics depuis n'importe quelle page clé du site ou de l'application, par exemple via un lien en pied de page ou dans les menus. Cette information doit également être visible au moment où les données sont collectées comme lors d'une inscription - avec un lien direct/ de redirection permettant de la lire avant de fournir ses données personnelles.
"en des termes clairs et simples"	+ Adoptez un langage simple et compréhensible dans vos documents et supports d'information (politique de confidentialité, portail de transparence, note d'information, etc.). Cela peut passer par l'usage de termes plus courants : par exemple, remplacer "traitement de données" par "utilisation de données". Le terme "traitement" a en effet un sens très large dans le RGPD, englobant toutes les opérations possibles sur les données personnelles (collecte, conservation, modification, suppression, etc.). À l'inverse, le mot "utilisation" parle davantage au grand public et évoque une action concrète dans un but précis, ce qui facilite la compréhension.

Pour la Cour, il ne suffit pas que le responsable de traitement communique des éléments bruts et techniques d'un algorithme. Elle affirme ainsi que :

"ne saurait satisfaire à ces exigences ni la simple communication d'une formule mathématique complexe, telle qu'un algorithme, ni la description détaillée de toutes les étapes d'une prise de décision automatisée."

Au lieu de cela, le responsable doit fournir une **explication accessible**, permettant à la personne concernée de comprendre, en termes simples, **quelles données ont été utilisées, quels critères ont été appliqués et comment ces éléments ont conduit au résultat obtenu**. Il doit décrire *"la procédure et les principes concrètement appliqués"* (pt 61), et, le cas échéant, informer sur *"la mesure dans laquelle une variation au niveau des données [...] aurait conduit à un résultat différent"* (pt 62).

La CJUE insiste aussi sur la forme de l'information qui doit être *"concise, transparente, compréhensible et aisément accessible"*, de sorte que la personne puisse réellement exercer ses droits, notamment celui de contester la décision. Ainsi, l'arrêt consacre une exigence à la fois de contenu explicatif (*données, critères, lien logique*) et de forme pédagogique, plaçant la compréhension de la personne concernée au cœur du droit d'accès.

X. Conclusion - *"De l'étendu de l'information"*.

Comme vous avez pu le lire, dans le jeu du RGPD, l'information est la première carte à poser sur la table. Mais ce jeu s'étend désormais à de nouveaux plateaux : aujourd'hui aux décisions automatisées, demain aux modèles et aux systèmes d'intelligence artificielle, parfois opaques. L'information ne dira plus seulement ***ce qui est fait*** , mais ***comment cela a été décidé et pourquoi*** . Sans cette transparence, il ne s'agira plus d'un jeu, mais d'une partie truquée.

Jean Mindaa Juriste | étudiant Diplômé d'un Master 2 en Droit européen des affaires et du numérique (Université de Pau et des pays de l'Adour)

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr - Règlement (UE) 2016/679 relatif à la protection des données à caractère personnel (RGPD).

[2] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf - EDPB/CEPD, 4 mai 2020, Lignes directrices 5/2020 portant sur le consentement au sens du RGPD, page 18, point 64

[3] Ibid, page 17, point 62.

[4] https://www.cnil.fr/fr/design-trompeur-les-resultats-de-laudit-du-global-privacy-enforcement-network - CNIL, Design trompeur : les résultats de l'audit du Global Privacy Enforcement Network

[5] https://www.cnil.fr/fr/information-des-personnes-la-cnil-encourage-lemploi-de-termes-plus-clairs-pour-le-grand-public – CNIL, Information des personnes : la CNIL encourage l'emploi de termes plus clairs pour le grand public

[6] https://linc.cnil.fr/dark-patterns-quelle-grille-de-lecture-pour-les-reguler - CNIL (LINC), Dark patterns : quelle grille de lecture pour les régule ?

[7] https://linc.cnil.fr/dark-patterns-quelle-grille-de-lecture-pour-les-reguler - CNIL (LINC), Dark patterns : quelle grille de lecture pour les réguler ?

[8] https://www.cnil.fr/fr/demande-dautorisation-dans-le-domaine-de-la-sante-hors-recherche-les-informations-fournir-et-les - CNIL, Demande d'autorisation dans le domaine de la santé (hors recherche) : les informations à fournir et les critères d'octroi.

[9] https://curia.europa.eu/juris/document/document.jsf;jsessionid=BF844206A410AA18EFFCCF166CE48D90?text=&docid=295841&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=28784587 - CJUE, 27 février 2025, affaire C-203/22

L'auteur déclare ne pas avoir utilisé l'IA générative pour la rédaction de cet article.