LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Publications de décembre 2024

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN RÉGLEMENTATION	10/01/2025	Tribunal – 8 janvier 2025 – Bindl c. Commission – T-354/22	Dans cet arrêt, le Tribunal de l'Union européenne a condamné la Commission européenne pour avoir effectué des transferts de données en dehors de l'Union européenne (aux Etats-Unis, en particulier), qui n'étaient pas couverts par des garanties adéquates. En effet, lors des transferts, le Privacy Shield avait été invalidé, et le Data Privacy Framework n'était pas encore en place. Aucune clause contractuelle type n'avait été signée.	Pour information
LE COIN RÉGLEMENTATION	10/01/2025	CJUE – 9 janvier 2025 – Mousse – C-394/23	La Cour de justice de l'Union européenne (CJUE) s'est prononcée sur une question préjudicielle du Conseil d'Etat concernant la licéité de la collecte par la SNCF de la civilité des clients dans le cadre de communications commerciales. Selon la Cour de justice, la collecte des informations relatives à la civilité n'est objectivement indispensable ni pour l'exécution du contrat entre la SNCF et ses clients, c'est-à-dire l'achat de titres de transport, ni sur le fondement de l'intérêt légitime de la SNCF à personnaliser sa prospection commerciale. Par ailleurs, la Cour a également indiqué que la collecte de ces informations pourrait représenter un risque de discrimination fondée sur l'identité de genre des clients, et que les libertés et droits fondamentaux de ces derniers prévalaient sur l'intérêt de la SNCF.	Pour information
LE COIN RÉGLEMENTATION	10/01/2025	CJUE – 9 janvier 2025 - Österreichische Datenschutzbehörde – C-416/23	La Cour de justice de l'Union européenne (CJUE) s'est prononcée, à la suite d'un renvoi préjudiciel de l'autorité de protection des données autrichienne, sur l'appréciation de la notion de demandes excessives par les autorités de contrôle. Elle a, à ce titre, rappelé que la notion de demandes excessives s'apprécie au regard du nombre de demandes sur une période déterminée, mais surtout au regard de	Pour information

			l'intension abusive de la personne. Cette intension abusive doit être démontrée par l'autorité de contrôle : le seul fait d'envoyer de nombreuses demandes à l'autorité de contrôle n'est pas suffisant pour qualifier des demandes comme étant excessive. Cela peut notamment provenir d'un nombre important de réclamations qui ne seraient pas objectivement nécessaires : par exemple lorsque les données ne sont pas traitées dans le cadre des traitements de données faisant l'objet des plaintes. La CJUE rappelle également la possibilité pour les autorités de protection des données de faire payer les réponses aux demandes excessives.	
 LE COIN SANTÉ  LE COIN DES FONDAMENTAUX	10/01/2025	Cour des comptes – La sécurité informatique des établissements de santé – Janvier 2025	Dans le prolongement de ses rapports de 2016 et 2020 respectivement sur la modernisation des systèmes d'information hospitaliers et sur les groupements hospitaliers de territoire, la Cour des comptes a actualisé son analyse de la cybermenace dans les établissements de santé dans ce rapport. L'objectif est d'analyser la manière dont le ministre de la santé a pris en compte la cybermenace, et les actions engagées pour inciter les établissements de santé à se protéger. Ainsi, la Cour des comptes a conclu que la vulnérabilité des établissements de santé est liée notamment à l'interconnexion accrue de leurs systèmes d'information avec l'extérieur et au sous-investissement chronique dans le numérique. Elle note également le retard de la réaction des autorités publiques : le pilotage d'un groupe de travail pour rédiger le programme CaRE n'a été confié à la DNS que début décembre 2022 à la suite des cyberattaques intervenues à l'été. Néanmoins, elle salue la mise en place de ce programme visant à combler le retard d'investissement et de ressources affectés à l'organisation des systèmes d'information hospitaliers.	 Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	10/01/2025	EDPS - Opinion 01-2025 on the Proposal for a Regulation on a public interface connected to the Internal Market Information System for the declaration of the posting of workers and amending Regulation (EU) N°1024/2012 – January 2025	Le Contrôleur européen a été consulté par la Commission concernant la proposition de règlement relatif à une interface publique connectée au système d'information du marché intérieur pour la déclaration de détachement des travailleurs. Le Contrôleur recommande de préciser les termes d'identité et de coordonnées auxquels se réfère la proposition de règlement. Par ailleurs, des précisions concernant les destinataires du service devraient également être apportées en cas de traitement des données.	Pour information
LE COIN RÉGLEMENTATION	10/01/2025	EDPS reprimands Frontex for non-compliance with Regulation (EU) 2019/1896 – January 2025	Le Contrôleur européen a sanctionné Frontex, Agence européenne de garde-frontières et de garde-côtes, pour non-respect du règlement Frontex (règlement (UE) 2019/1896 relatif au corps européen de garde-frontières et de garde-côtes du 13 novembre 2019) lors de la transmission de données personnelles de suspects de crimes transfrontaliers à Europol. Lors du partage d'informations concernant les personnes suspectes de criminalité transfrontalière, Frontex n'évaluait pas si ces données étaient strictement nécessaires pour qu'Europol puisse remplir sa mission. Dans la mesure où ce partage d'information a été interrompu 5 jours après le rapport d'audit, le contrôleur a décidé de se limiter à un blâme.	Pour information
LE COIN RÉGLEMENTATION	14/01/2025	EDPS - Formal comments on the draft Commission Delegated Regulation amending Delegated Regulation (EU) 2019/1122 supplementing Directive 2003/87/EC of the European Parliament and of the Council as regards the functioning of the Union Registry – V1 – January 2025	Le Contrôleur a été consulté par la Commission européenne sur le projet de règlement délégué de la Commission modifiant le règlement délégué (UE) 2019/1122 complétant la directive 2003/87/CE en ce qui concerne le fonctionnement du registre de l'Union. Ce projet n'entrainerait qu'un traitement de données limité à des coordonnées de personnes de contact professionnel, et non des coordonnées privées. A ce titre, le Contrôleur n'émet pas de commentaire particulier.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	14/01/2025	EDPS – Formal comments on the draft Commission Implementing Regulation on the arrangements for the publication of the lists of operators and groups of operators and the information relating to the certificate provided to operators and groups of operators in accordance with Article 35(1) of Regulation (EU) 2018/848 of the European Parliament and of the Council – V1 – January 2025	Le Contrôleur a été consulté par la Commission européenne sur le projet de règlement d'exécution de la Commission relatif aux modalités de publication des listes d'opérateurs et de groupes d'opérateurs et des informations relatives au certificat fourni aux opérateurs et aux groupes d'opérateurs conformément à l'article 35, paragraphes 1, 2 du règlement (UE) 2018/8483. Le Contrôleur n'émet pas de commentaire particulier, dans la mesure où le projet de règlement prévoit déjà de se conformer aux dispositions du RGPD.	Pour information
LE COIN RÉGLEMENTATION	17/01/2025	CNIL – Plan stratégique 2025-2028 : IA, mineurs, cybersécurité, quotidien numérique	Les axes du plan stratégique de la CNIL pour 2025-2028 ont été publiés et concernent quatre thématiques : l'intelligence artificielle, le droit des mineurs, la cybersécurité, et enfin les usages du quotidien numérique. S'agissant des usages du quotidien numérique, la CNIL se mobilise sur les usages centraux des Français, c'est-à-dire les applications mobiles, et le développement et déploiement de l'identité numérique.	Pour information
LE COIN RÉGLEMENTATION	17/01/2025	Délibération n° HABS-2025-001 du 9 janvier 2025 habilitant des agents de la Commission nationale de l'informatique et des libertés à établir un rapport en application du cinquième alinéa de l'article 22-1 de la loi n° 78-17 du 6 janvier 1978 modifiée	La liste des agents de la direction des contrôles et des sanctions de la CNIL, habilités à établir un rapport dans le cadre de la procédure simplifiée a été publiée par la CNIL.	Pour information
LE COIN RÉGLEMENTATION	17/01/2025	EDPB – EN CONSULTATION – Guidelines 01-2025 – Pseudonymisation	Le Comité européen de la protection des données a mis en consultation publique un projet de lignes directrices sur la pseudonymisation. La consultation est ouverte jusqu'au 28 février 2025.	Pour information

LE COIN RÉGLEMENTATION	22/01/2025	EDPS – Formal comments on the draft Commission Delegated Regulation supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the appropriate arrangements, systems and procedure as well as the templates to be used for preventing, detecting and reporting suspected market abuse, and on the coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse in cross-border market abuse situations – V1 – January 2025	Le Contrôleur a été consulté par la Commission sur le projet de règlement délégué concernant les normes techniques de réglementation précisant les dispositions, systèmes et procédures appropriés ainsi que les modèles à utiliser pour prévenir, détecter et signaler les abus de marché présumés, et les procédures de coordination entre les autorités compétentes concernées. Le Contrôleur recommande de préciser que les principes de protection des données sont applicables aux traitements effectués dans ce cadre, et notamment le principe de minimisation. Par ailleurs, des institutions européennes étant impliquées dans ce cadre, le Contrôleur recommande d'ajouter une référence au règlement (UE) 2018/1725 (ou EUDPR) concernant l'application de la protection des données aux traitements effectués par les institutions organes, organismes et agences de l'UE.	Pour information
LE COIN RÉGLEMENTATION	23/01/2025	CNIL – Réutilisation de bases de données : les vérifications nécessaires pour respecter la loi – Janvier 2025	La CNIL rappelle les vérifications à réaliser avant de réutiliser des bases de données mises à disposition, librement, ou fournies par des tiers. La constitution ou le partage de données ne doit pas être illicite. La CNIL indique les différentes règles à respecter. Ainsi, il faut notamment vérifier que la source est mentionnée, que la constitution ou diffusion de la base ne résulte pas d'un crime ou délit, qu'il n'y a eu aucune sanction publique entrainant une suppression ou interdiction d'exploiter ultérieurement les données. Un contrat avec le détenteur des données devra être signé pour s'assurer de la licéité de la réutilisation.	Pour information

LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN RÉGLEMENTATION	27/01/2025	EDPB – Opinion 01-2025 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Coface Group – V1 – January 2025	Le Comité européen de la protection des données considère que le projet de Binding Corporate Rules (BCR) ou règles d'entreprise contraignantes de la Compagnie Française d'Assurance pour le Commerce Extérieur et ses entités peut être adopté en l'état. Les BCR prévoient des garanties appropriées afin d'assurer un niveau de protection adéquat lorsque les données personnelles sont transférées et traitées par les membres du groupe basés dans des pays tiers.	 Pour information
 LE COIN DES FONDAMENTAUX	28/01/2025	Droit d'accès : bilan des contrôles de la CNIL dans le cadre d'une action coordonnée européenne – Janvier 2025	À l'occasion de l'action coordonnée au niveau européen sur le droit d'accès, des contrôles ont été effectués par la CNIL en 2024. Plusieurs rappels aux obligations légales ont été prononcés contre les organismes qui ne répondaient que partiellement aux personnes concernées : la copie des données traitées n'était pas fournie lors d'une réponse à une demande de droit d'accès, ou à l'inverse seule la copie était fournie sans fournir les informations complémentaires. D'autres organismes refusaient systématiquement de répondre concernant certains traitements, ou certaines catégories de données.	 Pour information
 LE COIN POUR ALLER PLUS LOIN	28/01/2025	Applications mobiles : comment intégrer des SDK et respecter la vie privée des utilisateurs ? Janvier 2025	La CNIL rappelle ses recommandations sur la manière d'intégrer des kits de développement de logiciels afin de garantir la conformité au RGPD. Elle rappelle qu'elle portera une attention particulière à la conformité des fournisseurs de ces kits, et qu'ils feront l'objet de contrôle à partir du printemps 2025.	 Pour information
 LE COIN DES FONDAMENTAUX	28/01/2025	CNIL – Violations massives de données en 2024 : quels sont les principaux enseignements et mesures à prendre ? Janvier 2025	La CNIL rappelle que les violations de données sont majoritairement liées à des défauts de sécurité récurrents : les informations de connexion utilisées pour l'attaque avaient été compromises, les intrusions et exfiltrations n'ont pas été détectées par l'organisme avant la mise en vente des jeux de données, et enfin une part significative des incidents impliquait un sous-traitant.	 Pour vérification

			Elle rappelle les mesures pouvant aider à prévenir ces risques.	
 LE COIN DES FONDAMENTAUX	28/01/2025	ANSSI – Se protéger des fuites de données – Janvier 2025	L'ANSSI met en ligne les onze pratiques permettant de protéger son organisation d'une fuite de données. En premier lieu, est mentionnée la sensibilisation de la direction et des salariés à leur rôle dans la protection des données.	 Pour information
 LE COIN DES FONDAMENTAUX	31/01/2025	Observatoire du droit d'accès sur les réseaux sociaux : le Laboratoire d'innovation numérique de la CNIL (LINC) publie son bilan – Janvier 2025	Le laboratoire d'innovation numérique de la CNIL (LINC) a mené une étude sur le parcours utilisateur sur l'exercice du droit d'accès sur les réseaux sociaux. 10 réseaux sociaux ont été sélectionnés, pour mettre en lumière les bonnes pratiques, et encourager l'amélioration de l'expérience utilisateur. Trois étapes principales ont été étudiées : l'information préalable fournie aux personnes concernées, le parcours permettant de demander une copie des données, les formats de transmission des données. De manière générale, les bonnes pratiques recensées sont mises en place : les informations sont rédigées clairement, et sont adaptées à l'âge des personnes concernées, des formulaires dédiés sont disponibles pour automatiser les demandes, des espaces de consultation en direct sont mis en place, une notification dès que les données sont disponibles permet aux personnes concernées de savoir quand télécharger leurs données.	 Pour information
 LE COIN RÉGLEMENTATION	31/01/2025	EDPS – Formal comments on the draft Commission Implementing Regulation on technical arrangements for developing, maintaining and employing electronic systems for the exchange and storage of information under Regulation (EU)	Le Contrôleur a été consulté par la Commission européenne sur le projet de règlement d'exécution relatif aux modalités techniques de développement, de maintenance et d'utilisation des systèmes électroniques d'échange et de stockage d'informations au titre du règlement (UE) n° 952/2013. Le Contrôleur considère que les finalités de traitement évoquées dans ce règlement ne sont pas suffisamment	 Pour information

		No 952/2013 of the European Parliament and the Council – January 2025	précises ; et ne permettent notamment pas de déterminer les catégories de données pertinentes. De la même manière, il recommande de préciser les éléments permettant aux responsables de traitement de limiter les droits des personnes concernées.	
 LE COIN DES FONDAMENTAUX	31/01/2025	CNIL - Guide pratique : Analyse d'impact des transferts de données - V1 - Janvier 2025	Ce guide, publié par la CNIL, vise à accompagner les organismes qui transfèrent des données en dehors de l'Union européenne. En cas de transferts de données sur la base d'outils tels que les clauses contractuelles types ou les règles d'entreprise contraignantes, les exportateurs ont l'obligation d'évaluer le niveau de protection dans les pays tiers de destination et la nécessité de mettre en place des garanties supplémentaires. Ce guide permet de réaliser cette analyse d'impact des transferts de données.	 Pour information

L'équipe du Coin du DPO vous souhaite une belle année 2025.