LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Janvier 2024

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE L'EUROPE	12/01/2024	EDPS - Opinion 3-2024 on the signing and conclusion on behalf of the European Union, of the Protocol amending the Agreement between the European Union and Japan for an Economic Partnership regarding free flow of data	Le 1er décembre 2023, la Commission européenne a publié deux propositions de décision du Conseil relative à la signature et à la conclusion d'un protocole modifiant l'accord de partenariat économique entre l'Union européenne et le Japon sur la libre circulation des données, en plus de la décision d'adéquation de la Commission accordée au Japon le 23 janvier 2019. Ces textes ont pour objectif d'assurer la sécurité et de simplifier les transferts de données de l'Espace économique européen vers le Japon. Ainsi, à la suite de ces deux propositions, le Contrôleur européen de protection des données recommande d'une part, de détailler les raisons pour lesquelles de nouvelles dispositions sur les flux transfrontaliers de données ont été considérées comme nécessaires, malgré l'existence de la décision d'adéquation de 2019. D'autre part, il conseille de prévoir que chaque partie puisse adopter et maintenir des garanties qu'elle juge appropriées pour assurer la protection des données, dans le cadre des transferts transfrontaliers de données.	 Pour information
LE COIN DE L'EUROPE	12/01/2024	EDPS - Opinion 1-2024 on the Proposal for a Regulation establishing an EU Talent Pool	Le 16 novembre 2023, la Commission européenne a publié une proposition de règlement du parlement européen et du conseil portant création d'un vivier européen de talents. L'objectif est de faciliter le recrutement international et d'offrir aux ressortissants des pays tiers la possibilité d'exercer des métiers à fort pénurie à l'échelle de l'Union européenne. Dans ce cadre, le Contrôleur européen de protection des données recommande	 Pour information

			de définir les catégories spécifiques de données qui peuvent être traitées, ainsi que les rôles des différents acteurs, en particulier concernant l'information des personnes. Par ailleurs, il préconise de spécifier les catégories de données qu'il sera interdit de traiter.	
 LE COIN SANTÉ	16/01/2024	CNIL - Essais cliniques décentralisés lancement d'une phase pilote par la DGS, la DGOS, l'ANSM et la CNIL - Communiqué de presse 8 janvier 2024	Le 8 janvier 2024, la Commission nationale de l'informatique et des libertés (CNIL), la Direction générale de la santé (DGS), la Direction générale de l'offre de soins (DGOS) ainsi que l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) ont annoncé mettre en place une phase pilote pour accompagner les promoteurs dans la conception de leurs projets de recherches cliniques décentralisés. Les projets concernés ne peuvent qu'être relatifs à un projet national n'impliquant pas une première administration à l'homme, à un médicament, un dispositif médical ou un dispositif médical de diagnostic in vitro, et en cours de conception avant la soumission du projet de recherche. Les promoteurs sont invités à déposer leur dossier pendant la phase pilote, du 8 janvier 2024 au 30 juin 2024. Le promoteur devra déposer un dossier comportant une question précise sur la composante décentralisée et la problématique rencontrée, ainsi qu'une proposition de scénario complet de mise en œuvre de l'élément décentralisé, un résumé du protocole et une notice d'information destinée aux futurs participants. A la suite de cette phase pilote, les promoteurs auront la possibilité de faire part de leur retour d'expérience, permettant notamment d'alimenter les travaux de mise à jour des méthodologies de référence de la CNIL.	 Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN DE L'EUROPE	18/01/2024	EDPB - 2023 Coordinated enforcement action - Designation and position of DPO - January 2024	Depuis 2020, le Comité européen de protection des données (CEPD) a décidé de mettre en place un cadre d'application coordonnés (CEF) en vue de rationnaliser la coopération entre les autorités de contrôle. Tout au long de l'année 2023, 25 autorités de contrôle de l'espace économique européen ont lancé des enquêtes coordonnées sur le rôle des délégués à la protection des données (DPD). Ce rapport regroupe les conclusions de toutes ces autorités sur le rôle du DPD. Tout d'abord, le rapport note une absence de désignation de DPD, dans les cas de désignation obligatoire. Ensuite, il met en lumière que les ressources à disposition du DPD sont insuffisantes, mais aussi que les DPD n'ont pas toujours des connaissances précises ou une formation suffisante pour exercer leurs responsabilités. Le rapport appuie également sur le fait que les DPD ne sont pas toujours entièrement chargés de l'ensemble des tâches requises par le RGPD. Les autorités de contrôle soulignent aussi que les DPD manquent d'indépendance vis-à-vis de l'organisme dans lequel ils exercent, et que de ce fait, un conflit d'intérêt peut exister, ce qui limite l'exercice de ce rôle. Enfin, le rapport souligne que le DPD ne reporte pas toujours au plus haut niveau de l'organisme. Toutes ces lacunes pourraient, selon le CEPD, être corrigées par une plus forte sensibilisation et une plus grande clarté sur le rôle du DPD. Une liste de recommandations est établie à l'intention des organismes afin de les aider à résoudre les problématiques identifiées par le rapport. Les autorités de contrôle ont lancé des investigations dont certaines sont encore en cours.	Pour information

			Le CEPD rappelle que ce rapport ne vise pas à lister les mesures à adopter mais à refléter les actions mises en place par les autorités de contrôle compétentes, et identifier les éventuels points d'attention. Le CEPD précise qu'il serait intéressant de mettre à jour ce rapport en tenant compte de l'avancement de procédures en cours et de l'éventuelle mise à jour des lignes directrices sur le DPD par le CEPD.	
 LE COIN DE LA FRANCE	18/01/2024	Délibération n°SAN-2023-024 du 29 décembre 2023 concernant la société YAHOO EMEA LIMITED	La Commission nationale de l'informatique et des libertés (CNIL) a prononcé une sanction de 10 millions d'euros à l'encontre de la société Yahoo au titre de manquements, notamment en matière de cookies et de consentement. D'une part la société déposait au moins 20 cookies sur le terminal de l'utilisateur sans son consentement, et laissait des cookies de sociétés tierces qu'elle hébergeait se déposer également sans le recueil du consentement de l'utilisateur. D'autre part, la société incitait l'utilisateur à ne pas retirer son consentement pour la collecte de ses données en liant l'utilisation du service de messagerie à l'inscription de cookies non strictement nécessaires, sans l'en informer dès le recueil du consentement initial. Par conséquent, la CNIL a considéré que la société rendait l'utilisateur captif de ses services, et que le consentement recueilli n'était pas libre.	 S'assurer de l'information complète des personnes concernées et notamment des modalités de retrait de leur consentement
 LE COIN	18/01/2024	One-Stop-Shop case digest on Security of Processing and Data Breach Notification - Publication in January 2024	Ce rapport analyse les décisions adoptées par les autorités de contrôle dans le cadre du mécanisme de guichet unique dans le domaine de la protection des données personnelles, notamment en termes	 Pour information

DES FONDAMENTAUX			de sécurité du traitement et de notification de la violation à l'autorité de contrôle. Ce rapport permet de comprendre comment les différentes autorités de contrôle évaluent la pertinence des mesures de sécurité au regard du risque considéré. Le rapport permet de présupposer de l'insuffisance ou de l'adéquation de certaines mesures de sécurité aux yeux des autorités de contrôle (notamment la mise en place de mécanisme de contrôle des accès via l'authentification individuelle des personnes autorisées à accéder aux données).	
		Annex: One-Stop-Shop case digest on Security of Processing and Data Breach Notification	L'annexe du rapport sur la sécurité du traitement et la notification de violation de données dans le cadre du guichet unique reprend toutes les décisions citées et analysées dans le rapport susvisé.	
LE COIN DE L'EUROPE	22/01/2024	EDPS - Results of the survey on the designation and position of the data protection officer in the EU institutions, bodies, offices and agencies - January 2024	Le 18 janvier 2024, le Contrôleur européen de protection des données a publié les résultats d'une enquête qui a débuté le 27 mars 2023, sur la désignation et la position du délégué à la protection des données (DPD). Ces résultats seront utilisés par le Contrôleur pour cibler les sujets nécessitant des recommandations spécifiques, ainsi que pour cibler ses audits et enquêtes. Le Contrôleur constate que les DPD ont un réel impact au sein de l'institution dans laquelle ils travaillent. Leur niveau de connaissances, d'expériences et d'expertise est également élevé, ce qui montre que la fonction se professionnalise. Bien que les DPD soient impliqués dans toutes les tâches qui leurs sont confiées, le principal obstacle	Pour information

			est leur manque de ressources, principalement un manque de temps pour accomplir leurs tâches et de moyens en ressources humaines. Le Contrôleur envisage d'opter pour un suivi minutieux du rôle du DPD, pour une plus grande sensibilisation, pour la publication d'orientations relatives aux rôles du DPD, avec éventuellement des mesures coercitives.	
LE COIN DE L'EUROPE	22/01/2024	EDPS - Opinion 2-2024 on the Proposal for a Regulation amending the Cybersecurity Act as regards managed security services	Le 18 avril 2023, la Commission européenne a publié une proposition de règlement du parlement européen et du conseil sur les services de sécurité gérés. Cette proposition a pour objectif de permettre l'adoption de systèmes européens de certification de cybersécurité pour les services de sécurité gérés. Le Contrôleur européen de protection des données recommande d'établir une obligation pour les prestataires d'auto-déclaration de conformité des services et mesures proposées par leur intermédiaire au cadre réglementaire applicable comme condition de certification.	Pour information
LE COIN DE LA FRANCE	23/01/2024	Délibération n°SAN-2023-021 du 27 décembre 2023 concernant la société AMAZON FRANCE LOGISTIQUE	La Commission nationale de l'informatique et des libertés (CNIL) a prononcé une sanction de 32 millions d'euros à l'encontre de la société Amazon France Logistique, soit 3% de son chiffre d'affaires réalisé en 2021. La CNIL a considéré que la société a manqué à la règlementation en matière de protection des données personnelles, en raison d'un système excessif de suivi de l'activité et des performances des salariés (mesure trop précise des interruptions d'activité, système excessif de mesure d'utilisation du scanner lors du rangement des articles, durée excessive de conservation des données). La société a également été sanctionnée pour ses manquements à l'obligation d'information	S'assurer de collecter uniquement les données nécessaires et adéquates au traitement

			(à l'égard des intérimaires, et concernant la vidéosurveillance). Pour déterminer la sanction, la CNIL s'est fondée notamment sur le fait que les outils de suivi utilisés par la société sortaient du cadre classique, et également sur le nombre de salariés touchés par les manquements.	
LE COIN DES FONDAMENTAUX	23/01/2024	CNIL - Fiche pratique - Les pratiques de chiffrement dans l'informatique en nuage (cloud) public - 22 janvier 2024	Le 22 janvier, la Commission nationale de l'informatique et des libertés (CNIL) a publié une fiche pratique sur le chiffrement, qu'elle considère comme l'un des mécanismes les plus efficaces pour protéger la confidentialité des données. Cette fiche clarifie la répartition des responsabilités entre fournisseurs et clients au titre du RGPD. La Commission revient sur les trois états de la données (au repos, en transit, en traitement), et précise les différentes approches possibles. Elle rappelle à ce titre l'importance de sélectionner l'approche la plus adaptée au traitement de données concerné. La CNIL rappelle qu'elle considère le chiffrement de bout-en-bout comme la solution la plus protectrice de la vie privée, bien qu'il ne soit pas applicable à chaque traitement.	Pour information
LE COIN DES FONDAMENTAUX	23/01/2024	CNIL - Fiche pratique - Les outils de sécurisation d'applications web dans l'informatique en nuage (cloud) - 22 janvier 2024	Le 22 janvier 2024, la Commission nationale de l'informatique et des libertés (CNIL) a publié une fiche pratique relative aux outils de sécurisation d'applications web dans l'informatique en nuage pour améliorer leur performance et lutter contre les attaques par déni de service distribuées (DDoS) ou les attaques dirigées contre les applications web (injections SQL).	Vérifier les outils utilisés et le cas échéant mettre en place un plan d'actions

			Elle rappelle que les outils de sécurisation des services cloud, ou d'amélioration des performances de ces services collectent des données personnelles. A ce titre, ils soulèvent des problématiques concernant la protection des données. Ainsi, sous forme de tableau, la CNIL répertorie les outils permettant d'améliorer la performance des sites et applications web et ceux pour la sécurité et la disponibilité des services web. Elle analyse les traitements de données qu'ils effectuent. La CNIL rappelle la nécessité de vérifier, auprès des fournisseurs de cloud, les transferts (dont les accès par les autorités de pays tiers) qui pourraient intervenir par le biais des outils de sécurité intégrés nativement. La Commission précise qu'il devrait être mis en place un plan d'action le cas échéant. Enfin, la CNIL fait une analyse du protocole TLS (« Transport Layer Security » ou « sécurité de la couche de transport ») qui permet de sécuriser l'échange des flux de données des services web, en complément des outils recommandés ci-dessus. Néanmoins, ce moyen n'évince pas tous les risques. Ainsi, il est nécessaire de prendre des mesures d'atténuation des risques.	