LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Décembre 2023

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	07/12/2023	EN PROJET - Arrêté modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel	Un projet d'arrêté a été publié sur la modification du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé (HDS) à caractère personnel. Concernant la certification des HDS, les principales modifications apportées concernent : - la clarification du périmètre des types d'activité pour lesquelles les hébergeurs ont obtenu la certification ; - l'amélioration de la lisibilité des garanties apportées par l'hébergeur à chaque prestataire faisant appel à ses services ; - la clarification des obligations contractuelles des hébergeurs ;l'intégration dans le référentiel de certification HDS des évolutions de la norme ISO 27001. Le référentiel HDS révisé propose d'ajouter quatre exigences relatives à la souveraineté des données et plus précisément : - la restriction du stockage des données de santé sur le territoire d'un Etat partie de l'Espace économique européen (EEE) ;	 Pour information

			- l'information des clients de tout transfert ou accès à distance à leurs données depuis un territoire situé hors de l'EEE qui n'assure pas un niveau de protection adéquat au sens du RGPD ; - l'information des clients d'une éventuelle sujétion à une réglementation extra-communautaire qui serait susceptible d'entraîner un risque d'accès aux données par un organisme situé dans un pays qui n'assure pas un niveau de protection adéquat au sens du RGPD ; - la transparence vis-à-vis des clients potentiels : l'hébergeur doit rendre public et tenir à jour des informations détaillées sur les éventuels transferts de données qu'il héberge vers un pays n'appartenant pas à l'EEE et sur les mesures prises pour assurer le respect du RGPD. Cet arrêté ne devrait pas être adopté avant le printemps 2024.	
LE COIN DE L'EUROPE	07/12/2023	EDPS - TechSonar - 2023-2024 Report	Le Contrôleur européen de la protection des données a publié le rapport « TechSonar » pour l'année 2023-2024. Ce rapport permet de faire un point sur les technologies émergentes afin de mieux anticiper et encadrer leur développement d'un point de vue protection des données. Ce rapport	Pour information

			pointe 5 tendances qui, à la fois, sont des opportunités technologiques et des défis en termes de protection des données : - Les grands modèles linguistiques (« Large Language Models « LLM ») qui sont des systèmes d'intelligences artificielle (IA) conçu pour apprendre la grammaire, la syntaxe et la sémantique de plusieurs langues afin de générer artificiellement un langage cohérent et adapté ; - Portefeuille d'identité numérique : qui est une application permettant le stockage, la gestion et le partage sécurisés de données d'identification personnelle ; - « l'Internet des comportements » (« Internet of Behaviours » « IoB ») : ce concept décrit un réseau dans lequel les données examinées permettraient d'établir des comportements sociologiques et psychologiques humains pour notamment les influencer. Le Contrôleur note la ressemblance avec le système de publicité ciblée, mais remarque que le système IoB est beaucoup plus large que celui de la publicité ciblée. - La réalité étendue connue sous le terme anglais « extended reality » ou « XR » désigne les technologies qui	

			créent des environnements et des objets générés par ordinateur, tels que les réalités virtuelles, augmentées et mixtes. - La détection de deepfakes : Les deepfakes permettent de manipuler ou de générer artificiellement du contenu numérique pour donner l'impression qu'une personne a fait quelque chose ou qu'un événement irréel c'est vraiment produit. Ce genre de pratique peut favoriser la désinformation et avoir des effets néfastes sur l'environnement numérique. Le Contrôleur note que ces cinq tendances s'inscrivent dans un contexte de développement de nouvelles technologies sans précédents. Cependant, le fait qu'elles utilisent une large quantité de données pour pouvoir se mettre en place peut présenter un risque pour la protection des données.	
 LE COIN DE LA FRANCE	15/12/2023	CNIL - Tables informatique et libertés - Edition 2024	Les Tables Informatique et Libertés publiées par la Commission nationale de l'informatique et des libertés (CNIL) visent à rassembler l'essentiel de la jurisprudence et des décisions pertinentes de la CNIL. En effet, même si les décisions de la formation restreinte sont pour la plupart publiques, les mesures correctrices ou les décisions de rejet de plaintes portées devant elle conduisent à des prises de position pratiques quotidiennes qui ne sont pas publiées. Dans ce document,	 Pour information

			la CNIL reprend des principes généraux du droit et regroupe de nombreuses décisions de juriidctions françaises (Conseil constitutionnel, Conseil d'Etat, Cour de cassation) et européennes (CJUE, CEDH) . La CNIL reprend : - les notions clés en terme de données personnelles : personnes concernées, données sensibles, anonymisation… ; - les règles principales d'un traitement : licéité, loyauté, base légale, durée de conservation des données... ; - les règles relatives aux responsables de traitement et aux sous-traitants ; - le respect des droits des personnes ; - les règles relatives aux transferts de données ; - les règles spécifiques à certains secteurs : santé, police, justice… ; - les règles en cas d'encadrement de traitements de données par des actes administratifs ; - le principe de coopération européenne : notions, procédure… Le recueil de toutes ces décisions début en janvier 2021. Ce document a vocation à être enrichi et mis régulièrement à jour.	

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN DES RH	15/12/2023	CNIL - Guide pratique - Services de prévention et de santé au travail	La Commission nationale de l'informatique et des libertés (CNIL) a mis en place un guide pour accompagner les services de prévention et de santé au travail (SPST) dans leur mise en conformité en termes de protection des données personnelles. Ce guide est composé de trois parties : - la première reprend les notions clés de la protection des données ; - la deuxième, sous forme de neuf fiches pratiques, concerne tous les principes fondamentaux en termes de protection des données communs aux différents fichiers de données personnelles constituées par les SPST dans le cadre de leur mission : finalités, responsable de traitement, base légale, durée de conservation, droits des personnes concernées… ; - la troisième partie, également rédigée sous forme de fiches pratiques, porte sur le dossier médical en santé au travail, les études et enquêtes, ainsi que la télésanté au travail. Cinq annexes proposent des outils pratiques : tableau de synthèse sur les finalités de traitements pour les SPST, modèle de fiches de registre des activités de traitement et de notices d'informations, cahier des charges pour s'assurer de la conformité au RGPD pour les données	 ⇨ A utiliser comme une checklist pour s'assurer de la conformité en tant que service de prévention et de santé au travail

			relatives au dossier médical en santé au travail.	
LE COIN SANTÉ	16/12/2023	EDPB - Contribution of the EDPB to the report on the application of the GDPR under Article 97 - December 2023	Le Comité européen de la protection des données (CEPD) a rendu un rapport sur l'évaluation et le réexamen du RGPD. Conformément à l'article 97 du RGPD, tous les 4 ans, le CEPD doit établir ce rapport, en examinant plus particulièrement le chapitre V du RGPD relatif aux transferts de données et le chapitre VII sur la coopération et la cohérence. Cinq ans et demi après l'entrée en application du RGPD, le CEPD considère que l'application du RGPD est un succès. Le CEPD note cependant qu'il doit faire face avec les autorités nationales aux rapides évolutions technologiques et légales : data governance act, digitakl services act, digital markets act et la proposition d'IA Act. Concernant les transferts internationaux, le CEPD note que les décisions d'adéquation demeurent un outil durable pour assurer la protection des données dans le cadre d'un transfert hors Union européenne. Il recommande à la Commission européenne d'élargir et de multiplier les négociations sur les décisions d'adéquation avec les pays tiers ou les organisations internationales. De plus, Le CEPD incite également à utiliser d'autres outils tels que les BCR (règles d'entreprise contraignantes) ou les codes de conduites. En raison de l'augmentation des transferts de données, le CEPD encourage toute initiative en plus de celles déjà citées pour assurer un	Pour information

			niveau de confiance élevée de protection des données personnelles. Sur le chapitre VII du RGPD dédiée à la coopération et à la cohérence, le CEDP revient sur le mécanisme de guichet unique. Malgré plusieurs problèmes notamment ceux liés aux différents droits nationaux, le CEPD a publié plusieurs lignes directrices qui ont abouti à l'adoption d'une proposition par la Commission relative l'harmonisation des règles de procédures. Ainsi, entre le 25 mai 2018 et le 3 novembre 2023 : 3 - 813 procédures ont été initiées pour identifier l'autorité de contrôle compétente, et 1436 projets de décisions ont été émis dont 990 ont abouti à des décisions finales Le CEPD revient également sur l'assistance mutuelle entre autorités de contrôle : 971 procédures ont été déclenchées. Sur la cohérence, le CEPD souligne qu'il y a des disparités selon les Etats membres entre les missions confiées aux autorités de contrôle et les ressources humaines et financières dont elles disposent. Même s'il existe une tendance à l'augmentation des ressources financières, le taux de croissance est insuffisant pour faire face à toutes les tâches et responsabilités confiées aux autorités de contrôle. Enfin, ce rapport revient sur l'application du RGPD par les autorités nationales en termes de traitement de plaintes, de sanctions notamment et sur la promotion de la sensibilisation aux droits et obligations. Sur ce point, le CEPD relève que les autorités	

			nationales y consacrent des ressources importantes. Des tableaux récapitulatifs par Etat membre citent quelques actions menées.	
LE COIN DE LA FRANCE	16/12/2023	Délibération n°HAB-2023-003 du 7 décembre 2023 habilitant des agents de la Commission nationale de l'informatique et des libertés à procéder à des missions de vérification	Par cette délibération, la CNIL fixe la liste des agents habilités à réaliser des contrôles et des vérifications dans le cadre de la mise en œuvre de la procédure de sanction ordinaire. Cette délibération abroge la délibération précédente.	Pour information
LE COIN DE LA FRANCE	19/12/2023	Délibération n°SAN-2023-018 du 12 décembre 2023 concernant la commune de KOUROU	La Commission nationale de l'informatique et des libertés (CNIL) a prononcé une amende administrative de 5 000 euros, avec une injonction de désigner un délégué à la protection des données dans les 2 mois suivants la décision, avec une astreinte de 150 euros par jour de retard, à l'encontre de la commune de Kourou située dans la collectivité territoriale unique de Guyane. Bien qu' une mise en demeure et une sanction prononcée dans le cadre de la procédure simplifiée aient été prononcées à l'encontre de la commune, celle-ci est restée muette et ne s'est pas mise en conformité. C'est pourquoi la CNIL a sanctionné la commune d'une amende couplée d'une astreinte via la procédure ordinaire de sanction.	⇨ Vérifier les cas de désignation obligatoire d'un DPO ⇨ S'assurer que la déclaration officielle de l'identité du DPO a bien été réalisée auprès de la CNIL
LE COIN DE L'EUROPE	19/12/2023	EDPS - Opinion 52-2023 on two Proposals for Council Decisions on the signing and conclusion of Agreement between the EU and Armenia on cooperation between Eurojust and the competent	Le 14 novembre 2023, la Commission européenne a publié deux propositions de décision du Conseil : la première relative à la conclusion et la seconde relative à la signature d'un accord entre l'Union européenne (UE) et la République d'Arménie sur la coopération entre l'Agence de l'UE sur	Pour information

		authorities for judicial cooperation in criminal matters of Armenia	la coopération judiciaire en matière pénale, dite « Eurojust », et les autorités arménienne compétente dans ce même domaine. L'objectif de ces deux décisions est de renforcer la coopération judiciaire entre Eurojust et les autorités arméniennes compétentes, notamment en autorisant des transferts de données afin d'enquêter et de poursuivre pénalement les auteurs de crimes, tel que le terrorisme. Le Contrôleur européen de la protection des données (CEPD) préconise, qu'en cas de transferts ultérieurs de données aux autorités d'un pays tiers ou à une organisation internationale, Eurojust évalue et indique si les conditions et garanties en matière de données personnelles applicables au transfert initial s'applique au transfert ultérieur. Il recommande également que la violation de la licéité du traitement soit comprise largement, ce qui permettrait aux personnes concernées le droit d'obtenir l'effacement de leurs données traitées par les autorités en cas de violation de l'accord. Enfin, il propose d'impliquer les autorités nationales de protection des données de l'UE et de l'Arménie dans les futurs examens et évaluations de l'accord.	
LE COIN DE L'EUROPE	19/12/2023	EDPS - Opinion 53-2023 on the Proposal for a Directive on Soil Monitoring and Resilience	Le 5 juillet 2023, la Commission européenne a publié une proposition de directive relative à la surveillance et la résilience des sols. L'objectif de cette directive est de mettre en place un cadre de surveillance des sols de l'Union européenne. En effet, le législateur européen rappelle que les sols constituent	 Pour information

			une ressource vitale, limitée, non renouvelable et irremplaçable. Il est don essentiel d'avoir des sols en bonne santé. Pour autant, les données complètes et harmonisées sur la santé des sols issues de la surveillance font défaut. Pour pallier ce manque actuel de connaissances, le projet de directive prévoit un système de surveillance basé sur les données de l'Union, des Etats membres et du secteur privé. Le Contrôleur européen de la protection des données (CEPD) recommande notamment de clarifier par qui les données seront traitées et à quelles fins et de faire référence au RGPD si des données personnelles sont traitées.	
LE COIN DE L'EUROPE	19/12/2023	EDPS - Opinion 54-2023 on the Proposals for a Council Decision on the conclusion and signing on behalf of the Union of the amendment of the Agreement between the European Union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of value added tax	Le 24 novembre 2023, la Commission européenne a publié deux propositions de décisions du Conseil : l'une relative à la conclusion et la seconde relative à la signature d'un accord entre l'Union européenne (UE) et le Royaume de Norvège sur la coopération administrative, la lutte contre la fraude et le recouvrement de créances dans le domaine de la taxe sur la valeur ajoutée. Le Contrôleur européen de la protection des données (CEPD) préconise de - faire la distinction entre les règles de confidentialité prévues par le droit national et celles prévues par la législation européenne ; - indiquer les intérêts publics visés dans l'accord et ce, de manière exhaustive	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

			- préciser les situations et les conditions dans lesquelles les droits des personnes concernées pourront être limités.	