LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Février 2023

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	03/02/2023	CNIL - Le Conseil national de l'Ordre des médecins et la CNIL signent une convention de partenariat - Communiqué de presse 3 février 2023	La CNIL et le Conseil national de l'Ordre des médecins (CNOM) ont signé une convention de partenariat concrétisant la collaboration essentielle entre les deux entités pour la protection des données de santé. L'objectif est de réaffirmer leurs engagements en matière de protection des données de santé et de sensibiliser davantage les acteurs concernés quant à la protection de ces données.	 Pour information

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN SANTÉ	07/02/2023	Délibération n°2022-124 du 13 octobre 2022 portant adoption d'un référentiel portant sur la description et les garanties de procédure permettant la mise à disposition en vue de leur traitement de l'échantillon du système national des données de santé (ESND) et des bases de données thématiques appelées « datamarts » du système national d'information interrégimes de l'assurance maladie (SNIIRAM) présentant un faible risque d'impact sur la vie privée et abrogeant la délibération n° 2020-072 du 16 juillet 2020	La CNIL a actualisé le référentiel encadrant la mise à disposition des données de l'échantillon généraliste des bénéficiaires (EGB) et des bases de données thématiques appelées datamarts du SNIIRAM établi par la délibération n°2020-072 du 16 juillet 2020. En effet, en octobre 2022, l'assurance maladie a fait évoluer l'EGB qui est devenu l'échantillon des données du SNDS (ESND). La mise à jour du référentiel porte sur - La profondeur historique d'accès aux données de l'ESND ; - L'information des personnes : information collective des personnes à faire figurer sur le site internet du responsable de traitement ainsi que du laboratoire de recherche ou du bureau d'études réalisant l'étude. Si un même responsable de traitement réalise plusieurs études à partir des données du SNDS, un portail de transparence devra être mis en place. La procédure d'accès simplifié pour la mise en œuvre d'études est maintenue. Aussi, les traitements présentant un faible risque d'impact sur la vie privée et sous réserve du respect d'un certain nombre de conditions telles que la finalité, les modalités d'accès ou la durée, feront l'objet d'un examen unique par la Plateforme des données de santé, il ne sera donc pas nécessaire d'obtenir l'avis du Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES), ni l'autorisation de la CNIL. L'examen de la	 ⇨ Pour information pour toute étude portant sur l'échantillon des données du SNDS (ESND) et datamarts du SNIIRAM

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			Plateforme est réalisé dans un délai de quinze jours. Ce référentiel est entré en vigueur le 5 février 2023.	

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN SANTÉ	16/02/2023	Décret n°2023-99 du 15 février 2023 modifiant le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n°2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, et le décret n°2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid-19	La loi du 30 juillet 2022 a mis fin aux régimes d'exception créés pour lutter contre la covid-19. A ce titre, ce décret modifie les textes autorisant les traitements de données à caractère personnel dans ce cadre. Le décret abroge les dispositions relatives au traitement de données à caractère personnel « Contact Covid » et modifie les modalités du traitement « SI-DEP » et des traitements mis en œuvre par les agences régionales de santé (ARS). Il modifie les finalités du traitement « SI-DEP » et des traitements des ARS, la liste et les destinataires des données traitées, et les modalités d'exercice de leurs droits par les personnes concernées. Il limite, du 1er février 2023 au 30 juin 2023, la possibilité de mettre en œuvre des systèmes d'informations dédiés à la lutte contre la covid-19 aux finalités suivantes : – Faciliter la surveillance épidémiologique aux niveaux national et local ainsi que la recherche sur le virus et sur les moyens de lutter contre sa propagation ; – La délivrance d'un justificatif d'absence de contamination par la covid-19 ou d'un certificat de rétablissement aux personnes ayant consenti au partage de leurs données dans ce but. Ce décret complète également la liste des données traitées dans le cadre du traitement de données à caractère personnel « Vaccin Covid » en y ajoutant l'identifiant unique de certificat de vaccination.	 Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE L'EUROPE	16/02/2023	EDPS - Avis 1-2023 concernant la proposition de règlement pour une Europe interopérable - Janvier 2023	Dans cet avis, le Contrôleur européen de la protection des données (Contrôleur) se prononce sur la proposition de règlement européen établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union européenne (règlement pour une Europe interopérable). L'objectif de ce règlement est de promouvoir l'interopérabilité des services publics au sein de l'Union, notamment dans le cadre d'infrastructures numériques. L'avis du contrôleur s'attarde principalement sur les dispositions relatives à la mise en place de bacs à sable réglementaires et aux traitements de données à caractère personnel mis en œuvre dans ces bacs à sable. Il propose des garanties supplémentaires pour assurer la protection des données à caractère personnel dans ce cadre.	Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE L'EUROPE	16/02/2023	EDPS - Avis 2-2023 sur les propositions de directives relatives à des normes applicables aux organismes pour l'égalité de traitement dans le domaine de l'égalité de traitement - Janvier 2023	Dans cet avis, le Contrôleur européen de la protection des données (Contrôleur) se prononce sur les propositions de directives relatives à des normes applicables aux organismes pour l'égalité de traitement dans le domaine de l'égalité de traitement. L'objectif de ces propositions est de garantir l'application du principe d'égalité de traitement par les organismes pour l'égalité de traitement en mettant en place des exigences minimales relatives à leur fonctionnement. Le Contrôleur considère qu'il est nécessaire de renforcer la sécurité juridique vis-à-vis des données sensibles, de clarifier le champ d'application des données traitées, d'énumérer de manière exhaustive les données sensibles pouvant être traitées dans le cadre de ces propositions, et de préciser les mesures de protection pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.	 Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE L'EUROPE	16/02/2023	EDPS - Opinion 2-2023 on the Proposal for a Council Regulation on jurisdiction, applicable law, recognition of decisions and acceptance of authentic instruments in matters of parenthood - February 2023	Dans cet avis, le Contrôleur européen de la protection des données (Contrôleur) se prononce sur la proposition de règlement européen relatif à la compétence, à la loi applicable, à la reconnaissance des décisions et à l'acceptation des actes authentiques en matière de filiation ainsi qu'à la création d'un certificat européen de filiation. L'objectif de cette proposition est de mettre en place des règles communes aux Etats membres concernant l'établissement de la filiation dans des situations transfrontières et de créer un certificat européen de filiation. Le Contrôleur accueille favorablement la proposition de règlement, notamment les références faites à l'application des législations européennes en matière de protection des données, la détermination des responsables de traitement ainsi que la clarification apportée concernant le traitement de données sensibles.	 Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN DE L'EUROPE	16/02/2023	EDPS - Avis 4-2022 sur la proposition de directive relative aux structures avec actions à votes multiples dans les entreprises qui demandent l'admission à la négociation de leurs actions sur un marché de croissance des PME - Février 2023	Dans cet avis, le Contrôleur européen de la protection des données (Contrôleur) se prononce sur la proposition de directive relative aux structures avec actions à vote multiples dans les entreprises qui demandent l'admission à la négociation de leurs actions sur un marché de croissance des petites et moyennes entreprises (PME). L'objectif de cette proposition est de mettre en place une harmonisation minimale des législations nationales sur les structures avec actions à votes multiples des entreprises cotées sur les marchés de la croissance des PME, en laissant une large marge de manœuvre aux Etats membres. Le Contrôleur considère que la proposition porte atteinte au droit au respect de la vie privée et à la protection de données à caractère personnel des personnes concernées, en prévoyant notamment la publication de l'identité des détenteurs d'actions à votes multiples ou des personnes habilitées à exercer des droits de vote en leur nom ou des détenteurs de titres bénéficiant de droits de contrôle spéciaux. A ce titre, il recommande d'ajouter un considérant précisant que le RGPD est applicable aux traitements de données à caractère personnel mis en œuvre dans le cadre de la proposition. Il indique également qu'il est nécessaire de préciser le ou les objectifs d'intérêt public poursuivis justifiant le caractère public des données concernées, et d'envisager un mécanisme permettant de limiter l'accès à ces données aux parties démontrant un intérêt légitimes lié aux objectifs de la proposition.	Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE L'EUROPE	16/02/2023	EDPS - Opinion 5-2023 on the Proposal for a Directive of the European Parliament and of the Council harmonising certain aspects of insolvency law - February 2023	Dans cet avis, le Contrôleur européen de la protection des données (Contrôleur) se prononce sur la proposition de directive harmonisant certains aspects du droit de l'insolvabilité. L'objectif de cette proposition est de mettre en place des règles afin de renforcer la convergence des dispositions nationales au sein de l'Union européenne concernant les procédures d'insolvabilité des entreprises non bancaires. Le Contrôleur se concentre ici sur les dispositions qui peuvent avoir un impact sur le droit fondamental à la protection des données. De manière générale, ces recommandations tendent au renforcement des garanties liées à la protection des données, notamment concernant l'accès aux différents registres concernés et l'interconnexion des plateformes d'enchères. A cet égard, le Contrôleur recommande également que les actes d'exécution de la Commission pour mettre en place cette interconnexion soient mis en place rapidement. Il est également nécessaire de clarifier si le futur règlement relatif à la numérisation de la coopération judiciaire et de l'accès à la justice dans les affaires transfrontières civiles, commerciales et pénales, sera utilisé comme référence pour les communications électroniques prévues par la proposition de directive.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN DE L'EUROPE	16/02/2023	EDPS - Opinion 6-2023 on the proposals for regulations on the collection and transfer of advance passenger information (API)	Dans cet avis, le Contrôleur européen de la protection des données (Contrôleur) se prononce sur les propositions de règlements relatifs à la collecte et au transfert des informations préalables sur les passagers (données API). Les objectifs de ces règlements sont notamment de renforcer et faciliter l'efficacité des contrôles aux frontières et de combattre l'immigration illégale ; de mettre en place des règles plus efficaces pour la collecte et le transfert des données API par les transporteurs aériens afin de prévenir, détecter, enquêter et poursuivre les infractions terroristes et crimes graves. Le Contrôleur se concentre sur la nécessité et la proportionnalité des traitements de données API des vols intra-UE envisagés par les propositions et leur compatibilité avec la directive relative aux données des passagers (dite directive PNR) telle qu'interprétée par la Cour de justice de l'Union (CJUE). Il considère que les dispositions mises en place par les propositions pour les vols intra-UE assurent la conformité au jugement de la CJUE concernant l'article 2 de la directive PNR (C-817/19 – cf. tableau des actualités Décembre 2022 / Coin Europe). Cependant, il encourage les législateurs européens à harmoniser les critères de sélection des vols intra-UE pour lesquels les données API devraient être collectées. Le Contrôleur recommande également de renforcer les garanties relatives à la protection des données traitées, notamment en ayant recours à la pseudonymisation ou au cryptage des données API.	Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	16/02/2023	Délibération n°2023-006 du 19 janvier 2023 portant avis sur un projet de décret modifiant le décret n°2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n°2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions et le décret n°2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid-19	Dans cette délibération, la CNIL se prononce sur le projet de décret mentionné. Ce décret vise à abroger les dispositions relatives à « Contact Covid », à modifier les modalités relatives au traitement « SI-DEP » et les finalités pour lesquelles les agences régionales de santé (ARS) peuvent mettre en œuvre des traitements de données dans le cadre de la lutte contre la covid-19, et à modifier la liste des données traitées dans le système d'information « Vaccin Covid ». La CNIL se prononce concernant le droit d'opposition et le droit d'effacement des personnes concernées dans le cadre du traitement « SI-DEP » et des traitements mis en œuvre par les ARS. A ce titre, elle considère qu'il est nécessaire de clarifier les modalités d'exercice des droits des personnes concernées.	 Pour information
 LE COIN DE LA FRANCE	16/02/2023	Délibération n°HAB-2023-001 du 9 février 2023 habilitant des agents de la Commission nationale de l'informatique et des libertés à procéder à des missions de vérification	Cette délibération fixe la liste des agents de la CNIL habilités à effectuer des visites et vérifications des lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel.	 Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	16/02/2023	CNIL - Enseignement supérieur mise en demeure de deux établissements pour non-conformité au RGPD - 13 février 2023	Fin 2022, la présidente de la CNIL a mis en demeure deux établissements de l'enseignement supérieur pour non-conformité au RGPD. Plusieurs manquements ont été relevés concernant : – La durée de conservation des données à caractère personnel des étudiants ; – L'information des étudiants ; – L'absence de contrats de sous-traitance encadrant les relations entre le responsable de traitement et ses sous-traitants ; – La sécurité des données. Les établissements ont été mis en demeure de se mettre en conformité dans un délai de deux mois. A défaut, une sanction pourra être prononcée.	 ⇨ Vérifier la durée de conservation des données ⇨ Vérifier les mesures d'information des personnes concernées ⇨ S'assurer de l'existence d'un contrat de sous-traitance précisant les missions du sous-traitant ⇨ Vérifier les mesures de sécurité mises en place

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE L'EUROPE	24/02/2023	EDPB - Work programme 2023-2024	Le 14 février 2023, le Comité européen de protection des données a adopté son programme de travail pour 2023/2024. Pendant ces deux années, le comité concentrera son travail autour de quatre piliers concernant la protection des données : – Faire progresser l'harmonisation et faciliter la mise en conformité avec la législation européenne ; – Soutenir une application effective et une coopération efficace entre les autorités nationales de protection des données ; – Mettre en œuvre une approche des nouvelles technologies fondée sur les droits fondamentaux ; – Prendre en compte la dimension mondiale relative à la protection des données en promouvant des standards communs pour le transfert de données hors-UE et un modèle commun de protection des données auprès de la communauté internationale.	 Pour information

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE L'EUROPE	24/02/2023	EDPS - EDPS pilot use of open-source-software - Press Release 2023	Le Contrôleur européen de la protection des données (Contrôleur) a commencé à tester l'utilisation du logiciel libre Nextcloud et LibreOffice Online. L'objectif est de permettre aux institutions, organes et agences de l'Union européenne de partager des documents, envoyer des messages, faire des appels vidéo et rédiger conjointement des documents dans un environnement sécurisé et conforme notamment au RGPD. Le logiciel étant fourni par un prestataire de services basé dans l'Union européenne, cela évite le transfert de données à caractère personnel en dehors de l'Union et garantit le respect de la législation européenne sur la protection des données.	⇨ En cas d'utilisation d'un système de partage de documents/messages ou appels, basé en dehors de l'Union européenne, s'assurer que les conditions générales d'utilisation prévoient la mise en place des clauses contractuelles types et des mesures de sécurité appropriées.

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN DES FONDAMENTAUX	24/02/2023	ENISA - Demand Side of Cyber Insurance in the EU	Ce rapport publié par l'Agence de l'Union européenne pour la cybersécurité (ENISA) analyse les défis et perspectives des opérateurs de services essentiels dans le cadre de l'acquisition de services de cyber assurance. Le rapport s'intéresse exclusivement à la partie demande du marché de la cyber assurance. Cette analyse aborde différentes modalités du processus de contractualisation d'une cyber assurance. Elle montre qu'une grande majorité des opérateurs de services essentiels considère les cyber assurances comme moins attrayantes, notamment du fait de leur prix élevé et de la diminution de leur couverture. Ce rapport fournit des conseils aux responsables de l'élaboration des politiques dans l'UE et aux Etats membres, ainsi qu'à l'ensemble des opérateurs de services essentiels. L'objectif est de détecter les potentiels obstacles qui empêchent les opérateurs de services essentiels d'acheter une cyber assurance, et de proposer des recommandations pour améliorer la cyber sécurité. Ce rapport fait écho à la récente loi française d'orientation et de programmation du ministère de l'intérieur (dite LOPMI) promulguée le 24 janvier 2023 qui a modifié le Code des assurances. Désormais, les clauses de remboursement des cyber-rançons par les assurances seront encadrées. Le remboursement sera conditionné au dépôt d'une plainte de la victime dans les 72 heures après connaissance de l'infraction. Applicable trois	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			mois après la promulgation de la loi, cette obligation sera limitée aux professionnels.	

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DES FONDAMENTAUX	24/02/2023	ENISA - Developing National Vulnerability Programmes	Ce rapport de l'Agence de l'Union européenne pour la cybersécurité (ENISA) se concentre sur la divulgation coordonnée des vulnérabilités. Cette divulgation consiste en un processus de coopération dans lequel les vulnérabilités sont signalées au propriétaire du système d'information afin de lui donner la possibilité d'y remédier avant que des informations sur ces vulnérabilités soient divulguées à des tiers ou au public. Ce rapport fait état de la fragmentation de l'écosystème européen de divulgation coordonnée des vulnérabilités. Malgré des approches et initiatives nationales intéressantes, des actions supplémentaires sont nécessaires, tant au niveau national qu'européen, dans un objectif d'uniformisation, notamment afin d'encourager le développement de pratiques plus efficaces en matière de sécurité. L'objectif de ce rapport est de comprendre les attentes des industries concernant les politiques de divulgation coordonnée des vulnérabilités, de s'intéresser aux défis concernant le développement de telles politiques, et d'identifier les tendances, perspectives, et désaccords partagés. En outre, le rapport fournit des informations permettant de mieux comprendre les composantes et acteurs inclus dans l'établissement et le développement des politiques et programmes de divulgation coordonnée des vulnérabilités.	Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DES FONDAMENTAUX	24/02/2023	ENISA & CERT-EU - Joint Publication - Sustained activity by specific threat actors	L'Agence de l'Union européenne pour la cybersécurité (ENISA), conjointement à l'Equipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE), a rédigé une publication pour alerter sur l'activité soutenue d'acteurs présentant une menace dans l'Union par leurs cyber activités malveillantes envers les entreprises et gouvernements européens. A ce titre, les deux entités ont émis des recommandations adressées aux organisations des secteurs public et privé afin de réduire ces menaces et limiter leurs impacts. Ces recommandations concernent notamment la prévention, la détection et la réponse à de telles menaces. La publication recense également les acteurs principaux représentant une menace et leurs récentes actions, et décrit les principales techniques utilisées par ces acteurs.	Pour information

LE **COIN** DU **DPO**
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DES FONDAMENTAUX	24/02/2023	ANSSI - Rapport de la cybermenace 2022	L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié un rapport sur les tendances de la cyber menace en France pour l'année 2022, fin janvier. L'Agence constate que malgré une diminution du nombre d'intrusions avérées entre 2021 et 2022, le niveau de la menace ne faiblit pas. Les acteurs malveillants améliorent leurs capacités, principalement à des fins de gain financier, d'espionnage et de déstabilisation. Le rapport indique que ce sont toujours les mêmes faiblesses qui sont exploitées, notamment les vulnérabilités, les usages numériques non maîtrisés et les faiblesses dans la sécurisation des données.	 ⇨ Veiller à : – Appliquer rigoureusement une politique de mise à jour ; – Sensibiliser régulièrement les utilisateurs ; – Développer/améliorer les capacités de détection et de traitement d'incidents.
 LE COIN SANTÉ	24/02/2023	CNIL - Carte Vitale électronique quelles conséquences pour les personnes - Communiqué de presse 22 février 2023	L'expérimentation de la « e-carte Vitale », débutée depuis 2019, a été généralisée à toute la France depuis le 1er janvier 2023. La e-carte Vitale est une version dématérialisée de la carte vitale. L'objectif est de permettre une dématérialisation complète des demandes de remboursements liées aux dépenses de santé et de faciliter l'identification sur les services numériques en santé. La CNIL a relevé plusieurs points d'attention lors de l'examen du projet de texte au regard de la protection de la vie privée et de la sécurité des données personnelles. L'ensemble des assurés sociaux devrait pouvoir bénéficier de la e-carte Vitale le 31 décembre 2025.	 Pour information