

OCTOBRE 2022

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	04/10/2022	Arrêté du 23 septembre 2022 relatif à la mise en œuvre du « Répertoire national des établissements sanitaires, médico-sociaux et sociaux » (FINESS)	Cet arrêté abroge l'arrêté du 13 novembre 2013 relatif à la mise en œuvre d'un répertoire national des établissements sanitaires et sociaux. Au sein du répertoire FINESS sont partagées des informations sur l'identité des personnes morales intervenants dans les secteurs sanitaire, social ou médico-social. L'arrêté détermine les conditions applicables au Répertoire national des établissements sanitaires, médicaux-sociaux et sociaux et précise que les autorités d'enregistrement des personnes morales dans ce répertoire sont responsables de la vérification et de la mise à jour des données.	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	04/10/2022	Arrêté du 23 septembre 2022 relatif à la mise en œuvre du « Répertoire partagé des professionnels intervenant dans le système de santé » (RPPS)	Cet arrêté traite du répertoire partagé des professionnels intervenant dans le système de santé (RPPS) et définit son champ d'application. Le RPPS est mis en œuvre par l'Agence du numérique en santé. Il vise à partager des informations de référence sur les professionnels du secteur sanitaire, social ou médico-social dès lors qu'ils interviennent ou sont susceptibles d'intervenir dans le système de santé. Deux catégories de professionnels de santé peuvent être enregistrés dans le RPSS : - les professionnels de santé tenus se faire enregistrer ; - les professionnels des secteurs sanitaire, médico-social et social appelés à bénéficier de moyens d'identification électronique leur permettant d'accéder de manière sécurisée à des services du numérique en santé. La liste de ces professionnels est publiée sur le site internet de l'Agence du numérique en santé. Les autorités d'enregistrement qui alimentent le RPSS ont jusqu'au 24 septembre 2023 pour adapter leur système d'information aux nouvelles catégories de données collectées.	 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	04/10/2022	CNIL – Communiqué de presse – Désignation d'un délégué à la protection des données : bilan des mises en demeure prononcées à l'encontre de 22 communes	La CNIL a clôturé 18 mises en demeure sur 22 à l'encontre de communes qui n'avaient pas désigner de DPO. En effet, aux termes du RGPD, la désignation d'un DPO est obligatoire pour tout traitement de données personnelles effectué par une autorité publique ou un organisme public. La CNIL rappelle que cette obligation concerne toutes les collectivités territoriales, indépendamment de leur taille. Sur les quatre mises en demeure restantes, deux communes sont en cours de désignation d'un DPO, les deux autres n'avaient pas, à la date du communiqué de presse, ni répondu à la CNIL, ni désigné officiellement un DPO via le téléservice de la CNIL.	 ⇒ S'assurer des cas de désignation d'un DPO dans votre organisme ⇒ En cas de désignation d'un DPO, vérifier que les démarches de désignation ont été effectuées sur le site internet de la CNIL
 LE COIN DE LA FRANCE	18/10/2022	Délibération n°2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés et abrogeant la délibération n°2017-012 du 19 janvier 2017	Face aux piratages et autres problèmes liés à la sécurité informatique, la CNIL met à jour sa recommandation de 2017 sur les mots de passe. La CNIL rappelle que les solutions d'authentification forte ou à plusieurs facteurs fournissent une meilleure protection que l'authentification par mots de passe. La CNIL revient sur les risques liés à une mauvaise gestion des mots de passe et apporte des recommandations sur la robustesse des mots de passe ou encore la conservation des mots de passe. Au titre des changements par rapport à 2017, la CNIL précise que le renouvellement périodique des mots de passe n'est pas une mesure réellement efficace.	 ⇒ Mettre à jour la politique des mots de passe au sein de votre organisme

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DES FONDAMENTAUX	18/10/2022	Décret n°2022-1327 du 17 octobre 022 portant injonction, au regard de la menace grave contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion	Afin de répondre à un objectif de sauvegarde de la sécurité nationale, les opérateurs de communications électroniques ainsi que toutes les personnes dont l'activité vise à offrir un accès à des services de communication au public en ligne sont tenus de conserver pour une durée d'un an les données de trafic et de localisation de leurs abonnés : date, horaire, durée de chaque communication ou connexion, destinataires des communications, localisation de la communication...	 ⇒ En cas de service de communication au public en ligne, vérifier la durée de conservation des données de trafic et de localisation

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	18/10/2022	Décret n°2022-1313 du 13 octobre 2022 relatif à l'encadrement des jours, horaires et fréquence des appels téléphoniques à des fins de prospection commerciale non-sollicitée	A compter du 1^{er} mars 2023, le décret n°2022-1313 fixe les jours, horaires et fréquence au cours desquels les consommateurs peuvent être sollicités par téléphone à des fins de prospection commerciale non sollicitée. Le décret précise que le démarchage téléphonique est autorisé du lundi au vendredi de 10 heures à 13 heures et de 14 heures à 20 heures. Il ne peut être réalisé le samedi, dimanche et jours fériés. Tous les consommateurs sont concernés aussi bien ceux inscrits sur la liste d'opposition Bloctel que ceux ayant un contrat en cours avec le prospecteur commercial. Le décret interdit également qu'un consommateur soit contacté à des fins de prospection commerciale plus de quatre fois par mois par le même professionnel ou une personne agissant pour son compte. S'il refuse tout démarchage téléphonique au cours d'une conversation avec un professionnel, le consommateur ne pourra pas être contacté par celui-ci pendant une période de soixante jours à compter du refus. Toute violation de ces dispositions expose son auteur à une amende de 75 000 € pour une personne physique et 375 000 € pour une personne morale.	 ⇒ En cas de prospection commerciale, préparer votre organisme à la modification de la réglementation

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE L'EUROPE	18/10/2022	European Commission – Questions & Answers : EU-U.S Data Privacy Framework	Le 25 mars 2022, la présidente de la Commission européenne et le Président américain Joe Biden annonçaient la conclusion d'un accord de principe pour la mise en place d'une décision d'adéquation entre l'Union européenne et les Etats-Unis sur la protection des données à caractère personnel. En effet, depuis l'invalidation du Privacy Shield par la Cour de justice de l'Union européenne, les transferts de données vers les Etats-Unis supposent d'être encadrés par des garanties complémentaires telles les clauses contractuelles types. La situation devrait changer dans les prochains mois. Le 7 octobre 2022, Joe Biden signait un décret exécutif permettant de mettre en place l'accord de principe annoncé en mars 2022. Dans ce contexte, la Commission européenne prépare un projet de décision d'adéquation. Ce Q&A répond aux questions posées dans le cadre de la mise en place de cette future réglementation.	 ⇒ Surveiller l'évolution des négociations sur l'adoption d'une décision d'adéquation avec les Etats-Unis

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE L'EUROPE	18/10/2022	EDPB – Statement 4-2022 on the design choices for a digital euro from the privacy and data perspective – October 2022	Face au développement des cryptomonnaies, la banque centrale européenne (BCE) a décidé de réaliser une période expérimentale de 24 mois afin de mettre en place un euro numérique. L'euro numérique serait l'équivalent des billets en euros sous forme dématérialisée accessibles aussi bien aux particuliers qu'aux entreprises. Cette monnaie existerait parallèlement aux espèces, sans les remplacer. La Commission européenne a annoncé, en février 2022, son intention de travailler sur un projet de réglementation relatif à la mise en place de l'euro numérique. Dans cette optique, le CEPD attire l'attention des autorités sur différents aspects : la confidentialité et la protection des données dès la conception et par défaut ; - le fait d'éviter la validation et le suivi systématique des transactions ; La mise en place d'un seuil de confidentialité hors-ligne et en ligne pour lequel il ne devrait y avoir de traçage des transactions ; - la mise en place d'un cadre réglementaire spécifique pour l'euro numérique - le renforcement du débat public sur la protection des données dans les paiements numériques.	 Pour information

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE L'EUROPE	18/10/2022	EN CONSULTATION - EDPB – Guidelines 9-2022 on personal data breach notification under GDPR – October 2022	Consultation jusqu'au 29 novembre 2022. Cette consultation publique concerne la mise à jour des lignes directrices de 2017 sur la notification de violation des données personnelles dans le cadre du RGPD. La consultation publique ne porte que sur un seul paragraphe des lignes directrices lequel précise que la présence d'un représentant dans un Etat membre ne déclenche pas le système de guichet unique. Ainsi, en cas de violation de données, celle-ci devra être notifiée à chaque autorité auprès de laquelle les personnes concernées résident. Cette notification devra être effectuée conformément au mandat donné par le responsable de traitement à son représentant et sous la responsabilité de celui-ci.	 Pour information

 LE COIN DE L'EUROPE	18/10/2022	EDPS – Opinion 20-2022 on the Recommendation for a Council Decision authorizing the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law	Le 18 août 2022, la Commission européenne a publié une recommandation à propos d'une décision du Conseil autorisant l'ouverture des négociations au nom de l'Union européenne pour une convention du Conseil de l'Europe sur l'intelligence artificielle (IA), les droits de l'homme, la démocratie et l'Etat de droit. La Convention sera régulée par l'Intelligence Artificial Act (AI Act). Considérant que la convention est une occasion de compléter l'AI Act, le Contrôleur européen pour la protection des données souhaite que la convention puisse fournir des garanties claires et fortes pour les personnes concernées par l'usage de l'intelligence artificielle. Le contrôleur a émis quatre (4) recommandations sur cette convention : - Donner une place plus importante à la sauvegarde des droits des individus - Inclure dans une directive spécifique la référence explicite à la conformité de la convention au cadre européen sur la protection des données - Interdire les systèmes d'Intelligence artificielle présentant des risques inacceptables - Promouvoir l'adoption de l'approche d'une protection des données dès la conception et par défaut à chaque étape du cycle de vie d'un système d'intelligence artificielle.	 Pour information
--	-------------------	---	---	---

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	20/10/2022	Délibération n°SAN-2022-019 du 17 octobre 2022 concernant la société CLEARVIEW AI	La CNIL a prononcé, le 17 octobre 2022, une sanction de 20 millions d'euros à l'encontre de la société CLEARVIEW AI. Après la réception de plaintes de particuliers en raison du logiciel de reconnaissance faciale Clearview AI, la CNIL a ouvert une enquête. L'enquête a permis de démontrer plusieurs manquements au RGPD et notamment un traitement illicite des données personnelles en raison d'une collecte et d'une utilisation de données personnelles sans base légale ainsi qu'un non-respect du droit des personnes. Mise en demeure en novembre 2021 de se mettre en conformité sous un délai de deux mois, la société CLEARVIEW AI n'a apporté aucune réponse à la CNIL. C'est pourquoi la CNIL a prononcé une sanction maximale à l'encontre de cette société, accompagnée d'une injonction de cesser la collecte, sans base légale, et l'utilisation des données de personnes se trouvant en France et de supprimer celles collectées dans un délai de deux mois. Cette injonction a été assortie d'une astreinte de 100 00 euros par jour de retard passé ce délai.	 ⇒ S'assurer que chaque traitement de données dispose d'une base légale prévue par le RGPD ⇒ Vérifier la procédure d'exercice des droits des personnes

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 OUTILS	26/10/2022	CNIL - Elections professionnelles et données personnelles : questions-réponses – Communiqué de presse 2 octobre 2022	Au cours des élections professionnelles, les données personnelles des électeurs sont utilisées et collectées par les employeurs publics et privés et les prestataires de solution de vote électronique. Par un question-réponse, la CNIL rappelle certains principes à respecter : les mentions que l'employeur peut faire figurer sur la liste électorale concernant ses salariés, les identifiants et mots de passe utilisés pour voter, l'information des électeurs sur l'utilisation de leurs données personnelles...	 ⇒ A utiliser comme une check-list au sein de votre organisme en cas d'organisation d'élections professionnelles
 LE COIN DE LA FRANCE	31/10/22	Conseil d'État, 21 octobre 2022, n°459254	Le Conseil d'Etat précise que la CNIL doit motiver son refus de donner suite aux plaintes fondées sur la méconnaissance du droit d'accès. En outre, le délégué à la protection des données peut faire l'objet d'un licenciement en raison de manquements aux règles applicables à l'ensemble des salariés d'une entreprise, dès lors que ces règles ne sont pas incompatibles avec son indépendance garantie par le RGPD.	 ⇒ En cas de volonté de licencier votre DPO sur ce fondement vérifier la compatibilité des règles applicables aux salariés de l'entreprise avec les règles d'indépendance applicables au DPO
 LE COIN DES OUTILS	31/10/22	Décret n°2022-1366 du 27 octobre 2022 complétant la liste des finalités et des catégories de responsables des traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire	Ce décret modifie le décret cadre « NIR » précisant les conditions spécifiques du traitement du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. Le décret élargit le nombre de cas dans lesquels le recours à cet identifiant est autorisé et souvent en dehors de la sphère médico-sociale.	 ⇒ En cas de collecte du NIR, s'assurer des cas autorisés par le décret

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 OUTILS	31/10/22	Délibération n°2022-087 du 21 juillet 2022 portant avis sur un projet de décret modifiant le décret n°2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire	La CNIL s'est prononcée sur le projet de décret visant à élargir les cas d'utilisation du NIR comme identifiant des personnes.	 Pour information
 LE COIN DE LA FRANCE	31/10/22	CNIL - L'autorité de protection des données de Corée du Sud (PIPC) et la CNIL signent une déclaration de coopération - Communiqué de presse 26 octobre 2022	Afin de renforcer leur compréhension des nouvelles technologies et faire face aux défis posés par la protection des données personnelles, l'autorité de protection des données de Corée du Sud (PIPC) et la CNIL ont signé une déclaration de coopération qui prévoit: - la conduite de recherches conjointes liées aux nouvelles technologies et aux questions de protection des données ; - le partage de bonnes pratiques et d'expérience ; - l'organisation d'ateliers de formation ; - l'échange d'agents entre les deux autorités.	 Pour information