

SEPTEMBRE 2022

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DES FONDAMENTAUX	08/09/2022	CNIL - Les jetons individuels de connexion ou token access - Communiqué de presse 8 septembre 2022	Dans ce communiqué, la CNIL aborde le sujet des token access ou jetons de connexion. Les jetons d'accès permettent une connexion sécurisée à un espace personnel, un compte ou des documents bureautiques. La CNIL revient sur les usages, les enjeux et les bonnes pratiques à appliquer en la matière. La CNIL insiste notamment sur les risques d'hameçonnage et autres risques de sécurité lorsqu'une authentification à double facteur n'a pas été mise en place.	 ⇒ A utiliser comme outil de contrôle pour s'assurer du respect de la réglementation
 LE COIN DE LA FRANCE	13/09/2022	Délibération n° HAB-2022-005 du 8 septembre 2022 habilitant des agents de la Commission nationale de l'informatique et des libertés à procéder à des missions de vérification	Délibération de la CNIL précisant la liste des agents habilités, en raison de leurs fonctions, à effectuer des vérifications auprès d'organismes.	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE L'EUROPE	13/09/2022	Opinion 19/2022 on the Proposal for a Regulation on standards of quality and safety for substances of human origin intended for human application and repealing Directives 2002/98/EC and 2004/23/EC	Cet avis du CEPS vise la proposition de règlement européen concernant les normes de qualité et de sécurité des substances d'origine humaine destinées à une application humaine et abrogeant les directives 2002/98/CE et 2004/23/CE. Cette proposition de règlement a pour objet de réglementer les normes de qualité et de sécurité pour les substances d'origine humaine destinées à une application humaine en garantissant la sécurité et la qualité pour les patients traités avec de thérapies à base de substances d'origine humaine et les protéger pleinement des risques évitables liés aux substances d'origine humaine. La proposition vise également à garantir la sécurité et la qualité pour les donneurs et pour les enfants nés de dons d'ovules, sperme ou d'embryons et ce, en renforçant et en permettant l'harmonisation des pratiques de surveillance entre les Etats membres. Pour le CEPS, cette proposition a un impact positif sur les droits fondamentaux des citoyens : protection de la santé, non-discrimination, vie privée, consentement éclairé. Le CEPS rappelle que le consentement éclairé du donneur au don de matériel dans le cadre de ce règlement, tout en étant une exigence éthique et juridique, n'est pas le même que le consentement mentionné dans le RGPD comme l'une des bases légales pour le traitement des données personnelles.	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	13/09/2022	Délibération de la formation restreinte n° SAN-2022-018 du 8 septembre 2022 concernant le GIE INFOGREFFE	La CNIL a sanctionné le GIE INFOGREFFE d'une amende de 250 000 euros pour deux manquements principaux : - Un manquement relatif à la durée de conservation des données - Un manquement concernant l'obligation d'assurer la sécurité des données personnelles. La CNIL relève notamment que si INFOGREFFE avait donné des instructions spécifiques en matière d'anonymisation et de sécurité à son sous-traitant, il apparaît qu'il n'a pas suivi l'exécution de ses instructions. Il n'a pas exercé un contrôle satisfaisant et régulier sur les mesures techniques et organisationnelles mises en œuvre par son sous-traitant pour assurer la conformité au RGPD et, notamment pour assurer l'anonymisation et la sécurité des données à caractère personnel traitées. Dans la mesure où INFOGREFFE regroupe les greffiers des tribunaux de commerce, la CNIL estime que l'organisme aurait dû faire preuve d'une particulière rigueur dans le respect de ses obligations légales et réglementaires.	 ⇒ Veiller au respect de la durée de conservation des données annoncées dans les procédures/politiques internes ⇒ Vérifier les mesures de sécurité mises en place notamment s'agissant de la robustesse des mots de passe

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE L'EUROPE	15/09/2022	EDPB – Statement 3-2022 on the European Police Cooperation – September 2022	En décembre 2021, la Commission européenne proposait un « code de coopération policière de l'Union européenne » visant à renforcer la coopération entre les services répressifs des Etats membres et, en particulier, l'échange d'informations entre les autorités compétentes. Le CEPD estime que la proposition de la Commission soulève certaines préoccupations. A titre d'exemple, le CEPD soulève que la nécessité de la recherche et de l'échange automatisé des données des dossiers de police n'est pas suffisamment démontrée et que pour évaluer la proportionnalité du système envisagé, un inventaire complet de toutes les bases de données concernées aurait été fondamental. Or, l'analyse d'impact accompagnant la proposition ne mentionne aucune étude sur la qualité des données contenues dans les fichiers de police nationaux, et ni dans quelle mesure ces données sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.	 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	15/09/2022	CNIL – Perte ou vol de matériel informatique nomade : les bons réflexes à avoir! – Communiqué de presse 15 septembre 2022	Dans ce communiqué de presse, la CNIL revient sur les risques engendrés en cas de perte ou de vol de matériel informatique nomade pouvant contenir des données personnelles. La CNIL rappelle les réflexes à avoir en la matière : - Gérer son parc et les ressources de ses utilisateurs ; - Mettre en place des procédures d'authentification ; - Chiffrer les données ; - Effectuer des sauvegardes régulières ; - Sensibiliser les utilisateurs.	 ⇒ A utiliser comme check-list au sein de votre organisme
 LE COIN DES FONDAMENTAUX	20/09/2022	EN CONSULTATION – CNIL – Projet de recommandation interfaces programmation applicatives api	Consultation jusqu'au 1er novembre 2022. Dans ce projet de recommandation, la CNIL précise que le recours aux interfaces de programmation applicatives (API) peut permettre un cadre technique favorable aux échanges de données personnelles entre administrations, organismes publics ou privés. Ainsi, ce projet de recommandation précise : - Les situations dans lesquelles l'utilisation d'une API est préconisée mais aussi les risques qui peuvent résulter de l'utilisation d'une API ; - Les bonnes pratiques à respecter par les détenteurs de données, les gestionnaires d'API et les réutilisateurs ; - Le champ de compétence de ces différents acteurs et leur rôle ; - Les conditions de mise en place d'une 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 L'EUROPE	20/09/2022	EDPB – Record fine for Instagram following EDPB intervention – Press Release 15 September 2022	Faisant suite à la décision contraignante 2/2022 du Comité européen de la protection des données du 28 juillet 2022, l'autorité de protection des données irlandaise a rendu une décision à l'encontre d'Instagram (Meta Platform Ireland Limited (Meta IE)) avec l'imposition d'une amende record de 405 millions d'euros. La décision de l'autorité irlandaise sanctionne les demandes imposées par Instagram aux enfants utilisant un compte professionnel et un paramétrage public par défaut pour les comptes Instagram personnels d'enfants. En effet, Instagram demandait aux enfants utilisant un compte professionnel de fournir leur adresse électronique et/ou leur numéro de téléphone. Meta IE s'appuyait alternativement sur deux bases juridiques pour justifier la finalité du traitement : l'exécution du contrat et l'intérêt légitime. Il a été considéré que le recueil de ces informations n'était pas nécessaire à la bonne exécution du contrat et ne présentait pas d'intérêt légitime. Ainsi, le traitement en cause était illégal car sans base juridique. Il s'agit de la première décision du Comité européen mentionnant le principe de licéité du traitement et en matière de droit des enfants sur la protection des données personnelles.	 ⇒ Vérifier que les données à caractère personnel collectées sont strictement nécessaires à la finalité du traitement
 LE COIN DE LA FRANCE	20/09/2022	CNIL – Amende record pour Instagram – Communiqué de presse 15 septembre 2022	cf EDPB – Record fine for Instagram following EDPB intervention – Press Release 15 September 2022	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE L'EUROPE	20/09/2022	EDPB – Opinion 25-2022 regarding the European Privacy Seal certification criteria for the certification of the processing operations by processors – September 2022	Le Comité européen de la protection des données a rendu un avis sur le système de certification EuroPriSe soumis par l'autorité allemande de protection des données de Rhénanie-du-Nord-Westphalie. Le CEPD considère que les critères de certification EuroPriSe ne sont pas compatibles avec les règles imposées par le RGPD. Afin d'être en accord avec le RGPD, particulièrement l'article 42 sur la certification, le CEPD a recommandé un certain nombre de modifications à apporter.	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE L'EUROPE	20/09/2022	AEPD-EDPS Joint Paper – 10 Misunderstandings about Machine Learning – September 2022	L'apprentissage automatique ou machine learning est une branche spécifique de l'intelligence artificielle appliqué à la résolution de problèmes spécifiques et limités – tels que les tâches de classification ou de prédiction. Le comportement d'un système d'apprentissage automatique n'est pas défini par un ensemble d'instructions prédéterminées. Les systèmes de machine learning s'adaptent de manière autonome aux modèles trouvés parmi les variables dans l'ensemble de données donné, en créant des corrélations. Une fois formés, ces systèmes utilisent les modèles appris pour produire leurs résultats. Les données d'apprentissage jouent donc un rôle important. L'objectif de ce document co-rédigé par l'agence espagnole de protection des données et le contrôleur européen de la protection des données est de déconstruire les idées préconçues entourant l'apprentissage automatique tout en soulignant l'importance de mettre en œuvre de telles technologies dans le respect de la réglementation encadrant les données à caractère personnel notamment. Ainsi, une liste de 10 idées reçues est énoncée ainsi que leurs contre-arguments : la corrélation implique la causalité, lors du développement de systèmes d'apprentissage plus la variété des données est grande, mieux c'est, les décisions automatiques prises par les algorithmes de machine learning ne peuvent pas être expliquées.	 ⇒ Document pour mieux comprendre le machine learning

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	23/09/2022	Conseil d'Etat – Intelligence artificielle et action publique : construire la confiance, servir la performance	Cette étude du Conseil d'Etat, réalisée à la demande du Premier ministre, se veut être une « stratégie de l'intelligence artificielle (IA) au service de la performance publique ». Cette étude se concentre principalement sur les opportunités de l'IA pour l'amélioration de la qualité du service public. Après être revenu sur la notion d'intelligence artificielle, le Conseil d'Etat propose d'accélérer le déploiement des systèmes d'IA publics, de définir et mettre en œuvre les principes et méthodes de l'IA dans le domaine public et, pour ce faire, de doter la France de ressources et de la gouvernance adaptées.	 Pour information
 LE COIN SANTÉ	28/09/2022	CNIL – Check-list de conformité – Référentiel relatif aux traitements de données personnelles mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé	En octobre 2021, la CNIL adoptait un référentiel sur les entrepôts de données de santé. Elle propose désormais un complément à ce référentiel sous la forme d'une check-list de conformité afin d'aider les responsables de traitement à s'assurer de leur conformité au référentiel. Cette check-list peut être utilisée par tout acteur souhaitant mettre en place un entrepôt de données de santé. En cas de non-conformité, la CNIL propose un plan d'action pour combler les écarts.	 ⇒ Check-list à utiliser pour la constitution d'un entrepôt de données de santé

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DES FONDAMENTAUX	28/09/2022	CNIL - Diffusion de données piratées à la suite d'une cyberattaque : quels sont les risques et les précautions à prendre ? - Communiqué de presse 26 septembre 2022	Dans ce communiqué de presse, la CNIL entend répondre aux questions des personnes potentiellement concernées par une violation de données résultant d'une attaque par rançongiciel. Après avoir rappelé que le responsable de traitement est tenu d'informer les personnes concernées, la CNIL précise les principaux risques pouvant découler de cette attaque : le hameçonnage ou usurpation d'identité, la perte de confidentialité des mots de passe. Elle revient sur son rôle d'accompagnateur de la personne concernée face à de telles situations.	 ⇒ Vérifier la procédure de violation de données ⇒ Vérifier les mesures de sécurité mises en place