LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Octobre 2023

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	02/10/2023	Délibération n°SAN-2023-013 du 18 septembre 2023 concernant la société SAF LOGISTICS	La Commission nationale de l'informatique et des libertés (CNIL) a prononcé une sanction de 200 000 euros à l'encontre de la société SAF LOGISTIC pour plusieurs manquements à la règlementation en matière de protection des données personnelles. Cette société, qui assure une activité de transport de fret aérien en provenance de la Chine et à destination de l'Europe, est composée majoritairement de salariés ressortissants chinois résidant et travaillant en France. La CNIL a considéré que la société avait manqué à : - l'obligation de minimisation des données en faisant circuler des questionnaires avec des informations non pertinentes et non justifiées au regard des finalités poursuivies. Dans le cadre de la collecte de contacts pour contacter les proches du salariés, la CNIL considère que les informations suivantes suffisent : nom, prénom, lien de parenté, numéro de téléphone ; - l'interdiction de traiter des données « sensibles » en application de l'article 9 du RGPD - l'interdiction de collecter ou traiter des données relatives aux condamnations pénales en application de l'article 10 RGPD;	 ⇨ Vérifier que les données collectées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités ⇨ S'assurer de l'effectivité de la base légale au titre de laquelle les données sensibles sont collectées

			- l'obligation de coopération avec les services de la CNIL en traduisant et partageant partiellement les informations et en évitant les informations litigieuses.	
LE COIN DE LA FRANCE	04/10/2023	Délibération n° 2023-092 du 14 septembre 2023 portant modification du règlement intérieur de la Commission nationale de l'informatique et des libertés	Le 14 septembre 2023, la CNIL a modifié l'article 85 de son règlement intérieur. Cet article est relatif aux indemnités à la vacation allouées au titre des autres activités et interventions des membres de la Commission, en doublant le nombre de vacations.	Pour information
LE COIN DE LA FRANCE	05/10/2023	Délibération n° SAN-2023-014 du 28 septembre 2023 relative à l'injonction prononcée à l'encontre de la société VOODOO par la délibération n°SAN-2022-026 du 29 décembre 2022	Ce 28 septembre, la formation restreinte de la (CNIL a clôturé l'injonction à l'encontre de la société VOODOO prononcée le 29 décembre 2022. La société recueillait l'« identifier for vendors » (IDFV) auprès de chaque utilisateur, sans leur consentement, ce qui permettait à la société de mesurer l'activité des utilisateurs sur ses applications et jeux vidéo, et, dans le même temps, de créer de la publicité personnalisée. La société avait 3 mois, du 16 janvier au 16 avril 2023, pour se mettre en conformité. Le 14 avril 2023, elle a présenté à la CNIL son nouveau dispositif de recueil du consentement de l'utilisateur pour l'IDFV à des fins publicitaires. Estimant que ce nouveau moyen de recueil du consentement était conforme à la réglementation, la CNIL a clôturé l'injonction.	⇨ En cas de recours à des cookies ou autres traceurs, s'assurer du recueil du consentement de l'utilisateur
LE COIN DE L'EUROPE	09/10/2023	ENISA - Health Threat Landscape	Agence de l'Union européenne spécialisée dans le domaine de la cybersécurité, l'ENISA a pour objectif d'assurer un niveau commun élevé de cybersécurité dans toute l'Union. Par cette première analyse dans le domaine	

			de la santé, l'ENISA cartographie et étudie les cybers incidents ciblant les organismes de santé, entre janvier 2021 et mars 2023. Durant cette période, le secteur de la santé a fait face à un nombre significatif d'incidents. L'ENISA constate que les prestataires de soins dans le domaine de la santé représentent 53% du total des incidents dont, 42% des incidents concernant des hôpitaux. L'industrie pharmaceutique est moins impactée avec 9% des incidents et 14% pour les autorités et agences de santé. Les violations et les vols de données représentent la majorité des incidents (43%), tandis que la perturbation des services de santé représente 22% des incidents. Au regard du nombre d'incidents par pays, la France est le pays de l'Union qui a connu le plus grand nombre de menaces sur la période, 43 au total, avec en deuxième position l'Espagne qui a subi 25 incidents. L'impact de ces incidents représente, pour l'ENISA, un danger pour les dossiers de santé électroniques et les données de patient ou encore les systèmes et service d'information sur la santé. Par conséquent, à la suite de ce rapport, l'ENISA recommande pour les professionnels de santé, de s'équiper de programmes dédiés à la défense contre les attaques cybercriminelles, de sensibilisation à la sécurité informatique et de réaliser des évaluations ou des analyses de risques. Enfin, elle recommande de pratiquer la cyber hygiène avec la mise en place de	⇨ S'assurer régulièrement des mesures de sécurité mises en place.

			sauvegardes de données critiques chiffrées hors ligne, mais aussi la mise en place d'analyse régulière des vulnérabilités, tout en mettant en place les bonnes pratiques en matière d'authentification (contrôle accès…) et notamment la prise en compte des exigences de la directive NIS 2.	
LE COIN SANTÉ	12/10/2023	MR007 – Délibération n° 2023-082 du 20 juillet 2023 portant homologation d'une méthodologie de référence	La CNIL a publié une nouvelle méthodologie de référence (MR) : la MR-007. Cette MR vise l'accès, par des organismes agissant dans le cadre de leur mission d'intérêt public, aux données de la base principale du Système national des données de santé (SNDS). Les responsables de traitement concernés sont des organismes pour lesquels la mise en œuvre de la recherche, étude ou évaluation dans le domaine de la santé est nécessaire à l'exécution d'une mission de service public : établissements de santé, fédérations hospitalières, laboratoires de recherche ou encore bureaux d'études. Les mesures de sécurité prévues devront être conformes au référentiel de sécurité applicable au SNDS. Cette nouvelle méthodologie prévoit la transmission d'un bilan par le responsable de traitement à la CNIL, tous les trois ans, visant à synthétiser les usages observés de la méthodologie en question.	Pour information
LE COIN SANTÉ	12/10/2023	MR008 – Délibération n° 2023-083 du 20 juillet 2023 portant homologation d'une méthodologie de référence	La MR-008, nouvelle méthodologie de référence (MR) publiée par la CNIL, vise les traitements de données de la base du SNDS mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé par les organismes agissent dans le cadre de leurs intérêts légitimes. Les	Pour information

			responsables de traitement sont le plus souvent des organismes privés et les sous-traitants sélectionnés par les responsables de traitement seront soit des établissements de santé, des fédérations hospitalières, des laboratoires de recherche ou encore des bureaux d'études. Cette nouvelle méthodologie prévoit la transmission d'un bilan tous les trois ans à la CNIL, visant à synthétiser les usages observés de la méthodologie en question.	
 LE COIN DES NOUVELLES TECHNOLOGIES	12/10/2023	CNIL - Appel à contributions sur la constitution de bases de données pour la conception de systèmes d'intelligence artificielle - Synthèse des contributions - Octobre 2023	La CNIL synthétise les contributions reçues lors de l'appel à consultation publique concernant la constitution de bases de données pour la conception de systèmes d'intelligence artificielle. Les participants à la consultation ont notamment confirmé qu'il était important de - définir une finalité reposant sur une référence aux modes de réutilisations envisagées ou envisageables des données personnelles ; - choisir une base légale adaptée pour le traitement des données et aussi des données sensibles ; - qualifier ce que recouvre la notion de traitement de « recherche scientifique », au sens du RGPD. Notamment, les participants ont proposé des critères inclusifs et exclusifs ; - minimiser les données. Les retours des participants se sont scindés en deux temps : la sélection des données et la	 Pour information

			détermination du processus de développement de l'IA le plus adapté ; - constituer une base de données de qualité, notamment via la qualité des données collectées, la réduction des biais et également la représentativité ; - enfin, protéger les données, notamment via la mise en place d'une protection dès la conception et par défaut, mais aussi avec des mesures de sécurité organisationnelles et structurelles.	
LE COIN DE L'EUROPE	16/10/2023	EDPS - Opinion 42-2023 on the Proposal for two Directives on AI liability rules - October 2023	Le 28 septembre 2022, la Commission européen a publié deux propositions de directives relatives, respectivement, à la responsabilité du fait des produits défectueux et à l'adaptation des règles de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (IA). Ces propositions ont pour objectif d'adapter les règles de responsabilité à l'ère numérique pour garantir aux victimes un niveau de protection équivalent à celui qui serait accordé pour un préjudice causé dans d'autres circonstances. Ces propositions font partie d'un ensemble de mesures visant à soutenir le déploiement de l'intelligence artificielle en Europe. Si le Contrôleur européen de protection des données soutient l'initiative du législateur européen dans son approche, il a néanmoins formulé quelques recommandations. Parmi celles-ci, il invite le législateur européen à veiller à ce que les personnes ayant subi un dommage causé par un système d'IA produit	Pour information

			et/ou utilisé par les institutions, organes et agences de l'Union bénéficient d'un niveau de protection équivalent à celui dont bénéficie les personnes ayant subi des dommages causés par des systèmes d'IA produits et/ou utilisés par des acteurs privés. Aussi, les garanties procédurales prévues par la proposition de directive relative à la responsabilité dans le domaine de l'IA devraient s'appliquer à tous les dommages causés par un système d'IA, indépendamment de sa classification en tant que système à haut risque ou non. Le Contrôleur recommande d'envisager des mesures supplémentaires pour alléger la charge de la preuve pour les victimes des systèmes d'intelligence artificielle dans le but de garantir l'efficacité des règles de responsabilités européens et nationales.	
LE COIN DE L'EUROPE	18/10/2023	EDPB-EDPS - Joint Opinion 02-2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro - October 2023	Le 28 juin 2023, la Commission européenne a adopté un « paquet législatif » relatif à l'euro numérique, comprenant une proposition de règlement relatif à l'euro numérique. Cette proposition a pour objectif d'encadrer les aspects essentiels d'un euro numérique émis par la Banque centrale européenne (BCE), euro qui serait utilisable aussi bien pour les paiements en ligne que pour les paiements hors ligne. L'avis conjoint du Comité européen de la protection des données (CEPD) et du Contrôleur européen de la protection des données insiste sur la protection de la vie privée, caractéristique la plus importante d'un euro numérique que ce soit pour les particuliers ou les	 Pour information

			professionnels. Il rappelle l'obligation pour les responsables de traitements concernés par l'euro numérique de réaliser une analyse d'impact sur la protection des données. Le CEPD et le Contrôleur relèvent également que la BCE devrait évaluer la nécessité de consulter le Contrôleur européen de la protection des données avant d'effectuer tout traitement relatif à l'euro numérique, du fait que ce type de traitement pourrait entrainer un risque élevé pour les personnes physiques concernées. Enfin, ils recommandent que d'intégrer à la proposition, l'obligation de mettre en place une analyse d'impact pour la BCE, ainsi que l'obligation pour cette dernière d'assurer concrètement la protection des données dès la conception et par défaut.	
 LE COIN DE LA FRANCE	18/10/2023	Délibération n° HAB-2023-002 du 12 octobre 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	19/10/2023	Délibération n°SAN-2023-015 du 12 octobre 2023 concernant la société GROUPE CANAL +	La CNIL a prononcé une sanction de 600 000 euros à l'encontre du Groupe Canal+ pour plusieurs manquements à la règlementation. La société ne respectait pas le RGPD en matière de prospection commerciale, notamment sur l'obligation d'information de l'identité du prospecteur et sur la capacité à démontrer la preuve du recueil du consentement éclairé et valable des prospects. Ont été reprochés des manquements à :	 ⇨ En cas de prospection commerciale, s'assurer du recueil du consentement des personnes ⇨ S'assurer de réaliser une information complète auprès des personnes concernées ⇨ Vérifier/mettre à jour la politique de confidentialité

			- l'obligation de recueillir le consentement de la personne concernée ; - l'obligation d'information et au respect de l'exercice des droits ; - l'obligation de mettre en place un contrat incluant toutes les mentions de l'article 28 du RGPD entre responsable de traitement et sous-traitant ; - l'obligation de sécurité en utilisant un algorithme de chiffrement non adéquat à l'état de l'art ; - l'obligation de notifier à la CNIL une violation de données.	⇨ Vérifier la conformité du système de sécurité au regard de l'état de l'art ⇨ Vérifier le contenu des contrats établis avec les sous-traitants
LE COIN DES FONDAMENTAUX	19/10/2023	ANSSI - Recommandations relatives au reconditionnement des ordinateurs de bureau ou portables	L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié la première version de son guide relatif au reconditionnement des ordinateurs de bureau et portables. Ce guide s'inscrit dans la continuité de la loi anti-gaspillage pour une économie circulaire afin de limiter la pollution. Tout d'abord, l'ANSSI précise que les acheteurs de l'administration centrale ou territoriale sont tenus d'opter pour des biens issus du reconditionnement. L'Agence relève les risques liés au reconditionnement en lui-même tels que la mise en place d'un code malveillant écrit sur le disque, le piégeage du matériel, le piégeage des bus (ensemble des lignes de communication connectant les composants d'un ordinateur) et ports de communications avec de périphériques internes ou externes ou encore la réécriture du « firmware » (nom générique désignant	⇨ A utiliser comme une check list afin d'assurer la protection des données personnelles et la sureté du matériel dans le cadre de la cession d'ordinateurs ou de l'achat d'ordinateurs reconditionnés

			tout logiciel embarqué dans un composant matériel de l'ordinateur). L'ANSSI précise que la cession d'ordinateurs suppose un certain nombre d'actions préalables afin d'éviter certains risques comme la fuite d'information si la totalité des données n'est pas correctement effacées par exemple, la compromission par un tiers si le reconditionnement a été effectué par un tiers, ou encore la diffusion de code malveillant si l'ordinateur reconditionné est infecté. Par conséquent, l'ANSSI propose une liste de 30 recommandations pour organiser le déploiement des ordinateurs reconditionnés, préparer techniquement le reconditionnement, rendre les données inaccessibles, dépersonnaliser les ordinateurs notamment, pour assurer un reconditionnement protecteur des données personnelles de l'ancien utilisateur, mais aussi du nouvel utilisateur.	
LE COIN DE L'EUROPE	24/10/2023	Data Brige UK-US - Factsheet for UK organisations	Depuis le 12 octobre 2023, les entreprises du Royaume-Uni peuvent transférer des données personnelles à des organisation américaines certifiées à l' « extension britannique » prévu par le RGPD du Royaume-Uni et figurant sur la liste prévue dans le cadre du Data Privacy Framework mis en place entre l'Union européenne et les Etats-Unis. Toutefois, certaines données sont exclues du champ de cette décision et ne pourront pas faire l'objet de transferts telles que les données journalistiques. Le gouvernement britannique rappelle, dans ce document, que si l'organisme souhaitant	 Pour information

			transférer des données ne peut pas s'appuyer sur l'extension britannique alors des garanties appropriées devront être mises en place comme l'addendum britannique aux clauses contractuelles types de l'Union européenne. Aussi, le gouvernement mentionne que l'organisme doive procéder à une évaluation des risques de transfert avant de valider les transferts.	