LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Août - Septembre 2023

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN DE LA FRANCE	31/08/2023	Délibération n°SAN-2023-12 du 13 juillet 2023 relative à l'injonction prononcée à l'encontre des sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED par la délibération n°SAN-2021-023 du 31 décembre 2021	La formation restreinte de la CNIL a clôturé l'injonction à l'encontre des sociétés Google LLC et Google Ireland. Sanctionnée le 31 décembre 2021, les sociétés avaient été, dans le même temps, enjointes de mettre en conformité leurs sites internet s'agissant des modalités de recueil du consentement des utilisateurs situés en France, sous trois mois sous peine d'une astreinte de 100 000 € par jour de retard. Estimant que le plan d'action des sociétés a répondu aux attentes dans les délais impartis, la CNIL a clôturé l'injonction prononcée se réservant le droit de contrôler à nouveau la conformité des sites internet en question.	Pour information
LE COIN DE L'EUROPE	31/08/2023	EDPS Opinion 37/2023 on the Proposal for a Council Directive on Faster and Safer Relief of Excess Withholding Taxes	Le 19 juin 2023, la Commission européenne a publié une proposition de directive relative au dégrèvement plus rapide et plus sûr de l'excédent des retenues à la source. Cette proposition vise à soutenir le bon fonctionnement de l'union des marchés des capitaux en facilitant les investissements transfrontières tout en garantissant la justice fiscale en prévenant la fraude et l'abus fiscal. Elle prévoit notamment que les Etats membres de l'Union européenne mettent en place un processus automatisé de délivrance d'un certificat de résidence fiscale numérique (CRFN) à des fins fiscales, qui implique un traitement de données personnelles. Le Contrôleur européen de la protection des données relève que si la proposition prévoit l'utilisation du CRFN à des fins autres que le dégrèvement de l'excédent de retenue à la source, le législateur européen n'a pas explicitement précisé les finalités supplémentaires. Aussi, il recommande soit	Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			de supprimer l'article litigieux soit de préciser l'ensemble des finalités pour lesquelles le CRFN serait utilisé et, par là même, les données personnelles pertinentes requises. Par ailleurs, la proposition limite les droits des personnes concernées pour réduire le risque de fraude ou d'évasion fiscales. A ce propos, le Contrôleur recommande de restreindre uniquement les droits des personnes concernées à la durée nécessaire de l'enquête fiscale et de lever cette restriction à la clôture de l'enquête par l'administration fiscale.	
LE COIN DE L'EUROPE	31/08/2023	EDPS Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access	Le 28 juin 2023, la Commission européenne a publié la proposition de règlement du Parlement européen et du Conseil relatif à un cadre pour l'accès aux données financières. Cette proposition vise à promouvoir le développement de services et produits financiers fondés sur les données en permettant aux consommateurs et aux entreprises de mieux contrôler l'accès à leurs données financières. Le Contrôleur européen de la protection des données a procédé à plus d'une vingtaine de recommandations parmi lesquelles : - préciser que le traitement de données soit effectué conformément au RGPD et à la directive E-Privacy ; - délimiter les catégories de données à caractère personnel concernées en tenant compte de la nature des services et produits financiers proposés par les entités concernées par le règlement ; - exclure explicitement les données créées à la suite d'un profilage ;	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			- préciser que le retrait de tout agréement accordé à un fournisseur de services d'informations financières est possible s'il aurait manqué à ses obligations.	
LE COIN DE L'EUROPE	31/08/2023	EDPS Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market	Le 28 juin 2023, la Commission européenne a publié une proposition de règlement relatif aux services de paiement dans le marché intérieur ainsi qu'une proposition de directive relative aux services de paiement et services de monnaie électronique dans le marché intérieur. Les services de paiement impliquent souvent le traitement de données personnelles pouvant révéler des informations « sensibles » sur une personne concernée. Le Contrôleur européen de protection des données (Contrôleur) propose plus d'une quinzaine de recommandations au législateur européen. Notamment, le Contrôleur suggère de - clarifier la définition de « données de paiement sensibles » en précisant notamment les types de données personnelles couverts par cette notion ; - préciser les services de paiement désignés pour lesquels les systèmes de paiement et le prestataire de services de paiement seraient habilités à traiter les catégories particulières de données personnelles ; - déterminer clairement les catégories de données personnelles que les prestataires de services de paiement seraient autorisés à traiter dans le cadre des mécanismes de suivi des transactions ;	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			- définir les durées de conservation appropriées pour les données personnelles collectées ; ou encore - mentionner explicitement les autorités de contrôle chargées du suivi et de l'application de la législation sur la protection des données.	
 LE COIN DE LA FRANCE	31/08/2023	EN CONSULTATION - CNIL - Projet de recommandation relative à la sécurité des traitements critiques	En consultation jusqu'au 22 octobre 2023. Dans ce projet, la CNIL propose de regrouper l'ensemble des pratiques de sécurité, déjà publié, dans un document unique de recommandation visant spécialement les traitements dits « critiques ». C'est-à-dire, tout traitement de données à grande échelle et dont la violation pourrait engendrer des conséquences très importantes soit pour les personnes concernées, soit pour la sûreté de l'Etat ou la société dans son ensemble. La CNIL rappelle, tout d'abord, que tout traitement de données personnelles implique la mise en place de mesures de sécurité élémentaires et lorsqu'il s'agit de données sensibles de la mise en place d'une analyse d'impact (AIPD ou PIA). La CNIL aborde également : - la gestion de la protection des données avec notamment la mise en place d'une gouvernance de la protection des données assurée par la direction générale de l'organisme, d'une démarche d'amélioration continue de sécurité et aussi la désignation d'un interlocuteur au cœur du traitement concerné avec les autorités; - la gestion des risques, avec la mise en place d'une analyse d'impact qui devra être mise à jour au moins tous les deux ans et à chaque changement affectant le traitement. La mise en place d'un processus d'homologation de	 ⇨ Si existence de traitements critiques, s'assurer de mettre en place les différentes recommandations de la CNIL

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			sécurité par le responsable hiérarchique du traitement avec la mise en place d'un plan d'action ; - la nécessité de cultiver une maturité élevée en sécurité et protection des données personnelles notamment grâce, d'une part, à la présence d'un responsable de la sécurité des systèmes d'information (RSSI) et d'équipes chargées des questions de sécurité et, d'autre part, à la sensibilisation à la sécurité informatique et protection des données personnelles ; - la mise en place d'une démarche de défense en profondeur, en s'inspirant de la logique « zéro confiance » (ou « zero trust »), consistant à mettre en place des mesures de cloisonnement, d'imputabilité et de maîtrise des accès ; - la nécessité de se préparer activement à d'éventuels incidents de sécurité ou violation de données avec, entre autres, des mesures d'analyse automatiques de journalisation ou encore par la mise en place de systèmes de traçabilité des traitements critiques distincts du reste des traitements et gérés par des équipes différentes. En pratique, cela se concrétiserait par un centre opérationnel de sécurité (COS ou SOC « security operation center ») et un protocole de réponse technique et organisationnelle générique applicable aux violations de données ; et enfin - la maîtrise des relations avec les tiers, vecteurs d'attaque potentiels et de vulnérabilités importantes. Pour ce faire, un encadrement contractuel doit être prévu dans lequel leurs	

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			exigences de sécurité seront explicitement formalisées et détaillées.	
LE COIN DE L'EUROPE	08/09/2023	EDPS Opinion 40/2023 on the Proposal for a Regulation on European Statistics	Le 10 juillet 2023, la Commission européenne a publié la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques européennes. Cette proposition vise à rendre le cadre juridique régissant les statistiques européennes adapté à l'avenir et à améliorer la réactivité du système statistique européen aux besoins en données. Le Contrôleur européen de protection des données (Contrôleur) recommande notamment de - faire référence à la mention sur le respect des garanties relatives au traitement des données à des fins statistiques, en particulier sur le fait que les données devraient être rendues anonymes ; - préciser que seules les données non personnelles donc anonymisées seront demandées aux titulaires de données privées ; - prévoir, d'une part, un cadre clair et complet des catégories de données pouvant être demandées et des types de sources à partir desquelles ces catégories de données peuvent être obtenues et, d'autre part les garanties spécifiques sur le partage des données notamment par la mise en place d'infrastructure sécurisée ;. - introduire l'obligation pour la Commission (Eurostat) et les Etats membres de tester et évaluer la pertinence des technologies permettant le partage de données.	 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	20/09/2023	CNIL - Codes de conduite les 8 bonnes pratiques de la CNIL	La CNIL a publié un guide avec huit conseils généraux pour aider les organismes dans l'élaboration d'un code de conduite. Les codes de conduite s'adressent à des professionnels d'un secteur et sont portés par une entité représentative de celui-ci. Il peut s'agir d'une association professionnelle ou d'une fédération par exemple. Les conseils de la CNIL sont les suivants : - vérifier la représentativité du porteur du projet de code ; - évaluer les connaissances des futurs adhérents en matière de protection des données ; - établir un plan correspondant aux pratiques des futurs adhérents et à leurs obligations en matière de protection des données conformément à la liste des sujets qui peuvent être traités par un code de conduite fournie à titre indicatif par le RGPD (article 40.2) - ne pas minimiser les potentiels coûts pour les professionnels du secteur, le code devant être validé par un organisme de contrôle agréé par la CNIL ; - rédiger le code en pensant aux lecteurs, c'est-à-dire avec contenu compréhensible, concret comprenant des indications auditables et réalisables ; - prévoir un mécanisme de gouvernance via des structures spécifiques et des procédures relatives au contrôle efficace et l'application des sanctions en cas de violation du code ; - encadrer l'activité de l'organisme de contrôle, c'est-à-dire prédéterminé les éléments qui seront évalués par les autorités de contrôle	 ⇨ A utiliser comme checklist en cas d'élaboration d'un code de conduite

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			dans le cadre de l'approbation du code de conduite ; et enfin - inclure la procédure d'approbation dans le calendrier puisque l'approbation nécessite des phases d'échanges avec l'autorité de contrôle compétente (CNIL en France) voire avec les autorités européennes pour les codes européens.	
LE COIN DE L'EUROPE	22/09/2023	EDPB-EDPS - Joint Opinion 01-2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679	Le 4 juillet 2023, la Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil établissant des règles de procédure supplémentaires relatives à l'application du RGPD. Conjointement, le Contrôleur européen de protection de données (Contrôleur) et le Comité européen de protection des données (CEPD) ont fait des recommandations sur : - la recevabilité et l'examen préliminaire des plaintes, - la procédure de coopération et de recherche de consensus, - la confidentialité, l'accès au dossier et traductions, - le règlement des litiges et procédures d'urgences, - les droits procéduraux des parties faisant l'objet de l'enquête, - les droits procéduraux du plaignant, ou encore notamment - la coopération entre le Contrôleur et les autorités nationales.	 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	22/09/2023	CNIL - Ordre national des pharmaciens - Guide pratique : Le pharmacien d'officine et la protection des données	Le Conseil national de l'Ordre des pharmaciens (CNOP) et la CNIL, ont publié un guide pratique sur la mise en conformité à la réglementation sur la protection des données des pharmaciens d'officine. Ce guide rappelle que le pharmacien d'officine est amené, d'une part, à gérer les données du personnel et d'autre part, à traiter les données de patients. Au titre des prérequis à toute conformité RGPD, le CNOP et la CNIL reviennent sur les mesures qui doivent, a minima, être mises en place : - la désignation d'un DPO pour les officines déclarant une activité globale annuelle de plus de 2 600 000 € HT. Les pharmaciens restent libre de ne pas désigner de DPO sous réserve de pouvoir justifier leur décision ; - l'identification des données traitées dans le cadre des activités ; - la mise en place d'un registre de traitement ; - la mise en place de mesures de protection des données ; - l'information des personnes concernées sur les traitements de données ; - la mise en place d'une procédure de traitements des demandes d'exercice de droit et de gestion des demandes d'accès concernant les personnes décédées ; - la détermination de durées de conservation ; - l'encadrement des relations avec les sous-traitants ; - l'encadrement de transfert de données hors Union européenne ; et - la réalisation des analyses d'impact pour les traitements concernés.	 ⇨ A utiliser par les officines comme checklist pour s'assurer d'être en conformité avec la réglementation ⇨ En cas de non-recours à un DPO, justifier, par écrit, les raisons de ce choix

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			Également, le guide propose des fiches pratiques sur obligations et comportements à adopter, notamment : - à l'égard des patients ; - à l'égard du personnel ; - avec les sous-traitants ; - en cas d'installation d'un dispositif de vidéo surveillance ; - les comportement à avoir en cas de violation de données ;et en cas de contrôle de la CNIL.	
LE COIN DE L'EUROPE	25/09/2023	EDPS - Opinion 41-2023 on the Proposal for a Regulation on European Union labour market statistics on businesses - September 2023	Le 28 juillet 2023, la Commission européenne a publié la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques européennes du marché du travail concernant les entreprises. Cette proposition vise à améliorer les statistiques du marché du travail, d'une part, pour disposer de statistiques européennes et, d'autre part, pour permettre à l'Union européenne d'exécuter les tâches qui lui sont confiées en termes de marché intérieur et de mise en place des politiques européennes, notamment politiques économiques et de l'emploi, politique monétaire, politique sociale… En effet, actuellement les données fournies à Eurostat, direction de la Commission européenne chargée de l'information statistique à l'échelle communautaire, ne peuvent pas être pleinement exploitées. Les données statistiques dans ce domaine peuvent être des données à caractère personnel d'employés. Après avoir rappelé, le principe de minimisation des données, le Contrôleur européen de la protection des données (Contrôleur) recommande, notamment, de préciser que les	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
			données transmises ne devraient pas permettre l'identification des personnes concernées et devraient être agrégées et anonymisées. Le Contrôleur recommande également faire référence à la directive « vie privée et communications électroniques ». Le CEPD recommande de limiter les techniques de « web scraping » si ce type de technique est utilisé pour traiter les données. Il s'agit d'une méthode permettant d'extraire un grand nombre d'informations sur les sites Internet et, ce, de manière automatisée.	