

AVRIL 2022

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN SANTÉ	28/04/2022	Décret n°2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information	Ce décret définit les catégories d'incidents de sécurité des systèmes d'information des établissements de santé, des hôpitaux des armées, des organismes et services exerçant des activités de prévention, de diagnostic ou de soins et des établissements médico-sociaux qui doivent faire l'objet d'un signalement aux autorités compétentes de l'Etat, ainsi que les conditions et modalités selon lesquelles ils sont traités. Cette déclaration doit être effectuée sans délai par le directeur l'établissement de santé, de l'organisme ou du service concerné.	 ⇒ A utiliser comme une grille de contrôle si organisme concerné
 LE COIN SANTÉ	28/04/2022	Délibération n°2022-046 du 14 avril 2022 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement	Demande d'avis concernant un projet de décret autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement.	 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 SANTÉ	28/04/2022	Décret n°2022-714 du 27 avril 2022 modifiant le décret n°2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques	Ce décret s'adresse aux agences régionales de santé (ARS), aux représentants de l'Etat dans le département et, à Paris, préfet de police, aux services de renseignement et aux personnes faisant l'objet de soins psychiatriques sans consentement. Ce décret modifie un décret de 2018 prévoyant les conditions de mise en relation entre deux traitements de données HOPSYXEB et FSPRT. Il étend aux représentants de l'Etat dans le département, à Paris, au préfet de police et aux services de renseignement limitativement désignés la possibilité d'accéder aux données d'identification et de nature administrative relatives aux personnes admises en soins psychiatriques sans consentement qui sont portées à la connaissance du préfet du lieu de l'hospitalisation. Ainsi, les finalités des traitements HOPSYWEB, les catégories de données traitées, les accédants et les destinataires de certaines des données qui y sont enregistrées, ainsi que les modalités d'exercice de leurs droits par les personnes concernées sont modifiées.	 Pour information

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DES NOUVELLES TECHNOLOGIES	28/04/2022	CNIL – L'enregistrement des conversations téléphoniques afin d'établir la preuve de la formation d'un contrat	Dans ce communiqué de presse, la CNIL revient sur les enregistrements de conversations téléphoniques à des fins de preuve de formation d'un contrat. La CNIL rappelle que l'enregistrement doit être nécessaire pour prouver la formation du contrat et que les enregistrements ne sont donc pas nécessaires pour les contrats écrits. Pour les contrats souscrits à l'oral, le principe de minimisation des données doit être gardé à l'esprit en cas d'enregistrement des conversations. Ainsi, les enregistrements ne peuvent être ni permanents ni systématiques. En outre, la CNIL rappelle également les règles pour protéger les droits des personnes : - Informer - Limiter de l'accès aux conversations aux seules personnes habilitées - Sécuriser les données personnelles - Limiter la durée de conservation des enregistrements - Désigner un DPO et tenir un registre de traitements	 ⇒ A utiliser comme une grille de contrôle en cas d'enregistrement des conversations
 LE COIN DE L'EUROPE	28/04/2022	EDPS – Annual Report 2021	Ce rapport revient sur les actions réalisées par le CEPD au cours de l'année 2021. Il précise notamment que le CEPD a accru ses pouvoirs de correction et a rendu un nombre recors de consultations législatives. Ceci démontre l'importance d'intégrer au sein du droit de l'Union la protection des données personnelles	 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	25/04/2022	Délibération n°HAB-2022-002 du 14 avril 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 visites et vérifications des organismes.	 Pour information ⇒ En cas de visite de la CNIL, vérifier que les agents présents figurent sur cette liste
 LE COIN DE LA FRANCE	25/04/2022	Délibération n° SAN-2022-009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE	La CNIL a sanctionné Dedalus Biologie, d'une amende de 1,5 million euros, pour défaut de sécurité ayant entraîné la fuite de données médicales de près de 500 000 personnes. Les manquements suivants ont été sanctionnés : - Manquement pour le sous-traitant de respecter les instructions du responsable de traitement - Manquement à la sécurité des données - Manquement à l'encadrement par un contrat des traitements effectués pour le compte du responsable de traitement	 ⇒ Vérifier les contrats avec les sous-traitants et leurs clauses ⇒ Vérifier les mesures de sécurité techniques et organisationnelles

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	13/04/2022	EDPB – Statement 01-2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework – April 2022	Par cette déclaration, le CEPD se félicite de l'annonce d'un accord politique de principe entre la Commission européenne et les Etats-Unis sur la mise en place d'un nouveau cadre transatlantique de protection des données. Le CEPD examinera comment cet accord politique se traduit en propositions juridiques concrètes pour répondre aux préoccupations qui avaient été soulevées par la Cour de justice de l'Union dans l'arrêt Schrems II. A ce stade, il ne s'agit donc encore nullement d'un cadre juridique sur lequel les exportateurs de données peuvent fonder leurs transferts de données vers les Etats-Unis.	 ⇒ Surveiller l'adoption d'une décision concernant les transferts vers les Etats-Unis
 LE COIN DE LA FRANCE	13/04/2022	Prospection commerciale : trois organismes mis en demeure pour des transmissions de données entre partenaires non conformes – Communiqué de presse – 7 avril 2022	La CNIL a adressé trois mises en demeure à des sociétés pour avoir transmis à des partenaires des données à caractère personnel de prospects sans avoir recueilli leur consentement. Les organismes en cause ont trois mois pour se mettre en conformité. Dans le cas contraire, ils encourent une sanction pouvant aller jusqu'à 20 millions d'euros ou 4% de leur chiffre d'affaires.	 ⇒ En cas de partage de données personnelles, s'assurer de l'information des personnes concernées et de leur consentement, le cas échéant

Icônes « Quelles actions ? » by Adrien Coquet

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DE LA FRANCE	13/04/2022	Délibération de la formation restreinte n°SAN-2022-008 du 31 mars 2022 relative à l'injonction prononcée à l'encontre de la société SPARTOO par la délibération n°SAN-2020-003 du 28 juillet 2020	La formation restreinte de la CNIL a clôturé l'injonction prononcée à l'encontre de Spartoo prononcée en juillet 2020. Il était reproché à Spartoo d'enregistrer intégralement les appels téléphoniques reçus par le service clients à des fins de formation des salariés, d'avoir conservé les données des clients au-delà de la durée et des finalités nécessaires, de ne pas avoir correctement informé les salariés de l'enregistrement des appels téléphoniques et enfin de ne pas avoir mis en place une politique de mot de passe sécurisée pour les clients.	 ⇒ Vérifier la politique des mots de passe ⇒ Vérifier la politique de conservation des données
 LE COIN DES OUTILS	11/04/2022	Formation Anticiper et gérer un contrôle CNIL – 3 juin 2022		 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	11/04/2022	Décret n°2022-517 du 8 avril 2022 modifiant le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Ce décret adapte les règles de procédures de mise en demeure et de sanctions de la CNIL. La procédure ordinaire est assouplie et une procédure simplifiée de sanction est mise en place. Cette nouvelle procédure écrite concernera les dossiers les moins complexes. La complexité sera analysée au regard du faible niveau de gravité de l'infraction et de la simplicité des questions de fait ou de droit soulevées. Les mesures pouvant être prononcées se limitent à un rappel à l'ordre, une injonction sous astreinte dans la limite de 100 euros par jour de retard et une amende d'un montant maximal de 20 000 euros. Les mesures rendues ne seront pas rendues publiques.	 Pour information
 LE COIN DE LA FRANCE	11/04/2022	Délibération n°2022-029 du 10 mars 2022 portant avis sur un projet de décret modifiant le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Cet avis de la CNIL concerne les modifications apportées à la loi informatique et libertés et notamment la simplification de la procédure ordinaire. La CNIL a accueilli favorablement ces modifications qui s'imposent au regard de l'augmentation sans cesse grandissante du nombre de plaintes adressées à l'Agence.	 Pour information
 LE COIN DES FONDAMENTAUX	11/04/2022	Délibération n°2021-131 du 23 septembre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales	La CNIL a publié un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales. Ce référentiel propose des pistes de mise en conformité pour les fichiers « clients » et « prospects » des organismes de droit privé ou public.	 ⇒ A utiliser comme une grille de contrôle

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN DES FONDAMENTAUX	11/04/2022	Délibération n°2021-130 du 23 septembre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des impayés dans une transaction commerciale	La CNIL a publié un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des impayés dans une transaction commerciale. Ce référentiel propose des pistes de mise en conformité pour la mise en œuvre par les organismes de droit privé ou public d'un traitement de données de gestion d'impayés avérés. Ce référentiel concerne les impayés faisant suite à une transaction commerciale portant sur des biens ou des services. Le document précise qu'il n'a pas vocation à s'appliquer aux traitements mis en œuvre pour détecter un risque d'impayé ou recenser des manquements autres que pécuniaires (comme, par exemple, des incivilités des clients).	 ⇒ A utiliser comme une grille de contrôle