NumSpot

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

Ce qu'il faut retenir de la nouvelle version du « guide de la sécurité des données personnelles » de la CNIL?

Le RGPD, qu'est-ce que c'est ?

Le **Règlement Général sur la Protection des Données (RGPD)** est un texte réglementaire européen qui encadre le traitement des données sur tout le territoire de l'Union européenne (UE)..

Entré en application le 25 mai 2018, il s'inscrit dans la continuité de la loi française «Informatique et Libertés» de 1978 et a pour objectif d'établir des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. Il protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel

Qu'entend-on par « données à caractère personnel » ?

« Données à caractère personnel » est défini par le RGPD comme **toute information se rapportant à une personne physique identifiée ou identifiable** ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

MAJ du sujet « droit d'accès en cas de violation de données »

La ligne directrice sur la notification des violations de données s'articule autour de **4 axes incontournables** à respecter dans le cadre du traitement d'une violation de données à caractère personnel :

- L'évaluation de la violation des données
- La notification aux autorités compétentes
- La notification aux clients concernés
- Les mesures de remédiation à mettre en œuvre

Clarification de la procédure à suivre par les entreprises localisées en dehors de l'espace économique européen

- Communication de la liste des liens et coordonnées pour déclarer une violation de données auprès de chacune des autorités de l'EEE, ainsi que les langues acceptées.
- Obligations de transparence et d'accès aux données personnelles des particuliers conservées par les entreprises. Mise en place obligatoire de processus appropriés pour assurer cet accès aux données personnelles.
- Le droit d'accès n'est soumis à aucune réserve générale de proportionnalité ; autrement dit, l'entreprise doit fournir les mêmes efforts de restitution des données personnelles, quelle que soit la quantité conservée.
- L'accès aux données ne doit pas porter atteinte aux droits et libertés d'autres personnes. (nécessité d'assurer l'omission ou l'illisibilité de certaines informations qui pourraient affecter négativement les droits d'autrui)

Mise à jour des lignes directrices sur l'autorité chef de file

Définition de la procédure du « **guichet unique** » :

- Harmonisation au niveau européen des décisions des autorités de protection des données concernant les traitements transfrontaliers.
- Précision de la notion d'établissement principal (lieu de l'administration centrale), permettant l'identification d'un seul responsable de traitement de données par entreprise et par pays. L'autorité de protection des données du pays où se trouve le siège principal d'une société, dite « autorité chef de file », est l'interlocutrice privilégiée pour le dépôt d'une plainte ou pour mener des actions répressives en cas de manquements.

Mise à jour de la ligne directrice sur l'utilisation de la technologie de reconnaissance faciale par les autorités répressives et judiciaires

- Nécessité d'une base légale adéquate et d'une autorisation spécifique pour traiter des données biométriques liées à l'identification des personnes.
- Nécessité d'allouer des ressources suffisantes aux autorités de protection des données, afin de garantir la protection des droits des personnes concernées.
- Vigilance sur les risques liés aux biais humains dans le traitement des résultats (préjugés, jugements, erreurs pouvant survenir lorsqu'une personne interprète ou analyse des données,

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot @NumSpotCloud