Image not found or type unknown

Les JO 2024 et la collecte des données personnelles

Conseils pratiques publié le **26/11/2024**, vu **140 fois**, Auteur : Murielle Cahen

sécurisées Les Jeux Olympiques, symbole d'unité et de compétition pacifique entre les nations, représentent l'apogée de l'excellence sportive et de la camaraderie internationale

. Cet événement d'envergure mondiale, suivi par des millions de personnes à travers le globe, requiert une organisation méticuleuse et une sécurité sans faille pour garantir le bon déroulement des compétitions et la protection des athlètes, des officiels et des spectateurs.

Dans cette ère numérique où la technologie occupe une place prépondérante, les organisateurs des Jeux Olympiques se trouvent confrontés à un défi de taille : la collecte et la gestion des données personnelles en zones sécurisées.

La sécurisation des lieux olympiques et la prévention des menaces potentielles exigent une surveillance constante et une analyse approfondie des informations collectées, allant des données biométriques aux données de localisation en passant par les historiques de navigation en ligne. Cette collecte massive de données vise à renforcer la sécurité des Jeux, à identifier et à neutraliser les risques éventuels, mais soulève également des questions sensibles relatives à la confidentialité, à la protection de la vie privée et à l'utilisation éthique des informations personnelles des individus.

La nécessité de concilier impératifs de sécurité et respect des droits individuels soulève des enjeux complexes et soulève des débats passionnés au sein de la communauté internationale. Les réglementations sur la protection des données, telles que le RGPD en Europe, imposent des normes strictes en matière de collecte, de stockage et de traitement des données personnelles, obligeant les organisateurs des Jeux Olympiques à mettre en place des mesures de sécurité et des protocoles de confidentialité rigoureux pour se conformer aux exigences légales et éthiques. Ainsi, la collecte des données personnelles en zones sécurisées lors des Jeux Olympiques soulève des enjeux multiples, allant de la sécurité des participants et du public à la protection de la vie privée et des libertés individuelles.

Trouver un équilibre entre ces impératifs divergents constitue un défi majeur pour les organisateurs et les autorités, appelés à garantir le succès et l'intégrité de cet événement international emblématique tout en préservant les droits et les valeurs fondamentales de chacun.

-

I. Présentation des Jeux olympiques de 2024 à Paris et Importance de la collecte des données personnelles en zones sécurisées

A. Présentation des Jeux olympiques de 2024 à Paris

Les Jeux olympiques de 2024 se tiendront à Paris, la Ville lumière, du 26 juillet au 11 août. Cet événement sportif international réunira des athlètes du monde entier pour célébrer l'excellence, la compétition et l'amitié.

Paris a été choisi comme ville hôte pour les Jeux olympiques de 2024 lors de la 131e session du CIO à Lima en 2017.

Les installations sportives emblématiques de Paris, telles que le Stade de France et le Château de Versailles, accueilleront les différentes compétitions.

L'organisation des JO 2024 implique la collecte de données personnelles des athlètes, des officiels, du personnel et des spectateurs.

Les données collectées comprennent des informations telles que les noms, les dates de naissance, les nationalités et les résultats sportifs.

En raison de la nature sensible des données collectées, des mesures de sécurité strictes seront mises en place pour protéger la vie privée et garantir la confidentialité des informations.

Les Jeux olympiques de 2024 à Paris promettent d'être un événement inoubliable, alliant sport, culture et innovation.

La collecte des données personnelles en zones sécurisées est essentielle pour assurer le bon déroulement des Jeux tout en respectant la vie privée de chacun.

B. Importance de la collecte des données personnelles en zones sécurisées

La collecte des données personnelles en zones sécurisées lors des Jeux olympiques de 2024 revêt une importance cruciale pour plusieurs raisons :

1. Sécurité des participants et des spectateurs : La collecte de données personnelles permet de garantir la sécurité des athlètes, des officiels et des spectateurs en cas d'urgence ou de situations critiques. Ces informations peuvent être utilisées pour faciliter les opérations de secours et de gestion de crise.

2. Accréditation et contrôle d’accès : La collecte de données personnelles est essentielle pour délivrer des accréditations et contrôler l'accès aux différentes zones sécurisées des sites olympiques. Cela permet de s'assurer que seules les personnes autorisées peuvent entrer dans ces espaces sensibles.

3. Gestion logistique efficace : En collectant des données personnelles telles que les horaires, les lieux de résidence et les préférences alimentaires des participants, les organisateurs peuvent planifier et organiser de manière efficace les activités liées aux Jeux olympiques, garantissant ainsi une expérience optimale pour tous les participants.

4. Suivi des performances et des résultats : La collecte de données personnelles des athlètes permet de suivre leurs performances, d'enregistrer les résultats des compétitions et de garantir l'intégrité des Jeux. Ces informations sont essentielles pour assurer le déroulement équitable des épreuves sportives.

La collecte des données personnelles en zones sécurisées pour les Jeux olympiques de 2024 est un élément clé pour assurer la sécurité, la gestion efficace des opérations et le bon déroulement des compétitions. Il est primordial de mettre en place des mesures de protection adéquates pour garantir la confidentialité et la sécurité des informations collectées.

II. Contexte des Jeux olympiques de 2024

A. Espaces et zones sécurisées définis pour l'événement

Depuis un arrêté du 2 mai 2011, il est possible en France de mettre en œuvre des traitements automatisés de données concernant les résidents de zones dites de « sécurité ». En effet, en cas « d'évènement majeur », des zones au sein desquelles la libre circulation et l'exercice de certaines activités sont restreintes pourront être constituées.

A ce titre, le Gouvernement est récemment intervenu pour actualiser les catégories de données pouvant être traitées dans ce cadre.

En effet, face à l'importance du risque terroriste, des zones de sécurité ont été définies par le préfet de Police pour l'organisation des Jeux, dont notamment :

Le périmètre noir (dit SILT Sécurité insécurité et lutte contre le terrorisme) qui concerne les sites de compétitions : la circulation des personnes et véhicules sera réglementée et des vérifications effectuées ;

Le périmètre rouge au sein duquel la circulation des véhicules sera interdite sauf dérogation spécifique.

Hormis l'achat d'un billet ou l'accréditation par le Comité d'organisation des Jeux olympiques et paralympiques (COJOP), pour accéder à ces périmètres il faudra obtenir un laissez-passer grâce à un enregistrement préalable sur une plateforme numérique ou en mairie, à compter du 13 mai 2024.

Or, la délivrance d'un laissez-passer entraînera nécessairement une collecte de données personnelles des personnes amenées à circuler dans les zones encadrées.

C'est dans ces circonstances que l'avis de la CNIL a été sollicité sur la légalité des modalités de cette collecte.

B. Enjeux de sécurité liés à la collecte des données personnelles

Les Jeux olympiques de 2024 à Paris sont un événement d'envergure mondiale qui soulève des enjeux majeurs en matière de sécurité, notamment en ce qui concerne la collecte et la gestion des données personnelles. Voici quelques-uns des principaux enjeux de sécurité liés à la collecte des données personnelles pour cet événement :

1. Protection des données sensibles : Les données personnelles collectées dans le cadre des Jeux olympiques de 2024, telles que les informations personnelles des athlètes, des officiels et des spectateurs, sont sensibles et doivent être protégées contre tout accès non autorisé ou toute utilisation abusive.

2. Confidentialité et respect de la vie privée : Il est essentiel de garantir la confidentialité et le respect de la vie privée des individus dont les données sont collectées. Les organisateurs des Jeux doivent mettre en place des mesures de sécurité adéquates pour prévenir toute violation de la vie privée.

3.Gestion sécurisée des données : La collecte et la gestion des données personnelles doivent être effectuées de manière sécurisée, en utilisant des protocoles de sécurité robustes pour garantir l'intégrité et la confidentialité des informations. Les données doivent être stockées et traitées de manière sécurisée pour éviter tout risque de piratage ou de fuite.

4. Consentement et transparence : Il est important d'obtenir le consentement des individus pour la collecte de leurs données personnelles et de leur expliquer clairement comment ces données seront utilisées. La transparence est essentielle pour établir la confiance des participants et du public dans la gestion de leurs données.

III. Collecte des données personnelles

A. Types de données collectées lors des JO 2024

Si la CNIL a admis la légitimité du dispositif du « laissez-passer », elle a toutefois émis quelques réserves sur la collecte supplémentaire de certaines données et les durées de conservation envisagées.

Sur le fondement de l’arrêté de 2011, il était d’ores et déjà possible de collecter le numéro du document d’identité de la personne concernée, son état civil, ses adresses postales et électroniques, ses coordonnées téléphoniques, ou encore son justificatif de résidence ou le titre d’accès à la zone.

Désormais pourront également être collectés :

La copie de l’un de ces documents justifiant l’identité de la personne concernée ;

Le justificatif d’accès à la zone de sécurité, dans le but de vérifier la conformité des informations remplies en lien avec les pièces justificatives fournies par la personne concernée.

La photographie de la personne concernée, afin d’établir le titre d’accès et d’identifier la personne lors du passage au point de contrôle.

Sur ce type de données, la CNIL a émis des réserves concernant la nécessité de la collecte. Cette dernière ne pourra être mise en œuvre que lorsqu'un grand nombre de personnes sont attendues simultanément dans la zone, et sera ainsi limitée aux évènements de cette ampleur.

Face aux incertitudes sur la nécessité de recueillir la photographie, l'arrêté du 3 mai 2024 précise le caractère facultatif de cette collecte, apprécié au regard de l'ampleur des contrôles à mener pendant les Jeux.

B. Méthodes de collecte et stockage sécurisées

La collecte et le stockage des données personnelles lors des Jeux olympiques de 2024 à Paris doivent être effectués de manière sécurisée pour garantir la confidentialité, l'intégrité et la protection des informations sensibles des participants, des athlètes, des officiels et des spectateurs. Voici quelques méthodes de collecte et de stockage sécurisées qui pourraient être mises en place pour assurer la sécurité des données personnelles :

1. Collecte des données sécurisée : La collecte des données personnelles doit se faire de manière sécurisée, en utilisant des protocoles de sécurité tels que le chiffrement des données, les connexions sécurisées et les mesures de protection contre les attaques informatiques.

2. Accès restreint aux données : Seules les personnes autorisées et nécessitant l'accès aux données personnelles devraient être autorisées à les consulter. Des contrôles d'accès stricts doivent être mis en place pour limiter l'accès aux informations sensibles.

3. Stockage sécurisé des données : Les données personnelles collectées doivent être stockées de manière sécurisée, en utilisant des systèmes de stockage sécurisés et des mesures de protection des données telles que le cryptage, la sauvegarde régulière et la surveillance continue.

4. Gestion des données conforme aux réglementations : La collecte et le stockage des données personnelles doivent être conformes aux réglementations en vigueur en matière de protection des données, telles que le Règlement général sur la Protection des Données (RGPD) en Europe.

5. Formation du personnel : Le personnel chargé de la collecte et du traitement des données personnelles doit être formé aux meilleures pratiques en matière de protection des données et de sécurité informatique pour garantir le respect des normes de confidentialité et de sécurité.

C. Protection de la vie privée des participants et des spectateurs

Lors des Jeux olympiques de 2024 à Paris, la collecte des données personnelles des participants et des spectateurs est une pratique courante pour assurer la sécurité, la gestion efficace de l'événement et le suivi des performances des athlètes. Cependant, il est crucial de protéger la vie privée des individus dont les données sont collectées. Voici quelques mesures clés pour garantir la protection de la vie privée des participants et des spectateurs lors de la collecte de données personnelles :

1. Consentement éclairé : Il est essentiel d'obtenir le consentement éclairé des participants et des spectateurs pour la collecte et le traitement de leurs données personnelles. Les individus doivent être informés de manière transparente sur les types de données collectées, les finalités de leur utilisation et les mesures de sécurité mises en place pour protéger leurs informations.

2. Minimisation des données : Seules les données personnelles nécessaires aux fins spécifiques des Jeux olympiques doivent être collectées. Il est important de limiter la collecte de données au strict nécessaire pour éviter la collecte excessive d'informations sensibles.

3. Sécurité des données : Les données personnelles collectées doivent être stockées et traitées de manière sécurisée, en utilisant des mesures de sécurité telles que le chiffrement des données, les connexions sécurisées et les protocoles de protection contre les cyberattaques.

4. Transparence et confidentialité : Les organisateurs des Jeux olympiques doivent être transparents sur la manière dont les données personnelles sont collectées, utilisées et partagées. Les informations des participants et des spectateurs doivent être traitées de manière confidentielle et ne doivent pas être divulguées à des tiers sans leur consentement.

5. Droit d'accès et de rectification : Les individus doivent avoir le droit d'accéder à leurs données personnelles collectées et de demander des corrections ou des suppressions si nécessaire. Les organisateurs des Jeux doivent mettre en place des procédures pour permettre aux individus d'exercer leurs droits en matière de protection des données.

D. La durée de conservation des données personnelles collectées lors des Jeux olympiques de 2024

La durée de conservation des données personnelles collectées lors des Jeux olympiques de 2024 est un aspect important à prendre en compte pour garantir la protection de la vie privée des participants et des spectateurs.

Concernant ce nouveau traitement, la CNIL a estimé qu’il n’était pertinent que pour instruire les demandes et l’établissement des titres d’accès. En ce sens, ces données ne seront conservées que jusqu’à la délivrance du titre d’accès, tandis que les autres données seront conservées trois (3) mois à compter de la fin de l’évènement.

IV. Implications et enjeux

A. Risques associés à la collecte des données personnelles en zones sécurisées

La collecte des données personnelles lors des Jeux olympiques de 2024 en zones sécurisées soulève plusieurs risques et enjeux qui doivent être pris en compte pour garantir la protection de la vie privée et la sécurité des informations sensibles. Voici quelques risques associés à la collecte des données personnelles en zones sécurisées lors de l'événement :

1. Risque de violation de la vie privée : La collecte des données personnelles en zones sécurisées peut entraîner un risque de violation de la vie privée des participants, des athlètes, des officiels et des spectateurs si les informations sensibles sont mal gérées, divulguées ou utilisées de manière inappropriée.

2. Risque de piratage informatique : Les zones sécurisées des Jeux olympiques sont souvent la cible des cybercriminels qui cherchent à accéder aux données personnelles sensibles. Un piratage informatique pourrait compromettre la sécurité des informations et entraîner des conséquences graves pour les individus concernés.

3. Risque de surveillance excessive : La collecte des données personnelles en zones sécurisées peut entraîner une surveillance excessive des individus, ce qui soulève des préoccupations en matière de respect de la vie privée et de libertés individuelles. Il est important de garantir que la collecte des données est proportionnée et justifiée par des finalités légitimes.

4. Risque de non-conformité aux réglementations sur la protection des données : La collecte des données personnelles doit être conforme aux réglementations en vigueur en matière de protection des données, telles que le RGPD en Europe. Tout manquement aux obligations légales en matière de protection de la vie privée peut entraîner des sanctions financières et des dommages à la réputation des organisateurs.

5. Risque de fuite d'informations sensibles : La collecte des données personnelles en zones sécurisées peut augmenter le risque de fuite d'informations sensibles si les mesures de sécurité ne sont pas adéquates. Il est crucial de mettre en place des protocoles de sécurité robustes pour protéger les données personnelles contre tout accès non autorisé.

B. Mesures prises pour garantir la sécurité des données

Pour garantir la sécurité des données personnelles collectées en zones sécurisées lors des Jeux olympiques de 2024, les organisateurs doivent mettre en place des mesures de sécurité robustes et des protocoles de protection des informations sensibles. Voici quelques mesures clés qui peuvent être prises pour assurer la sécurité des données personnelles :

1. Chiffrement des données : Toutes les données personnelles collectées doivent être chiffrées pour protéger les informations sensibles contre tout accès non autorisé. Le chiffrement des données garantit que seules les personnes autorisées peuvent accéder aux informations et réduit les risques de fuite ou de vol de données.

2. Contrôles d'accès : Mettre en place des contrôles d'accès stricts pour limiter l'accès aux données personnelles aux seules personnes autorisées. Les identifiants uniques, les mots de passe forts et l'authentification à deux facteurs peuvent être utilisés pour renforcer la sécurité des informations.

3. Sauvegarde des données : Mettre en place des systèmes de sauvegarde réguliers pour garantir la disponibilité des données en cas de panne ou de sinistre. Les sauvegardes doivent être stockées de manière sécurisée et être facilement récupérables en cas de besoin.

4. Formation du personnel : Sensibiliser et former le personnel sur les bonnes pratiques en matière de protection des données et de sécurité informatique. Le personnel doit être conscient des risques potentiels liés à la collecte et au traitement des données personnelles et être formé pour les identifier et y réagir de manière adéquate.

5. Audit de sécurité : Réaliser régulièrement des audits de sécurité pour évaluer la robustesse des mesures de sécurité mises en place et détecter d'éventuelles failles ou vulnérabilités. Les audits de sécurité permettent d'identifier et de corriger les risques de sécurité avant qu'ils ne soient exploités par des cybercriminels.

6. Conformité aux normes de protection des données : Assurer la conformité aux réglementations en vigueur en matière de protection des données, telles que le RGPD en Europe. Les organisateurs des Jeux olympiques doivent respecter les principes de protection des données, tels que la minimisation des données, la transparence et le respect des droits des individus sur leurs informations personnelles.

C. Conformité aux réglementations sur la protection des données

La collecte des données personnelles en zones sécurisées lors des Jeux olympiques de 2024 soulève des enjeux majeurs en matière de conformité aux réglementations sur la protection des données, notamment le Règlement général sur la Protection des Données (RGPD) en Europe.

Il est crucial pour les organisateurs de l'événement de garantir le respect des principes et des obligations énoncés dans ces réglementations pour protéger la vie privée des individus et éviter les sanctions financières et les dommages à la réputation liés à une violation des règles de protection des données. Voici quelques considérations importantes pour assurer la conformité aux réglementations sur la protection des données lors de la collecte des données personnelles en zones sécurisées :

1. Consentement des individus : Les organisateurs doivent obtenir le consentement explicite des individus pour collecter et traiter leurs données personnelles. Le consentement doit être libre, spécifique, éclairé et univoque, et les individus doivent être informés de la finalité de la collecte des données, des droits dont ils disposent et de la durée pendant laquelle leurs données seront conservées.

2. Minimisation des données : Les données personnelles collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire pour atteindre la finalité pour laquelle elles sont traitées. Il est essentiel de minimiser la quantité de données collectées et de ne pas conserver les informations plus longtemps que nécessaire.

3. Transparence et information : Les individus doivent être informés de manière transparente et claire sur la manière dont leurs données personnelles sont collectées, traitées et utilisées. Une politique de confidentialité détaillée doit être mise à disposition des individus pour expliquer les pratiques de traitement des données et les droits dont ils disposent.

4. Droit d'accès et de rectification : Les individus ont le droit d'accéder aux données personnelles les concernant, de les rectifier si elles sont inexactes et de demander leur suppression si elles ne sont plus nécessaires. Les organisateurs doivent mettre en place des procédures pour répondre aux demandes d'exercice de ces droits dans les délais prescrits par la réglementation.

5. Sécurité des données : Les données personnelles doivent être protégées par des mesures de sécurité appropriées pour prévenir tout accès non autorisé, toute divulgation, toute altération ou toute perte des informations sensibles. Le chiffrement des données, les contrôles d'accès et les

audits de sécurité sont des mesures essentielles pour garantir la sécurité des données.

V. Recommandations et bonnes pratiques

A. Protéger les données sensibles

Pour protéger les données sensibles collectées en zones sécurisées lors des Jeux olympiques de 2024, il est essentiel de mettre en place des recommandations et des bonnes pratiques en matière de sécurité des données. Voici quelques recommandations clés pour protéger efficacement les données sensibles :

1. Classification des données : Classer les données en fonction de leur sensibilité et de leur importance pour déterminer les mesures de sécurité appropriées à mettre en place. Les données sensibles, telles que les informations médicales, les données biométriques ou les informations financières, doivent bénéficier d'un niveau de protection plus élevé.

2. Chiffrement des données : Chiffrer les données sensibles en transit et au repos pour protéger les informations contre tout accès non autorisé. Le chiffrement garantit que seules les personnes autorisées peuvent accéder aux données et réduit les risques de fuite ou de vol d'informations sensibles.

3. Contrôles d'accès : Mettre en place des contrôles d'accès stricts pour limiter l'accès aux données sensibles aux seules personnes autorisées. Utiliser des mécanismes d'authentification forte, tels que l'authentification à deux facteurs, pour renforcer la sécurité des informations et prévenir les accès non autorisés.

4. Gestion des identités : Mettre en place des processus de gestion des identités pour contrôler et surveiller l'accès aux données sensibles. Suivre et auditer les activités des utilisateurs pour détecter toute activité suspecte et réagir rapidement en cas de violation de la sécurité.

5.Sécurité physique : Protéger physiquement les équipements et les infrastructures utilisés pour stocker et traiter les données sensibles. Limiter l'accès aux zones sécurisées et mettre en place des dispositifs de surveillance pour prévenir les intrusions et les vols de matériel.

6. Formation du personnel : Sensibiliser et former le personnel sur les bonnes pratiques en matière de sécurité des données et de protection de la vie privée. Le personnel doit être conscient des risques potentiels liés à la collecte et au traitement des données sensibles et être formé pour les prévenir et y réagir de manière adéquate.

7. Audit de sécurité : Réaliser régulièrement des audits de sécurité pour évaluer l'efficacité des mesures de sécurité mises en place et détecter d'éventuelles failles ou vulnérabilités. Les audits de sécurité permettent d'identifier et de corriger les risques de sécurité avant qu'ils ne soient exploités par des cybercriminels.

B. Sensibilisation à la sécurité des données

Pour assurer la protection des données personnelles collectées en zones sécurisées lors des Jeux olympiques de 2024, il est essentiel de sensibiliser tous les acteurs impliqués à la sécurité des données. Voici quelques recommandations et bonnes pratiques pour sensibiliser efficacement à la sécurité des données :

1. Formation en sécurité des données : Organiser des sessions de formation régulières pour sensibiliser le personnel, les bénévoles et les prestataires de services à l'importance de la sécurité des données. La formation devrait couvrir les bonnes pratiques en matière de protection des données, les risques potentiels liés à la collecte et au traitement des informations personnelles, ainsi que les mesures de sécurité à mettre en place.

2. Communication sur la confidentialité : Communiquer de manière transparente sur les politiques de confidentialité et les pratiques de traitement des données mises en place lors des Jeux olympiques. Informer les participants, les spectateurs et les autres parties prenantes sur la manière dont leurs données personnelles sont collectées, utilisées et protégées pour renforcer la confiance et la transparence.

3. Responsabilisation des acteurs : Sensibiliser les acteurs impliqués à leur responsabilité individuelle dans la protection des données personnelles. Insister sur l'importance de respecter les règles de confidentialité, de ne pas divulguer d'informations sensibles et de signaler tout incident de sécurité ou toute violation de données dès qu'ils en ont connaissance.

4. Gestion des risques : Sensibiliser à l'identification et à la gestion des risques liés à la sécurité des données. Encourager les acteurs à être vigilants face aux menaces potentielles, telles que les cyberattaques, les fuites de données ou les erreurs humaines, et à adopter des comportements sécurisés pour prévenir les incidents de sécurité.

5. Support et assistance : Mettre en place des canaux de support et d'assistance pour répondre aux questions et aux préoccupations des acteurs concernant la sécurité des données. Fournir des ressources et des conseils pratiques pour aider les personnes à adopter des pratiques sécurisées et à protéger efficacement les informations personnelles.

6. Sensibilisation continue : Assurer une sensibilisation continue à la sécurité des données tout au long de l'événement en organisant des rappels réguliers, en diffusant des messages de sensibilisation et en mettant à jour les connaissances sur les meilleures pratiques en matière de protection des données.

C. Collaboration avec les autorités compétentes et les organismes de protection des données

Pour garantir la protection des données personnelles collectées en zones sécurisées lors des Jeux olympiques de 2024, il est essentiel de collaborer étroitement avec les autorités compétentes et les organismes de protection des données. Voici quelques recommandations et bonnes pratiques pour une collaboration efficace dans ce domaine :

1. Respect de la réglementation en vigueur : Assurer la conformité avec les lois et réglementations en matière de protection des données, telles que le Règlement général sur la Protection des Données (RGPD) en Europe. Collaborer avec les autorités compétentes pour s'assurer que les pratiques de collecte, de traitement et de stockage des données sont en conformité avec la législation en vigueur.

2. Consultation des autorités de protection des données : Consulter les autorités de protection des données dès le stade de la planification pour obtenir des conseils et des recommandations sur les mesures de sécurité à mettre en place pour protéger les données personnelles. Les autorités

compétentes peuvent fournir des orientations spécifiques pour garantir la conformité et la sécurité des informations collectées.

3. Notification des violations de données : Mettre en place des procédures de notification des violations de données et informer rapidement les autorités de protection des données en cas d'incident de sécurité affectant les données personnelles collectées. Collaborer avec les autorités pour gérer efficacement les incidents de sécurité et minimiser les risques pour les personnes concernées.

4. Audit et contrôle des pratiques de traitement des données : Collaborer avec les autorités compétentes pour réaliser des audits et des contrôles des pratiques de traitement des données personnelles en zones sécurisées. Permettre aux autorités de vérifier la conformité des mesures de sécurité mises en place et de recommander des ajustements si nécessaire.

5. Partage d'informations et de bonnes pratiques : Échanger des informations et des bonnes pratiques avec les autorités compétentes et d'autres organismes de protection des données pour renforcer la sécurité des données collectées. Partager les enseignements tirés, les solutions innovantes et les stratégies efficaces pour protéger les informations personnelles de manière collaborative.

6. Formation et sensibilisation : Collaborer avec les autorités compétentes pour sensibiliser le personnel, les bénévoles et les prestataires de services à l'importance de la protection des données et aux bonnes pratiques en matière de sécurité des informations. Organiser des sessions de formation en partenariat avec les autorités pour renforcer les compétences et les connaissances en matière de protection des données.

Sources :

1. Les JO 2024 et la collecte des données personnelles en zones sécurisées (haas-avocats.com)

2. Délibération 2024-034 du 25 avril 2024 - Légifrance (legifrance.gouv.fr)

3. Arrêté du 2 mai 2011 relatif aux traitements automatisés de données à caractère personnel dénommés « fichiers des résidents des zones de sécurité » créés à l'occasion d'un événement majeur - Légifrance (legifrance.gouv.fr)