Relevé d'Informations, de Décisions et d'Actions du 15/04/2024

1. Informations

30 septembre 2020 : fourniture des tablettes et des ordiphones avec mise en place d'un compte Google générique – adresse mail unique. Le mot de passe du compte est connu uniquement du service informatique (2 personnes)

- 11 Tablettes fournies aux agents : MDM (gestion de flotte mobile) en place entre le 8 et le 31 janvier 2024
- 15 Tablettes fournies à l'ensemble des conseillers municipaux (non enrôlés MDM)
- 32 téléphones portables fournis aux agents (25 flottes MDM depuis le 8 janvier 2024 et 5 non enrôlés au MDM)
- 2 téléphones portable élus de la commune (2 flottes MDM depuis le 8 janvier 2024)

Lors du conseil municipal du 11 avril 2024 : les élus de l'opposition ont signalé qu'ils avaient accès à des données caractère personnel auxquelles ils n'auraient pas dû avoir accès (compte Google unique sur l'ensemble des tablettes).

[date inconnue - avant le 11 avril 2024]

- constat d'huissier à la demande des élus minoritaires des tablettes qui ont étés mises sous scellés
- plainte contre X auprès du procureur de la République
- plainte remise en copie Préfecture et sous-préfecture

Données à caractère personnel constatées en interne (investigation du 12/04/2024)

- 17 contacts (prénom + téléphone)
- Photos d'ordre privé (6Go)
- Historique de navigation : données de géolocalisation d'une personne

Données à caractère personnel indiquées par les élus de la minorité (non vérifié) :

- Trajet détaillé d'employés communaux
- Agenda du Maire avec rendez-vous privés
- Numéros de téléphone personnels agents et élus + mots de passe

D'autres informations telles que des accès à des sites illégaux et diverses recherches personnelles ont été mentionnés sans précisions sur d'éventuelles données à caractère personnel.

Personnes concernées identifiées à ce jour :

- Le Maire
- Le DGS
- 1 agent de la DSI et 1 agent des services techniques

Le 15 avril 2024 : 3 personnes concernées par la violation (l'agent des services techniques n'a pas été interrogé) ont évalué la gravité d'atteinte à la vie privée :

- Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale)
- Refus de continuer à utiliser le SI
- Difficultés relationnelles avec l'entourage

Gravité évaluée à « limité » (2 sur échelle de 4)

Échelle et règles pour estimer la gravité

	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[3]	Exemples d'impacts matériels[4]	Exemples d'impacts moraux[5]
Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	- Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) - Maux de tête passagers	- Perte de temps pour réitérer des démarches ou pour attendre de les réaliser - Réception de courriers non sollicités (ex. : spams) - Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) - Publicité ciblée pour des produits de consommation courants	- Simple contrariété par rapport à l'information reçue ou demandée - Peur de perdre le contrôle de ses données - Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale) - Perte de temps pour paramétrer ses données - Non respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)
Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	- Affection physique mineure (ex. : maladie bénigne suite au non-respect de contre-indications) - Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) - Diffamation donnant lieu à des représailles physiques ou psychiques	- Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement - Refus d'accès à des services administratifs ou prestations commerciales - Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) - Promotion professionnelle manquée - Compte à des services en ligne bloqué (ex. : jeux, administration) - Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées - Élévation de coûts (ex. : augmentation du prix d'assurance) - Données non mises à jour (ex. : poste antérieurement occupé) - Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) - Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) - Profilage imprécis ou abusif	- Refus de continuer à utiliser les systèmes d'information (whistleblowing, réseaux sociaux) - Affection psychologique mineure mais objective (diffamation, réputation) - Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) - Sentiment d'atteinte à la vie privée sans préjudice irrémédiable - Intimidation sur les réseaux sociaux
Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	- Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non respect de contre-indications) - Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	- Détournements d'argent non indemnisé - Difficultés financières non temporaires (ex. : obligation de contracter un prêt) - Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) - Interdiction bancaire - Dégradation de biens - Perte de logement - Perte d'emploi - Séparation ou divorce - Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage - phishing) - Bloqué à l'étranger	- Affection psychologique grave (ex. : dépression, développement d'une phobie) - Sentiment d'atteinte à la vie privée et de préjudice irrémédiable - Sentiment de vulnérabilité à la suite d'une assignation en justice - Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) - Victime de chantage - Cyberbullying et harcèlement moral

Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	- Affection physique de longue durée ou permanente (ex. : suite au non-respect d'une contre- indication)- Décès (ex. : meurtre, suicide, accident mortel)- Altération définitive del'intégrité physique	- Péril financier- Dettes importantes- Impossibilité de travailler- Impossibilité de se reloger- Perte de preuves dans le cadre d'un contentieux- Perte d'accès à une infrastructure vitale (eau, électricité)	- Affection psychologique de longue durée ou permanente- Sanction pénale- Enlèvement- Perte de lien familial- Impossibilité d'ester en justice- Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

Il est préconisé par le DPD Mutualisé de notifier à la CNIL même si le risque semble limité à ce jour car :

- il n'y a pas suffisamment d'éléments pour recenser de manière exhaustive les données personnelles ni les personnes concernées par cette violation. Par conséquent, une approche pessimiste est recommandée par la CNIL dans le cadre procédure de notification.

- la plainte en cours empêche le responsable du traitement de prendre les mesures de sécurité utiles pour stopper la violation de façon sûre (suppression des données). C'est la raison pour laquelle toutes les tablettes doivent être mise sous scellés afin de limiter la violation de données et non réinitialisées.

Communication aux personnes concernées :

Une communication **générale aux utilisateurs des terminaux** concernés devrait être privilégiée (plutôt qu'individuelle) car le responsable du traitement ne dispose pas suffisamment d'éléments permettant d'identifier de manière exhaustive les personnes concernées.

2. Décisions

Effectuer une déclaration initiale auprès de la CNIL et informer les personnes concernées.

Demande écrite formulée par Monsieur Le Maire

Suite à la notification, un **mail de la CNIL rappelant l'interdiction d'utilisation de comptes génériques a été reçue (le jour même, 1h après)**

A noter : la mairie est conseillée par Soluris sur les démarches d'homologation de son système d'information au Référentiel Général de Sécurité (RGS) et de conformité au Règlement Général sur la Protection des Données (RGPD) ainsi qu'un avocat en droit du numérique.

3. Actions

N°	Quoi	Qui	Quand	Statut
	Mettre en place les premières mesures de sécurité sur ce traitement (voir préconisations AGR-Soluris)		12/04/2024	Terminé
	Effectuer une déclaration auprès de la CNIL		15/04/2024	Terminé
	Récupérer en urgence l'ensemble des tablettes concernées pour limiter la violation de données. Courrier à faire par le maire (DGS). (La suppression des données n'est pas possible à ce jour car doit être conservée en tant que preuve dans le cadre de l'enquête.)	Responsable de Traitement (RT)	15/04/2024	En cours
	Rédiger une communication aux personnes concernées	RT	La plus rapidement possible	
	Compléter la déclaration CNIL avec les éléments de communication aux personnes concernées et mesures/décisions prises	RT	Dès que des éléments nouveaux permettent de le faire	
	Réaliser une démarche de sécurisation globale de la collectivité	RT	Rapidement	
	Réaliser une AIPD sur ce traitement	RT	Rapidement	
	Se préparer à un contrôle de la CNIL	RT	28/06/2024	
	Faire le suivi RGPD et mettre à jour la collectivité	RT	28/06/2024	
	RGPD ! Lister les traitements à risques	RT	30/04/2024	

4. Annexes :

- Demande écrite du responsable du traitement déclaration CNIL et information des personnes
- Copie de la notification initiale faite à la CNIL
- Copie de la réponse de la CNIL