Extrait du Registre des activités de traitement
Produit Infractions

Registre des activités de traitement (RPA)

Le registre des activités de traitement est un document qui recense et détaille tous les traitements de données personnelles réalisés par une organisation. Il vise à documenter les différents flux de données, en identifiant les types de données collectées, les finalités de leur traitement, et les modalités de gestion de ces données, notamment en matière de sécurité et de protection.

Information documentaire	
Numéro de document	30-00
Suivi de la documentation	Version : 2.3 – Statut : Final – Date édition : 17/01/2025
Editeur	DPO
Classification	Interne ou général : tous les employés (non restreint). Données de l'organisation qui ne sont pas destinées à une consommation publique.

Historique du document

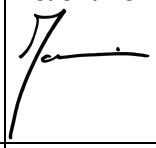
Version	Date	Auteur	Modification
1.0	02/12/2024	Didier Marcelis	Création (Draft)
2.0	13/12/2024	Didier Marcelis	Révisions (Draft)
2.1	17/12/2024	Didier Marcelis	Révisions (Draft)
2.2	07/01/2025	Gwendoline Grimont	Révisions, corrections, validation (Draft)
2.3	16/01/2025	Didier Marcelis	Révisions (Final)

Groupe de travail

Nom ou Fonction	Organisation
Aménagement du territoire & NOS DPO, Legal & Administration	SIGI

Approbation

Dans le cas où la version majeure ne peut pas être approuvée en utilisant une signature électronique, le document signé de manière manuscrite sera téléversé dans la bibliothèque en version PDF/A par le DPO (avec signature électronique de celui-ci).

Nom	Rôle	Responsabilité	Date & Signature
Didier Marcelis	DPO	Documenter, assurer la conformité. (*)	20/01/2025 
Philippe Meyers	Président	Approbation	26/01/2025  Philippe Meyers (Jan 26, 2025 12:18 GMT+1)
Sylvain Momin	Directeur	Mise en application	21/01/2025 

(*) Synthèse de la responsabilité du DPO :

- Documenter et tenir à jour le registre des traitements.
- Assurer la conformité des traitements avec les exigences du RGPD.
- Enregistrer et valider les activités de traitement.
- Agir comme point de contact pour les responsables du traitement et l'autorité de contrôle (CNPD).
- Superviser les mesures de sécurité et contribuer à leur mise en œuvre.
- Sensibiliser les parties prenantes à la gestion de la protection des données.

Coordonnées du responsable de l'organisme :

Le Bureau, constitué de :

Philippe Meyers ..... Président (Échevin Dippach) ..... meyers@dippach.lu

Guy Breden ..... 1er Vice-président (Conseiller Kehlen) ..... guy.breden@kehlen.lu

Josiane Di Bartolomeo-Ries ..... 2e Vice-président (Échevine Dudelange) ..... josiane.ries@dudelange.lu

Marc Ries ..... Membre (Bourgmestre Betzdorf) ..... ries.marc@pt.lu

Luc Feller ..... Membre (Bourgmestre Mamer) ..... luc.feller@hcpn.etat.lu

Alex Donnersbach ..... Membre (Député-échevin Walferdange) ..... alex.donnersbach@walfer.lu

Gérard Hartung ..... Membre (Échevin Differdange) ..... gerard.hartung@differdange.lu

Syndicat Intercommunal de Gestion Informatique (SIGI)

11 rue Edmond Reuter

L-5326 Contern

Tél. : +352 35 00 99 1

https://www.sigi.lu/

Coordonnées du délégué à la protection des données (DPO) :

Didier Marcelis ..... DPO ..... didier.marcelis@sigi.lu

Syndicat Intercommunal de Gestion Informatique (SIGI)

11 rue Edmond Reuter

L-5326 Contern

Tél. : +352 35 00 99 245

https://www.sigi.lu/aspects-legaux/

Table des matières

1. Avertissements taxés

Date de création	17/09/2021
Date mise en œuvre	17/09/2021
Date mise à jour	10/01/2025
Etat	Actif
Responsable du Traitement	Administrations Communales
Coordonnées responsable du traitement	Administrations Communales membres du syndicat
Coordonnées DPO	DPO des Administrations Communales
Nom responsable conjoint traitement	NA
Produit, logiciel, application concerné	Infractions
Code Acronyme	AT
Service CDC Département	Aménagement du territoire & NOS
Description	Permettre l'enregistrement, la gestion et l'archivage des avertissements émis par les agents municipaux pour des infractions mineures, telles que les infractions de stationnement, à l'aide d'une application mobile dédiée.
Finalités, objectifs du traitement	Constater, enregistrer, gérer, transférer et archiver les avertissements taxés émis par les agents municipaux pour des infractions constatées sur la voie publique (par exemple : infractions de stationnement).
Base légale, juridique du traitement Légitimité	• Le traitement est nécessaire à l'exécution de la mission d'intérêt public et de l'exercice de l'autorité publique de la commune (RGPD article 6.1e). • Article 15 de la loi modifiée du 14 février 1955 portant réglementation de la circulation sur toutes les voies publiques (Code de la route). • Fondement juridique : Le code de la route 20210310 (Legilux) • Avertissement Taxé, Mémorial A n1986-26 • Avertissement Taxé, Mémorial A n2002-142 • Avertissement Taxé, Mémorial A n2004-209 • Avertissement Taxé, Mémorial A n2015-180
Catégorie de personnes concernées	• Contrevenants (propriétaires ou utilisateurs des véhicules) • Agents municipaux habilités
Catégorie de données traitées	• Localisation • Temporelles • Relatives aux infractions • Relatives aux véhicules
Source des données	• Personne concernée • Agent municipal • Garde champêtre • CTIE • Registre des adresses (SIGI) • Indigo Neo
Catégories de destinataires des données	• Services municipaux pour le suivi et recouvrement • Plateformes tierces (Indigo Neo pour le contrôle du stationnement) • SIGI pour le stockage et le transfert des données • Autorités administratives et judiciaires • Police pour le suivi et la réception / contrôle des paiements
Transfert hors UE	non

Transfert organisation	• Administration Communale concernée • Syndicat Intercommunal de Gestion Informatique (SIGI) • Centre des technologies de l'information de l'Etat (CTIE) • Indigo Neo
DPIA	non
Justification DPIA	NA
Mesures de sécurité (Protection des données)	Les mesures de sécurité sont mises en oeuvre conformément à la politique de sécurité des systèmes d'information (SGSI) du SIGI (réf. POL_00-00_PolSec) • Authentification forte • Chiffrement des données • Accès restreint aux agents habilités, verrouillage de l'application mobile via Face ID ou empreinte digitale • Traçabilité des actions (audit et logs), journal des logs d'activités réalisées sur les données au sein des applications. • Chaque application accessible aux communes est accédée au travers d'une connexion sécurisée par des protocoles et mécanismes d'échanges tels que TLS et MPLS. • Les accès aux bâtiments sont régulés par un système d'identification par badge. • Le Virtual Private Cloud est protégé contre les risques environnementaux (système anti-feu sur les sites, redondance des sites) • La politique du bureau propre et écran vide est appliquée. • Les performances des serveurs sont contrôlées en temps réel. • Aucune activité de développement n'est techniquement possible sur l'environnement de production. • Les environnements de développement, de test et de production sont cloisonnés. • Les bases de données font l'objet d'un backup dont la fréquence est fixée par les besoins spécifiques du métier. • Un journal des évènements est maintenu sur chaque serveur. • Chaque environnement bénéficie de son propre réseau qui est sécurisé et cloisonné. • L'ensemble des systèmes est redondant et des tests de continuité sont réalisés annuellement.
Mesures techniques et organisationnelles	Les mesures de sécurité sont mises en oeuvre conformément à la politique de sécurité des systèmes d'information (SGSI) du SIGI (réf. POL_00-00_PolSec) • Le SIGI entretient des relations régulières avec les autorités/spécialistes. • Le SIGI s'est doté d'une politique de gestion de la sécurité de l'information (ISO 27001). • Les procédures de test de restauration de base de données sont exécutées annuellement. • Le déploiement de solutions logicielles en production est réalisé uniquement par des administrateurs désignés spécifiquement pour cette tâche. • Des procédures de rollback sont prévues en cas de problèmes liés au déploiement. • Les développements des solutions logicielles sont réalisés sur des environnements de développement sécurisés. • Les contrats avec les fournisseurs reprennent l'ensemble des exigences de sécurité prescrites par le SIGI. • Des SLA (Service Level Agreement) sont convenus avec les fournisseurs et sont revus à échéance fixe. Les échéances de ces révisions sont fixées contractuellement avec chaque fournisseur. • Des mesures de contrôle d'accès aux informations sont prescrites par le SIGI et appliquées lors de l'octroi de chaque accès.

	• Chaque évènement significatif relatif à la gestion des identités est maintenu dans un registre. • Une procédure spécifique gère l'accueil et le départ de chaque collaborateur au sein de la structure du SIGI. • Chaque collaborateur ainsi que les entreprises sous-traitantes signent une charte de confidentialité. • L'ensemble des collaborateurs sont sensibilisés à la gestion de la sécurité de l'information ainsi qu'au GDPR. • La gestion du changement est contrôlée par une procédure et validée par les responsables métiers. • Toute procédure fait l'objet d'une documentation mise à la disponibilité des collaborateurs concernés. • Des échanges réguliers avec l'autorité de contrôle (CNPD) ainsi qu'avec des spécialistes juridiques et techniques sont organisés régulièrement sur les thématiques liées à la gestion de la sécurité des informations. • La mise à jour des anti-virus est pilotée par la politique de sécurité prescrite par le SIGI. • Les codes sources ne sont pas disponibles dans l'environnement d'exploitation La gestion des codes sources est encadrée par des procédures spécifiques. • Conformément à la loi luxembourgeoise, les données sont conservées au Luxembourg. La conformité à la loi luxembourgeoise est assurée par le secrétaire du SIGI.
Données à Caractère Personnel (DCP)	*NomDCP;Catégorie;Donnée sensible;Personne concernée* PlaqueImmatriculation;Identification;non;Citoyen NomAgent;Identification;non;Agent PrénomAgent;Identification;non;Agent
Durée, rétention des données Période de conservation Durée d'utilité Administrative (DUA)	• Avertissements actifs : 45 jours correspondant au délai de réclamation avant effacement, augmenté d'un mois pour les non résidents ou jusqu'à recouvrement des amendes. • Anonymisation : Après 76 jours (procédure BR-Infr-TraitementsSystème-02). • Logs de transfert conservés 76 jours augmeté d'un mois pour les non résidents.
DCP - Infos complémentaires	NA
Sous-traitants et description	*Sous-traitant;Description du service opéré par le sous-traitant* SIGI, 11 rue Edmond Reuter, L-5326 Contern;Hébergement, maintenance de la solution et maintien des systèmes Indigo Neo, RDC Bâtiment C, (Buzz City), 21, rue Jean Fischbach, L-3372 LEUDELANGE;Consultation du statut et des informations des ticket de parking payant Excellium Services S.A., 5 Rue Goell, L-5326 Contern;Vulnerability scan, Pentest audit intene, sécurité réseaux informatique POST Luxembourg, 38 place de la Gare, L-1616 Luxembourg;Infrastructure Cloud (IaaS) redondante et réseau de communication dédié (MPLS) INOWAI,52 route d'Esch, L-1470 Luxembourg;Mise à disposition de bureaux et sécurité environnementale des installations Brinks Security Luxembourg S.A., 8 rue de Bitbourg, L-1273 Hamm;Sécurité Physique des locaux du SIGI

2. Sanctions Administratives

Date de création	04/08/2023
Date mise en œuvre	21/01/2025
Date mise à jour	10/01/2025
Etat	Actif
Responsable du Traitement	Administrations Communales
Coordonnées responsable du traitement	Administrations Communales membres du syndicat
Coordonnées DPO	DPO des Administrations Communales
Nom responsable conjoint traitement	NA
Produit, logiciel, application concerné	Infractions
Code Acronyme	SAC
Service CDC Département	Aménagement du territoire & NOS
Description	Permettre l'enregistrement, la gestion, l'impression et le transfert des constats d'infractions passibles de sanctions administratives (SAC) par les agents municipaux, conformément à la réglementation en vigueur.
Finalités, objectifs du traitement	Enregistrer, gérer, imprimer et transférer les constats d'infractions passibles de sanctions administratives (SAC), en application de la loi et des règlements municipaux.
Base légale, juridique du traitement Légitimité	• Le traitement est nécessaire à l'exécution de la mission d'intérêt public et de l'exercice de l'autorité publique de la commune (RGPD article 6.1e). • Loi du 27 juillet 2022 relative aux sanctions administratives communales et à l'élargissement des compétences des agents municipaux. • Circulaire n° 4191(1)(2), élargissement des compétences des agents municipaux • Règlement général de police de chaque commune utilisatrice, préalablement validé par le ministère • Les infractions spécifiques donnant lieu à des avertissements taxés sont définies dans les règlements communaux applicables, qui doivent être consultés pour déterminer les dispositions pertinentes et spécifique.
Catégorie de personnes concernées	• Contrevenants • Témoins éventuels • Agents municipaux habilités • Gardes champêtres • Receveur communal
Catégorie de données traitées	• Identification, signalétique • Localisation • Temporelles • Relatives aux infractions • Données des témoins relatives à l'agent constatateur
Source des données	• Personne concernée • Agent municipal • Registre des adresses (SIGI)
Catégories de destinataires des données	• Services municipaux pour gestion et recouvrement • Plateforme SIGI pour traitement des constats • Autorités judiciaires et administratives

Transfert hors UE	non
Transfert organisation	• Administration Communale concernée • Syndicat Intercommunal de Gestion Informatique (SIGI) • Autorités judiciaires
DPIA	non
Justification DPIA	NA
Mesures de sécurité (Protection des données)	Les mesures de sécurité sont mises en oeuvre conformément à la politique de sécurité des systèmes d'information (SGSI) du SIGI (réf. POL_00-00_PolSec) • Authentification forte • Chiffrement des données • Accès restreint aux agents habilités • Verrouillage de l'application mobile via Face ID ou empreinte digitale • Traçabilité des actions (audit et logs), journal des logs d'activités réalisées sur les données au sein des applications. • Chaque application accessible aux communes est accédée au travers d'une connexion sécurisée par des protocoles et mécanismes d'échanges tels que TLS et MPLS. • Les accès aux bâtiments sont régulés par un système d'identification par badge. • Le Virtual Private Cloud est protégé contre les risques environnementaux (système anti-feu sur les sites, redondance des sites) • La politique du bureau propre et écran vide est appliquée. • Les performances des serveurs sont contrôlées en temps réel. • Aucune activité de développement n'est techniquement possible sur l'environnement de production. • Les environnements de développement, de test et de production sont cloisonnés. • Les bases de données font l'objet d'un backup dont la fréquence est fixée par les besoins spécifiques du métier. • Un journal des évènements est maintenu sur chaque serveur. • Chaque environnement bénéficie de son propre réseau qui est sécurisé et cloisonné. • L'ensemble des systèmes est redondant et des tests de continuité sont réalisés annuellement.
Mesures techniques et organisationnelles	Les mesures de sécurité sont mises en oeuvre conformément à la politique de sécurité des systèmes d'information (SGSI) du SIGI (réf. POL_00-00_PolSec) • Le SIGI entretient des relations régulières avec les autorités/spécialistes. • Le SIGI s'est doté d'une politique de gestion de la sécurité de l'information (ISO 27001). • Les procédures de test de restauration de base de données sont exécutées annuellement. • Le déploiement de solutions logicielles en production est réalisé uniquement par des administrateurs désignés spécifiquement pour cette tâche. • Des procédures de rollback sont prévues en cas de problèmes liés au déploiement. • Les développements des solutions logicielles sont réalisés sur des environnements de développement sécurisés. • Les contrats avec les fournisseurs reprennent l'ensemble des exigences de sécurité prescrites par le SIGI. • Des SLA (Service Level Agreement) sont convenus avec les fournisseurs et sont revus à échéance fixe. Les échéances de ces révisions sont fixées contractuellement avec chaque fournisseur. • Des mesures de contrôle d'accès aux informations sont prescrites par le SIGI et appliquées lors de l'octroi de chaque accès.

	• Chaque évènement significatif relatif à la gestion des identités est maintenu dans un registre. • Une procédure spécifique gère l'accueil et le départ de chaque collaborateur au sein de la structure du SIGI. • Chaque collaborateur ainsi que les entreprises sous-traitantes signent une charte de confidentialité. • L'ensemble des collaborateurs sont sensibilisés à la gestion de la sécurité de l'information ainsi qu'au GDPR. • La gestion du changement est contrôlée par une procédure et validée par les responsables métiers. • Toute procédure fait l'objet d'une documentation mise à la disponibilité des collaborateurs concernés. • Des échanges réguliers avec l'autorité de contrôle (CNPD) ainsi qu'avec des spécialistes juridiques et techniques sont organisés régulièrement sur les thématiques liées à la gestion de la sécurité des informations. • La mise à jour des anti-virus est pilotée par la politique de sécurité prescrite par le SIGI. • Les codes sources ne sont pas disponibles dans l'environnement d'exploitation La gestion des codes sources est encadrée par des procédures spécifiques. • Conformément à la loi luxembourgeoise, les données sont conservées au Luxembourg. La conformité à la loi luxembourgeoise est assurée par le secrétaire du SIGI.
Données à Caractère Personnel (DCP)	*NomDCP;Catégorie;Donnée sensible;Personne concernée* NomAgent;Identification;non;Agent PrénomAgent;Identification;non;Agent CodeAgent;Identification;non;Agent FonctionAgent;Identification;non;Agent NomTémoin;Identification;non;Citoyen PrénomTémoin;Identification;non;Citoyen AdresseTémoin;Identification;non;Citoyen NomContrevenant;Identification;non;Citoyen PrénomContrevenant;Identification;non;Citoyen DateNaissanceContrevenant;Identification;non;Citoyen LieuNaissanceContrevenant;Identification;non;Citoyen NationalitéContrevenant;Identification;non;Citoyen AdresseContrevenant;Identification;non;Citoyen
Durée, rétention des données Période de conservation Durée d'utilité Administrative (DUA)	• Sanctions actives jusqu'au recouvrement complet de l'amende ou résolution de l'infraction. • En cours de discussion avec le ministère pour la définition des règles d'anonymisation des données en cas de paiement / non paiement du constat
DCP - Infos complémentaires	NA
Sous-traitants et description	*Sous-traitant;Description du service opéré par le sous-traitant* SIGI, 11 rue Edmond Reuter, L-5326 Contern;Hébergement, maintenance de la solution et maintien des systèmes Excellium Services S.A., 5 Rue Goell, L-5326 Contern;Vulnerability scan, Pentest audit intene, sécurité réseaux informatique POST Luxembourg, 38 place de la Gare, L-1616 Luxembourg;Infrastructure Cloud (IaaS) redondante et réseau de communication dédié (MPLS) INOWAI,52 route d'Esch, L-1470 Luxembourg;Mise à disposition de bureaux et sécurité environnementale des installations Brinks Security Luxembourg S.A., 8 rue de Bitbourg, L-1273 Hamm;Sécurité Physique des locaux du SIGI

Extrait du Registre des activités de traitement - Produit Infractions

Final Audit Report 2025-01-26

Created:	2025-01-20
By:	Didier Marcelis (didier.marcelis@pt.lu)
Status:	Signed
Transaction ID:	CBJCHBCAABAA2--0cjae7qcxAa3AfCV8iUZA8wDQbHFB

"Extrait du Registre des activités de traitement - Produit Infractions" History

Document created by Didier Marcelis (didier.marcelis@pt.lu)
2025-01-20 - 9:47:31 AM GMT

Document emailed to Didier Marcelis (didier.marcelis@sigi.lu) for signature
2025-01-20 - 9:47:36 AM GMT

Document emailed to Philippe Meyers (philippe.meyers@sigi.lu) for signature
2025-01-20 - 9:47:37 AM GMT

Document emailed to Sylvain Momin (sylvain.momin@sigi.lu) for signature
2025-01-20 - 9:47:37 AM GMT

Email viewed by Didier Marcelis (didier.marcelis@sigi.lu)
2025-01-20 - 1:16:54 PM GMT

Document e-signed by Didier Marcelis (didier.marcelis@sigi.lu)
Signature Date: 2025-01-20 - 1:18:27 PM GMT - Time Source: server

Email viewed by Sylvain Momin (sylvain.momin@sigi.lu)
2025-01-21 - 9:19:50 AM GMT

Document e-signed by Sylvain Momin (sylvain.momin@sigi.lu)
Signature Date: 2025-01-21 - 9:30:06 AM GMT - Time Source: server

Email viewed by Philippe Meyers (philippe.meyers@sigi.lu)
2025-01-26 - 11:17:51 AM GMT

Document e-signed by Philippe Meyers (philippe.meyers@sigi.lu)
Signature Date: 2025-01-26 - 11:18:23 AM GMT - Time Source: server

Agreement completed.

2025-01-26 - 11:18:23 AM GMT