La loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)

INTRODUCTION

Rappel historique :

- Avant 2001
- 1ère étape : l'accès aux documents officiels en mains de l'Etat
- 2ème étape en 2008 : ajout du volet protection des données personnelles.
- 2023-2024: révision du volet protection des données: PL 13347

CHAMP D'APPLICATION DE LA LOI

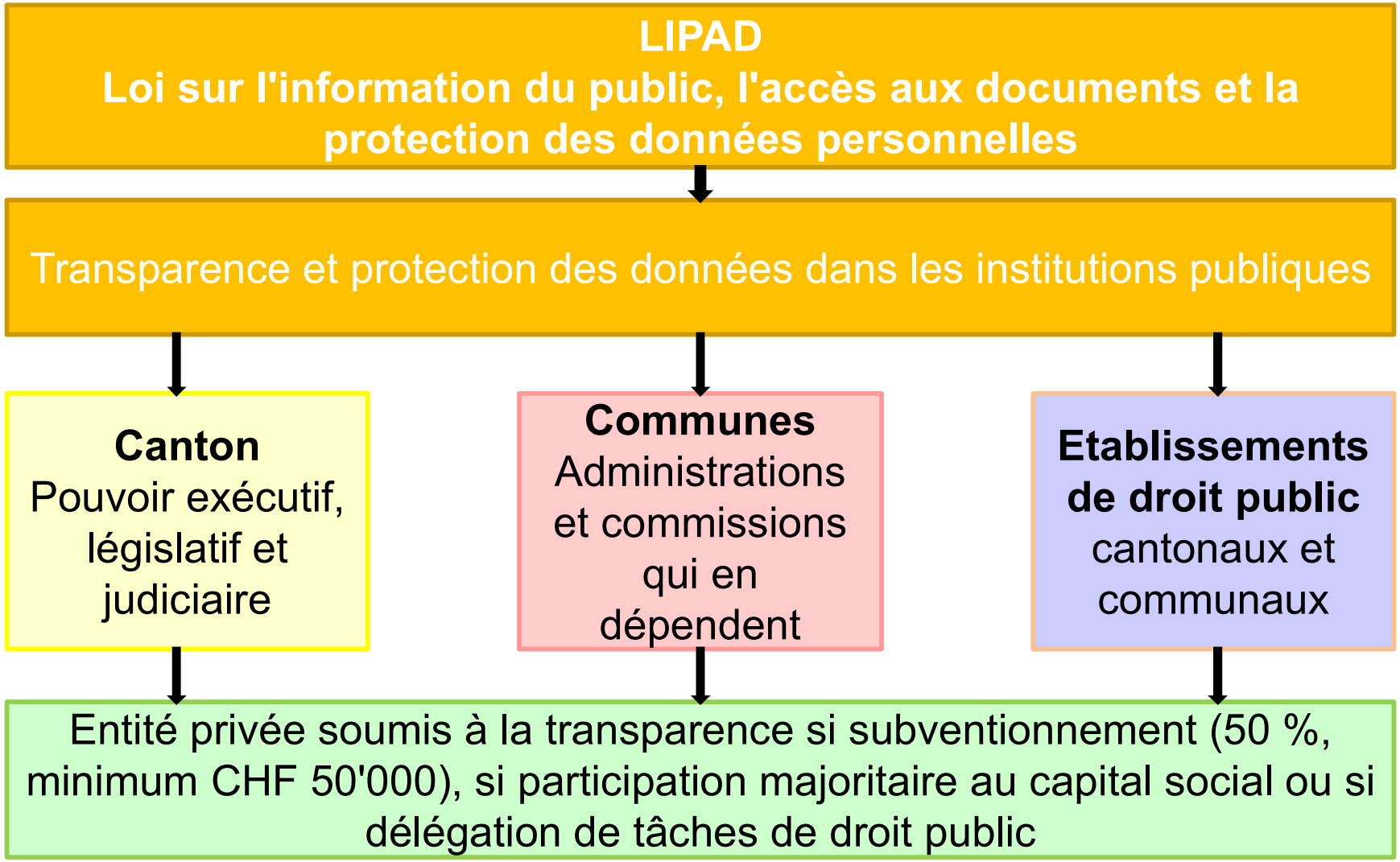
2 volets :

- Transparence
- Protection des données

Les deux volets s'appliquent aux institutions cantonales et communales.

Seul le volet transparence s'applique aux institutions de droit privé subventionnées.

LA LIPAD


LIPAD
Loi sur l'information du public, l'accès aux documents et la protection des données personnelles
Transparence et protection des données dans les institutions publiques
Canton
Pouvoir exécutif, législatif et judiciaire
Communes
Administrations et commissions qui en dépendent
Etablissements de droit public
cantonaux et communaux
Entité privée soumis à la transparence si subventionnement (50 %, minimum CHF 50'000), si participation majoritaire au capital social ou si délégation de tâches de droit public

LIPAD

Loi sur l'information du public, l'accès aux documents et la protection des données personnelles

1ère étape:
qualifier le domaine auquel la demande faite à l'institution doit être rattachée

•Transparence ?

•Accès à un document existant dans l'institution

Priorité à l'information

Sauf si contraire au droit fédéral, à une base légale genevoise formelle ou si un intérêt public ou privé prépondérant s'y oppose
En cas de désaccord, le Préposé cantonal propose une **médiation**

Protection des données ?

Renseignement(s) comportant des données personnelles

Priorité à la protection

Pas d'information - Consentement préalable nécessaire – si engendre un travail disproportionné – le **préavis** du Préposé cantonal est requis

Transparence

- Le principe: l'accès

- Les exceptions: un intérêt public ou privé prépondérant (sécurité publique, protection des données personnelles, procédure judiciaire…)

- La procédure à suivre: peu formelle, pas besoin de faire valoir un intérêt digne de protection, demande auprès de l'institution publique qui détient le document

Quelques exemples en pratique

- Directives du Ministère public
- Grand livre de comptes d'une commune
- Rapport d'audit d'un service
- Budget relatif aux indicateurs de la police

PROTECTION DES DONNEES

La protection des données, un droit constitutionnel.

Toute personne a droit (art. 13 Cst) :

- au respect de sa vie privée et familiale;
- au respect de son domicile;
- au respect de sa correspondance;
- à la protection contre l'emploi abusif des données qui la concernent.

Principes fondamentaux

- Le traitement de données personnelles par une institution publique doit être prévu par une loi ou un règlement (principe de licéité – art. 35 al. 1 LIPAD) et/ou
- les données traitées doivent être pertinentes et nécessaires (principe de proportionnalité – art. 36 LIPAD); et
- exactes et mises à jour (principe d'exactitude – art. 36 LIPAD);
- collectées de manière reconnaissable (principe de transparence de la collecte) et loyale (principe de la bonne foi – art. 38 LIPAD);
- sécurisées (principes de sécurité – art. 37 LIPAD) : protégées contre tout traitement illicite, intactes, disponibles, tenues confidentielles;
- Détruites ou rendues anonymes, si nécessaire.

Les exigences de la loi s'appliquent à tout traitement de données personnelles :

- Quels que soit la forme (orale ou écrite) et le support (papier ou informatique);
- Collecte ciblée des seules informations nécessaires;
- Le traitement des données sensibles requiert une base légale formelle et doit être absolument indispensable à l'accomplissement des tâches légales;
- Les données personnelles sensibles sont tenues confidentielles.

La vidéosurveillance

Art. 42 Vidéosurveillance

[1] Dans la mesure où elles ne sont pas dictées par l'accomplissement légal de tâches au sens de l'article 35, la création et l'exploitation d'un système de vidéosurveillance ne sont licites que si, **cumulativement** :

a) la vidéosurveillance est propre et nécessaire à garantir la **sécurité des personnes et des biens** se trouvant dans ou à proximité immédiate de lieux publics ou affectés à l'activité d'institutions publiques, en prévenant la commission d'agressions ou de déprédations et en contribuant à l'établissement des infractions commises le cas échéant;

b) l'existence d'un système de vidéosurveillance est **signalée** de manière adéquate au public et au personnel des institutions;

c) le champ de la surveillance est **limité au périmètre nécessaire** à l'accomplissement de celle-ci;

d) dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel des institutions publiques n'entrent pas dans le champ de vision des caméras ou, à défaut, sont rendus d'emblée non identifiables par un procédé technique approprié.

La vidéosurveillance

[2] L'éventuel enregistrement de données résultant de la surveillance doit être détruit en principe dans un délai de 7 jours. Ce délai peut être porté à 3 mois en cas d'atteinte avérée aux personnes ou aux biens et, en cas d'ouverture d'une information pénale, jusqu'à l'issue de la procédure.

[3] Les responsables des institutions prennent les mesures organisationnelles et techniques appropriées afin de :

- a) limiter le visionnement des données, enregistrées ou non, à un cercle restreint de personnes dûment autorisées, dont la liste doit être régulièrement tenue à jour et communiquée au préposé cantonal;
- b) garantir la sécurité des installations de surveillance et des données éventuellement enregistrées.

La vidéosurveillance

[4] En dérogation à l'article 39, la communication à des tiers de données obtenues au moyen d'un système de vidéosurveillance ne peut avoir lieu que s'il s'agit de renseigner :

a) les instances hiérarchiques supérieures dont l'institution dépend;

b) les autorités judiciaires, soit aux conditions de l'article 39, alinéa 3, soit aux fins de dénoncer une infraction pénale dont la vidéosurveillance aurait révélé la commission.

La vidéosurveillance – art. 16 RIPAD

L'art. 16 du Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD) complète l'art. 42 LIPAD.

Directive quant au processus de traitement d’un dossier de vidéosurveillance par une commune

1. La commune constitue un dossier justifiant l'installation d'un système de vidéosurveillance.

2. Le dossier doit comprendre les documents suivants :

a) un descriptif des lieux d’installation et du matériel utilisé, y compris l'existence et la portée d'un éventuel système de cryptage ou de floutage des données ;

b) un plan précis définissant l’emplacement de chaque caméra avec son champ de prise de vue et sa portée (dimensions) ;

c) les avis préalables des entités propriétaires et exploitantes des bâtiments se trouvant dans le champ des caméras (ex : préavis du département de l'instruction publique dans le cadre des écoles primaires) ;

d) les horaires d’utilisation et la durée de conservation des bandes

e) les autres mesures prises pour assurer la sécurité des lieux ;

f) les motifs justifiant, pour la commune, l'installation d'un système de vidéosurveillance (ex : les infractions déjà commises dans un secteur) ;

g) la liste des personnes (et leur fonction) habilitées à visionner les données et les modalités de visualisation

3. L'exécutif de la commune prépare un projet de délibération ouvrant un crédit d'investissement, en vue de son approbation par le conseil municipal.

4. Le conseil municipal vote le projet de délibération.

5. La délibération ouvrant le crédit d'investissement est transmise au SAFCO avec le dossier.

6. Le SAFCO établit un projet d’arrêté du Conseil d’Etat ou de décision départementale approuvant la délibération.

Voir les articles: 42 LIPAD, 16 RIPAD, 30,48, 82 et 88 LAC, et 19 et 30 RAC.

Nouvelle LIPAD et vidéosurveillance

- Art. 42 n'est pas modifié

- Exigence d'analyse d'impact en cas de traitement de données personnelles susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 37B al. 1 nLIPAD)

- Un tel risque existe en cas de surveillance de grandes parties du domaine public (art. 37B al. 2 litt. c nLIPAD)

Dispositions spécifiques relatives à la vidéosurveillance - exemples

- Police (Loi sur la police, Règlement sur l'organisation de la police)

- Domaine pénitentiaire (Loi sur l’organisation des établissements et le statut du personnel pénitentiaires et son règlement d'application; loi sur le convoyage et la surveillance des détenus hors établissements pénitentiaires)

- Déchetterie?

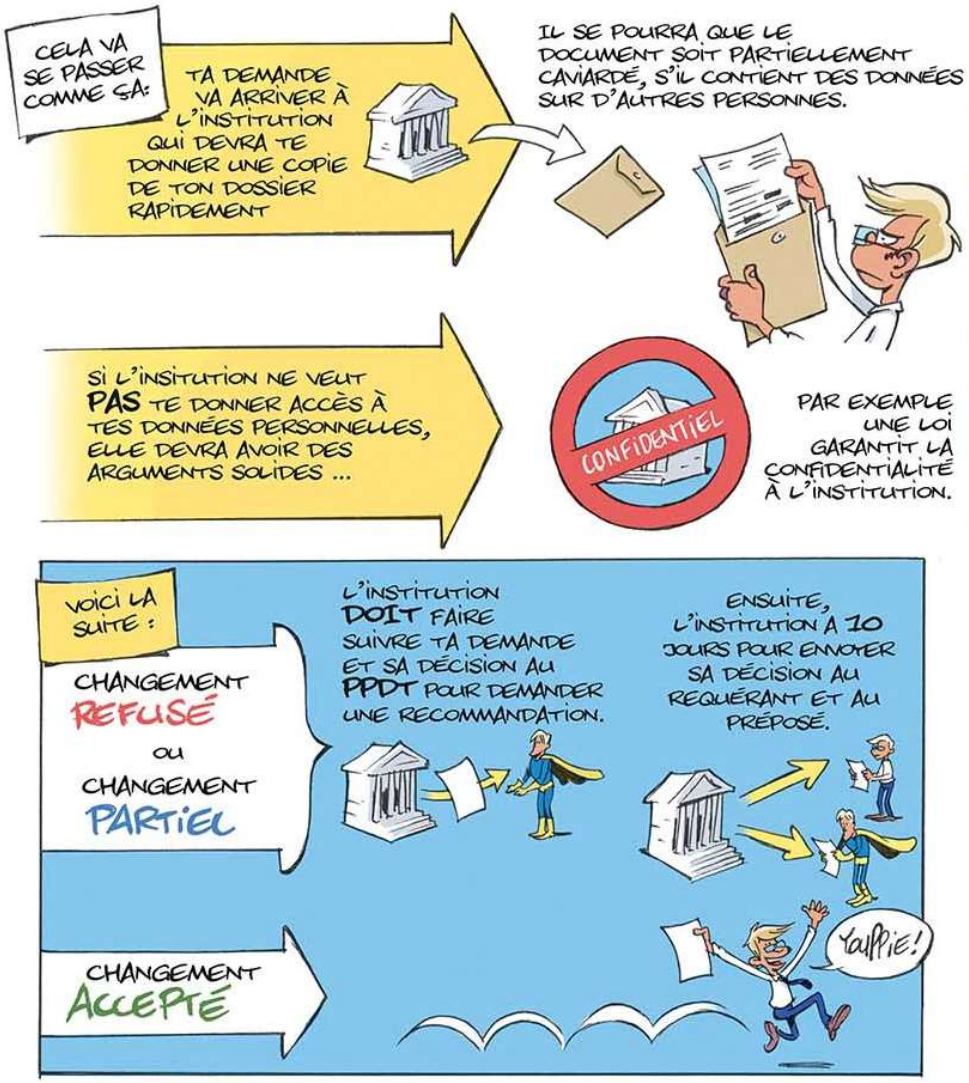
L'accès à ses données personnelles propres, 1ère étape

- Demande écrite au responsable LIPAD;
- Justifier de son identité;
- Quel(s) fichier(s) et quelles données sur moi ?
- Restrictions ? Voir art. 46 LIPAD;
- Réponse écrite et gratuite (sauf si cela implique un travail disproportionné);
- Un accès partiel est préférable à un refus.

L'accès à ses données personnelles propres, 2ème étape

- Actions concrètes possibles : détruire – rectifier – compléter – mettre à jour, à défaut, porter mention, s'abstenir de communiquer, publier – communiquer la décision;
- Traitement "avec célérité";
- En cas de refus, transfert au PPDT.

→ https://www.ge.ch/document/ppdt-formulaire-demande-relative-aux-donnees-personnelles



Les responsables LIPAD

Chaque institution publique désigne un responsable LIPAD (son nom est indiqué dans le catalogue des fichiers).

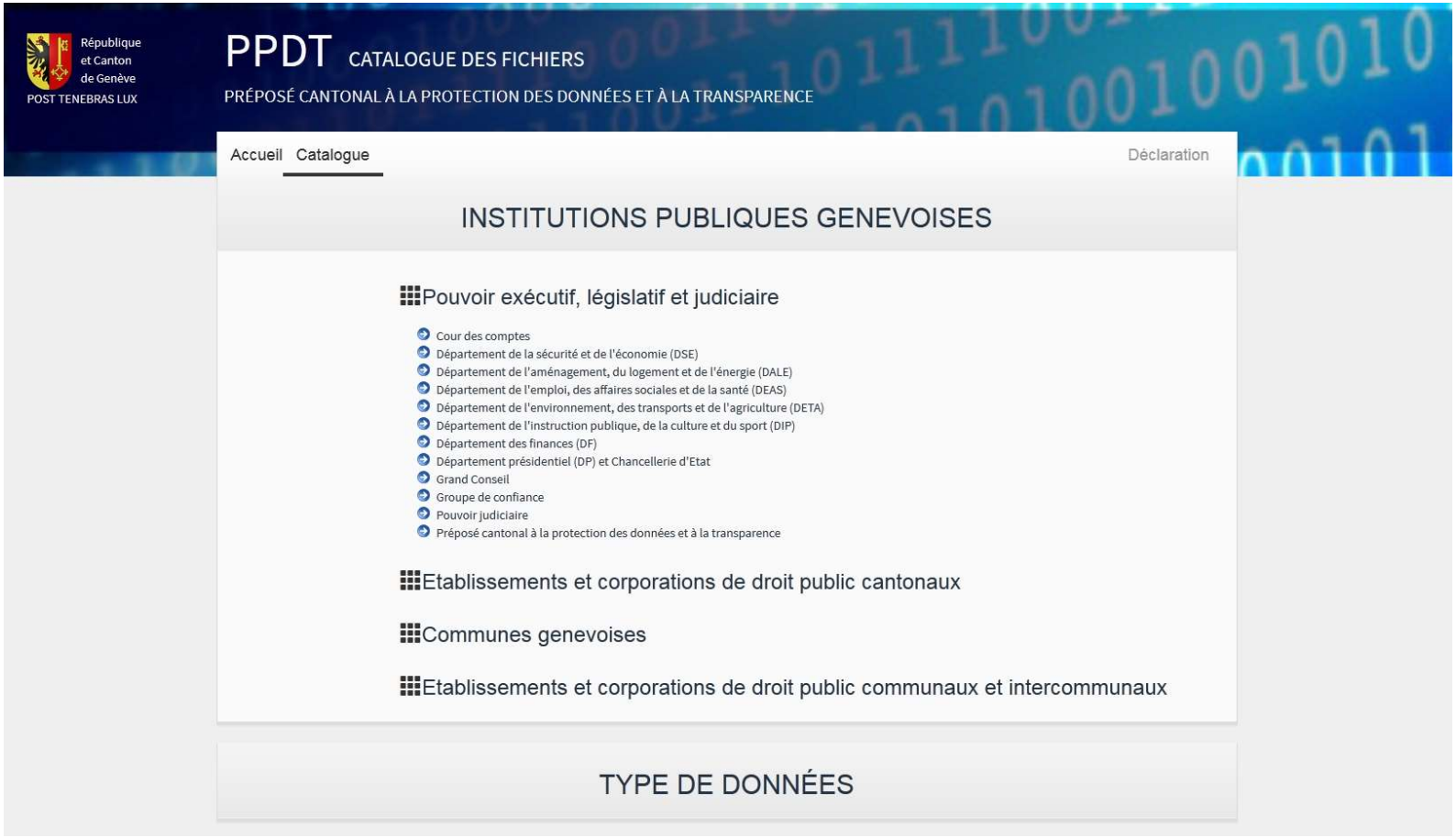
Relais du Préposé cantonal sur le terrain: C'est en priorité au responsable LIPAD que les membres des institutions publiques doivent s’adresser pour toute question relative à l’application de la LIPAD.

Le Préposé cantonal, rôle et missions

Le Préposé cantonal a pour mission de surveiller la bonne application de la LIPAD. Cette dernière lui confie notamment les tâches suivantes:

- Donner des conseils aux institutions publiques et aux particuliers.
- Rendre les avis, préavis et recommandations prévus par la loi.
- Tenir le catalogue des fichiers de données personnelles (CATFICH).

CATFICH


République
et Canton
de Genève
POST TENEBRAS LUX
PPDT CATALOGUE DES FICHIERS
PRÉPOSÉ CANTONAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE
Accueil
Catalogue
Déclaration
INSTITUTIONS PUBLIQUES GENEVOISES
Pouvoir exécutif, législatif et judiciaire
Cour des comptes
Département de la sécurité et de l'économie (DSE)
Département de l'aménagement, du logement et de l'énergie (DALE)
Département de l'emploi, des affaires sociales et de la santé (DEAS)
Département de l'environnement, des transports et de l'agriculture (DETA)
Département de l'instruction publique, de la culture et du sport (DIP)
Département des finances (DF)
Département présidentiel (DP) et Chancellerie d'Etat
Grand Conseil
Groupe de confiance
Pouvoir judiciaire
Préposé cantonal à la protection des données et à la transparence
Etablissements et corporations de droit public cantonaux
Communes genevoises
Etablissements et corporations de droit public communaux et intercommunaux
TYPE DE DONNÉES

"Contrôles Schengen"

"Le SIS est un système électronique européen de données de recherches portant sur des personnes et des objets qui est géré conjointement par les États Schengen. Il contient des informations sur des personnes portées disparues, recherchées par la police et la justice ou frappées d'une interdiction d'entrée, ainsi que sur des objets volés (p. ex. voitures, armes). Il constitue la clef de voûte de la coopération policière et judiciaire dans l'espace Schengen. En tant que pays associé à l'espace Schengen, la Suisse a également accès au SIS" (PFPDT, feuille d'information "SCHENGEN" ET VOS DONNÉES PERSONNELLES, février 2024).

"Contrôles Schengen"

En Suisse, le contrôle de l'utilisation du SIS par les organes fédéraux relève de la compétence du PFPDT.

L'utilisation du SIS par les cantons et les communes (p. ex. police cantonale / municipale) est surveillée par les autorités cantonales chargées de la protection des données. A Genève, le Préposé cantonal peut procéder à des "contrôles Schengen".

Merci de votre attention

Boulevard Helvétique 27
1207 Genève

Tél. 022/546.52.40
ppdt@ge.ch
https://www.ge.ch/organisation/protection-donnees-transparence