Informations du PIA

Nom du PIA
(IMPORT) Atelier fiscal

Nom de l'auteur
Marc DEBOMY

Nom de l'évaluateur
Fédéric PLANTE

Nom du validateur
DPO - Sebastion SAVATER

Date de création
02/02/2018

Contexte

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?
Le traitement concerne les traitements automatisés mis en oeuvre par les collectivités locales qui permettent d'exploiter les rôles d'impôts directs locaux, le cadastre et la vacance des locaux.

Quelles sont les responsabilités liées au traitement ?

Les responsabilités liées au traitement sont partagées entre Fiscalité & Territoire et la collectivité.

Fiscalité & Territoire

- Traite les données seulement sur instruction de la collectivité;
- Veille à ce que les personnes qui traitent les données soient engagées à une obligation de confidentialité;
- Met en oeuvre des mesures de sécurité;
- Respecte les mêmes obligations que celle la collectivité pour le recrutement d'un autre sous-traitant;
- Aide la collectivité à mettre en oeuvre les droits des personnes;
- Aide la collectivité à garantir la sécurité et à la réalisation d'analyses d'impact relatives à la protection des données (AIPD);
- Supprime les données traitées à la fin du contrat;
- Met à disposition de la collectivité les moyens nécessaires afin de réaliser des audits;
- Met à disposition son Privacy Impact Assessment (PIA).

Quels sont les référentiels applicables ?

Les CD-ROM contenant les données issues du cadastre ne doivent plus être déclarés à la CNIL lors de leur première acquisition (dispense 16).
Les CD-ROM contenant les données issues des rôles des impôts locaux d'une collectivité locale doivent être déclarés à la CNIL lors de leur première acquisition (norme simplifiée 45). Leur mise à jour annuelle, délivrée par la DGFiP, n'est soumise à aucune formalité. Le récépissé délivré reste valable tant que l'utilisation des données est inchangée. De la même manière, le fait que les CD-Rom "Vis-DGI" aient été rebaptisés "Visu-DGFiP" est sans incidence sur leur contenu. Cette modification ne doit donc pas non plus être notifiée à la CNIL.

Les collectivités qui ont déjà déclaré l'utilisation des CD-Rom transmis par les services fiscaux (cadastre ou rôles des impôts) n'ont pas à établir de nouvelle formalité. **Les mises à jour peuvent être obtenues en fournissant le récépissé de la déclaration initiale.**

Dans un souci d'actualisation, la CNIL invite toutefois les collectivités à prendre connaissance de la délibération n°2012-088 qui abroge la norme simplifiée 44 (cadastre) et créé la dispense 16.
Les collectivités qui reçoivent pour la première fois ces CD-Rom, ou qui n'ont pas déclaré les versions précédentes, doivent effectuer les formalités suivantes auprès de la CNIL :

- Prendre connaissance de la dispense de déclaration n°16 (délibération n°2012-088) pour consulter le cadastre, extraire des relevés de propriétés en application du Livre des procédures fiscales ou diffuser sur Internet une "base géographique de référence" au sens des articles L.127-10, R.127-10 et suivants du Code de l'environnement.
- Réaliser un engagement de conformité à la norme simplifiée n° 45 (rôles des impôts locaux, taxes foncières, taxe d'habitation et taxe professionnelle).
- Si l'utilisation des données ne respecte pas le cadre fixé par ces textes : réaliser une déclaration normale.
- Un engagement de conformité à l'autorisation unique n° 1 (AU-001) pour exploiter, notamment dans un système d'information géographique (SIG), des fichiers bruts du cadastre ("données MAJIC") en relation avec d'autres types de données issues d'autres traitements à finalités différentes.
- Si l'utilisation des données ne respecte pas le cadre fixé par ces textes : demander une autorisation auprès de la CNIL.

Ces déclarations se font par téléprocédure sur le site de la CNIL. Le récépissé délivré devant être communiqué aux services fiscaux pour l'obtention des mises à jour annuelles, il doit être conservé par la collectivité. S'il a été égaré, il convient de demander un duplicata auprès des services de la CNIL.

Évaluation : En attente

Données, processus et supports

Quelles sont les données traitées ?

L'ensemble des fichiers transmis par la DGI au travers du portail de la gestion publiques.

- Le cadastre
- La taxes foncières
- La liste 41 hab, cbd
- La taxe d'habitation
- La CFE/IFER
- La TASCOM
- La CVAE
- La TH format 3
- La 1767 biscom
- La RLCFE

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

1. Téléchargement des données de la part du responsable du traitement au sein de la collectivité au travers d'un import sécurisé sur serveur.
2. Import automatique des données dans l'Atelier Serveur localisé en France
3. Exploitation des données au travers de l'Atelier fiscal
4. Elles sont conservées 2 ans puis effacées.
5. Aucun enrichissement, ni mise à jour des données transmises par l'administration ne peut être effectué.

Quels sont les supports des données ?

Les collectivités recoivent les données de la DGFIP au travers d'un portail sous la forme de fichiers textes ou CSV.

Nous les transformons en base de données

La collectivité peut sous certaine condition :

- Imprimer une fiche d'évaluation d'un local, ou une fiche d'imposition
- Exporté les données au format CSV

Principes fondamentaux

Proportionnalité et nécessité

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Ces traitements ont notamment pour objet de :

- Répondre aux demandes de renseignements des contribuables sur leur situation fiscale personnelle ;
- Vérifier ponctuellement que les électeurs dont la carte électorale a été retournée en mairie et leur conjoint ne sont pas inscrits au rôle de l'une des contributions directes communales ;
- Analyser la répartition et l'évolution de l'assiette des impôts locaux (ex. : valeur locative cadastrale, causes d'abattement) et des ressources qui en résultent, à partir de données statistiques non nominatives établies au niveau de la commune ou d'un quartier, à l'exclusion de toute analyse au niveau de la rue ou de l'adresse précise ;
- Réaliser des études de même nature en matière de taxe professionnelle sur un échantillon de contribuables représentatif ou correspondant à une part significative de l'assiette de cette imposition ;
- Réaliser des études et simulations globales sur les conséquences d'une modification des taux d'imposition ou de la politique d'abattement ;
- Analyser la situation économique des entreprises, par secteur ou zone d'activité.

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Délibération n°2004-083 du 04/11/2004 portant adoption d'une norme simplifiée concernant certains traitements automatisés mis en oeuvre par les communes et les établissements publics de coopération intercommunale à partir des rôles des impôts directs locaux.

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

Les données collectées permettent de répondre aux demandes des contribuables, à savoir :

- expliquer l'évaluer de leur bien,
- expliquer les taxations qui en déroule
- et l'évolution de celles-ci

Les données sont-elles exactes et tenues à jour ?

Les données sont conformes à celles transmises par les services fiscaux et mis à jour une foie par an par la DGFIP

Quelle est la durée de conservation des données ?

La conservation des données est de 2 ans.

La suppression des données est de la responsabilité de la collectivité et de Fiscalité & Territoire à la fin du contrat.

Mesures protectrices des droits

Comment les personnes concernées sont-elles informées à propos du traitement ?

Les personnes concernées sont informées par la collectivité :

- par un communiqué publié dans la presse locale ou le bulletin municipal ;
- par le site internet de la commune ou de l'EPCI

des finalités du traitement, des destinataires des données, ainsi que des modalités d'exercice des droits d'accès et de rectification aux données les concernant.

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Le droit d'opposition ne s'applique pas aux traitements régis par la présente norme.

Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

Le droit d'opposition ne s'applique pas aux traitements régis par la présente norme

Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

Le droit d'opposition ne s'applique pas aux traitements régis par la présente norme

Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

Le droit d'opposition ne s'applique pas aux traitements régis par la présente norme

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Nous faisons appel uniquement à des sous-traitants présentant des garanties suffisantes (notamment en termes de connaissances spécialisées, de fiabilité et de ressources).

Nous exigeons la communication par le prestataire de sa politique de sécurité des systèmes d'information.

Nous nous **assurons l'effectivité des garanties offertes par le sous-traitant** en matière de protection des données. Ces garanties incluent notamment :

- le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées si cela n'est pas nécessaire à l'exécution de son contrat ;
- le chiffrement des transmissions de données en HTTPS
- des garanties en matière de protection du réseau, de traçabilité (logs), de gestion des habilitations, d'authentification, etc.

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Les données ne quitent jamais l'Union européenne.

Risques

Mesures existantes ou prévues

Protéger le réseau informatique

Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place.

- **Limiter les accès Internet** en bloquant les services non nécessaires
- **Gérer les réseaux Wi-Fi.** Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne.
- **S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet.** La télémaintenance doit s'effectuer à travers un VPN.
- **Limiter les flux réseau au strict nécessaire** en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.).

Défendre l'espace de travail

Chaque poste de travail, ordinateur portable ou smartphone fournit une porte d'entrée potentielle aux attaques malveillantes.

Pour les postes fixes

- Verrouillage automatiquement de la session en cas de non-utilisation du poste pendant un temps donné.
- Mises à jour de sécurité dès que cela est possible pour:
    - le système d'exploitation
    - les applications.

- Stockage des données sur un espace de stockage sauvegardé en temps réel dès que le réseau est disponible
- Limitation de la connexion de supports mobiles (clés USB, disques durs externes, etc.) à l'indispensable.
- Désactivation de l'exécution automatique (*« autorun »*) depuis des supports amovibles.
- Aucune assistance à distance des postes de travail
- Utilisation d'un coffre fort numérique pour :
    - les mots de passe
    - les notes sensibles

Anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile.

Pour les ordinateurs portable

- Mise en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation des postes nomades, pour se prémunir contre la disparition des données stockées.
- Chiffrement des postes nomades

Pour les smartphone

- Verrouillage automatique du terminal
- Mot de passe

Sauvegarder et prévoir la continuité d'activité

Des copies de sauvegarde sont réalisées et testées régulièrement.

Un plan de continuité et de reprise d'activité anticipant les éventuels incidents est préparé.

S'agissant de la sauvegarde des données

- **Effectuer des sauvegardes fréquentes des données** avec des sauvegardes incrémentales quotidiennes et des sauvegardes complètes à intervalles réguliers.
- **Stocker les sauvegardes sur un site extérieur**

S'agissant de la reprise et de la continuité d'activité

- **Rédiger un plan de reprise et de continuité d'activité informatique** même sommaire, incluant la liste des intervenants.
- **S'assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d'incident.**
- **Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.**

Encadrer la maintenance et la destruction des données

Les opérations de maintenance sont encadrées pour maitriser l'accès aux données par les prestataires.

- Enregistrer les interventions de maintenance dans une main courante.
- Insérer une clause de sécurité dans les contrats de maintenance effectuée par des prestataires.
- Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin du contrat de location.

Gérer la sous-traitance

Nous faisons appel uniquement à des sous-traitants présentant des garanties suffisantes (notamment en termes de connaissances spécialisées, de fiabilité et de ressources). Nous exigeons la communication par le prestataire de sa politique de sécurité des systèmes d'information.

Nous nous **assurons l'effectivité des garanties offertes par le sous-traitant** en matière de protection des données. Ces garanties incluent notamment :

- le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées si cela n'est pas nécessaire à l'exécution de son contrat ;

- le chiffrement des transmissions de données (ex : connexion de type HTTPS, VPN, etc.) ;
- des garanties en matière de protection du réseau, de traçabilité (journaux, audits), de gestion des habilitations, d'authentification, etc.

Nous contactualisons sur les points suivant :

- leur obligation en matière de **confidentialité des données personnelles** confiées ;
- des **contraintes minimales en matière d'authentification** des utilisateurs ;
- **les conditions de restitution et/ou de destruction des données** en fin du contrat ;
- **les règles de gestion et de notification des incidents**.

Tracer les accès et gérer les incidents

Nous traçons les accès afin de pouvoir réagir en cas de violation de données

Les informations journalisées (logs) concernent notamment :

- connexion succès/échec,
- adresse IP utilisée,
- date et heure de connexion, Pays, etc.…
- actions effectués

Ces informations sont stockées pour procèder, à des fins de sécurité, à une analyse.

Authentifier les utilisateurs

Pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il est doté d'un **identifiant qui lui est propre** et doit **s'authentifier** avant toute utilisation des moyens informatiques.

Avec un identifiant unique par utilisateur

Avec un mot de passe :

- Complexe
- Stocké de façon sécurisée (sous forme de Hash)

Amélioration possible :

- une temporisation d'accès au compte après plusieurs échecs
- un verrouillage du compte après 10 échecs
- un avis sur la complexité du mot de passe

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée.

Nous sensibilisons les utilisateurs :

- Lors de la création de leur compte utilisateur, en cochant un engagement de confidentialité.
- En le rapellant dans nos sessions de formation
- En portant une mention visible et explicite sur chaque fiche ou impression

Gérer les habilitations

Limiter les accès aux seules données dont l'utilisateur a besoin.

- Gestions de l'administration
- Gestion des fonctionnalités
- Gestion des permissions
- Gestion des fichiers
- Gestion des territoires

Amélioration possible :

Réaliser une revue annuelle des habilitations afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

Sécuriser les serveurs

La sécurité des serveurs est une priorité

- Nous sommes en mesure de suivre chaque programme en cours d'exécution
- Nous sommes sûrs qu'ils sont à jour
- Nous disposons d'un système complet pour installer toutes les mises à jour et les corrections
- Nous eefctuons des sauvegardes et les vérifions régulièrements

Protéger les locaux

Renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux.

- L'accès aux locaux est contrôlé pour éviter ou ralentir un accès direct, non autorisé, que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs.
- Installer des alarmes anti-intrusion et les vérifier périodiquement.
- Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies, et les inspecter annuellement.
- Protéger les clés permettant l'accès aux locaux et les codes d'alarme.
  Distinguer les zones des bâtiments selon les risques (par exemple prévoir un contrôle d'accès dédié pour la salle informatique).
- Tenir à jour une liste des personnes ou catégories de personnes autorisées à pénétrer dans chaque zone.
- Établir les règles et moyens de contrôle d'accès des visiteurs, au minimum en faisant accompagner les visiteurs, en dehors des zones d'accueil du public par une personne appartenant à l'organisme.
- Protéger physiquement les matériels informatiques par des moyens spécifiques (système anti-incendie dédié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation, etc.).

- Conserver une trace des accès aux salles ou bureaux susceptibles d'héberger du matériel contenant des données personnelles pouvant avoir un impact négatif grave sur les personnes concernées. **Informer les utilisateurs** de la mise en place d'un tel système, après information et consultation des représentants du personnel.
- Assurer que seul le personnel dûment habilité soit admis dans les zones à accès restreint. Par exemple :
  - à l'intérieur des zones à accès réglementé, exiger le port d'un moyen d'identification visible pour toutes les personnes;
  - les visiteurs (personnel en charge de l'assistance technique, etc.) doivent avoir un accès limité. La date et l'heure de leur arrivée et départ doivent être consignées ;
  - réexaminer et mettre à jour régulièrement les permissions d'accès aux zones sécurisées et les suppri- mer si nécessaire.

Encadrer les développements informatiques

Nous intégrons la sécurité dès le début de la conception des fonctionnalités

La protection des données à caractère personnel est intégrée au développement informatique dès les phases de conception afin d'offrir une meilleure maîtrise et de limiter les erreurs, pertes, modifications non autorisée, ou mauvais usages de celles-ci dans les applications.

- par des choix d'architecture, des fonctionnalités (anonymisation à bref délai, minimisation des données), de technologies (chiffrement des communications), etc.

- en effectuant les développements informatiques et les tests dans un environnement informatique distinct de celui de la production et sur des données anonymisées.

Accès illégitime à des données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Connaître son patrimoine sur le territoire, Connaître le cout des taxes sur le territoire

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les cyberattaques, Négligence du personnel, des sous-traitants ou des utilisateurs, Malveillance du personnel, des sous-traitants ou des utilisateurs

Quelles sources de risques pourraient-elles en être à l'origine ?

Une faille système, Une session gardé ouverte par un utilisateur, Vol de données par un membre de la société, un sous-traitant, un utilisateur

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée., Authentifier les utilisateurs, Gérer les habilitations, Tracer les accès et gérer les incidents, Défendre l'espace de travail, Protéger le réseau informatique, Sécuriser les serveurs, Gérer la sous-traitance, Protéger les locaux, Encadrer les développements informatiques, Encadrer la maintenance et la destruction des données, Sauvegarder et prévoir la continuité d'activité

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée,

Caractère identifiant des donnée ayant fait l'objet de la violation :

4.Maximal : il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant (ex. : identifier quelqu'un au sein de la population française en connaissant son nom, son prénom, sa date de naissance et son adresse postale)

Caractère préjudiciable de la violation sur les personnes concernés :

1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou

pour attendre de les réaliser, simple contrariété…)

Gravité : Soit une valeur de 5 Limité

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Limitée, Limitée

Modification non désirées de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Mauvaise information aux administrés et aux élus

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les cyberattaques, Négligence du personnel, des sous-traitants ou des utilisateurs, Malveillance du personnel, des sous-traitants ou des utilisateurs

Quelles sources de risques pourraient-elles en être à l'origine ?

attaquant externe,

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée., Authentifier les utilisateurs, Gérer les habilitations, Tracer les accès et gérer les incidents, Défendre l'espace de travail, Protéger le réseau informatique, Sécuriser les serveurs, Sauvegarder et prévoir la continuité d'activité, Encadrer la maintenance et la destruction des données, Gérer la sous-traitance, Encadrer les développements informatiques, Protéger les locaux

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée,

Caractère identifiant des donnée ayant fait l'objet de la violation :

4.Maximal : il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant (ex. : identifier quelqu'un au sein de la population française en connaissant son nom, son prénom, sa date de naissance et son adresse

postale)

Caractère préjudiciable de la violation sur les personnes concernés :

1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou

pour attendre de les réaliser, simple contrariété…)

Gravité : Soit une valeur de 5 Limité

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Limitée, Limitée

Disparition de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Aucune, compte tenu que la DGFIP possède les originaux

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les cyberattaques, un crash serveur, Négligence du personnel, des sous-traitants ou des administarteurs, Malveillance du personnel, des sous-traitants ou des administateurs

Quelles sources de risques pourraient-elles en être à l'origine ?

Attaque, panne electrique

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée., Authentifier les utilisateurs, Gérer les habilitations, Tracer les accès et gérer les incidents, Défendre l'espace de travail, Protéger le réseau informatique, Sécuriser les serveurs, Sauvegarder et prévoir la continuité d'activité, Encadrer la maintenance et la destruction des données, Gérer la sous-traitance, Encadrer les développements informatiques, Protéger les locaux

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Négligeable

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Négligeable

Plan d'action

Principes fondamentaux

Aucun plan d'action enregistré.

Mesures existantes ou prévues

Aucun plan d'action enregistré.

Risques

Aucun plan d'action enregistré.