Comment se passe un contrôle en protection des données

10 novembre 2026

Comment se passe un contrôle en protection des données

Base légale - LIPAD

Selon l’art. 56 al. 3 litt. c et d LIPAD, le Préposé cantonal est chargé de conseiller les instances compétentes au sein des institutions publiques sur les mesures d'organisation et les procédures à prescrire en leur sein et d'assister les responsables désignés au sein des institutions publiques dans l'accomplissement de leurs tâches.

Dans ce cadre, il a décidé, dès 2016, d'initier des contrôles concernant la protection des données personnelles auprès des institutions publiques en lien avec des fichiers annoncés ou non au catalogue.

Comment se passe un contrôle en protection des données

But des contrôles

Le but de ces contrôles est d'examiner l'activité de l'organisation, sous l'angle des dispositions légales relatives à la protection des données personnelles (art. 35 à 43 LIPAD), plus particulièrement la collecte, le traitement, la communication, le droit d'accès, la conservation, la destruction ou l'archivage des données personnelles, ainsi que les mesures techniques et organisationnelles de sécurité.

La démarche vise essentiellement à la sensibilisation et au respect des règles relatives à la protection des données personnelles.

Le cas échéant, des propositions peuvent être formulées pour renforcer celles-ci.

Comment se passe un contrôle en protection des données

Autres contrôles

L’utilisation des bases de données de l'espace Schengen (SIS/VIS/EES) par les cantons et les communes est surveillée par les autorités cantonales chargées de la protection des données.

Dans ce cadre, il a été décidé, dès 2014, d'initier des contrôles concernant la protection des données personnelles auprès des institutions ayant un accès au SIS.

Un contrôle portant sur le VIS a été effectué cette année.

Le système EES est entré en vigueur cette année et fera l'objet d'un prochain contrôle.

Comment se passe un contrôle en protection des données

Les différentes étapes

Travaux préliminaires

- Choix de l'entité et annonce
- Séance de lancement
- Identification des risques et délimitation du contrôle
  - Plan de mission
  - Programme de travail

Contrôle

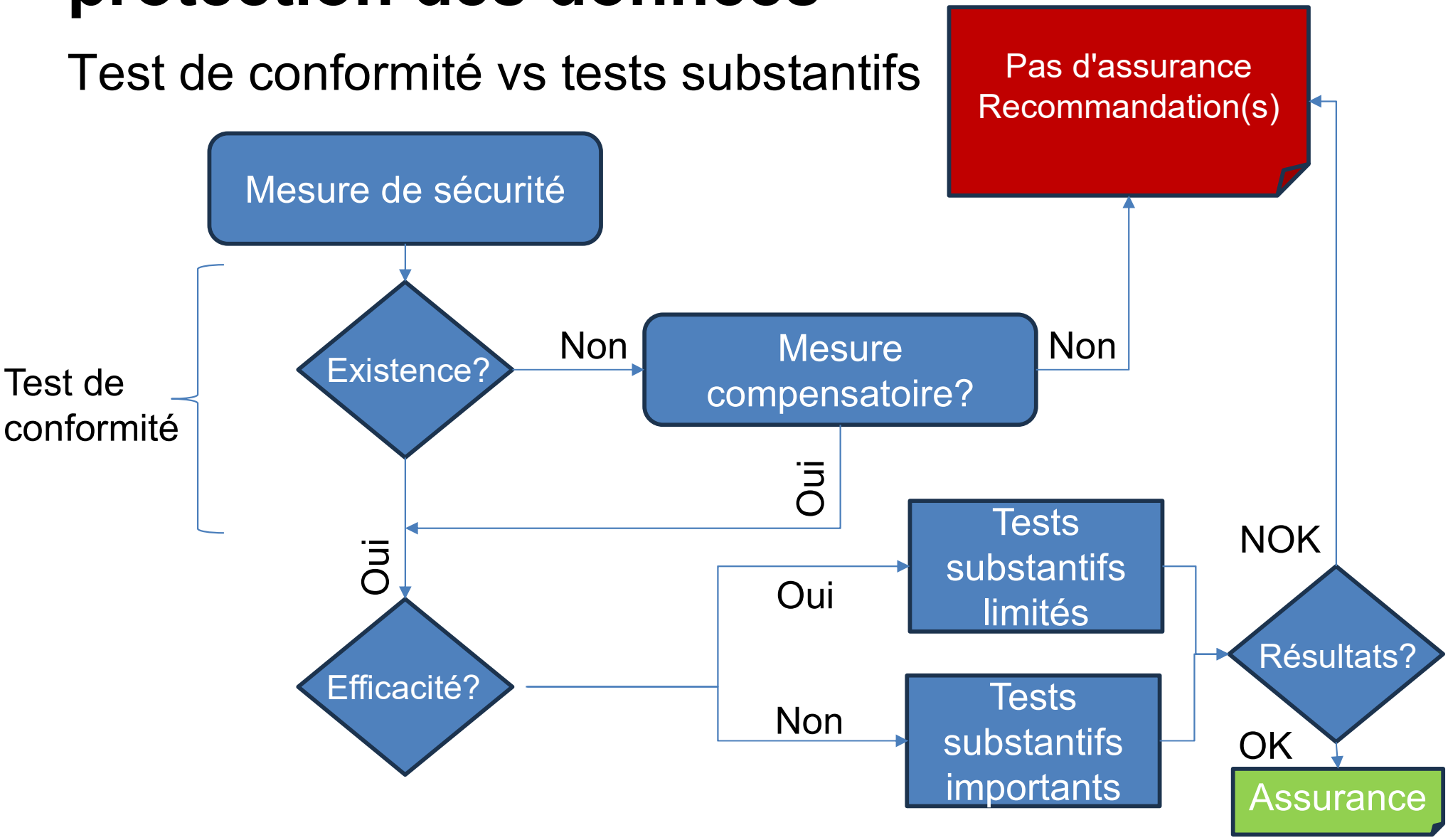
- Travaux d'audit
  - Entretiens
  - Revue de la documentation
  - Tests de conformité et tests substantifs

Rapport et suivi

- Séance de présentation des résultats
- Rapport de contrôle
- Suivi des recommandations

Comment se passe un contrôle en protection des données

Test de conformité vs tests substantifs



Comment se passe un contrôle en protection des données

Approche basée sur les risques

L'analyse des risques est nécessaire dès la planification du contrôle, elle permet d'identifier les risques et les vulnérabilités et en conséquence de déterminer les contrôles nécessaires pour les mitiger.

L'auditeur IT se focalise sur les risques élevés en lien avec la confidentialité, la disponibilité et l'intégrité des données sensibles et critiques.

Comment se passe un contrôle en protection des données

Les types de contrôles

Type	Fonctions	Exemples
Préventif	Prévenir les problèmes avant qu'ils n'arrivent Prévenir une erreur, une omission ou un acte malveillant	Séparation des fonctions Contrôle d'accès physique et logique Chiffrement des données
Détectif	Détecter et rapporter la survenance d'une erreur, d'une omission ou d'un acte malveillant	Revue de logs pour détecter des activités inappropriées Alertes des outils de sécurité
Correctif	Minimiser l'impact d'une menace Remédier aux problèmes découverts par les outils détectifs Modifier les systèmes pour minimiser les futures récurrences	Plan de continuité Sauvegardes Mises à jour

Comment se passe un contrôle en protection des données

Les techniques utilisées lors des contrôles

- Renseignement et confirmation
- Inspection
- Observations
- Analyse de données

Comment se passe un contrôle en protection des données

Les évidences

Toutes informations utilisées pour déterminer si l'entité contrôlée a mis en œuvre les mesures techniques et organisationnelles appropriées et qui supportent les conclusions du contrôle.

Les conclusions sont basées sur des évidences suffisantes et appropriées.

Les évidences sont, par exemple: les observations de l'auditeur, les notes d'entretiens, la documentation, les confirmations d'autres parties prenantes et les résultats des tests.

Comment se passe un contrôle en protection des données

Les résultats

Les résultats de l'audit sont formalisés dans un rapport qui représente une "assurance raisonnable" de la maîtrise des processus contrôlés.

Les résultats attestent de l'existence et/ou de l'efficacité/efficience des contrôles identifiés.

Les recommandations émises indiquent à l'organe contrôlé "quoi faire" pour réduire le risque résiduel identifié et non "comment" le réduire.

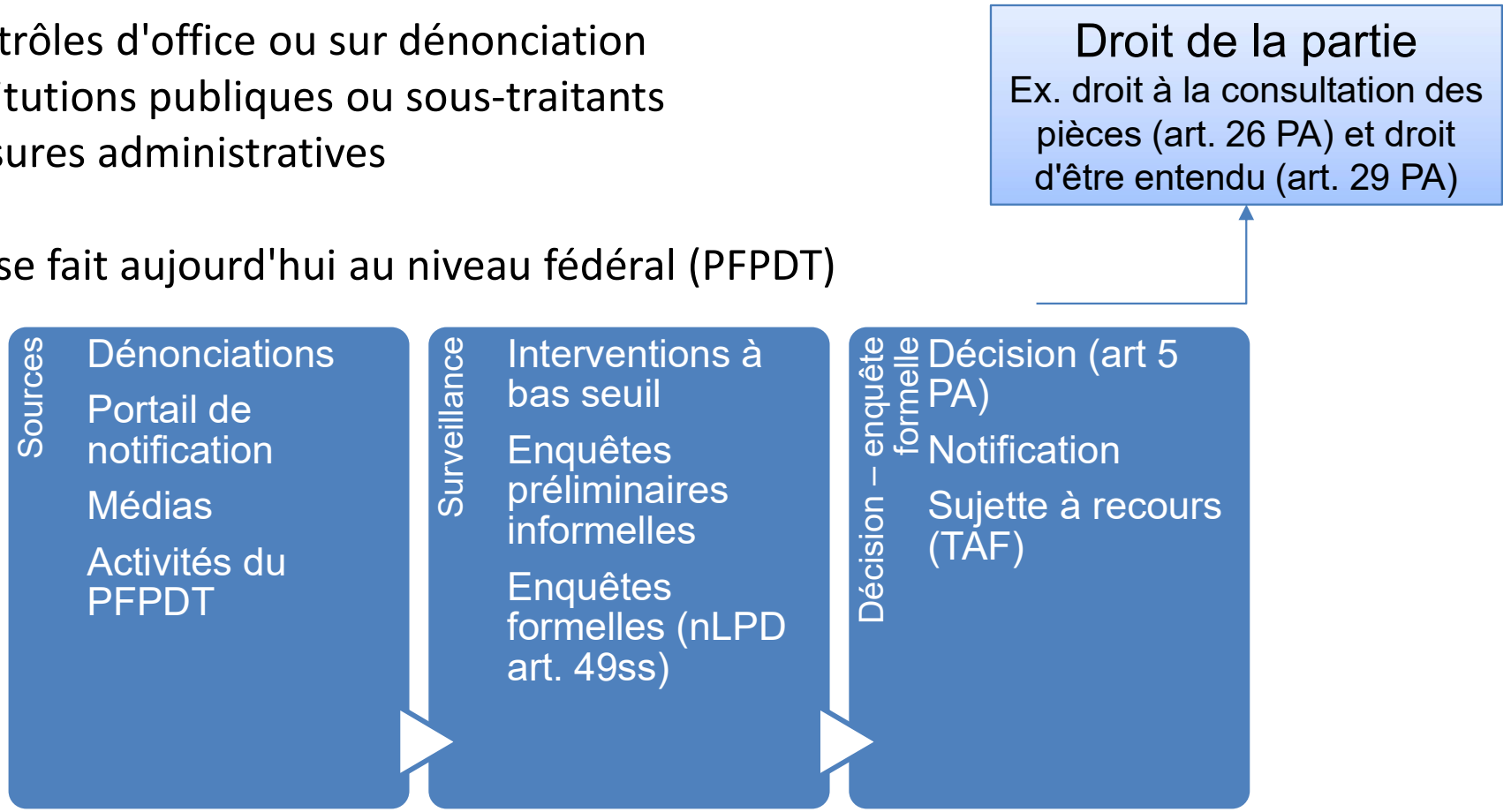
L'organe contrôlé peut se prononcer sur les recommandations en indiquant le plan d'action qui sera mis en œuvre, par quel responsable et dans quel délai.

Comment se passe un contrôle en protection des données

nLIPAD – Quels changements?

- Contrôles d'office ou sur dénonciation
- Institutions publiques ou sous-traitants
- Mesures administratives

Ce qui se fait aujourd'hui au niveau fédéral (PFPDT)



Merci pour votre attention

Boulevard Helvétique 27
1207 Genève

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