



“ **La Confédération est-elle capable de réussir un projet informatique** ”

Sébastien Fanti - CV

- Licence en droit (Master) utriusque juris de l'Université de Fribourg
- Avocat au Barreau valaisan, Notaire et fondateur du réseau Lexing
- Conseiller en protection des données HEIG-VD (2014)
- Information Security Lead Auditor ISO 27001 :2013 (2015)
- Security Management Lead Implementer ISO 27001 :2013 (2015)
- Certified Lead Privacy Implementer ISO 29100 (2015)
- Chargé de cours à l'Université Pierre et Marie Curie (UPMC) – la Sorbonne : DE Data Strategist, Paris (depuis 2017)
- Élu Préposé à la protection des données et à la transparence du Canton du Valais (2015 – 2022)
- Certified Information Privacy Professional / Europe (2018)
- Auditeur RGPD certifié Bureau Veritas (2019)
- CAS Digital Finance Law UNIGE (2020)
- CAS Financial Regulation UNIBE-GE (2022)



Sommaire de l'exposé

- Prolégomènes accusatoires
- Constats objectifs (tentative de diagnostic)
- Exemples
- Perspectives d'améliorations
- Questions et réponses

< Prolégomènes accusatoires >

13.4062 POSTULAT

Projets informatiques de la Confédération. Et maintenant?

Déposé par:



EDER JOACHIM

Groupe libéral-radical
PLR.Les Libéraux-Radicaux

Date de dépôt:

04.12.2013

Déposé au:

Conseil des Etats

Etat des délibérations:

Classé

TOUT MASQUER

TEXTE DÉPOSÉ

Suite aux graves dysfonctionnements et aux divers fiascos qui ont marqué la politique informatique de l'administration fédérale au cours des dernières années, le Conseil fédéral est prié d'établir un rapport qui abordera notamment les points suivants:

1. stratégie du Conseil fédéral, y compris des mesures permettant d'améliorer rapidement l'organisation, le pilotage et le contrôle des projets informatiques;
2. démonstration de la manière de mener à terme des projets grâce au nécessaire accroissement de l'efficacité, sans diminution de la qualité et dans un cadre financier raisonnable;
3. résultats de l'évaluation processus des projets échoués en vue d'améliorations;
4. vue d'ensemble des projets informatiques en cours sous l'angle de l'état du financement et du degré de réalisation;
5. planification des dépenses pour tous les projets informatiques à partir de 500 000 francs pour les dix ans à venir;
6. relation des dépenses effectuées dans le domaine informatique au cours des cinq dernières années entre contrats d'entreprise, sous forme de "sourcing" (facturation au temps passé) et de prestation interne;
7. vérification de l'opportunité de confier le pilotage et la mise en oeuvre au niveau interdépartemental des projets informatiques de la Confédération à un "Chief Information and Technology Officer" (CIO) central.

ARCinfo

▲ RÉSERVÉ AUX ABONNÉS

Le cafouillage informatique est généralisé à la Confédération

La mise à pied du chef du fisc fédéral révèle l'ampleur des problèmes.
Un contrôle centralisé est exigé.

Suisse

06 août 2015, 10:03



< Prolégomènes accusatoires >

Grand et critiqué

L'OFIT est l'un des cinq prestataires de services informatiques les plus importants de Suisse. Avec près de 1200 collaborateurs, il fournit pour plus de 450 millions de francs de prestations et n'a pas été épargné par les critiques ces dernières années.

Selon un audit du Contrôle des finances publié début avril, l'OFIT a des progrès à faire dans la fourniture de prestations. Le remplacement fréquent de responsables des projets et leurs connaissances techniques insuffisantes sont mal perçus par les clients. Il faut améliorer les outils d'aide et les directives de même que les contrôles de qualité des objets à livrer.

En mars, le Conseil fédéral a annoncé de son côté que la Confédération risquait de ne pas atteindre tous les objectifs de sa stratégie informatique quadriennale d'ici à fin 2019. La gestion de l'architecture et la planification intégrale n'ont pas pu avancer comme prévu, justifiait-il.



Débâcles en série dans l'administration

Les Chambres fédérales doivent se pencher lors de la session d'hiver 2014 sur le scandale informatique INSIEME. Mais la Confédération a connu plusieurs coups et scandales dans le domaine ces dernières années.

Eidgenössische Steuerverwaltung EStV
Amministrazione federale delle contribuzioni AFC
Administration fédérale des contributions AF
Swiss Federal Tax Administration FTA



< Prolégomènes accusatoires >

2012, INSIEME, projet informatique développé au sein de l'administration fédérale des contributions, perte estimée: 105 millions de francs

2014, scandale des marchés IT à l'OFROU

2017, système de conduite FIS de l'armée suisse en partie abandonné, perte de 125 millions de francs

2021, affaire des pots de vins du SECO, perte pour la Confédération estimée à 18,5 millions de francs

2022, swisstransplant, Mesvaccins.ch

2023, ?

< Prolégomènes accusatoires >

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLIO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE



[ACCUEIL](#)

[PUBLICATIONS](#) ▼

[TRANSPARENCE](#)

[WHISTLEBLOWING](#)

[VOS SUGGESTIONS](#)

[A PROPOS DE NOUS](#) ▼

Vous vous trouvez ici: [Publications](#) / Projets informatiques /

PUBLICATIONS
Projets informatiques



Dans cette section, vous trouverez les audits du CDF sur les grands projets informatiques de la Confédération.



ARCHIVES PROJETS INFORMATIQUES



< Constats objectifs >

- Le CDF a réalisé 6 audits en 2022, 10 audits en 2021, 8 audits en 2020, 14 audits en 2019, 14 audits en 2018 (parfois sur les mêmes sujets) = manque évident de ressources
- Proximité toxique et tentation permanente
- Rémunérations trop faibles
- Dystopie des compétences
- Turn-over du personnel
- Absence de transparence dans certains secteurs
- Manque de coordination et de communication interne (fonctionnement en silo)
- Répartition des compétences (notamment Confédération – Canton) qui favorise les tricheurs
- Etc.

< Exemples >

Cher Monsieur Fanti

Nous vous remercions de votre demande. Les avertissements quant aux failles de sécurité reçues reposaient sur des informations de tiers (chercheurs en sécurité). Nous avons vérifié les informations et avons ensuite écrit à qui de droit. Actuellement, nous ne disposons d'aucune base légale nous permettant de transmettre de telles informations et devons donc les traiter de manière confidentielle.

Si vous êtes d'avis que nous devrions pouvoir échanger directement de telles données à l'avenir, nous vous rendons attentif à la consultation actuellement en cours sur la révision de la loi sur la sécurité de l'information (LSI) : https://fedlex.data.admin.ch/eli/dl/proj/2021/70/cons_1. Le projet règle à l'avenir la collaboration légale entre le NCSC et les autorités publiques. Il pourrait être judicieux de compléter le projet en ce qui concerne la collaboration entre NCSC et les préposés cantonaux à la protection des données.

Nous comptons sur votre compréhension concernant notre position et nous nous tenons toujours prêts à collaborer dans le cadre de nos possibilités légales.



Sébastien Fanti

Avocat au Barreau valaisan & Notaire,
CIPP/E, ISO 29100 LI, ISO 27001 LA & LI
Auditeur RGPD certifié Bureau Veritas
Chargé de cours à la Sorbonne

Sion, le 2 avril 2020

Recommandation

au titre de l'article 37 alinéa 1 let. d
de la loi sur l'information du public, la protection des données et l'archivage du 9 octobre 2008
(RS 170.2 ; abrégée ci-après LIPDA)

émette à l'intention des autorités au sens de l'article 3 al. 1 let. a LIPDA, soit :

1. les pouvoirs législatif, exécutif et judiciaire cantonaux, communaux et bourgeoisiaux, leurs organes et administrations, ainsi que les commissions qui en dépendent,
2. les collectivités ou établissements de droit public cantonaux et communaux, leurs organes et administrations, ainsi que les commissions qui en dépendent,
3. les personnes morales ou autres organismes de droit privé dans lesquels une collectivité détient une participation majoritaire ou exerce une influence prépondérante,
4. les personnes physiques ou morales et organismes chargés de remplir des tâches de droit public cantonal ou communal, dans les limites de l'accomplissement des dites tâches,
5. les groupements d'autorités.

concernant Zoom,

Vidéosurveillance: le Valais restera sans loi, mais la bataille juridique va commencer

Face à l'opposition des communes, le Conseil d'Etat renonce à créer une base légale cantonale en matière de vidéosurveillance. Réagissant à cette annonce, le préposé à la protection des données, Me Sébastien Fanti, confirme que des investigations d'envergure contre des fonctionnaires et des autorités communales vont être menées.

Valais

Valais : le dossier électronique du patient pas assez sécurisé

Mehdi Atmani

A la veille de son introduction en Valais, le 1^{er} septembre, le dossier électronique du patient ne remplira pas tous les critères pour garantir la sécurité des données personnelles des utilisateurs. Les doutes émis par Sébastien Fanti, le préposé valaisan à la protection des données, à la suite des enquêtes menées par le Parti pirate suisse, ont été entendus. La ministre en charge de la Santé, Esther Waeber-Kalbermatten, suspend l'introduction d'Infomed jusqu'au résultat des audits externes. Ils seront conduits par Dominique Vidal, expert en sécurité informatique et fondateur de SecuLabs.

Le Parti pirate, qui milite entre autres pour la transparence numérique et les libertés individuelles sur Internet, a obtenu, avec de «simples outils accessibles au grand public, une série d'informations permettant de mettre en évidence de graves dysfonctionnements en matière de sécurité informatique» autour des plateformes valaisannes et genevoises.

Les tests effectués ont révélé qu'Infomed croise des informations avec le moteur de recherche Google et porte atteinte à la sphère privée, la plateforme utilisant Google Analytics sur sa page d'accueil. Les tests pointent aussi l'absence de conditions générales d'utilisation qui informent le patient sur la manière de gérer ses données personnelles et de les effacer.

Après avoir constaté vendredi dernier divers «singularismes en termes de sécurité informatique», Sébastien Fanti n'avait pas caché sa stupeur. Après avoir fait appel à des experts, ses doutes ont été confortés durant le week-end, au terme d'analyses élémentaires mettant en exergue une «lancinante vacuité dans l'analyse du risque».

Dans son collimateur, Alex Gnaegi, chef du projet Infomed, qui a tenu jeudi dernier une conférence de presse pour annoncer l'introduction du projet le 1^{er} septembre. «Je l'ai appris dans un communiqué», précise le préposé valaisan, qui a ouvert le jour même une procédure. «Je lui ai fait part de ma surprise, qui est allée grandissante ces derniers jours. Je suis donc intervenu. Avec la Commission de protection des données, nous étions d'avis que le projet devait être suspendu, le temps de conduire les audits et les examens de conformité nécessaires.»

< Perspectives d'amélioration >

- Garanties contractuelles fortes
- Investigations préliminaires (références)
- Certification des entreprises (ISO 27001)
- Relocalisation des données (Cloud Act)?
- Révision de la politique salariale
- Contrôles externes de la qualité du code (SonarSource) – collaboration public – privé
- Recours aux EPF et aux HES (tiers ou référent de confiance)
- Investissements dans des solutions propriétaires
- Création d'un fonds souverain du numérique
- Name and shame



“Obedient to Your interest





www.twitter.com/sebastienfanti



www.facebook.com/sebastien.fanti



ch.linkedin.com/in/sebastienfanti



sebastien.fanti@sebastienfanti.ch

