Audit de l'environnement applicatif informatique
Office fédéral des transports

L'essentiel en bref

En tant qu'autorité de surveillance, l'Office fédéral des transports (OFT) est responsable des transports publics en Suisse. Les domaines des chemins de fer, des installations de transport à câbles, des trolleybus, des tramways, des autobus et de la navigation relèvent de sa compétence. L'OFT attribue à cet effet des moyens financiers s'élevant annuellement à environ 4 milliards de francs aux entreprises de transport partenaires pour maintenir la substance des infrastructures et indemniser les frais d'exploitation.

Le Contrôle fédéral des finances (CDF) a mené une analyse préliminaire de l'environnement applicatif informatique auprès de l'OFT et effectué un audit approfondi de l'application « Répertoire des entreprises de transport » (RET). Le CDF a évalué la stabilité, la sécurité, la fiabilité et la rentabilité du RET. Il a en outre vérifié l'échange des informations relatives à la comptabilité dans RET dans le système comptable de SAP.

La maintenance de RET est assurée par l'entreprise Geocloud AG et son exploitation par l'Office fédéral de l'informatique et de la communication.

Une haute priorité devrait être accordée au respect de la loi sur la protection des données

En décembre 2015, des champs de données supplémentaires ont été introduits dans RET dans le cadre d'une modification de cette application. Il ne s'agit pas uniquement de données personnelles telles que le nom, le prénom, la date de naissance et le lieu d'origine, mais aussi de données particulièrement sensibles, par exemple des informations concernant des infractions ou des sanctions pénales et des indications sur des problèmes médicaux. Or l'application RET n'était pas conçue pour protéger ces données, ce qui signifie que des directives de la loi sur la protection des données n'ont pas été respectées. Le CDF a informé l'OFT et les services compétents du département (notamment le Préposé fédéral à la protection des données) par écrit.

L'OFT a alors pris des mesures immédiates et présenté un plan d'action au CDF. En l'état des connaissances actuelles, ce dernier juge le plan d'action approprié pour réaliser les améliorations nécessaires. Étant donné qu'un processus formel n'est pas encore défini pour apporter des modifications à des applications, l'OFT doit élaborer et appliquer un processus de changement clair en réglementant l'autorisation des modifications, leurs tests et validation ainsi qu'en attribuant des fonctions distinctes à chaque service concerné.

Un concept de protection des accès et de rôles doit être établi et mis en œuvre

Des processus clairs doivent être définis et appliqués pour l'administration et la gestion des droits d'accès des comptes d'utilisateurs dans l'application RET. La documentation correspondante, comme l'analyse des besoins de protection, devrait également être mise en jour.

Texte original en allemand