LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

GIOVANNI BUTTARELLI
LE CONTROLEUR ADJOINT

Monsieur Jean-Philippe MINNAERT
Délégué à la protection des données
Banque Européenne d'Investissement
100, boulevard Konrad Adenauer
L - 2950 LUXEMBOURG

Bruxelles, le 26 mars 2010
GB/LB/ktl D(2010)446 **C 2009-0854**

Cher Monsieur Minnaert,

Je fais suite à votre lettre du 18 décembre dernier concernant l'accès des administrateurs IT de la BEI aux données personnelles contenues dans les systèmes informatiques de cette institution. Cette lettre sera considérée comme une consultation au titre de l'article 46 (d) du règlement 45/2001.

Cette problématique est en général traitée par l'application du principe de ségrégation ou séparation des taches. Conformément à l'article 22 du règlement 45/2001, l'objectif est bien entendu de réduire les risques d'accès non-autorisés à un niveau considéré comme acceptable par l'institution. Ce niveau est établi en fonction de la sensibilité de l'information à protéger pour laquelle seront prises en compte les obligations de sécurité, de protection des données et de vie privée.

Pour répondre au mieux a cette problématique il convient donc d'adopter à la fois des mesures techniques et organisationnelles.

Concernant les aspects techniques, certaines applications permettent déjà une ségrégation des accès au niveau administrateur system. Ce dernier peut gérer le serveur sur lequel est déployée l'application mais les données relatives à l'application ne sont accessibles que par les utilisateurs ainsi que par l'administrateur de l'application. Cette situation offre une ségrégation des taches plus efficace qui permet de renforcer la sécurité et la protection des données. Le CEPD recommande donc d'explorer les possibilités offertes par ce type d'applications et favorise leur adoption en tout premier lieu.

Comme vous l'avez très justement souligné dans votre lettre, la limitation technique des accès de l'administrateur system peut et dans certains cas doit être complétée par un contrôle de ces accès. Il convient alors de mettre en place un système cohérent de production de logs qui

permettra de vérifier a posteriori et si nécessaire en temps réel les accès des administrateurs system aux serveurs et applications. Ici encore, le principe de ségrégation des taches doit être respecté. Même si ces logs pourront être accessibles (en lecture seulement) aux administrateurs du/des systèmes, ils devront être gérés en effet par une tierce partie (service d'audit, DPO, etc.).
Il convient également d'utiliser des plateformes (OS) qui offrent la possibilité de créer plusieurs comptes d'administrateurs system afin de ne pas utiliser seulement le "root access" pour l'administration du système, celui-ci ne permettant pas une "indépendance" suffisante des logs d'accès. Afin d'éviter dans la mesure du possible, toute ambiguïté, il convient également de définir des comptes spécifiques pour les administrateurs qui seront différents de leur compte d'utilisateur habituel. La pertinence de ces comptes spécifiques doit être réévaluée régulièrement et leur utilisation doit être limité dans le temps.
L'application rigoureuse du principe de proportionnalité à la quantité et à la nature de l'information contenue dans les logs administrateur et a fortiori des logs utilisateurs permettra également de réduire l'impact de possible accès non-autorisés. Il conviendra donc de limiter les informations contenues dans ces logs aux seules finalités établies par la politique de sécurité de l'institution.

Le CEPD recommande que l'ensemble de ces actions soient détaillées dans une politique de gestion des logs expliquant notamment la ou les finalités précises d'accès à ces logs. Celle-ci devra être clairement documentée et accessible a tous. Elle pourra éventuellement couvrir aussi la gestion des logs en général a laquelle vous faites référence dans la dernière partie de votre lettre. Cette politique et les mesures qui la composent devront être périodiquement réévaluées afin d'en garantir la pertinence.

(...)

Je vous prie d'agréer, cher Monsieur Minnaert, l'expression de ma considération distinguée.

(signé)

Giovanni BUTTARELLI