Service public fédéral Intérieur
Direction générale Institutions et Population
Registre national

Aux utilisateurs du Registre national.

Votre correspondant	**T**	**Votre référence**	**Annexes**
C. Rouma	02 518 20 31]		1
E-mail	**F**	**Notre référence**	**Bruxelles**
christiane.rouma@ibz.fgov.be	02 518 21 25	III/30/1794/08	12 mars 2008

Protection de la vie privée à l'égard des traitements de données à caractère personnel - Accès aux informations du Registre national - Mesures de sécurité visant à garantir la confidentialité et l'intégrité des données, l'authentification des utilisateurs et la conservation de la trace des activités exécutées sur les systèmes d'information.

Mesdames,

Messieurs,

Dans ma circulaire du 24 septembre 2007 (référence III30/5650/07), jointe en annexe, j'attirais votre attention sur l'obligation incombant à toutes les autorités et à tous les organismes autorisés à accéder en mise à jour et/ou en consultation au fichier des personnes physiques de mettre en place les mesures techniques et organisationnelles de nature à assurer, compte tenu de l'état de la technique, la sécurité, l'intégrité, la confidentialité et l'exactitude des données.

Lors de la rencontre, qui a eu lieu le 13 février dernier, entre les membres du Comité sectoriel du Registre national et les représentants de la Direction générale Institutions et Population, certains points importants ont été mis en exergue quant à la détermination des mesures de sécurité de nature à garantir la protection des informations du Registre national dans le cadre des traitements dont celles-ci font l'objet.

Il me paraît nécessaire de porter à votre connaissance ces points d'attention induisant, le cas échéant, la mise en place de nouvelles dispositions d'ordre organisationnel et/ou technique visant à pallier les risques d'atteinte à la vie privée.

1.Sécurisation logique des accès :

Les personnes habilitées à accéder et à traiter les données du Registre national et leurs pouvoirs respectifs doivent être clairement identifiés. La liste de ces personnes doit être tenue à jour et actualisée.

L'étendue des autorisations doit être strictement précisée et ces habilitations doivent être traduites par la mise en place de dispositifs techniques de contrôle d'accès non seulement aux données elles-mêmes mais aussi aux éléments informatiques (programmes, équipements de télécommunication, support de stockage). L'identification

des intervenants sera complétée par une procédure d'authentification permettant de réaliser le suivi complet de la procédure dans le respect de la protection de la vie privée. Un système de gestion interne des accès aux différentes applications et fonctionnalités du système informatique, combiné à un archivage de toutes les interventions exécutées, permet de répondre à cet objectif.

Dans cette perspective, un système interne centralisé de gestion des accès aux applications « IAM » sera mis en place prochainement au sein du Registre national, système reposant sur l'authentification des agents accédant auxdites applications, via la carte d'identité électronique.

Des mesures organisationnelles peuvent venir compléter utilement les dispositions techniques de contrôle et d'accès, par certains membres du personnel, à certaines applications critiques telles que, par exemple, le système de gestion des utilisateurs ou les programmes de traitement des archivages. Des erreurs, des usages inappropriés ou des malveillances commis à ce niveau peuvent, en effet, avoir des conséquences graves pour la protection de la vie privée (autorisation d'accès indue accordée à certaines personnes, effacement ou traces de manipulations effectuées). Il convient, dans ce contexte, d'organiser le travail de manière telle que ces opérations ne soient pas réalisées par un opérateur dans un cadre isolé.

2.Communication des informations du Registre national sous forme d'extraits.

La communication d'informations du Registre national (sous forme d'extraits) aux autorités et organismes visés à l'article 5 de la loi du 8 août 1983 organisant un Registre national est autorisée par le Comité sectoriel sous certaines conditions. Cette autorisation est octroyée dans le cadre de finalités déterminées.

Les conditions dans lesquelles les données peuvent être utilisées et la durée pendant laquelle elles peuvent être conservées sont également précisées dans la délibération du Comité sectoriel.

Le consultant en sécurité désigné par les autorités responsables au niveau de l'organisme utilisateur est en particulier chargé de veiller au respect des conditions précitées.

Le comité sectoriel du Registre national nous signale que certains organismes, qui ont obtenu l'autorisation d'obtenir la communication de certaines données pour la réalisation de finalités déterminées, moyennant le respect de conditions explicites portant sur le délai de conservation (délai limité impliquant un effacement des données à l'expiration de celui-ci) et sur l'usage des données (usage interne expressément stipulé), ne respectent pas lesdites conditions , soit qu'ils conservent les données au-delà des délais fixés soit qu'ils communiquent les données à des tiers au mépris de leur engagement de n'en faire qu'un usage interne. De telles pratiques sont, faut-il le souligner, tout à fait illégales. Elles exposent ceux qui s'y livrent aux sanctions pénales fixées à l'article 13 de la loi du 8 août 1983 organisant un registre national des personnes physiques et aux articles 38 à 43 de la loi du 18 décembre 1992 relative à la protection de la vie privée à l'égard des traitements à caractère personnel.

Parc Atrium
Rue des Colonies 11 T 02 518 21 31 callcenter.rrn@rrn.fgov.be
1000 Bruxelles F 02 518 26 31 www.ibz.rrn.fgov.be

3. Les mesures techniques et organisationnelles de sécurité doivent être vérifiées quant à leur efficacité et mises à jour en fonction des évolutions.

Il convient de mettre en place un système de surveillance permettant de s'assurer que les mesures de sécurité mises en place en vue de protéger les informations traitées atteignent bien l'objectif visé. Un réexamen au moins annuel desdites mesures s'impose afin d'apporter, si nécessaire, les corrections et adaptations nécessaires.

Un audit réalisé par un organisme externe peut, dans ce contexte, s'avérer très utile.

4. L'importance de la communication (information et formation du personnel).

La sécurisation des systèmes d'information est fortement dépendante de l'information correcte du personnel intervenant directement ou indirectement dans le traitement des informations.

Les précautions, obligations et responsabilités incombant à chacun doivent être expliquées lors de séances d'information comportant un rappel des procédures définies pour assurer le respect de l'intégrité et de la confidentialité des données.

Parmi ces procédures, il convient de veiller à la gestion rigoureuse des clefs d'accès au Registre national (clefs variables : login – mot de passe ou clefs fixes) en particulier quant à l'identification des titulaires des clefs (en ce qui concerne les clefs variables) et à la tenue à jour des informations y relatives. De même, l'attention des titulaires des clefs doit être attirée concernant l'obligation de garantir la confidentialité desdites clefs (la transcription des logins et mots de passe sur support papier exposée à la vue des tiers est proscrite).

En tant qu'utilisateurs du Registre national, vous êtes nos partenaires dans la poursuite de l'objectif visant à améliorer constamment la sécurité des informations du Registre national afin de garantir le plus haut niveau possible de protection contre les atteintes à la vie privée dans le cadre du traitement de ces données.

Veuillez agréer, Mesdames, Messieurs, l'expression de ma considération très distinguée.

L. VANNESTE.
Directeur général.

Parc Atrium
Rue des Colonies 11 T 02 518 21 31 callcenter.rrn@rrn.fgov.be
1000 Bruxelles F 02 518 26 31 www.ibz.rrn.fgov.be