



COMMUNIQUÉ DE PRESSE

CEPD/2016/08

Bruxelles, le 21 mars 2016

Guide du CEPD pour la sécurisation des informations et la continuité des activités

Dans le présent [guide](#) sur la *Gestion des risques liés à la sécurité de l'information* publié aujourd'hui, le contrôleur européen de la protection des données (CEPD) conseille les institutions européennes sur la façon de garantir un environnement numérique sécurisé et fiable pour les informations essentielles au fonctionnement de leurs services.

Wojciech Wiewiórowski, contrôleur adjoint à la protection des données: *"La sécurité des données à caractère personnel est une obligation légale, mais elle est également nécessaire dans l'intérêt des organisations qui se basent sur l'utilisation d'informations pour leurs activités quotidiennes. Il est indispensable qu'elles maintiennent des niveaux de sécurité appropriés pour les informations car la valeur et l'efficacité de leur travail en dépendent largement. J'encourage les hiérarchies des institutions européennes à s'engager dans l'élaboration et l'utilisation sur mesure de procédures de gestion des risques liés à la sécurité de l'information pour répondre aux besoins spécifiques de leur organisation".*

Différentes organisations sont exposées à différents risques liés à la sécurité de l'information qu'elles utilisent. Par conséquent, des méthodes d'évaluation des risques de pointe constituent un moyen efficace d'identification des solutions appropriées pour les risques spécifiques auxquels une institution peut être confrontée et peuvent justifier l'utilisation de ressources financières et informatiques pour développer ces solutions.

La gestion des risques liés à la sécurité de l'information pour les données à caractère personnel nécessite l'expertise de spécialistes en matière de sécurité de l'information et de sécurité informatique ainsi qu'en matière de protection des données. [Les délégués à la protection des données](#) (DPD) doivent soutenir les experts en sécurité de l'information et informatique dans l'élaboration de ces procédures.

Les solutions techniques de sécurité ne peuvent résoudre seules le problème de la sécurité de l'information. La hiérarchie d'une organisation est responsable de la mise en œuvre des décisions qui affectent les applications et les infrastructures informatiques qui les hébergent. La direction doit soutenir l'élaboration et la mise en œuvre des politiques et mobiliser les ressources nécessaires pour contrer les risques pour les informations auxquels une organisation est confrontée.

Bien que ce guide soit principalement destiné aux institutions européennes, toute personne concernée par la protection des données pourrait le trouver utile. Le règlement sur la protection des données [[règlement \(CE\) n° 45/2001](#)] est similaire à de nombreux égards à la [directive 95/46/CE](#) relative à la protection des données, transposée dans les législations nationales des États membres de l'UE, ainsi qu'en Islande, au Liechtenstein et en Norvège.

Le guide conservera toute son utilité avec l'entrée en vigueur du nouveau [règlement général sur la protection des données](#) qui maintient le principe de gestion des risques pour la sécurité et renforce la responsabilité globale et les exigences en matière de gouvernance en présentant de façon explicite le principe de **responsabilité** dans le respect des obligations en matière de protection des données.

Informations complémentaires

Les règles relatives à la protection des données dans les institutions européennes, tout comme les obligations du contrôleur européen de la protection des données (CEPD), sont énoncées dans le [règlement \(CE\) n° 45/2001](#). Le CEPD est une autorité de contrôle indépendante relativement nouvelle, mais de plus en plus influente, qui est chargée de contrôler le traitement des données à caractère personnel par les [institutions et organes de l'UE](#), de donner des conseils sur les politiques et les textes législatifs qui touchent à la vie privée et de coopérer avec les autorités de même nature afin de garantir une protection des données qui soit cohérente.

Giovanni Buttarelli (CEPD) et **Wojciech Wiewiórowski** (contrôleur adjoint) sont membres de l'institution et ont été nommés par une décision conjointe du Parlement européen et du Conseil. Ils sont entrés en fonction le 4 décembre 2014, pour un mandat de cinq ans.

Informations ou données à caractère personnel: toute information concernant une personne physique (vivante) identifiée ou identifiable. À titre d'exemples: noms, dates de naissance, photographies, séquences vidéo, adresses électroniques et numéros de téléphone. D'autres informations telles que des adresses IP et le contenu de communications se rapportant à des utilisateurs finaux de services de communication ou fournies par ces derniers sont également considérées comme des données à caractère personnel.

Respect de la vie privée: droit d'une personne à être laissée tranquille et à contrôler les informations la concernant. Le droit au respect de la vie privée est inscrit dans la Déclaration universelle des droits de l'homme (article 12), dans la Convention européenne des droits de l'homme (article 8) et dans la [Charte des droits fondamentaux de l'Union européenne](#) (article 7). La Charte contient également un droit explicite à la protection des données à caractère personnel (article 8).

Traitement des données à caractère personnel: aux termes de l'article 2, point b), du règlement (CE) n° 45/2001, on entend par «traitement de données à caractère personnel: toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.» Voir le [glossaire](#) sur le site internet du CEPD.

L'[article 22 du règlement n° 45/2001](#) contient la disposition juridique qui permet aux institutions européennes d'atténuer les risques lorsqu'elles traitent des données à caractère personnel;

- dans leur analyse, la gestion des risques liés à la sécurité de l'information doit également couvrir les risques pour la sécurité de l'information qui concernent des données à caractère personnel;
- à partir de cette analyse, un ensemble de mesures de sécurité adaptées peuvent être définies et mises en œuvre.

Les mesures de sécurité protégeant les données à caractère personnel ne peuvent pas être définies de façon générique dans la mesure où elles doivent émaner du processus de gestion des risques liés à la sécurité de l'information, qui tient compte du contexte spécifique dans lequel les données à caractère personnel sont traitées.

Les experts en sécurité de l'information sont spécialisés dans l'élaboration de méthodes visant à protéger les informations et systèmes d'informations contre tout accès, utilisation, divulgation, atteinte, modification ou destruction non autorisée.

Les experts en sécurité informatique sont spécialisés dans l'élaboration de méthodes visant à protéger les informations en utilisant diverses technologies pour créer, stocker, utiliser et échanger de telles informations en les protégeant contre tout accès non autorisé, abus, dysfonctionnement, modification, destruction ou divulgation inappropriée.

Le contrôleur européen de la protection des données (CEPD) est une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et la vie privée et de promouvoir les bonnes pratiques dans les institutions et organes de l'UE. À cet effet, il remplit les tâches suivantes:

- contrôler les traitements de données à caractère personnel effectués par l'administration de l'UE;
- donner des conseils sur les politiques et les textes législatifs qui touchent à la vie privée; et
- coopérer avec les autorités de même nature afin de garantir une protection des données qui soit cohérente.

Le [guide](#) du CEPD est disponible sur le site web du CEPD.

Les questions peuvent être adressées à l'adresse suivante: press@edps.europa.eu

CEPD – Le gardien européen de la protection des données

www.edps.europa.eu



Suivez-nous sur Twitter: [@EU_EDPS](https://twitter.com/EU_EDPS)