LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Newsletter du CEPD

N° 40 | Décembre 2013

DANS CE NUMÉRO

FAITS MARQUANTS

Respect de la vie privée et protection des données peuvent rétablir la confiance des consommateurs dans la société numérique

La proposition de la Commission européenne d'harmoniser les services de communications électroniques dans l'Union européenne limitera indûment la liberté sur Internet selon le Contrôleur européen de la protection des données (CEPD).

Tout type de surveillance et de restriction de l'activité des internautes ne devrait viser qu'un but bien précis, spécifique et légitime. La surveillance à grande échelle et la restriction des communications des utilisateurs de l'internet, prévues dans cette proposition, sont contraires à la législation européenne sur la protection des données ainsi qu'à la Charte des droits fondamentaux de l'UE. Cette ingérence dans les droits à la protection des données à caractère personnel, à la confidentialité des communications et au respect de la vie privée ne contribuera guère à restaurer la confiance des consommateurs dans le marché des communications électroniques en Europe.

Peter Hustinx, CEPD

Avis du CEPD

Communiqué de presse du CEPD

TEN-T EA : assurer la protection des lanceurs d'alerte

European Commission | Trans-European Transport Network Executive Agency

Conformément au statut des fonctionnaires des institutions et des organes de l'Union européenne, le personnel qui prend connaissance de faits qui peuvent laisser présumer une activité illégale, notamment une fraude ou une corruption, doit en informer la hiérarchie. Afin que le personnel puisse rapporter les activités illégales suspectées en toute sécurité et dans un climat de confiance, les institutions et les organes de l'UE ont mis en place une procédure visant à protéger les lanceurs d'alerte. Dans notre avis du 28 octobre 2013, nous analysons le projet de procédure préparé par l'Agence exécutive du réseau transeuropéen de transport (TEN-T EA) et émettons les recommandations suivantes:

- les informations inutiles et non pertinentes fournies par des lanceurs d'alerte ne doivent pas être conservées plus longtemps que nécessaire;
- le traitement d'informations à caractère personnel doit se limiter aux données strictement nécessaires à la vérification des allégations;
- la confidentialité des lanceurs d'alerte doit être assurée de manière systématique plutôt que sur demande; et
- le principe de confidentialité doit être appliqué de manière large et pas seulement vis-à-vis des personnes mises en cause.

Nous nous sommes réjouis que la procédure précise quelles informations sont pertinentes ou non dans le cadre de la procédure, mais nous avons souligné l'importance de la mise en œuvre de limitations et d'une confidentialité des données plus strictes afin de protéger les lanceurs d'alerte. TEN-T EA a finalisé sa procédure conformément à nos commentaires.

Avis du CEPD

SUPERVISION

Lignes directrices sur les congés et les horaires flexibles: notifications relatives aux opérations de traitement des données

En décembre 2012, nous avons publié des lignes directrices sur les congés et les horaires flexibles. Dans ce document, le CEPD demande aux institutions et aux organes de l'UE de lui adresser des notifications concernant les opérations de traitement n'ayant pas encore été analysées afin d'assurer la mise en œuvre correcte des exigences en matière de protection des données lors des opérations de traitement en matière de congé et d'horaire flexible. Depuis lors, nous avons reçu un total de 47 notifications concernant une série d'opérations de traitement. Nous y avons répondu par des avis succincts se concentrant uniquement sur des domaines qui diffèrent des lignes directrices existantes.

L'analyse de ces notifications a révélé que le problème principal, pour toutes les opérations, est la durée pendant laquelle les données collectées sont conservées. Un problème a également été constaté avec la clause relative à la protection des données qui doit être signée par le personnel des ressources humaines. Cette clause est spécifiquement liée au traitement des données en matière de santé et nous insistons pour que le personnel concerné signe une déclaration de confidentialité. Nous avons également souligné l'importance de donner aux membres du personnel et à leurs proches des informations pertinentes sur ces opérations lorsque celles-ci impliquent le traitement de leurs données à caractère personnel.

Nous avons répondu à presque toutes les notifications et les avons publiées – ou sommes en train de les publier – sur notre site web.

Lignes directrices du CEPD

Contrôles préalables *ex post* – résorber le retard accumulé

Les contrôles préalables *ex post* comprennent des opérations de traitement de données à caractère personnel qui ont déjà débuté, mais aussi ceux qui ont débuté avant le 17 janvier 2004 (date de la nomination du premier contrôleur européen de la protection des données et du contrôleur adjoint) ou qui ont débuté avant l'entrée en vigueur du *règlement*. Quand le CEPD a commencé ses activités, un retard avait été accumulé dans les dossiers de contrôle préalable *ex post*. Les institutions et organes de l'UE disposant maintenant du temps nécessaire pour notifier leurs activités de traitement existantes, nous avons invité les institutions et organes de l'UE à s'assurer que toutes les opérations de traitement en suspens nous avaient été notifiées avant la fin du mois de juin 2013. Des exceptions étaient prévues pour certaines activités menées par des organes créés récemment et qui n'auraient pas été en mesure d'envoyer leurs notifications à l'avance, dans le cas d'un recrutement, par exemple. Du fait de cette date butoir, nous avons reçu un total de 180 notifications entre le début du mois de juin 2012 et la fin du mois de juillet 2013. Nous avons estimé que 29 d'entre elles n'étaient pas sujettes à un contrôle préalable en 2013, contre 8 en 2012.

Création d'une plateforme de consultation des données d'enquête

Cette plateforme, l'Investigative Data Consultation Platform (IDCP), est un projet de base de données qui vise à faciliter l'échange d'informations entre l'OLAF et les autorités internationales partenaires dans le cadre d'enquêtes anti-fraude. Une fois opérationnelle, l'IDCP permettra aux utilisateurs de contrôler si des informations spécifiques sont incluses dans les fichiers des partenaires, comme les noms des personnes faisant l'objet d'une enquête, leur numéro de téléphone, leur adresse, etc.

Dans notre avis, nous avons émis plusieurs recommandations à ce sujet, notamment:

- assurer un droit d'accès approprié aux personnes concernées;
- réduire la durée de conservation des données; et
- assurer la qualité des données.

Les activités de l'IDCP entraînant des transferts structurels de données à caractère personnel au titre de l'article 9 du *règlement* n°45/2001, le système ne peut commencer à fonctionner sans une autorisation distincte du CEPD au titre de l'article 9, paragraphe 7, du règlement. L'IDCP ne pourra donc pas être active tant que le CEPD ne lui aura pas accordé une telle autorisation.

Avis du CEPD

OLAF
EUROPEAN ANTI-FRAUD OFFICE

CONSULTATION

Insistons sur les garanties pour le système eCall

Le système eCall 112 est une initiative visant à fournir une assistance rapide aux automobilistes impliqués dans une collision ou dans un accident de la route au sein de l'Union européenne. Dans notre avis du 29 octobre 2013 sur *la proposition de la Commission concernant les exigences en matière de réception par type pour le déploiement du système eCall*, nous avons souligné le caractère potentiellement intrusif du système. Si nous nous sommes réjouis que le règlement inclue des garanties sur la protection des données essentielles, nous avons toutefois insisté pour que des garanties complémentaires soient ajoutées. À partir du 1er octobre 2015, l'intégration des appareils eCall sera obligatoire pour tous les nouveaux véhicules. Ce déploiement élargi devrait permettre *d'exploiter commercialement* (par exemple concernant les modèles d'assurances ciblées, la recherche de véhicules volés, la fonctionnalité eTolling) les capacités de la plateforme de la technologie eCall (modules de positionnement, de traitement et de communication). Étant donné les risques que cela implique en matière de protection des données, nous avons souligné la nécessité d'un niveau de garanties équivalent en matière de protection des données.

Avis du CEPD

Accord UE-Canada sur les données PNR : pas de décollage sans améliorations de la protection des données

La proposition de décision du Conseil relative à la conclusion de l'accord entre le Canada et l'UE sur le transfert et le traitement de données des dossiers passagers (données PNR) soulève des questions sur la nécessité et la proportionnalité de telles mesures. Dans notre avis du 30 septembre 2013, nous avons à nouveau mis en doute la nécessité et la portée de modèles PNR et du transfert important de données PNR. Nous avons aussi mis en doute la base légale de l'accord et exprimé notre inquiétude concernant l'absence flagrante de possibilités, pour les citoyens européens, de recours devant une instance indépendante. Nous avons émis plusieurs recommandations sur des questions telles que:

- l'exclusion du traitement des données sensibles;
- une période de conservation réduite et justifiée;
- un nombre limité de catégories de données PNR à traiter; et
- une mention explicite du rôle de superviseur attribué à l'autorité indépendante.

Avis du CEPD

Surveillance des risques en matière de protection des données dans le cadre de la facturation électronique

Les services d'appel d'offres public de toute l'Union européenne commencent à réclamer un système de facturation exclusivement électronique. Cependant, les normes et les critères relatifs au contenu, au format, à la mise en page, aux besoins techniques et à d'autres aspects de la facturation varient considérablement d'un État membre à l'autre. La *proposition de directive de la Commission relative à la facturation électronique dans le cadre des marchés publics* vise à encourager l'utilisation de la facturation électronique et à améliorer l'interopérabilité entre les États membres. Dans notre avis du 11 novembre 2013 relatif à cette proposition, nous avons attiré l'attention sur l'accroissement des risques pesant sur la protection des données et le respect de la vie privée, associés à la disponibilité de données de facturation sans support papier et dans un format lisible par machine. Nous nous sommes réjouis de ce pas en direction d'une facturation électronique sans support papier, mais avons attiré l'attention sur l'importance de questions telles que l'utilisation des informations à caractère personnel au-delà des limites permises, pour le profilage automatique ou l'exploration des données. De telles utilisations seront sans doute incompatibles avec les droits relatifs à la protection des données ou exigeraient des garanties supplémentaires.

Avis du CEPD

La fiscalité ne devrait pas se faire au détriment de la protection des données et de la transparence

La Commission prévoit d'amender sa *directive sur l'échange automatique et obligatoire d'informations dans le domaine fiscal* afin d'en étendre la portée et d'inclure des catégories d'informations telles que les dividendes, les plus-values, les soldes de compte et autres rentrées financières. Cette extension contribuera à assurer l'égalité de traitement entre les différents types d'actifs. Dans notre lettre à la Commission, nous lui avons recommandé de mieux définir le type d'informations à caractère personnel concerné, ainsi que les raisons pour lesquelles ces informations peuvent être échangées. Nous avons également exprimé notre inquiétude concernant le manque de dispositions, tant dans la directive actuelle que dans la nouvelle proposition, relatives à la manière dont le principe de transparence doit être mis en œuvre. Nous avons exhorté le législateur à tenir compte des problèmes de définition des différents types d'informations à caractère personnel concernés, de la transparence, ainsi que de la nécessité et de la proportionnalité des mesures incluses dans cette nouvelle proposition.

Observations du CEPD

Évaluation du risque et mesures de sécurité au sein des institutions de l'UE

De récentes révélations sur les activités de surveillance et d'espionnage des services de renseignements des États membres et de pays tiers suggèrent que les communications électroniques des institutions et des délégations de l'UE ont été prises pour cible. Certains craignent également que des outils de sécurité et de cryptographie disponibles sur le marché aient été intentionnellement affaiblis pour rendre l'interception des communications plus aisée. Au vu de ces préoccupations, le CEPD souhaite vérifier si les institutions de l'UE estiment toujours valable l'évaluation des risques relatifs à leurs opérations de protection des données et si elles considèrent toujours les mesures de sécurité actuelles comme adéquates. À cette fin, nous organisons des rencontres avec le Parlement européen, avec la Commission et avec le Conseil pour en savoir davantage sur leurs réactions face à ces révélations et aux étapes suivantes.

Réflexions sur la sécurité: les concepteurs de l'internet ripostent contre la surveillance

L'Internet Engineering Task Force (IETF), l'organe qui conçoit les normes de fonctionnement de l'internet, s'est réuni à Vancouver du 3 au 8 novembre 2013 pour réfléchir aux moyens d'améliorer l'état des connaissances en matière de sécurité en ligne. Au début du mois de septembre, *The Guardian* a publié un *article* de Bruce Schneier, célèbre cryptographe, expert en sécurité et écrivain, qui a demandé aux concepteurs de l'internet d'agir et de consacrer cette réunion à l'omniprésence de la surveillance. Il semblerait que les ingénieurs informatiques, eux aussi, en aient eu assez de cette surveillance généralisée. Après les révélations de cet été sur la NSA et après avoir attentivement écouté le message de Bruce Schneier, l'IETF en est arrivé à la conclusion que cette surveillance omniprésente doit être considérée comme une attaque de nature technique et a accepté de rendre les normes de l'IETF plus strictes. Il s'agit là d'un des nombreux avancements accomplis au sein de la grande communauté Internet pour développer des contre-mesures techniques solides contre ce type de surveillance. Cependant, développer et publier des spécifications techniques de qualité ne constitue qu'une première étape. Celles-ci doivent être mises en œuvre et puis déployées pour réellement améliorer la vie privée sur Internet. Cela peut prendre du temps et cela demandera la participation d'autres parties prenantes.

Pour en savoir plus:

«Leading Engineers Agree to Upgrade Standards to Improve Internet Privacy and Security»

«Pervasive Monitoring is an Attack»

L'*Intro* de LinkedIn: connectez-vous avec prudence

Le réseau social professionnel en ligne, LinkedIn, a lancé *Intro*, une nouvelle application destinée aux produits d'Apple sous iOS. Cette application, qui permet aux utilisateurs de visualiser des profils LinkedIn par le biais de leur application de messagerie électronique, sur leur iPhone ou sur leur iPad, redirige les courriers électroniques des utilisateurs à travers les serveurs de LinkedIn. Les métadonnées du profil LinkedIn sont ici ajoutées aux courriers électroniques que reçoivent les utilisateurs d'*Intro*, la société s'octroyant au passage l'accès à toutes les communications par courrier électronique. Le CEPD s'inquiète des risques que cette application fait peser sur la vie privée puisque les communications par courrier électronique des utilisateurs d'*Intro* sont exposées. Nous vous recommandons vivement de ne pas installer cette application sur vos appareils Apple.

Pour en savoir plus sur l'application *Intro* de LinkedIn, vous pouvez lire ces deux blogs sur la sécurité tenus par un groupe de sécurité tiers en cliquant *ici* et *ici*.

Intro: manuel de désinstallation, la *FAQ* de LinkedIn et *sa déclaration sur la vie privée*.

ÉVÉNEMENTS

Réunion des DPD

La 34e réunion semestrielle des délégués à la protection des données (DPD), accueillie pour la première fois par le CEPD, a eu lieu à Bruxelles du 20 au 22 novembre 2013. La réunion portait principalement sur les développements en matière de protection des données en Europe et dans le monde, une attention toute particulière ayant été accordée à la réforme de la législation européenne relative à la protection des données, ainsi qu'au rôle des DPD. Le directeur de la DG Droits fondamentaux et citoyenneté de l'Union de la Commission européenne, M. Paul Nemitz, a donné une présentation devant le réseau de DPD. Un atelier sur la protection des données et la transparence a également été organisé et a donné lieu à de vastes et fructueuses discussions. Le CEPD a informé le groupe des derniers développements réalisés dans de nombreux domaines en relation avec son travail, notamment concernant les procédures de contrôle préalable, les lignes directrices, les premières réactions à notre sondage 2013 et les informations de tierces parties dans les plaintes. Il s'est avéré que la réunion était également un forum utile pour discuter de nos futures lignes directrices sur les conflits d'intérêt, auquel les différents DPD ont participé avec enthousiasme.

Tous les DPD souhaitaient partager leurs précieux points de vue et leur expérience de premier plan en matière de protection des données. Cela a sans aucun doute contribué aux réactions positives et au succès de la réunion.

DISCOURS ET PUBLICATIONS

- Discours (*pdf*) prononcé par Giovanni Buttarelli à Budapest, «Data Protection in the Judiciary: The Challenges for Modern Management» (24 octobre 2013)

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Nominations récentes

- M. Gabriele Borla, Agence européenne de défense (AED)
- M. Nikolaos Chatzimichalakis, Institut d'études de sécurité de l'Union européenne (IESUE)
- M. Andrej Gras, Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures (FRONTEX)
- M. Luca Zampaglione, par interim, eu-LISA

Best wishes

Meilleurs voeux

Frohes Fest

À propos de cette newsletter

Cette newsletter est publiée par le Contrôleur européen de la protection des données, une autorité européenne indépendante créée en 2004 en vue de:

- superviser le traitement des données à caractère personnel dans les institutions et organes de l'UE;
- conseiller les institutions européennes sur la législation en matière de protection des données;
- coopérer avec les autorités similaires afin de promouvoir la cohérence de la protection des données à caractère personnel.

Vous pouvez vous abonner à cette newsletter ou vous en désabonner sur notre web.

COORDONNÉES

www.edps.europa.eu
Tél.: +32 (0)2 283 19 00
Fax: +32 (0)2 283 19 50
NewsletterEDPS@edps.europa.eu

ADRESSE POSTALE

CEPD
Rue Wiertz 60 – Bât. MTS
B-1047 Bruxelles
BELGIQUE

ADRESSE BUREAUX

Rue Montoyer 30
B-1000 Bruxelles
BELGIQUE

Suivez-nous sur Twitter: @EU_EDPS

CEPD – Le Contrôleur européen de la protection des données