«Essai de l'outil Système d'information géographique au sein de l'ECDC»

Avis de contrôle préalable

Dossier 2016-0759

***

L'ECDC a pour mission de renforcer les défenses contre les maladies infectieuses en Europe en décelant, en évaluant et en communiquant les menaces actuelles et émergentes que ces maladies peuvent représenter pour la santé humaine. Aux fins de lutter contre la légionellose, l'ECDC a développé un outil qui permettra aux épidémiologistes au niveau national de procéder à une analyse spatiale pendant les épidémies de cette maladie. Avant de mettre l'outil à la disposition des épidémiologistes des États membres, l'ECDC entreprendra de tester l'outil afin d'en vérifier la précision, en utilisant les données d'une épidémie de légionellose en Norvège en 2005. Pendant l'essai, les données traitées contiendront des informations personnelles relatives à la santé, puisqu'elles incluent les coordonnées géographiques des patients soignés pendant cette épidémie. Pour cette raison, il est important de s'assurer qu'il existe une base juridique spécifique pour le développement de l'outil, y compris l'essai, et que les personnes concernées sont correctement informées du traitement des données relatives à la santé les concernant.

***

Bruxelles, le 17 janvier 2017

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 30 - B-1000 Bruxelles
Adresse électronique: edps@edps.europa.eu - Site web: www.edps.europa.eu
Tél.: +32 2-283 19 00 – Fax: +32 2-283 19 50

1) Les faits

Le Centre européen de prévention et de contrôle des maladies (ECDC) a développé un outil appelé *Système d'information géographique* (l'outil SIG), qui permet aux épidémiologistes de procéder à une analyse spatiale de base pendant les épidémies de légionellose. La finalité du traitement soumis au contrôle préalable est un essai de l'outil SIG en vue d'en valider la précision. Dans le cadre de la future utilisation de l'outil SIG, l'ECDC agira comme simple sous-traitant et hébergera l'outil qui sera mis à la disposition d'instituts, d'autorités et de chercheurs des États membres.

L'essai consiste à reproduire l'analyse d'un compte rendu publié[1], en se basant sur les cas et les sites d'origine potentiels, d'une épidémie de légionellose à Sarpsborg (Norvège), en 2005. Les données qui seront traitées sont les coordonnées géographiques de 49 foyers et de huit sources potentielles (tours de refroidissement), la densité de population et des données relatives à la vitesse et à la direction du vent au moment de l'épidémie. Seules les données de l'épidémie de 2005 à Sarpsborg seront traitées. Selon les informations reçues, les données seront transférées depuis l'Institut norvégien de la santé publique (NIPH), qui est en possession des données nécessaires pour tester l'outil SIG.

La finalité du traitement est de comparer les résultats de l'outil SIG développé par l'ECDC avec le compte rendu publié contenant les résultats d'enquête des enquêteurs norvégiens pour s'assurer de la précision de l'outil SIG. L'essai a pour objectif de vérifier que l'outil SIG donne les résultats escomptés (carte et tableau similaires à ceux figurant dans le compte rendu publié). Dès que l'essai de l'outil sera terminé et le compte rendu de l'essai établi, l'ECDC effacera les données. Aucune donnée à caractère personnel ne sera divulguée lors de la présentation des résultats de l'essai. En outre, la comparaison sera utilisée pour servir de base à la formulation d'exigences supplémentaires en vue de perfectionner l'outil.

Les données collectées comprennent des données relatives à la santé étant donné qu'elles incluent l'emplacement (coordonnées géographiques) des personnes chez qui la légionellose a été diagnostiquée pendant l'épidémie de 2005. Bien qu'aucun nom ni aucune autre information personnelle n'accompagne les coordonnées géographiques, les patients concernés peuvent être identifiés via leur lieu de résidence.

Dans la notification, l'ECDC indique que l'essai de l'outil SIG est soumis au contrôle préalable sur la base de l'article 27, paragraphe 2, point a), étant donné qu'il comprend le traitement de données relatives à la santé. À cet égard, l'ECDC fait valoir que «*la combinaison des données collectées pourrait en théorie être utilisée pour identifier les personnes qui fournissent des informations rétrospectives sur leur santé*».

2) Analyse juridique

Le présent avis de contrôle préalable[2] au titre de l'article 27 du règlement (CE) nº 45/2001[3] (ci-après le «règlement») portera sur les aspects qui soulèvent des problèmes de conformité avec le

[1] http://cid.oxfordjournals.org/content/46/1/61.full

[2] Conformément à l'article 27, paragraphe 4, du règlement, le CEPD rend son avis dans les deux mois qui suivent la réception de la notification, hors suspensions. La notification a été reçue le 1er septembre 2016. Le dossier a été suspendu du 2 septembre au 6 septembre 2016; du 13 septembre au 11 novembre 2016 et du 16 décembre 2016 au 13 janvier 2017. Le CEPD rendra donc son avis au plus tard le 31 janvier 2017.

[3] JO L 8 du 12.1.2001, p. 1.

règlement ou qui méritent une analyse plus approfondie. En ce qui concerne les aspects qui ne sont pas abordés dans le présent avis, le CEPD n'émet, sur la base des documents fournis, aucun commentaire.

a) Base juridique, données sensibles, licéité

Selon la notification, la base juridique du traitement est prévue aux articles 3, 5, 9, 10 et 11 du règlement (CE) nº 851/2004[4].

La licéité d'un traitement doit être justifiée sur la base de l'une des cinq conditions juridiques prévues à l'article 5 du règlement. La notification ne comprend aucune information quant à la licéité de l'essai de l'outil SIG. Le CEPD considère néanmoins que le traitement en cause doit être considéré comme licite aux termes de l'article 5, point a), du règlement.

Conformément à l'article 5, point a), du règlement, le traitement doit être nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités ou d'un autre acte législatif de l'UE.

En outre, le traitement en cause concerne des données relatives à la santé, qui sont considérées comme sensibles en vertu du règlement, et dont le traitement nécessite une base juridique spécifique. L'article 10, paragraphe 1, du règlement interdit le traitement de données à caractère personnel relatives à la santé, sauf si l'un des motifs visés à l'article 10, paragraphe 2, 3 ou 4, du règlement peut être invoqué.

L'article 10, paragraphe 4, du règlement dispose que «*sous réserve de garanties appropriées, et pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2 peuvent être prévues par les traités*» ou «***d'autres actes législatifs adoptés sur la base de ces traités***» (caractères gras ajoutés).

L'ECDC a pour mission «*de déceler, d'évaluer et de communiquer les menaces actuelles et émergentes que des maladies transmissibles représentent pour la santé*» afin de «*renforcer la capacité de la Communauté et de ses États membres à protéger la santé humaine en prenant des mesures de prévention et de contrôle des maladies humaines*»[5]. Le développement de l'outil SIG semble relever de cette mission, étant donné que (une fois que l'essai aura été achevé avec succès), l'outil sera mis à la disposition des épidémiologistes des États membres et il leur permettra de procéder à une analyse spatiale pendant les épidémies de légionellose. Cependant, cette base juridique n'est pas suffisamment spécifique étant donné que le traitement concerne des données sensibles. Les dispositions visées dans le règlement 851/2004 ne portent pas explicitement sur le développement d'un tel outil et, plus particulièrement, sur la nécessité de réaliser un essai sur la base de données relatives à la santé se rapportant aux personnes concernées. L'ECDC devrait prendre une décision en interne ou conclure un accord avec les États membres concernant le développement de cet outil spécifique (y compris la phase d'essai). Cette base juridique devrait notamment prévoir le développement de l'outil, ses liens avec les missions générales de l'ECDC, la nécessité d'entreprendre une phase d'essai reposant sur des

[4] Règlement (CE) nº 851/2004 du Parlement européen et du Conseil du 21 avril 2004 instituant un Centre européen de prévention et de contrôle des maladies (JO L 142 du 30.4.2004, p. 1)
[5] Article 3 du règlement (CE) 851/2004.

données réelles, l'utilisation ultérieure de l'outil par des entités nationales et le rôle de l'ECDC dans ce contexte[6].

L'ECDC devrait fournir au CEPD une copie de la décision interne ou de l'accord avec les États membres mentionnés ci-dessus. S'il n'existe aucun instrument juridique de la sorte, l'ECDC devrait en adopter un.

Le CEPD **recommande vivement** à l'ECDC de s'assurer de l'existence d'une base juridique spécifique, par exemple une décision interne de l'ECDC ou un accord avec les États membres, concernant le développement de l'outil SIG. S'il n'existe aucun instrument juridique de la sorte, l'ECDC devrait en adopter un. Le CEPD attend de recevoir une copie de la décision interne de l'ECDC ou d'un accord avec les États membres.

b) Information des personnes concernées

Lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement doit fournir à la personne concernée certaines informations conformément à l'article 12, paragraphe 1, du règlement. Le paragraphe 2 du même article prévoit une dérogation lorsque, en particulier pour un traitement à finalité de recherche historique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés.

Le CEPD salue le fait que l'ECDC ait l'intention de publier un avis concernant la protection des données sur la page web qui héberge l'outil SIG. Cependant, les informations requises devraient être fournies non seulement en publiant l'avis concernant la protection des données sur le site web de l'ECDC comme proposé, mais aussi en demandant au fournisseur de données, le NIHP, de prendre directement contact avec chaque personne concernée et de lui fournir l'avis concernant la protection des données rédigé par l'ECDC. Selon les informations fournies, moins de 50 personnes sont concernées (49 foyers à analyser). Par conséquent, il ne semble ni impossible ni disproportionné de prendre directement contact avec elles. Dès lors, l'exonération de l'obligation d'informer la personne concernée visée à l'article 12, paragraphe 2, ne semble pas applicable dans ce cas, à moins que le NIHP ne fasse valoir que l'information des personnes concernées se révélerait en effet impossible ou impliquerait des efforts disproportionnés[7].

Le CEPD attire l'attention de l'ECDC sur le fait qu'en sa qualité de responsable du traitement, il est responsable en dernier ressort de l'information des personnes concernées au titre du règlement et il doit donc s'assurer que le NIHP s'est correctement acquitté de cette mission pour son compte.

Le CEPD **recommande** à l'ECDC de publier un avis concernant la protection des données sur son site web, y compris toutes les informations pertinentes sur l'essai de l'outil SIG. En outre, l'ECDC devrait demander au fournisseur de données (NIHP) de prendre directement contact avec chaque personne concernée et de lui fournir l'avis concernant la protection des données, et de confirmer à l'ECDC qu'il s'est bien acquitté de cette mission (avant le début du traitement) à moins que cela ne se révèle impossible ou implique des efforts disproportionnés. Le CEPD attend de recevoir une copie de l'avis concernant la protection des données et de la demande adressée au NIHP concernant la diffusion aux personnes concernées de l'avis concernant la protection des données.

---

[6] À savoir comme sous-traitant seulement, ou chargé de gérer/améliorer l'outil et donc en tant que sorte de coresponsable du traitement.

[7] Voir dossier 2015-0082.

c) Droits des personnes concernées

L'ECDC indique dans la notification que les demandes d'exercice du droit d'accès, de rectification, de verrouillage, d'effacement et d'opposition doivent être adressées au fournisseur de données, c'est-à-dire le NIHP, étant donné que l'ECDC ne connaît pas l'identité des personnes concernées. L'ECDC indique qu'il publiera un avis à cet effet sur la page web où l'outil SIG est hébergé, informant le public qu'étant donné qu'il est impossible d'identifier les personnes d'après les données contenues dans l'outil SIG, les demandes émanant de ces personnes concernées seront adressées au fournisseur de données, qui sera peut-être en mesure de récupérer les informations.

Le CEPD souligne le fait que, en tant que responsable du traitement de l'essai, l'ECDC est chargé de veiller au respect du règlement, y compris l'octroi des droits des personnes concernées. Dans la pratique, étant donné que c'est le NIHP qui est en mesure d'identifier les personnes concernées, l'ECDC devrait déléguer au NIHP la tâche de centralisation de toutes les demandes concernant l'outil SIG. Le NIHP devrait, après avoir vérifié si la personne concernée figure dans la base de données, soumettre les demandes correspondantes (d'accès, de rectification, de verrouillage et d'effacement) à l'ECDC qui accordera les droits. Ce partage des responsabilités devrait être défini dans un accord entre l'ECDC et le NIHP et l'avis concernant la protection des données devrait être rédigé de sorte à refléter clairement ce partage des tâches.

Le CEPD **recommande** de définir le partage des responsabilités s'agissant des droits des personnes concernées dans un accord conclu entre l'ECDC et le NIHP. En outre, ce partage des tâches devrait être clairement reflété dans l'avis concernant la protection des données.

d) Mesures de sécurité

Selon l'article 22 du règlement, des mesures techniques et organisationnelles doivent être mises en œuvre pour empêcher, notamment, toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite. Ces mesures doivent assurer «*un niveau de sécurité approprié au regard des risques présentés par le traitement*».

Le CEPD a reçu la *politique de sécurité de l'information* de l'ECDC[8], dans laquelle le processus de *gestion des risques liés à la sécurité de l'information* est mentionné et défini. Il est aussi clairement indiqué dans ce document que le processus doit être appliqué à «*tous les systèmes d'information classés comme SPÉCIFIQUES*». Un système d'information prenant en charge un traitement soumis au contrôle préalable comme celui en cause mérite probablement d'être considéré comme tel[9]. Cependant, le processus mentionné ci-dessus n'a pas été appliqué à ce traitement et aucune *évaluation des risques liés à la sécurité de l'information* n'a été réalisée.

L'ECDC devrait réaliser une évaluation des risques liés à la sécurité de l'information suivant une méthode d'évaluation commune des risques liés à la sécurité de l'information qui tiendrait compte de tous les risques en la matière en lien avec le traitement de données à caractère personnel effectué sur la base de la notification.

[8] Ce document n'est plus d'actualité étant donné qu'il indique qu'il aurait dû être révisé au plus tard le 29 mai 2013.
[9] Les orientations de classification sur ce qui est STANDARD et ce qui est SPÉCIFIQUE ne permettent pas d'établir avec certitude si des «systèmes» soumis à un contrôle préalable devraient être STANDARD ou SPÉCIFIQUES.

Le CEPD invite dès lors l'ECDC à tenir compte de la liste non exhaustive suivante:

- Magerit[10],
- EBIOS[11], ou
- Octave[12].

Ces méthodes donnent des informations liées aux menaces, aux atouts, aux vulnérabilités, etc., et au processus en lui-même que l'ECDC pourrait envisager d'utiliser lorsqu'il réalise une évaluation des risques liés à la sécurité de l'information.

Le CEPD **recommande** à l'ECDC de réaliser une évaluation des risques liés à la sécurité de l'information en suivant une méthode d'évaluation commune des risques liés à la sécurité de l'information qui tiendrait compte de tous les risques en la matière en lien avec le traitement de données à caractère personnel effectué sur la base de la notification.

***

3) Recommandations et suggestions d'améliorations

Dans le présent avis, le CEPD a formulé des recommandations visant à garantir la conformité avec le règlement. Sous réserve de la mise en application des recommandations ci-dessus, le CEPD considère qu'il n'existe aucune raison de conclure à une violation des dispositions du règlement.

En ce qui concerne les **recommandations** suivantes, le CEPD attend leur **mise en application et des justificatifs** attestant de leur mise en application dans un délai de **trois mois** suivant la date de publication du présent avis:

1. S'assurer de l'existence d'une base juridique spécifique, par exemple une décision interne de l'ECDC ou un accord avec les États membres, concernant le développement de l'outil SIG.
2. Publier un avis concernant la protection des données sur le site web de l'ECDC, comprenant toutes les informations pertinentes sur l'essai de l'outil SIG et demander au fournisseur de données de prendre directement contact avec chaque personne concernée et de lui fournir un avis concernant la protection des données.
3. Définir le partage des responsabilités s'agissant des droits des personnes concernées dans un accord entre l'ECDC et le NIHP et veiller à ce que ce partage des tâches soit clairement reflété dans l'avis concernant la protection des données.

[10] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.VjHuoUbCfw0
[11] http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
[12] http://www.cert.org/resilience/products-services/octave/

4. Réaliser une évaluation des risques liés à la sécurité de l'information suivant une méthode d'évaluation commune des risques liés à la sécurité de l'information.

Fait à Bruxelles, le 17 janvier 2017

Wojciech Rafał WIEWIÓROWSKI