Avis de contrôle préalable

"Gestion des rapports d'incidents – Cour de justice"
Case 2013-0786

***

La Cour de justice a confié à une société de gardiennage le soin d'établir des rapports en cas d'incidents concernant toute anomalie, dysfonctionnement, secours à la personne ou problème lié à la sécurité ou à la sûreté des personnes, des biens et des immeubles survenant dans l'enceinte de la Cour. Ces rapports peuvent contenir des données personnelles, par exemple au sujet de personnes victimes d'un accident, d'un incendie, d'un malaise ou encore surprises en train de commettre un vol dans les locaux de la Cour.

***

Bruxelles, le 12 septembre 2016

Adresse postale : rue Wiertz 60 - B-1047 Bruxelles
Bureaux : rue Montoyer 30 - B-1000 Bruxelles
E-mail : edps@edps.europa.eu - Site Internet : http://www.edps.europa.eu
Tél.: 32-2-283 19 00 - Fax : 32-2-283 19 50

1. Procédure

Le 27 juin 2013, le Contrôleur européen de la protection des données (ci-après le "***CEPD***") a reçu de la Cour de justice de l'Union européenne (ci-après "***la Cour***") une notification pour contrôle préalable au titre de l'article 27 §2(a) du règlement n° 45/2001 (ci-après "***le règlement***") concernant la gestion des rapports d'incidents.

La notification était accompagnée des annexes suivantes :

- une description des mesures de sécurité;
- la notice informative concernant le traitement des données personnelles;
- la réglementation du Grand-Duché de Luxembourg du 16 octobre 1997 sur la protection des travailleurs - Prescriptions de sécurité types (ITM-ET 32.10) (ci-après "***la réglementation ITM-ET***");
- un extrait du contrat de gardiennage CJ-03/2010[1].

Divers échanges de correspondance ont eu lieu entre la Cour et le CEPD. Des documents complémentaires[2] et une notification modifiée ont été communiqués au CEPD le 16 mars 2016.

S'agissant d'un contrôle préalable *ex post*, le délai de deux mois dans lequel le CEPD doit, en principe, rendre son avis ne s'applique pas[3].

2. Faits pertinents

En 2010 la Cour a contracté avec une société de gardiennage pour prester des services de sécurité générale et de sécurité incendie. Dans ce cadre, les agents de ladite société ont l'obligation de rédiger des **rapports d'incidents** concernant toute anomalie, dysfonctionnement, secours à la personne ou problème lié à la sécurité ou à la sûreté des personnes, des biens et des immeubles survenant dans l'enceinte de la Cour. Ces rapports sont transmis par e-mail à la Section Sécurité et Sureté (rattachée à la Direction des Bâtiments de la Cour) dans un délai de 24 heures. Tous les matins ouvrés, une synthèse des rapports des dernières 24 heures est établie et transmise par e-mail à la Section Sécurité et Sureté. Environ 1.500 à 2.000 rapports d'incidents sont établis chaque année.

2.1. Base légale et licéité du traitement

Selon la Cour, les **bases légales** du traitement sont:
- l'article 26 de la réglementation ITM-ET (Inspection du Travail et des Mines luxembourgeoise); cette disposition concerne les installations de sécurité (dispositifs anti-

[1] La Cour a ultérieurement produit une copie de l'intégralité des contrats de gardiennage pertinents: contrat CJ-03/2010 applicable pour la période du 16/12/2010 au 15/07/2015 et contrat CJ 12-2014 applicable pour la période du 16/07/2015 au 15/07/2020.

[2] Modèle de rapport d'incident; modèle de rapport de synthèse; extrait du cahier des charges relatif aux prestations de la société de gardiennage.

[3] Le CEPD a adressé une série de questions au DPD en date du 18 décembre 2013, ainsi qu'un rappel et un projet d'exposé des faits en date du 16 octobre 2015. Le DPD y a répondu le 16 novembre 2015. Le projet d'avis a été envoyé au DPD de la Cour le 16 juin 2016. La Cour a communiqué ses commentaires le 5 août 2016.

incendie, de surveillance de l'air, de détection des gaz, etc.) et l'obligation de tenir des registres des vérifications effectuées sur ces installations;
- l'article 4.2 du Cahier des Charges relatif aux prestations de la société de gardiennage "GS4 Security Services"; cette disposition oblige la société de gardiennage à (i) mettre en place une gestion informatisée des rapports d'incidents et de leur suivi; (ii) remettre à la Cour tous les rapports d'activités exigés par celle-ci.

La notification initiale faisait également référence au "*Schéma Directeur de mise en sureté globale du complexe immobilier de la Cour de justice de l'UE*". La notification mise à jour ne fait plus état de ce document[4].

Les bases de **licéité** du traitement sont les articles 5(a) et 10 §2, b) du règlement.

2.2. Les personnes concernées

Il s'agit des personnes impliquées dans un incident se produisant dans les bâtiments de la Cour ou ses environs immédiats, qu'elles fassent partie ou non du personnel de la Cour.

2.3. Catégories de données

Les **rapports d'incidents** peuvent contenir les données personnelles suivantes:

- coordonnées des personnes impliquées dans l'incident (noms et prénoms, numéros de téléphone et de télécopieur, adresse de courrier électronique);
- informations contenues dans les documents d'identité de ces personnes (passeport, permis de conduire...);
- nature des faits (accident, vol, secours à une personne, état de santé de la victime, suspicion d'infraction, etc.);
- numéros d'immatriculation des véhicules;
- lieu, date, heure et origine de l'incident;
- dégâts constatés et actions provisoires.

Outre les rapports d'incidents, la société de gardiennage prépare chaque matin ouvré une **synthèse** des rapports établis dans les dernières 24 heures en les regroupant selon cinq catégories :
- incidents techniques;
- incidents liés à la sécurité incendie;
- incidents liés à la sûreté;
- secours à la personne
- divers.

Cette synthèse consiste en un tableau reprenant le nombre d'incidents par catégories, l'objet de chaque rapport, son numéro ainsi que des observations.

2.4. Destinataires des données

Les rapports d'incidents et les synthèses des rapports sont transmis par voie électronique (e-mail) en format pdf.

[4] Voir e-mail du DPD de la Cour de justice du 16 mars 2016.

Les **destinataires** de ces données sont:
- les fonctionnaires et agents de la Section Sécurité et Sûreté de la Cour[5];
- le directeur des bâtiments;
- les agents de la société de gardiennage qui assurent les fonctions de sécurité;
- les autorités administratives et pénales luxembourgeoises en vue de l'exercice de leurs compétences en matière de poursuite d'infractions (destinataires relevant de la législation nationale adoptée en application de la directive 95/46/CE). Selon la portée de l'incident, la Section Sécurité et Sûreté peut transmettre le rapport à ces autorités.

D'autres destinataires sont susceptibles de recevoir les données dans des cas particuliers[6].

2.5. Information fournie aux personnes concernées

Personnel de la Cour: une notice informative[7] et la notification du traitement sont disponibles sur l'intranet de la Cour.

Autres personnes: la notice d'information n'est pas disponible sur le site internet de la Cour[8]. Les agents de sécurité assignés à la réception du public tiennent une version papier de la notice à disposition du public.

2.6. Stockage, mesures de sécurité et délai de conservation des données

[...]

Le **délai de conservation** des rapports est de 10 ans et un jour. Selon le responsable du traitement, cette durée, qui ne résulte pas d'une obligation légale, est fondée sur un usage général au Grand-Duché de Luxembourg en matière de gestion des registres de sécurité[9].

Aucun archivage papier n'est prévu.

---

[5] L'unité Affaires immobilières et sécurité de la Cour, mentionnée dans la notification initiale, a entre-temps été supprimée. La Section sécurité et sûreté est désormais directement rattachée à la Direction des Bâtiments.

[6] - le Président et le Greffier de la Cour et les fonctionnaires qui les assistent dans le cadre des responsabilités qui leur sont dévolues par l'article 20, paragraphe 4, du règlement de procédure de la Cour;
- la Cour de justice, le Tribunal et/ou le Tribunal de la fonction publique, ou un juge national, ainsi que les avocats et agents des parties dans l'hypothèse d'un litige;
- l'instance de la Cour, du Tribunal ou du TFP chargée d'examiner les réclamations, le Président et le Greffier de la juridiction concernée, ainsi que le conseiller juridique pour les affaires administratives, en cas de réclamation introduite en application de l'article 90, paragraphe 2, du statut des fonctionnaires;
- l'OLAF en cas d'enquête effectuée en application du règlement n° 883/2013 et de la décision de la Cour de justice du 12 juillet 2011 relative aux conditions et modalités des enquêtes internes en matière de lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts de l'Union européenne;
- l'auditeur interne dans le cadre des fonctions qui lui sont dévolues par les articles 98 et 99 du règlement n°966/2012 relatif aux règles financières;
- le CEPD conformément à l'article 47, paragraphe 2, du règlement;
- le DPD de la Cour conformément au point 4 de l'annexe du règlement;
- le Médiateur européen dans le cadre de l'article 228 TFUE.

[7] Jointe à la notification.

[8] Précision communiquée par le DPD par e-mail du 5 août 2016.

[9] L'article 26 de la réglementation ITM-ET prévoit que les registres doivent être tenus à la disposition des organes de contrôle, c'est-à-dire de l'Inspection du Travail et des Mines. Aucune durée de conservation n'est, en revanche, prévue.

3. Analyse légale

3.1. Contrôle préalable

Le traitement de données personnelles est effectué par une institution de l'Union européenne à l'aide de procédés partiellement automatisés. Par conséquent, le règlement est applicable. Cette activité de traitement est soumise à un contrôle préalable du CEPD car elle présente des risques particuliers, liés au traitement d'informations relatives à la santé et à des suspicions d'infractions (Article 27 §2 a) du règlement)[10].

3.2. Base légale et licéité

Des rapports d'incidents peuvent être établis dans des circonstances et pour des finalités très diverses:
- sécurité technique des installations (y compris incendies) et subséquemment indirectement des personnes;
- sécurité des personnes (employées ou non par la Cour) sans lien avec les installations (vol, etc.);
- santé des personnes (employées ou non par la Cour) sans lien avec les installations (malaise, accident).

a. Base légale

La Cour mentionne deux bases légales à l'appui du traitement:
- l'article 26 de la réglementation ITM-ET;
- l'article 4.2 du Cahier des Charges relatif aux prestations de la société de gardiennage "GS4 Security Services"[11] .

Compte tenu de son champ d'application[12], la réglementation ITM-ET ne constitue une base légale au traitement que pour les rapports liés à la sécurité des installations. Quant au cahier des charges, il ne constitue pas la base légale du traitement (établissement de rapports) en soi, mais uniquement de la sous-traitance de cette activité à la société de gardiennage.

Par conséquent, la Cour doit adopter une décision interne prévoyant l'établissement de rapports pour les différentes finalités décrites ci-avant.

b. Licéité

[10] L'article 27 du règlement soumet au contrôle préalable du CEPD les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités. L'article 27(2) du règlement énumère les traitements susceptibles de présenter de tels risques, et notamment au point a), les traitements de données relatives à des suspicions, infractions condamnations pénales ou mesures de sûreté. Par contre, les traitements qui n'impliquent de telles données qu'exceptionnellement ou ponctuellement ne sont pas soumis au contrôle préalable. Vu les éléments fournis par la Cour, il ne semble pas que cela soit le cas ici; le traitement est donc soumis au contrôle préalable.
[11] Voir résumé des faits pertinents, section 2.1.
[12] Voir Article 1er - Objectif et domaine d'application.

Pour les **rapports d'incidents liés à la sécurité technique** des installations **et aux incendies**, le traitement peut être considéré comme licite en vertu de l'article 5(a) (à la lumière du considérant 27 du règlement).

Les traitements de données effectués dans les **rapports d'incidents de santé** (par ex.: malaise d'un employé ou d'une personne extérieure), ainsi que dans les rapports **de sécurité non liés aux installations** (vols et autres infractions dans les bâtiments et leurs alentours immédiats), sont licites en vertu des mêmes dispositions, sous réserve de l'adoption d'une décision interne de la Cour prévoyant l'établissement de tels rapports (voir point a. ci-avant).

Les différents types de rapports susmentionnés peuvent inclure des données liées à la santé et des suspicions d'infractions, y compris les rapports concernant la sécurité des installations[13]. Le traitement de ces catégories de données est licite respectivement en vertu des articles 10(2)(a) (pour les personnes extérieures à la Cour - si un consentement valide a été donné), (b) (pour le personnel de la Cour) et 10(5) du règlement. Cependant, afin de renforcer la licéité du traitement, en particulier concernant les personnes qui ne font pas partie du personnel de la Cour, la décision susmentionnée devrait expressément prévoir que les rapports sont susceptibles d'inclure ce type de données.

Les mêmes règles s'appliquent aux synthèses des rapports dans la mesure où elles comportent des données personnelles.

Au demeurant, comme indiqué à la section 3.3. ci-dessous, il convient de **limiter** autant que faire se peut **la collecte** de données personnelles, en particulier celles visées à l'article 10 du règlement.

Recommandation

1. Adopter une décision interne prévoyant l'établissement de rapports d'incidents pour les différentes catégories de rapports susmentionnés et autorisant dans ce cadre le traitement de catégories particulières de données mentionnées à l'article 10 du règlement.
2. Veiller, en cas de collecte de données relatives à la santé de personnes extérieures à la Cour, d'obtenir l'accord de ces dernières sur le traitement de leurs données, conformément à l'article 10(2)(a) du règlement; donner des instructions en ce sens à la société de gardiennage.

3.3. Qualité des données

En vertu de l'article 4(1)(c) du règlement, les données traitées doivent être "*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement*". Selon la notification et la notice informative et compte tenu du format du rapport d'incident, les agents de sécurité sont susceptibles de collecter un grand nombre de données. Il revient à la Section de Sécurité et Sureté de rappeler au sous-traitant de ne traiter que les données adéquates, pertinentes et limitées à ce qui est strictement nécessaire au regard des finalités pour lesquelles elles sont traitées, à savoir l'établissement de rapports permettant à la Cour de prendre, le cas échéant, les mesures de suivi qui s'imposeraient en matière de sécurité

[13] Par ex.: personnes blessées suite à incident des installations, personnes soupçonnées d'avoir saboté une installation.

et de sûreté Ainsi, dans la plupart des cas, la collecte de données relatives à la santé des personnes concernées ne semble pas nécessaire au regard de cet objectif.

Recommandation

3. Rappeler à la société de gardiennage le principe de minimisation des données, en particulier en ce qui concerne les données relatives à la santé.

3.4. Sous-traitant

En vertu de l'article 23 du règlement, si un traitement de données est réalisé par un sous-traitant pour le compte du responsable du traitement, un contrat ou un acte juridique doit être conclu entre le sous-traitant et le responsable du traitement. Le contrat doit prévoir que le sous-traitant agira selon les instructions du responsable du traitement (pour ce qui est du traitement des données). Le sous-traitant doit assurer la conformité avec les obligations de confidentialité et de sécurité établies, en l'espèce, dans les règles nationales applicables mettant en œuvre l'article 17 de la directive 95/46/CE.

Cette obligation est satisfaite par les contrats conclus avec le sous-traitant[14]. [...]

3.5. Information des personnes concernées

Les articles 11 et 12 du règlement établissent les modalités d'information des personnes concernées afin d'assurer à l'égard des personnes concernées un traitement transparent et loyal des données.

En ce qui concerne les **destinataires des données**, la notification et la notice informative mentionnent de nombreux destinataires potentiels, dont le Médiateur européen et le CEPD. Pour information, le CEPD rappelle que les autorités recevant des données à caractère personnel dans le cadre d'enquêtes spécifiques ne sont pas considérées comme des "destinataires" au sens de l'article 2(g) du règlement et n'ont pas à être mentionnées comme tels dans la notice informative.

En ce qui concerne la **base juridique du traitement**, elle doit être modifiée conformément à la recommandation n° 1.

Recommandation

5. Compléter la notification et la notice informative en ce qui concerne la base juridique du traitement, conformément à la recommandation n° 1.
6. Publier la notice informative sur le site internet de la Cour de justice.

3.6. Durée de conservation des données

En vertu de l'article 4(1)(e) du règlement, les données à caractère personnel doivent être *"conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement"*.

[14] Article 16.2 du contrat du 16 novembre 2010 et article II.6.1 du contrat du 1er juillet 2015.

Le délai de conservation indiqué dans la notification est de 10 ans. La Cour déclare se référer à cet égard à un usage général au Grand-Duché de Luxembourg en matière de gestion des registres de sécurité.

Cette durée de conservation particulièrement longue, qui n'a pas de fondement légal et qui est appliquée sans distinguer le type de rapport, la gravité de l'incident et les suites données aux rapports, est disproportionnée et ne respecte pas le prescrit de l'article 4(1)(e) du règlement.
S'il peut être justifié, au regard d'un usage général au Grand-Duché de Luxembourg, de conserver les rapports d'incidents liés à la sécurité des installations pendant 10 ans, cette durée ne semble pas justifiée par exemple pour un rapport d'incident relatant un accrochage intervenu entre deux véhicules dans un parking de la Cour n'ayant occasionné que des dégâts matériels peu importants ou un rapport sur un malaise léger ressenti par un visiteur de la Cour.

La durée de conservation des rapports et des synthèses de rapports devrait être réévaluée par la Cour.

Recommandation

7. Réévaluer la durée de conservation des rapports et des synthèses de rapports en tenant compte notamment de la nature des rapports et des suites qui y sont données.

* *
*

Sous réserve des rappels et recommandations figurant dans le présent avis, le traitement de données effectué par la Cour dans le cadre de la gestion des rapports d'incidents semble être en conformité avec le règlement.

Le CEPD invite la Cour à lui communiquer, dans un délai de **quatre mois**, les mesures prises pour se conformer aux recommandations formulées dans le présent avis.

Fait à Bruxelles, le 12 septembre 2016

(signé)

Wojciech RAFAŁ WIEWIÓROWSKI