

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES



**RAPPORT
ANNUEL**

| 2016

Résumé

Des informations complémentaires sur le CEPD sont disponibles sur notre site internet: <http://www.edps.europa.eu>.

Le site internet donne aussi des informations sur l'[abonnement](#) à notre newsletter.

**Europe Direct est un service destiné à vous aider à trouver
des réponses aux questions que vous vous posez
sur l'Union européenne.**

**Un numéro unique gratuit (*):
00 800 6 7 8 9 10 11**

(*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

De nombreuses autres informations sur l'Union européenne sont disponibles sur l'internet via le serveur Europa (<http://europa.eu>).

Luxembourg: Office des publications de l'Union européenne, 2017

Print	ISBN 978-92-9242-206-6	ISSN 1831-0516	doi:10.2804/151658	QT-AB-17-001-FR-C
PDF	ISBN 978-92-9242-241-7	ISSN 1977-8341	doi:10.2804/50825	QT-AB-17-001-FR-N

© Union européenne, 2017

© Photos: iStockphoto/EDPS & Union européenne

Reproduction autorisée, moyennant mention de la source



RAPPORT ANNUEL

| 2 0 1 6

Résumé

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

| Introduction

L'année 2016 a été riche en événements importants, dont il est encore trop tôt pour prédire les répercussions à long terme. Mais, avec sa réforme de la législation sur la protection des données, l'Union européenne a certainement accompli le travail d'une génération entière. Le règlement général sur la protection des données (RGPD) et la directive sur la protection des données en matière pénale et judiciaire, qui ont été publiés au Journal officiel l'année dernière, pourraient se révéler être une avancée majeure non seulement pour les droits fondamentaux à l'ère numérique mais aussi, dans le sens où ils sont le fruit de plusieurs années d'habiles négociations, pour la démocratie européenne.

Le RGPD a toujours été, et restera, notre point de référence. Comme indiqué dans la stratégie relative à notre mandat, notre mission consiste à rendre la protection des données aussi simple et efficace que possible pour toutes les parties concernées. Le RGPD revêt une importance stratégique pour notre institution car il définit les paramètres du traitement des données et du contrôle au sein même des institutions de l'Union européenne. Nous promovons activement le concept de responsabilisation auprès des dirigeants des institutions et organes de l'Union européenne, en mettant à leur disposition des outils pratiques qui leur permettent d'assurer et de démontrer la conformité à la réglementation. Dans le cadre de nos activités en tant qu'autorité de contrôle et que médiateur au service des citoyens, nous avons constaté que le public prenait de plus en plus conscience de l'importance de la protection des données à caractère personnel. Aujourd'hui plus que jamais, les citoyens sont conscients des risques qu'ils encourent si leurs données personnelles ne sont pas gérées de manière responsable; il est de notre devoir, et de celui de toutes les autorités chargées de la protection des données (APD), de veiller à ce qu'elles le soient.

Comme les autres APD, et en tant qu'autorités de contrôle et que conseillers des personnes en charge de l'élaboration, de l'examen et de la révision de la législation, nous avons déployé une énergie considérable pour nous préparer à l'entrée en vigueur des nouvelles dispositions. Nous travaillons en étroite collaboration avec le groupe de travail «Article 29» afin d'être sûrs de pouvoir assister efficacement le nouveau comité européen de la protection des données, et nous avons renforcé et intensifié notre coopération loyale avec d'autres autorités réglementaires à travers le monde.

Nous savons également que, pour être efficaces, les APD doivent être au fait des technologies fondées sur des données. Notre document de référence sur l'intelligence artificielle représente un pas dans cette direction. Les APD devront faire en sorte que nous soyons préparés à affronter les changements amenés par le progrès technologique.

Les flux de données sont une réalité mondiale et l'année 2016 pourrait bien avoir marqué un tournant dans la régulation de ces flux. Nous avons conseillé le législateur européen sur l'*accord-cadre* et le «bouclier de protection des données» (Privacy Shield) concernant les transferts de données entre l'Union européenne et les États-Unis, et nous avons dialogué avec des commissaires à la protection des données et au respect de la vie privée de chaque continent afin de tenter d'établir un nouveau consensus sur les droits à l'ère numérique.

Nous sommes conscients du fait que la législation sur la protection des données ne s'applique pas isolément et, en janvier 2016, nous avons mis sur pied le groupe consultatif sur l'éthique. Ce groupe composé de six personnalités éminentes, toutes expertes dans leurs domaines respectifs, est chargé de trouver des moyens innovants et efficaces d'assurer le respect des valeurs européennes à l'ère de l'omniprésence des données et des machines intelligentes. Nous avons également mis en place une «Digital Clearing House» (chambre de compensation numérique) pour permettre aux autorités des domaines de la concurrence, de la protection des consommateurs et de la protection des données de partager des informations et des idées sur la meilleure façon de servir l'intérêt des citoyens dans des cas spécifiques.

L'un des éléments innovants du RGPD est l'obligation faite à chaque responsable du traitement des données de désigner un délégué à la protection des données (DPD). Les institutions de l'Union européenne collaborent avec les DPD depuis près de vingt ans, et ce grâce au règlement (CE) n° 45/2001. Nous espérons et sommes convaincus que, avec notre aide, elles deviendront une figure de proue du traitement responsable des données; un exemple dont pourront s'inspirer les responsables du traitement des données, aussi bien dans le secteur public que dans le secteur privé.

Ce sera là notre priorité.



Giovanni Buttarelli
Contrôleur européen de la protection des données



Wojciech Wiewiórowski
Contrôleur adjoint

Vue d'ensemble de 2016

Dans notre [stratégie 2015-2019](#), nous avons exposé notre vision, celle d'une Union européenne qui montre l'exemple dans le dialogue mondial sur la protection des données et le respect de la vie privée à l'ère numérique. Le 4 mai 2016, le [règlement général sur la protection des données](#) (RGPD) a été publié au Journal officiel de l'Union européenne, ce qui représente un grand pas vers la réalisation de cet objectif. Le RGPD permettra de définir une norme numérique mondiale pour le respect de la vie privée et la protection des données, une norme axée sur les individus, leurs droits et leurs libertés ainsi que sur leur identité personnelle et leur sécurité. Il reste toutefois beaucoup à faire pour transformer cette vision en réalité.



Se préparer aux changements à venir

En 2016, notre travail a essentiellement porté sur la préparation au RGPD et sur sa mise en œuvre. Nous avons travaillé en étroite coopération avec nos collègues du [groupe de travail «Article 29»](#) (G29), d'une part pour élaborer un document d'orientation sur la nouvelle législation et, d'autre part, pour nous préparer à assurer le secrétariat du nouveau comité européen de la protection des données et à y intervenir en tant que membre indépendant.

La nouvelle législation prévoit le remplacement du G29 par le comité européen de la protection des données, qui sera chargé de veiller à ce que le RGPD soit appliqué de façon uniforme dans les différents pays de l'Union. Il est donc primordial que ce comité soit pleinement opérationnel pour le 25 mai 2018, date à partir de laquelle s'appliquera le RGPD. Tout au long de

l'année 2016, nous avons travaillé main dans la main avec le G29 afin de jeter les bases d'un règlement intérieur et d'examiner les différentes possibilités d'accords en matière d'informatique, de budget et de niveau de service pour ce nouvel organisme.

Si nous voulons que l'Europe reste à l'avant-garde du débat sur la protection des données et le respect de la vie privée, nous devons aussi mettre en place un cadre juridique moderne sur le respect de la vie privée dans les communications électroniques qui, à la fois, garantisse le droit fondamental à la confidentialité des communications et complète les protections prévues dans le RGPD. À la demande de la Commission, en juillet 2016, nous avons formulé un [avis](#) préliminaire sur la proposition de réexamen de la directive «vie privée et communications électroniques». Nous continuerons, tout au long du processus de négociation, de plaider en faveur d'une directive renforcée, plus intelligente et plus claire, dont la portée reflète véritablement les réalités technologiques et sociologiques du monde numérique.

Faire avancer le débat au niveau mondial



Dans le cadre de notre stratégie, nous nous sommes engagés à développer une dimension éthique de la protection des données. En janvier 2016, nous avons mis sur pied le [groupe consultatif sur l'éthique](#), qui est chargé d'examiner l'éthique numérique sous différents points de vue théoriques et pratiques. Notre objectif était de lancer un débat international sur la dimension éthique de la protection des données à l'ère numérique.

Le groupe a tenu son premier atelier en mai 2016. Il poursuivra ses activités jusqu'en 2018 et présentera ses conclusions lors de la conférence internationale des commissaires à la protection des données et à la

vie privée, qui sera organisée par le CEPD et l'APD bulgare.

La session à huis clos de la conférence internationale de 2016 a été consacrée à un thème également tourné vers l'avenir: les répercussions de l'intelligence artificielle, de l'apprentissage automatique et de la robotique sur la protection des données et le respect de la vie privée. Dans sa stratégie, le CEPD s'est engagé à faire en sorte que la protection des données devienne numérique. Nous avons donc voulu enrichir et guider le débat à ce sujet en publiant un [document de référence](#) pour alimenter les discussions lors de la conférence, document qui a reçu un accueil très favorable.

La technologie évolue sans cesse, et il est essentiel que toutes les autorités en charge de la protection des données, y compris le CEDP, se préparent aux défis que poseront ces évolutions. Pour aider à relever ces défis, le CEPD a créé en 2014 le [réseau d'ingénierie de la vie privée sur Internet](#) (IPEN). Le groupe, composé d'experts des technologies de l'information issus de tous les horizons, sert de plateforme de coopération et d'échange d'informations sur les méthodes et outils d'ingénierie qui intègrent les exigences relatives à la protection des données et au respect de la vie privée dans les nouvelles technologies. L'adoption du RGPD, qui impose à toute personne responsable du traitement de données à caractère personnel de respecter les principes de [protection des données dès la conception](#) et de protection des données par défaut, a donné davantage de visibilité au groupe et à ses activités, et a incité les chercheurs, les développeurs et les autorités de réglementation en charge de la protection des données à redoubler d'efforts pour renforcer et améliorer la dimension technologique de la protection des données.

Les institutions européennes montrent l'exemple

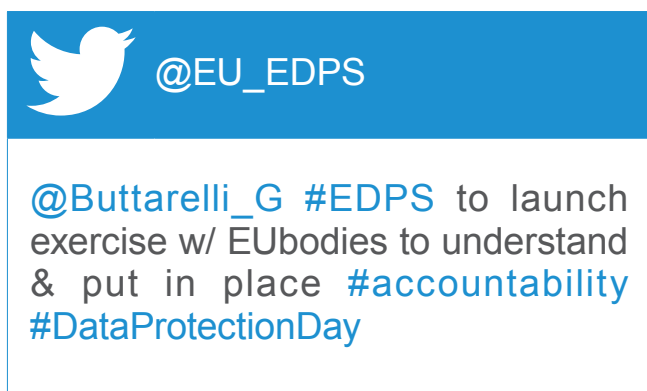
Toutefois, si nous voulons réussir à imposer l'Union européenne comme leader de la protection des données sur la scène mondiale, il est essentiel que les institutions de l'Union montrent l'exemple au niveau européen. En tant qu'autorité indépendante chargée de contrôler le traitement des données à caractère personnel à ce niveau, nous travaillons activement aux côtés des institutions et organes de l'Union européenne afin de les aider à se préparer aux changements à venir. S'il est vrai que le RGPD ne s'applique pas à leurs activités, les dispositions qui régissent ces activités seront adaptées et alignées sur le RGPD au cours de l'année 2017.



En 2016, nous avons poursuivi nos efforts pour développer et renforcer notre coopération avec les [délégués à la protection des données](#) (DPD) des institutions et organes de l'UE. Ces délégués à la protection des données, qui veillent à ce que les institutions auxquelles ils appartiennent se conforment à la législation sur la protection des données, sont nos partenaires les plus proches au niveau institutionnel. Tout au long de l'année, nous avons travaillé à leurs côtés, tant au niveau collectif qu'au niveau individuel, afin de les préparer aux changements législatifs. Nous les avons notamment familiarisés avec de nouveaux concepts, tels que les [analyses d'impact relatives à la protection des données](#), que les nouvelles dispositions rendront probablement obligatoires, comme elles le sont dans le RGPD, et nous avons continué de leur fournir des conseils au travers de [lignes directrices](#) et d'[avis de contrôle préalable](#). Nous avons également sollicité leur point de vue sur la révision du [règlement \(CE\) n° 45/2001](#) avant de conseiller le législateur à ce sujet.

Le RGPD fait explicitement référence au principe de [responsabilisation](#), dont nous pouvons raisonnablement supposer qu'il s'appliquera également aux institutions et organes de l'UE. Il exige que les organisations mettent en place des mesures techniques et organisationnelles transférant la responsabilité de démontrer la conformité reposant sur les autorités chargées de la protection des données (APD) et les délégués à la protection des données (DPD), aux organisations elles-mêmes. En 2016, nous avons lancé l'«Accountability Initiative» (initiative de responsabilisation), destinée à donner aux institutions de l'UE, à commencer par le CEPD lui-même en sa qualité de responsable du traitement, les moyens de montrer la voie à suivre pour se conformer et démontrer leur conformité aux [règles en matière de protection des données](#). Dans le cadre de cette initiative, nous avons mis au point un *outil* d'évaluation de la responsabilisation, que nous avons d'abord expérimenté sur nous-mêmes, en tant qu'institution.

Nous avons ensuite rencontré les plus hauts responsables de sept organes de l'UE afin de promouvoir notre initiative, et nous poursuivrons ce processus en 2017.



Au cours de l'année, nous avons également publié plusieurs [lignes directrices](#) à l'intention des institutions européennes. Les lignes directrices du CEPD fournissent des conseils pratiques sur la façon de se conformer aux dispositions relatives à la protection des données dans des situations spécifiques. Elles servent de documents de référence sur lesquels les institutions peuvent se fonder pour évaluer leurs activités et, à ce titre, constituent un outil très utile pour améliorer la responsabilisation. Le plus souvent, nos lignes directrices peuvent aussi se rapporter et s'appliquer au travail d'autres organisations.

Les communications numériques jouant un rôle de plus en plus important dans le travail quotidien des institutions européennes, nous avons publié, en novembre 2016, des lignes directrices sur les services en ligne et sur les applications mobiles. Ces documents proposent des conseils pratiques sur la façon d'intégrer les principes de la protection des données dans le développement et la gestion des services en ligne et des applications mobiles, et présentent les avis d'experts des institutions et organes de l'UE, ainsi que de DPD, en veillant à ce qu'ils demeurent pertinents dans la pratique et ne se résument pas à une simple approche théorique. Nous avons également publié un [document d'orientation](#) sur la gestion des risques liés à la sécurité de l'information (Information Security Risk Management – ISRM), conçu pour aider les responsables de la sécurité de l'information à analyser efficacement les risques pour la protection des données et à définir un ensemble de mesures de sécurité à mettre en œuvre, afin de respecter les principes de conformité et de responsabilisation.

Plusieurs de nos lignes directrices ont été élaborées dans le but d'aider les institutions européennes à se conformer aux spécifications du [statut des fonctionnaires de l'Union européenne](#) tout en respectant les droits au respect de la vie privée et à la protection des données. En juillet 2016, nous avons publié des [lignes directrices](#) relatives au traitement d'informations à caractère personnel dans le cadre d'une procédure d'alerte éthique. Ces lignes directrices contiennent des recommandations sur la façon d'établir des procédures sûres pour signaler les fraudes, assurer la confidentialité des informations reçues et protéger l'identité de toute personne en lien avec l'affaire concernée.

En novembre 2016, nous avons publié des [lignes directrices](#) relatives au traitement des informations à caractère personnel dans le cadre d'enquêtes administratives et de procédures disciplinaires. Ce document fournit aux institutions européennes le cadre juridique nécessaire pour mener des enquêtes administratives et garantir que les procédures pertinentes sont mises en œuvre en traitant les données à caractère personnel de façon légale, juste et transparente, dans le respect de leurs obligations en matière de protection des données.

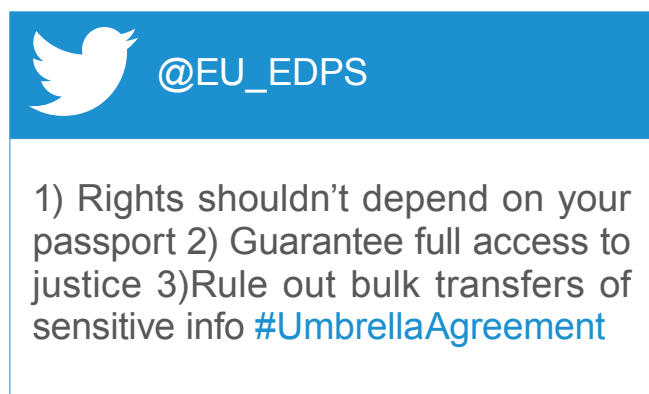


Le CEPD s'est également préparé à assumer de nouvelles responsabilités de contrôle. Le nouveau cadre juridique d'Europol, approuvé le 11 mai 2016, prévoit en effet que le CEPD prenne en charge le contrôle du traitement des données à caractère personnel au sein d'Europol, et qu'il assure le secrétariat d'un nouveau conseil de coopération. Ce conseil doit faciliter la coopération entre nous-mêmes et les APD nationales dans les affaires liées aux données provenant des États membres. Cette nouvelle compétence constitue un nouveau défi, que le CEPD et Europol s'efforceront de relever d'une façon qui reflète le professionnalisme et la fiabilité des institutions de l'UE dans le domaine de la protection des données.

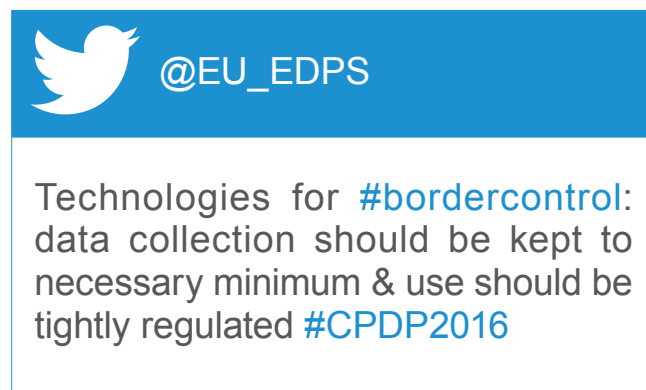
Une approche responsable des politiques communautaires

Pour que le RGPD reste crédible sur la scène internationale, il est essentiel que le niveau d'exigence élevé qu'il impose soit encouragé dans toutes les politiques de l'Union. En notre qualité de conseiller de la Commission, du Parlement et du Conseil, notre but est de faire en sorte que tel soit le cas. En 2016, l'Union a entrepris l'élaboration de nouvelles politiques, notamment dans deux domaines particulièrement importants: les transferts de données internationaux et la gestion des frontières.

À la suite de l'invalidation de la décision «Sphère de sécurité» (Safe Harbour) par la Cour de justice de l'Union européenne en 2015, la Commission a négocié avec les États-Unis une nouvelle décision d'adéquation au sujet de laquelle nous avons été consultés en 2016. Dans notre avis concernant le «Bouclier de protection des données» (Privacy Shield), qui prévoit le transfert de données entre l'Union européenne et les États-Unis, nous avons demandé un renforcement du système d'autocertification tout en insistant sur la nécessité de renforcer les garanties concernant l'accès des autorités publiques américaines aux données à caractère personnel et d'améliorer les mécanismes de surveillance et de recours.



Nous avons également publié un [avis](#) relatif à l'*accord-cadre* entre les États-Unis et l'Union européenne concernant la protection des données à caractère personnel transférées entre l'Union européenne et les États-Unis à des fins répressives. Dans nos recommandations, nous avons souligné la nécessité de veiller à ce que l'accord fasse respecter les droits fondamentaux, notamment en ce qui concerne le recours juridictionnel. Nous avons aussi insisté sur la nécessité de renforcer les garanties pour tous et noté qu'il était important de clarifier que l'accord interdit les transferts massifs de données sensibles.



La politique en matière de frontières a continué d'occuper le devant de la scène européenne en 2017, et l'Union a lancé plusieurs nouvelles initiatives stratégiques visant à sécuriser ses frontières. La législation dans ce domaine soulève des questions particulièrement épineuses, qui nécessitent de trouver un équilibre entre le besoin de sécurité et le droit à la protection des données.

En 2016, nous avons publié des [recommandations](#) sur la façon de garantir le respect des droits des migrants et des réfugiés, en réponse à la proposition de règlement relatif au corps européen de garde-frontières et de garde-côtes. Dans le prolongement de ces recommandations, nous avons fourni des [conseils à Frontex](#) sur la façon d'utiliser les pouvoirs que lui confère le nouveau règlement pour gérer efficacement les données à caractère personnel dans le cadre des analyses de risque en rapport avec le trafic d'êtres humains.

Nous avons également publié un avis sur la proposition révisée de la Commission concernant l'établissement d'un [système d'enregistrement des entrées/sorties](#) (EES) pour tous les ressortissants de pays tiers qui entrent dans/sortent de l'Union, et un avis sur le [régime d'asile européen commun](#). Dans les deux cas, nous avons demandé à la Commission d'examiner si certaines des mesures proposées étaient vraiment nécessaires à la réalisation des objectifs visés.

Administration interne

Si nous voulons être pris au sérieux en tant qu'autorité de contrôle et de conseil, nous devons veiller à appliquer nous-mêmes des pratiques appropriées et efficaces en matière d'administration interne et de protection des données. Cela est d'autant plus important que nous assurerons une fonction administrative auprès du nouveau comité européen de la protection des données.

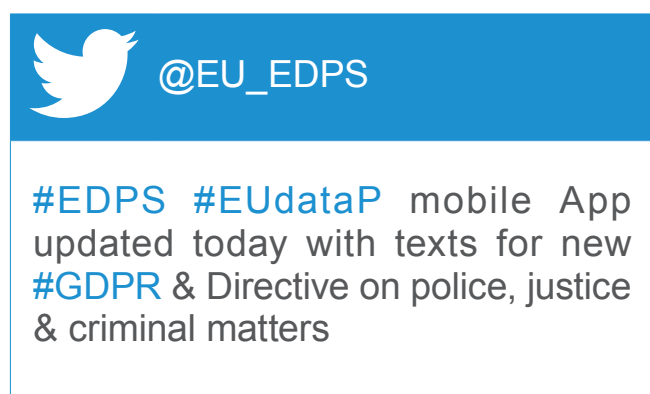
En 2016, le personnel de l'unité «Ressources humaines, budget et administration» du CEPD a travaillé en étroite collaboration avec le DPD en vue de l'élaboration et de l'expérimentation de notre outil de responsabilisation. Nous avons également mis en œuvre des politiques internes, notamment un cadre éthique, destinées à accroître la transparence et à encourager le professionnalisme.

Dans le cadre de nos préparatifs pour le lancement du comité européen de la protection des données, nous devons veiller à ce que l'autorité budgétaire alloue au nouvel organisme des moyens humains et financiers suffisants et à ce que la structure administrative nécessaire à son fonctionnement soit bien en place. Ces travaux se sont accélérés en 2016 et ont été consignés dans une série de fiches d'information sur le comité européen de la protection des données présentant notre vision afin de tenir nos partenaires du GT art.29 informés de nos activités.

Par ailleurs, nous nous conformons pleinement à notre obligation de répondre aux demandes d'accès à des documents et nous employons à accroître la transparence de nos travaux, notamment par le lancement du nouveau site web du CEPD au début de 2017.

Diffuser notre message

Les travaux que nous menons pour définir des priorités en matière de protection des données et montrer l'exemple sur la scène internationale dépendent de notre visibilité.



Nous informons le public de nos activités par le biais de différents outils, notamment les médias, la presse, des

événements et des publications en ligne. Notre application concernant le RGPD, qui a été mise à jour en 2016 afin d'y intégrer les versions finales du règlement général et de la directive relative aux affaires policières, judiciaires et pénales telles qu'elles ont été adoptées, a été un exercice particulièrement réussi sur le plan de la transparence et de la responsabilisation législative. En 2016, nous avons aussi lancé un blog afin de donner un aperçu plus détaillé du travail des contrôleurs.

Nous nous efforçons sans cesse d'atteindre de nouveaux publics, que ce soit en ligne ou hors ligne, soit par le biais de nos médias sociaux, qui se développent très rapidement, soit par des visites et des événements.

Alors que le monde entier a les yeux rivés sur l'Europe, le CEPD continuera de collaborer avec ses partenaires de la protection des données afin de concrétiser sa vision d'une Union européenne qui montre l'exemple dans le dialogue mondial sur la protection des données et la vie privée à l'ère numérique.

Indicateurs clés de performance 2016

À la suite de l'adoption de la stratégie 2015-2019 du CEPD, en mars 2015, nous avons réévalué nos indicateurs clés de performance (ICP) de façon à y intégrer nos nouveaux objectifs et priorités. Les nouveaux ICP nous permettront de contrôler et d'ajuster, si nécessaire, les incidences de nos activités et la façon dont nous utilisons les ressources.

Le tableau ci-dessous présente nos performances en 2016, conformément aux objectifs stratégiques et au plan d'action définis dans la stratégie du CEPD.

Le tableau de bord des ICP comprend une description succincte de chaque ICP, les résultats obtenus au 31 décembre 2016 et l'objectif fixé. Dans la plupart des cas, les indicateurs sont mesurés par rapport à des objectifs de départ mais, pour deux d'entre eux, il s'agit d'une toute première évaluation: ICP 5 et ICP 9.

Les résultats montrent que la mise en œuvre de la stratégie est sur la bonne voie, tous les ICP correspondants atteignant ou dépassant leurs objectifs respectifs. Par conséquent, aucune mesure corrective n'est nécessaire à ce stade.

INDICATEURS CLÉS DE PERFORMANCE		RÉSULTATS AU 31.12.2016	OBJECTIF 2016
Objectif 1 – La protection des données passe au numérique			
ICP 1	Nombre d'initiatives visant à promouvoir les technologies destinées à améliorer le respect de la vie privée et la protection des données organisées ou co-organisées par le CEPD	9	9
ICP 2	Nombre d'activités axées sur des solutions stratégiques interdisciplinaires (internes et externes)	8	8
Objectif 2 – Forger des partenariats à l'échelle mondiale			
ICP 3	Nombre d'initiatives prises concernant des accords internationaux	8	5
ICP 4	Nombre d'affaires traitées au niveau international (GT art. 29, CdE, OCDE, GPEN, conférences internationales) pour lesquelles le CEPD a fourni une contribution écrite importante	18	13
Objectif 3 – Ouvrir un nouveau chapitre consacré à la protection des données dans l'Union			
ICP 5	Analyse de l'incidence de la contribution du CEPD au RGPD et à la directive relative aux affaires pénales et judiciaires	RGPD: forte incidence Directive: incidence moyenne	L'année 2016 sert de valeur de référence
ICP 6	Niveau de satisfaction des DPD/CPD/responsables du traitement sur la coopération avec le CEPD et lignes directrices, y compris la satisfaction des personnes concernées en ce qui concerne les formations	88%	60%
ICP 7	Taux d'exécution des dossiers dans la liste de priorité du CEPD (régulièrement mise à jour) sous la forme de commentaires informels et d'avis formels	93%	90%
Facteurs – Communication et gestion des ressources			
ICP 8	Nombre de visites sur le site web du CEPD	459 370 visites sur le site web	L'année 2015 sert de valeur de référence, + 10 % (195 715 visites du site web; 3 631 followers sur Twitter)
(indicateur composite)	Nombres de followers sur le compte Twitter du CEPD	6 122 followers sur Twitter	
ICP 9	Niveau de satisfaction du personnel	75%	L'année 2016 sert de valeur de référence – enquête biennale

| Principaux objectifs pour 2017

Les objectifs énoncés ci-après ont été retenus pour 2017 dans le cadre de la stratégie générale pour 2015-2019. Les résultats seront consignés dans le rapport annuel 2017.

Garantir la confidentialité et le respect de la vie privée dans les communications électroniques

Dans le cadre du train de réformes en matière de protection des données, qui inclura le [RGPD](#) et la révision des dispositions applicables aux institutions et organes de l'UE, la Commission européenne prévoit également d'adopter de nouvelles dispositions sur le respect de la vie privée dans les communications électroniques. Nous participerons au réexamen en cours de la [directive «vie privée et communications électroniques»](#). Nous concentrerons notamment notre action sur la nécessité de traduire de façon adéquate dans le droit européen le principe de confidentialité des communications électroniques, garanti par l'article 7 de la [Charte des droits fondamentaux de l'Union européenne](#) et l'article 8 de la [Convention européenne des droits de l'homme](#).

Se préparer à la nouvelle version du règlement n° 45/2001

Au début de 2017, la Commission publiera une proposition de nouveau règlement qui remplacera les [dispositions](#) régissant actuellement la protection des données au sein des institutions européennes. Cette révision concerne directement le CEPD puisque ce règlement définit notre rôle et nos compétences en tant qu'autorité de contrôle et fixe les règles dont nous assurerons la mise en application au sein des institutions et organes de l'Union européenne. Compte tenu de son importance, nous nous investirons pleinement dans le processus de révision en 2017, afin de nous assurer que les règles qui s'appliqueront aux institutions, aux organes, aux organismes et aux agences de l'Union en matière de traitement des données sont aussi proches que possible des principes du RGPD. Une fois le texte finalisé, nous adapterons nos procédures internes en conséquence et nous aiderons les institutions et organes de l'Union à mettre en œuvre les nouvelles dispositions.

Faciliter l'évaluation de la nécessité et de la proportionnalité

En 2016, nous avons publié un [document de référence](#) sur la notion de nécessité et lancé une consultation des parties prenantes. En 2017, le CEPD publiera une boîte à outils à ce sujet, en tenant compte des commentaires reçus. Cette boîte à outils fournira des indications aux responsables politiques et aux législateurs de l'Union chargés d'élaborer des mesures qui impliquent le traitement de données à caractère personnel et qui touchent au droit à la protection des données personnelles. Dans la même optique, nous publierons également un document de référence sur le principe de proportionnalité dans la législation de l'UE en matière de protection des données et nous organiserons des ateliers sur des domaines stratégiques spécifiques de l'Union afin de former le personnel de la Commission et de le sensibiliser aux questions liées à la protection des données.

Promouvoir un renforcement des frontières fondé sur le respect des droits fondamentaux

Plusieurs nouvelles initiatives ont été proposées pour aider l'Union à surmonter les difficultés auxquelles elle est confrontée en matière de migration et de sécurité intérieure. Le CEPD continuera de proposer ses conseils sur les conséquences pour la protection des données des propositions de l'Union liées à la mise en œuvre du programme européen en matière de sécurité et du Plan d'action pour renforcer la lutte contre le financement du terrorisme de la Commission. Nous offrirons également des conseils sur plusieurs projets d'initiatives en rapport avec les frontières de l'Union et la sécurité, comme le système européen d'information et d'autorisation concernant les voyages (ETIAS), la révision du [système d'information Schengen de deuxième génération \(SIS II\)](#) et du système européen d'information sur les casiers judiciaires (ECRIS), et l'interopérabilité de ces systèmes.

Nous surveillerons de près les possibles répercussions sur la protection des données du nouveau cadre des [décisions d'adéquation](#) concernant l'échange de données à caractère personnel avec des pays tiers, des nouveaux accords commerciaux et des éventuels accords dans le secteur de la répression. Nous continuerons par ailleurs à consolider nos liens avec le

Parlement européen et le Conseil, en leur offrant une aide et des conseils lorsque nécessaire.

Préparer les institutions européennes aux analyses d'impact relatives à la protection des données

Nos activités visant à préparer les **DPD** et les **responsables du traitement des données** des institutions européennes à leurs nouvelles obligations porteront plus particulièrement sur les **analyses d'impact relatives à la protection des données**. Ces analyses d'impact s'inscrivent dans le cadre d'une réorientation globale vers la **responsabilisation**, permettant le renforcement des capacités des institutions européennes afin qu'elles puissent assurer la conformité. Elles servent de cadres pour l'évaluation des risques des traitements de données considérés à haut risque pour la protection des données et le respect de la vie privée, et aident les personnes responsables du traitement des données à porter leurs efforts là où ils sont le plus nécessaires. Nous poursuivrons nos travaux sur les analyses d'impact lors de nos réunions avec le réseau de DPD et, le cas échéant, nous proposerons des conseils individuels.

Fournir des orientations sur la technologie et la protection des données

En 2017, nous publierons des lignes directrices sur la gouvernance et la gestion des technologies de l'information et sur l'informatique en nuage. Nous poursuivrons également le travail entrepris avec les lignes directrices sur les **services web** et sur les **applications mobiles** en nous concentrant plus particulièrement sur l'aspect pratique de leur mise en œuvre au sein des institutions et organes de l'UE placés sous notre supervision. Nous fournirons des conseils pratiques concernant des cas concrets sur la base d'une analyse détaillée de sites web et d'applications spécifiques.

Réviser les lignes directrices sur les données en matière de santé

En 2017, nous réviserons nos lignes directrices concernant le traitement des données relatives à la santé sur le lieu de travail et renforcerons notre expertise dans le domaine des mégadonnées et de la santé. Ces lignes directrices sont nécessaires pour expliquer la forte augmentation du traitement des

données relatives à la santé à des fins statistiques, scientifiques et de recherche. Notre but est de présenter toutes les dispositions pertinentes en matière de protection des données et de les illustrer par des exemples spécifiques que nous avons nous-mêmes rencontrés dans le cadre de notifications, de consultations et de plaintes. Nous impliquerons activement certains DPD des institutions et organes de l'Union qui souhaitent partager leurs expériences dans ce domaine.

Mener l'enquête de printemps

Tous les deux ans, le CEPD effectue une enquête générale sur les institutions et organes de l'UE. Cette enquête est un outil efficace pour contrôler et garantir l'application des **règles en matière de protection des données** au sein des institutions européennes, et complète les outils de contrôle tels que les visites ou inspections. La prochaine enquête de printemps sera réalisée en 2017.

Renforcer notre expertise en matière de sécurité informatique

Nous continuerons de renforcer notre expertise en matière de sécurité informatique et la mettrons à profit dans nos activités d'inspection et d'audit. Cela inclut la poursuite de nos activités de contrôle concernant les **systèmes d'information à grande échelle** et l'extension de ces activités à de nouveaux domaines, comme le contrôle d'Europol. Nous utiliserons également ces connaissances dans le cadre de la préparation de l'infrastructure du comité européen de la protection des données, en partenariat avec les APD nationales.

Renforcer la coopération internationale

En 2017, il sera essentiel de poursuivre notre coopération avec les APD nationales. Outre la poursuite de nos préparatifs conjoints en vue du RGPD, nous collaborerons avec le **G29** sur différents sujets, parmi lesquels le programme en matière de sécurité et les nouvelles mesures de lutte contre le terrorisme, les transferts internationaux, les données financières, la santé et l'évolution des technologies de l'information. Nous coopérerons aussi avec les APD en tant que secrétariat européen de la protection des données, non seulement pour le comité européen de la protection des données, mais également dans le cadre de nos travaux sur le contrôle coordonné des systèmes d'information à grande échelle et du contrôle d'Europol.

Nous contribuerons, dans la mesure du possible, aux débats internationaux sur la protection des données et le respect de la vie privée, et nous poursuivrons notre dialogue avec les organisations internationales, notamment en organisant un atelier conjoint au mois de mai 2017.

Mener à bien le projet relatif à la responsabilisation

Nous organiserons des visites d'information et de sensibilisation afin d'expliquer les répercussions de la prochaine révision du [règlement \(CE\) n° 45/2001](#) sur les institutions et organes de l'UE. L'objectif premier de ces visites sera d'encourager les institutions de l'Union à mettre en œuvre le principe de responsabilisation ainsi que les exigences spécifiques des nouvelles dispositions sur la protection des données dans les institutions de l'UE. Afin de montrer l'exemple, l'unité «Contrôle et mise en application» du CEPD s'emploiera, en coopération avec le DPD du CEPD, à pousser plus avant la mise en œuvre du principe de responsabilisation au niveau interne. Nous partagerons nos expériences avec le réseau de DPD.

Développer une dimension éthique de la protection des données

Développer une dimension éthique de la protection des données est l'une des [priorités](#) du mandat actuel du CEPD. Les activités menées par le CEPD et le [groupe consultatif sur l'éthique](#) en 2016 ont permis de sensibiliser la communauté de la protection des données à l'éthique numérique. En 2017, le CEPD continuera de soutenir les actions du groupe consultatif sur l'éthique et veillera à ce que le débat mondial sur l'éthique numérique reste une priorité. Le groupe consultatif publiera son premier rapport intermédiaire et organisera un atelier conjointement avec le CEPD afin de sensibiliser la communauté scientifique. Le CEPD commencera également à intégrer des aspects éthiques dans ses activités journalières en tant qu'organisme de réglementation indépendant et conseiller stratégique, et à préparer la session publique de la conférence internationale des commissaires à la protection des données et à la vie privée de 2018, qui sera organisée par le CEPD et l'APD bulgare et consacrée à l'éthique numérique.

Accroître la diffusion des travaux du CEPD en matière de suivi de la technologie

Le CEPD suit l'évolution des nouvelles technologies et analyse leur incidence sur le respect de la vie privée,

conformément à son objectif d'intégrer la protection des données dans le numérique, tel qu'énoncé dans sa [stratégie](#). Toutefois, nos travaux dans ce domaine ne sont pas suffisamment diffusés. Nous avons donc l'intention d'accroître la visibilité de ces activités et de rendre nos conclusions plus accessibles grâce à une meilleure communication. Dans cette optique, nous pourrions, par exemple, organiser ou participer à des ateliers qui nous permettraient d'affiner nos analyses et de mieux cibler nos contributions au débat public. Nous continuerons de développer notre coopération avec l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) et prévoyons d'organiser un atelier avec des chercheurs universitaires du secteur technologique dans le but d'améliorer la coopération directe avec le milieu universitaire.

Numériser la protection des données

L'article 25 du RGPD rend obligatoires [la protection des données dès la conception](#) et la protection des données par défaut. Cette obligation a suscité un regain d'intérêt pour l'approche scientifique du respect de la vie privée et inspiré de nouveaux partenariats dans les domaines commercial et de la recherche. L'[IPEN](#), avec ses partenaires du milieu universitaire, de la société civile, de l'administration et de l'industrie, souhaite collaborer à ce type d'initiatives. Nous continuerons d'améliorer les outils de communication du réseau et nous renforcerons la coopération et la cohérence en vue de faciliter le lancement et le soutien de nouvelles initiatives. Nous pourrions organiser davantage d'événements IPEN à mesure que le réseau se développera.

Préparer la mise en place du comité européen de la protection des données

Le RGPD prévoit le remplacement du G29 par le comité européen de la protection des données. Étant donné que le CEPD assurera le secrétariat de ce comité, nous devons veiller à ce que la nouvelle structure soit opérationnelle dès que le RGPD sera pleinement applicable. Les travaux préparatoires nécessaires seront menés en étroite coopération avec le G29 et nous ferons en sorte de mettre en place des dispositions transitoires adéquates afin de permettre un transfert en douceur. Nous continuerons donc de participer au groupe de travail «comité européen de la protection des données-GT art.29» en vue de l'organisation du secrétariat du comité. Il s'agira notamment de garantir l'existence d'une infrastructure informatique appropriée, d'établir des méthodes de travail et un règlement intérieur et d'assurer l'allocation de ressources humaines et financières adéquates.

Effectuer un contrôle efficace d'Europol

Dès le 1^{er} mai 2017, Europol sera régi par un **nouveau cadre de protection des données**, en vertu duquel le CEPD prendra en charge le contrôle du traitement des données à caractère personnel au sein d'Europol. Nous nous sommes préparés à cette nouvelle mission sur les plans organisationnels et des ressources humaines, et nous poursuivrons ces préparatifs jusqu'au 1^{er} mai 2017, lorsque commencera réellement notre travail de contrôle. Cette nouvelle mission consistera notamment à effectuer nos tâches de supervision habituelles, par exemple le traitement des plaintes, les consultations, le traitement des demandes d'information et la réalisation d'inspections ainsi que la coopération avec les autorités nationales en charge des contrôles au sein du nouveau conseil de coopération.

Mettre sur pied la «Digital Clearing House»

En 2016, nous avons annoncé notre intention de créer une «Digital Clearing House» (chambre de compensation numérique). Cette structure regroupera des organismes actifs dans les domaines de la

concurrence, de la protection des consommateurs et de la protection des données qui souhaitent partager des informations et discuter ensemble de la façon de faire appliquer les dispositions qui défendent les intérêts du citoyen dans l'espace numérique. À la fin de l'année 2016, nous avons publié un questionnaire à l'intention de tous les organismes désireux de participer. En 2017, nous discuterons, à partir des résultats du questionnaire, des mesures pratiques à mettre en œuvre pour faire respecter plus efficacement les droits. Le réseau devrait se réunir au printemps 2017, réunion qui serait suivie d'une conférence ou d'une première réunion publique de la «Clearing House» à l'automne 2017.

Récompenser les organismes qui utilisent des technologies de protection de la vie privée

Le CEPD souhaite encourager les concepteurs à utiliser des technologies de protection de la vie privée (PET) dans leurs nouvelles applications. Nous créerons donc un prix récompensant les applications mobiles dans le domaine de la santé (mHealth) respectueuses de la vie privée, qui sera lancé en 2017.

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- un seul exemplaire:
sur le site EU Bookshop (<http://bookshop.europa.eu>);
- exemplaires multiples/posters/cartes:
auprès des représentations de l'Union européenne (http://ec.europa.eu/represent_fr.htm),
des délégations dans les pays hors UE (http://eeas.europa.eu/delegations/index_fr.htm), en
contactant le réseau Europe Direct (http://europa.eu/europedirect/index_fr.htm)
ou le numéro 00 800 6 7 8 9 10 11 (gratuit dans toute l'UE) (*).

(*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

Publications payantes:

- sur le site EU Bookshop (<http://bookshop.europa.eu>).

www.edps.europa.eu

 @EU_EDPS

 EDPS

 European Data Protection Supervisor



Office des publications