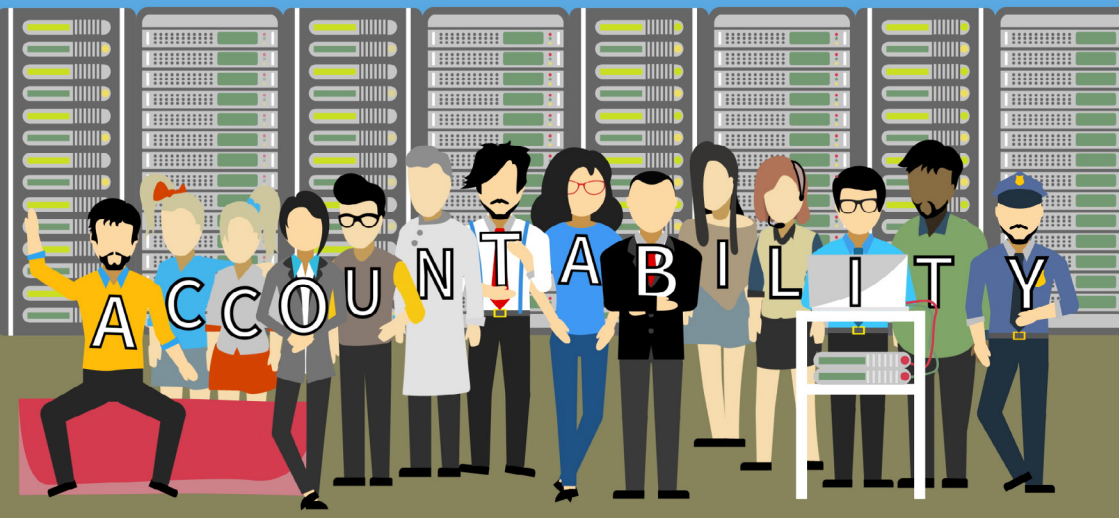
EDPS

Nouvelles règles de protection des données pour les institutions de l'UE: leur incidence sur VOUS



Print ISBN: 978-92-9242-390-2 DOI: 10.2804/762344 QT-05-18-174-FR-C
PDF ISBN: 978-92-9242-388-9 DOI: 10.2804/26015 QT-05-18-174-FR-N

Le traitement des données à caractère personnel par votre institution a évolué. Ces changements, introduits dans le cadre de la révision des règles sur la protection des données dans les institutions de l'UE, auront une incidence sur vous:

1 lorsque vous traitez des données à caractère personnel dans le cadre de votre travail au sein d'une institution de l'UE;

2 lorsque vous préparez des propositions législatives, des actes d'exécution ou des actes délégués (ou des accords internationaux) qui pourraient impliquer le traitement de données à caractère personnel;

3 lorsque votre institution européenne traite vos propres données à caractère personnel, dans le cadre d'un recrutement, d'une évaluation ou d'un congé de maladie par exemple.

Règles de l'UE en matière de protection des données: responsabilité et transparence

Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité
(considérant 4 du règlement général sur la protection des données – RGPD)

La protection des données à caractère personnel concerne les personnes. C'est un droit fondamental. Les nouvelles règles permettent aux citoyens de mieux contrôler leurs données à caractère personnel. Elles visent à assurer la protection de ces données, quel que soit le lieu de leur transmission, de leur traitement ou de leur stockage.

La réforme met l'accent sur la **responsabilité**. Cela signifie qu'il incombe désormais à votre institution de respecter les règles relatives à la protection des données et d'être en mesure de démontrer ce respect. Il s'ensuit que la protection des données est maintenant l'affaire de tous, indépendamment de votre place dans la hiérarchie de l'UE.

Chaque institution, organe et agence de l'UE dispose d'un délégué à la protection des données (DPD). Votre DPD est votre allié interne et peut jouer le rôle de conseiller sur les questions de protection des données. Si vous voulez éviter les écueils potentiels, essayez d'impliquer votre DPD à un stade précoce, à chaque fois que vous prévoyez de travailler avec des données à caractère personnel.

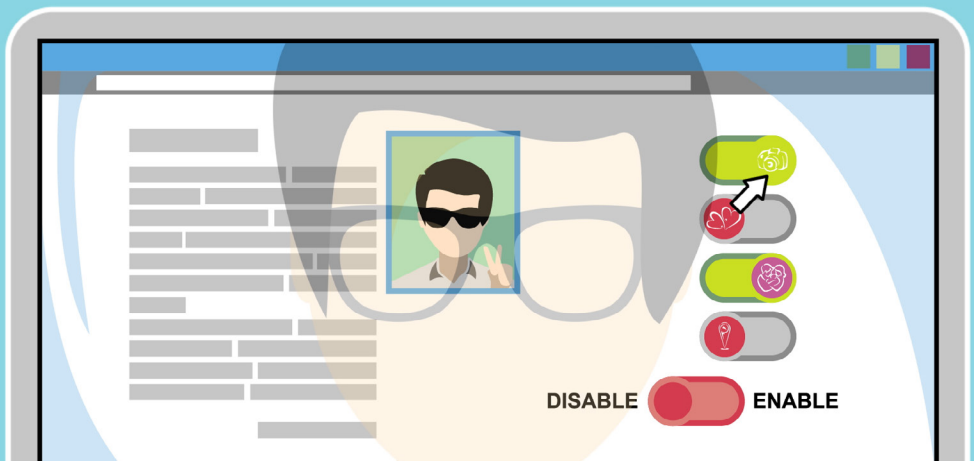
Incidence des nouvelles règles sur les personnes: pensez à la protection des données!

Des droits renforcés pour les particuliers

Avant de collecter des données à caractère personnel, utilisez une notification concernant la protection des données pour informer les personnes de la manière dont votre institution entend traiter leurs données à caractère personnel. Les particuliers ont le droit de demander l'accès à leurs propres données à caractère personnel et de recevoir une copie de toutes celles qui ont été traitées par votre institution. Ils ont également le droit de rectifier leurs données à caractère personnel et, dans certains cas, de les supprimer. Le nouveau droit à la portabilité des données permet aux personnes d'obtenir et de réutiliser leurs données à caractère personnel pour leurs propres besoins dans différents services. Il leur permet de déplacer, de copier ou de transférer aisément des données à caractère personnel d'un environnement informatique à un autre, de manière sûre et sécurisée, sans nuire à leur utilité.

Veillez au respect de la protection des données et conservez des pièces justificatives

Identifiez les opérations de traitement relevant de votre responsabilité et informez-en votre DPD. Gardez une trace écrite des raisons pour lesquelles votre institution traite des données à caractère personnel, et des méthodes employées.



Pensez dès le début au respect de la vie privée - *protection des données dès la conception et par défaut*

Intégrez la protection des données dans vos manuels, vos procédures et toutes les opérations de traitement avant de commencer à traiter des données à caractère personnel. Vous devez garantir la mise en œuvre effective des principes de protection des données à chaque fois que l'opération est réalisée. Parmi les principes pertinents figurent le traitement loyal et licite, la minimisation des données, la limitation des durées de conservation des données, et des mesures de sécurité appropriées. Demandez conseil à votre DPD dès le départ. Examinez périodiquement les mesures techniques et organisationnelles en place pendant que l'opération de traitement est en cours. Votre DPD peut également vous aider à identifier les opérations de traitement des données qui nécessitent une analyse d'impact relative à la protection des données et vous fournir des informations sur la manière d'effectuer cette analyse.

Évaluation des risques

Évaluez les risques que chacune de vos opérations de traitement peut représenter pour les droits et les libertés des personnes concernées, et choisissez les garanties appropriées.

Analyses d'impact relatives à la protection des données (AIPD)

Dans certains cas, vous devrez effectuer une AIPD formelle, en étudiant plus précisément les risques induits par les opérations de traitement que vous avez prévues, en choisissant les contrôles et en fournissant des pièces justificatives. Ceci s'applique, par exemple, au traitement à grande échelle des données sensibles telles que les données médicales.

Externalisation, passation de marchés, ANS et protocoles d'accord

Votre institution est également responsable de tout traitement de données personnelles effectué pour son compte par des tiers ou des contractants externes. Identifiez les risques liés aux opérations de traitement, incluez des exigences relatives à la protection des données dès la phase de rédaction de l'appel d'offres, choisissez des contractants appropriés, et insérez des **clauses contractuelles relatives à la protection des données**. Des considérations similaires s'appliquent lorsque vous partagez une opération de traitement avec une ou plusieurs institutions de l'UE, au moyen d'un accord de niveau de service (ANS) ou d'un protocole d'accord. Révisez vos contrats existants et actualisez-les afin de refléter les nouvelles obligations.

Transfert de données vers des pays extérieurs à l'UE

Les transferts de données à caractère personnel vers des pays extérieurs à l'UE et à l'Espace économique européen ne sont autorisés que sur la base d'une décision d'adéquation, adoptée par la Commission, ou si des garanties appropriées sont mises en œuvre, telles des clauses contractuelles spécifiques.

Le DPD: votre allié et conseiller interne

Si l'institution et l'ensemble du personnel sont responsables du respect des règles de protection des données, chaque institution doit également désigner un délégué à la protection des données (DPD). Ce dernier travaille en tant que conseiller interne indépendant auprès de l'ensemble du personnel de l'institution. Il est également la personne à contacter si quelqu'un souhaite exercer ses droits en matière de protection des données ou déposer une plainte, et il peut ouvrir des enquêtes sur des questions relatives à la protection des données au sein de l'institution européenne.

Détectez et signalez les violations de données à caractère personnel

Dès que vous découvrez l'existence d'une violation de données à caractère personnel, signalez-la à la hiérarchie de votre institution! Votre institution doit informer le DPD, évaluer l'incident et atténuer ses effets. La plupart des violations de données à caractère personnel doivent également être signalées au CEPD au plus tard 72 heures après que votre institution a pris connaissance de l'infraction. Les violations de données pourraient inclure le vol de données à caractère personnel, la perte d'une clé USB contenant des noms, ou la publication accidentelle d'annuaires internes du personnel.

Responsabilité et sanctions

Le non-respect des règles de protection des données peut entraîner des sanctions disciplinaires pour les membres du personnel de l'UE. Les personnes ayant subi un dommage matériel ou un préjudice moral du fait d'une violation des règles en matière de protection des données à caractère personnel ont le droit d'obtenir réparation de la part de votre institution. Le CEPD peut adopter des mesures correctrices, telles qu'un avertissement ou une interdiction de traitement. Il pourra également infliger des amendes aux institutions de l'UE (jusqu'à 500 000 EUR par an).


assurer le respect
appliquer des mesures
de sauvegarde
démontrer
l'efficacité des mesures
de sauvegarde
vérifier le respect
mesurer le respect

Les **données à caractère personnel** désignent toute information relative à une **personne physique** (directement ou indirectement) identifiable. Une personne physique identifiable est une personne physique qui peut être identifiée, directement ou indirectement, notamment en se référant à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou encore à un ou plusieurs facteurs propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Exemples: le nom, l'adresse électronique, le dossier d'évaluation annuel et les dossiers médicaux, mais aussi des informations indirectement identifiables, telles que le numéro de personnel, l'adresse IP, les journaux de connexion, le numéro de télécopieur, les données biométriques, etc.

On entend par **traitement** toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou à des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Exemples: procédure de recrutement, procédure d'octroi de subventions, liste d'experts externes, gestion d'un événement, publication d'images, création d'une plateforme collaborative en ligne pour les citoyens ou les membres du personnel.

Le traitement intervient également lorsque les institutions européennes fournissent aux États membres un outil technique ou une solution pour faciliter l'échange d'informations, tout en conservant l'accès aux données à caractère personnel concernées ou en tenant un registre des journaux de connexion relatifs à la plateforme.

Pour en savoir plus sur les nouvelles règles en matière de protection des données, consultez nos autres fiches d'information:

- **Le RGPD pour les institutions de l'UE: vos droits à l'ère numérique**
- **Documentation du traitement des données personnelles: le guide du CEPD pour la responsabilisation**

ou consultez le site web du CEPD

Cette fiche d'information est publiée par le Contrôleur européen de la protection des données (CEPD), une autorité européenne indépendante créée en 2004 pour:

- contrôler le traitement des données à caractère personnel par les institutions et organes de l'UE;
- donner des conseils sur la législation relative à la protection des données;
- coopérer avec les autorités de même nature, pour garantir la cohérence en matière de protection des données.

QT-05-18-174-FR-N

www.edps.europa.eu


@EU_EDPS


EDPS


European Data Protection Supervisor

ISBN: 978-92-9242-388-9