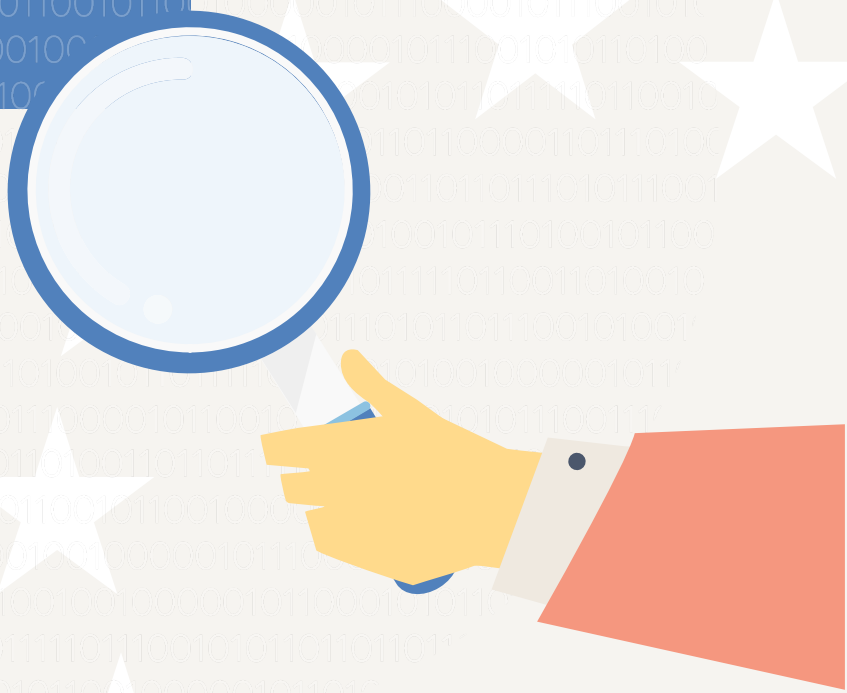
EDPS

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

À QUOI S'ATTENDRE LORSQUE NOUS INSPECTONS?

Les audits sur la protection des données en quelques explications



QUI SOMMES-NOUS?

Le Contrôleur européen de la protection des données (CEPD) est l'autorité indépendante de protection des données de l'Union européenne, chargée de vérifier et de s'assurer que les institutions et organes de l'UE (institutions de l'UE) respectent les règles européennes en matière de protection des données, énoncées dans le règlement (UE) 2018/1725, lorsqu'ils traitent des informations personnelles, en d'autres termes des données à caractère personnel.

La protection des données est un droit fondamental, protégé par la législation européenne et inscrit à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. L'administration de l'UE doit non seulement respecter le règlement (UE) 2018/1725, mais aussi démontrer qu'elle respecte ce règlement. Le CEPD vérifie la conformité à ce règlement, et tient les institutions de l'UE responsables, conformément à son règlement intérieur. Le CEPD encourage également le personnel des institutions de l'UE, en particulier ceux qui sont responsables du traitement des données à caractère personnel, à favoriser une culture de la protection des données au sein de leurs institutions respectives.

Les audits sont l'un des outils utilisés par le CEPD pour s'assurer que les institutions de l'UE respectent les règles sur la protection des données. Au cours d'un audit, nous sommes en mesure de vérifier la conformité avec ces règles sur place et de formuler des recommandations si nous découvrons des points à améliorer. Les pouvoirs du CEPD en matière d'audit sont définis à l'article 52, paragraphe 3, à l'article 57, paragraphe 1, point b), et à l'article 58, paragraphe 1, points b), d) et e), du règlement (UE) 2018/1725.

QUAND, POURQUOI ET QUELLES INSTITUTIONS DE L'UE SONT CONTRÔLÉES?

Nous effectuons des audits conformément à notre plan d'inspection annuel. Pour établir ce plan, nous procédons à une analyse des risques et tenons compte des ressources disponibles pour la réalisation des audits. Les audits de sécurité des applications et systèmes informatiques à grande échelle se déroulent conformément aux lois régissant leur supervision.

Bien que nous nous réservions le droit d'effectuer des audits de manière aléatoire, nous étudions divers facteurs pour décider quelles institutions de l'UE contrôler:

- les catégories de données traitées par les institutions de l'UE (par exemple, les données sur la santé sont particulièrement sensibles);
- le nombre de réclamations que nous avons reçues au sujet d'une institution de l'UE;
- la régularité du transfert de données effectué par les institutions de l'UE et les destinataires de ces données;
- le respect des précédentes décisions du CEPD par l'institution;
- les antécédents de la coopération de l'institution avec le CEPD.

La COVID-19 ayant empêché le CEPD de mener des travaux sur le terrain, nous avons adapté notre planification des audits et effectué des audits à distance, en inspectant par exemple les registres publics des institutions de l'UE et leurs procédures de gestion des abonnements aux newsletters. Les audits à distance devraient se poursuivre au-delà de la pandémie de COVID-19, dans certaines circonstances.

QUELLES SONT LES 3 ÉTAPES D'UN AUDIT DU CEPD?

1.

L'institution de l'UE est généralement informée au moins quatre semaines **avant l'inspection du CEPD**. À ce stade, l'institution concernée ou son délégué à la protection des données (DPD) peuvent être invités à fournir des renseignements et des documents au CEPD.

2.

Au cours d'un audit sur place, le CEPD rencontre les membres du personnel chargés du traitement des données à caractère personnel au sein de l'institution de l'UE. Le CEPD demande également des informations et des démonstrations concernant le traitement des données à caractère personnel effectué lors des tâches quotidiennes de l'institution. Les résultats de ces réunions, entretiens et démonstrations, ainsi que tous les éléments de preuve recueillis, sont enregistrés par le CEPD et sont ensuite présentés à l'institution contrôlée pour qu'elle formule ses observations. Afin de garantir la conformité, nous devons nous assurer que tous les faits enregistrés sont corrects. La consultation de l'institution concernée permet à l'ensemble des acteurs impliqués dans l'audit de signaler tout malentendu au sujet d'événements survenus.

3.

Après un audit, le CEPD fournit toujours des commentaires appropriés à l'institution concernée dans un rapport d'audit contenant une feuille de route des recommandations à appliquer le cas échéant. Si le CEPD ne publie pas les détails de ses rapports d'audit, il fournit régulièrement des informations sur ses activités d'audit dans ses rapports annuels et autres publications. Le CEPD vérifie toujours si les recommandations figurant dans la feuille de route ont été mises en œuvre.

EN TANT QUE MEMBRE DU PERSONNEL, COMMENT POURRIEZ-VOUS ÊTRE ÉVENTUELLEMENT AMENÉ À PARTICIPER À UN AUDIT DU CEPD?

Le CEPD s'efforce d'accompagner les audits de sessions d'information sur la protection des données, organisées en coopération avec le DPD de votre institution. Si vous êtes invité à assister à une formation sur la protection des données, nous vous encourageons à nous rejoindre!

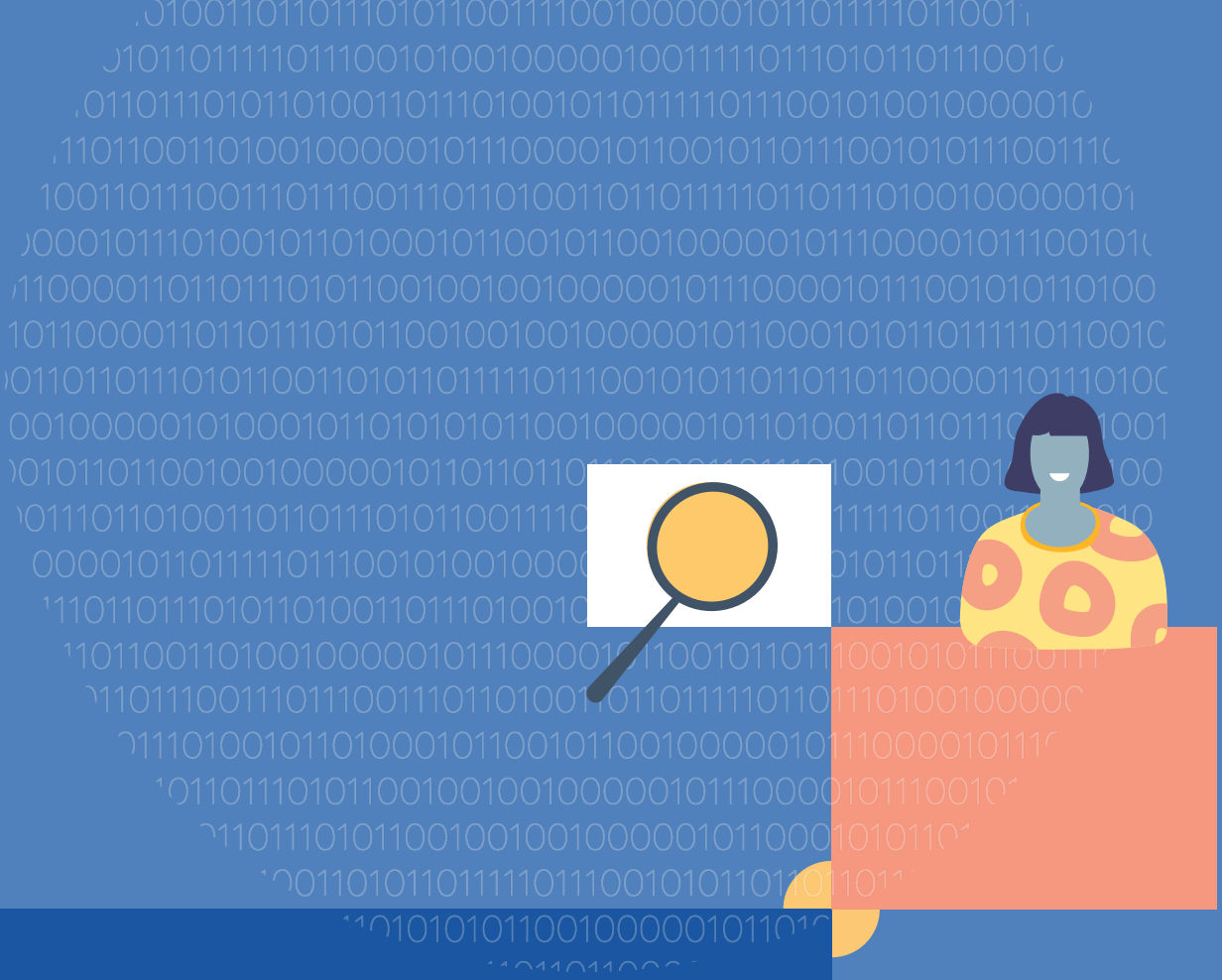
Si vous êtes un membre du personnel chargé d'effectuer l'une des opérations de traitement des données contrôlées par le CEPD, nous vous demanderons peut-être de nous accorder un entretien ou d'organiser une démonstration sur place. Vous serez généralement informé de cette demande par votre DPD, qui vous remettra également une déclaration de protection des données contenant de plus amples informations. Tous les membres du personnel du CEPD, y compris les auditeurs, sont soumis à des obligations strictes en matière de confidentialité.

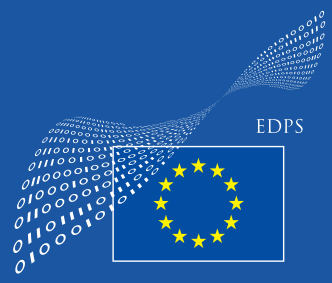
Toutes les institutions de l'UE sont tenues d'assister les auditeurs du CEPD à la demande de ces derniers, en vertu de l'article 32 du règlement (UE) 2018/1725. Cette obligation d'assistance vous incombe aussi en votre qualité de membre du personnel. Nous vous demanderons donc peut-être de nous fournir des informations sur les activités de traitement des données que vous effectuez dans le cadre de votre travail quotidien, de nous permettre d'accéder aux données à caractère personnel et à vos locaux, et de nous autoriser à recueillir les éléments de preuve nécessaires à l'audit. Nous sommes conscients que cette sollicitation augmentera votre charge de travail, et nous nous efforcerons donc de réduire au minimum et autant que possible le dérangement occasionné par notre présence. Les auditeurs du CEPD n'inspecteront les locaux et ne rechercheront des éléments de preuve eux-mêmes que dans des circonstances exceptionnelles, par exemple en l'absence de coopération adéquate de la part du personnel ou de l'institution, ou à la suite de l'indisponibilité du ou des membre(s) compétent(s) du personnel.

LECTURES COMPLÉMENTAIRES

- **Politique en matière d'audit**
- **Lignes directrices en matière d'audit**
- **Rapport sur l'inspection à distance des registres accessibles au public, au titre de l'article 31, paragraphe 5, du règlement**
- **Règlement (EU) 2018/1725:** article 58, paragraphe 1, points b), d) et e) sur les pouvoirs du Contrôleur européen de la protection des données lors de la réalisation des audits
- **Règlement (EU) 2018/1725**: article 32 sur l'obligation des responsables du traitement des données d'assister le CEPD

Tous les documents du CEPD énumérés dans cette section sont disponibles sur le site web du CEPD.





edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

QT-02-21-642-FR-N ISBN: 978-92-9242-694-1 DOI: 10.2804/925002