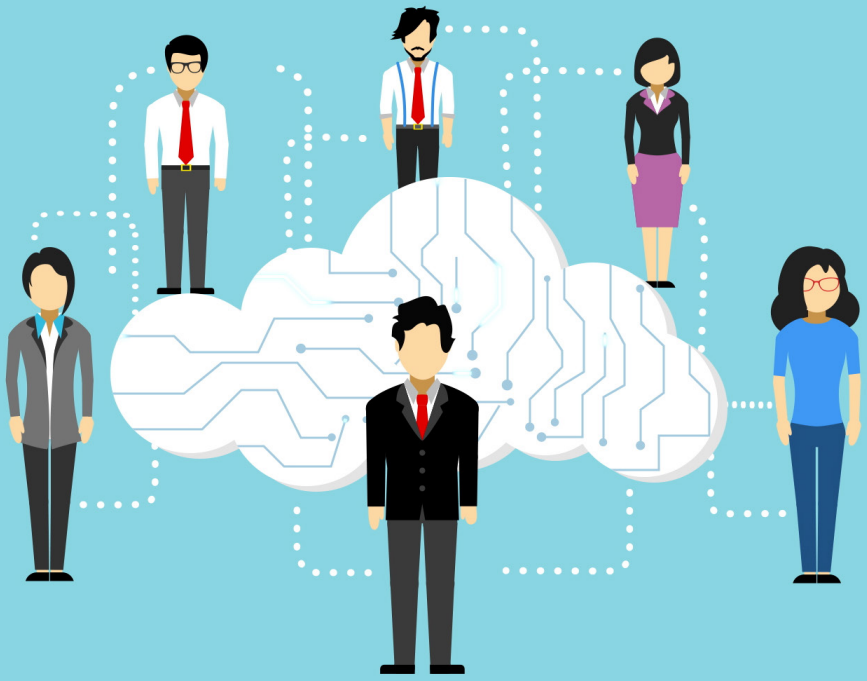


Documenter le traitement des données: le guide du CEPD pour garantir l'obligation de rendre compte

Print ISBN: 978-92-9242-383-4 DOI: 10.2804/024481 QT-05-18-173-FR-C
PDF ISBN: 978-92-9242-386-5 DOI: 10.2804/196635 QT-05-18-173-FR-N

Responsabilisation sur le terrain

Le traitement illicite des données peut avoir de graves conséquences sur la vie et les droits des personnes dont nous traitons les données. C'est pourquoi le principe de responsabilité, qui consiste à démontrer le respect de la protection des données, doit être au cœur de toute activité de traitement des données que nous effectuons.

Les institutions, organes et agences de l'UE doivent respecter certaines règles lors du traitement de données à caractère personnel.

Si vous êtes responsable du traitement de données à caractère personnel pour le compte de votre institution européenne, vous devez pouvoir expliquer ce que vous faites, pourquoi vous le faites, et comment vous le faites. Cela signifie que vous devez vous assurer que vous respectez les lois sur la protection des données, mais aussi que vous pouvez prouver cette conformité.

Une façon de la démontrer est de documenter toutes les opérations de traitement qui ont lieu au sein de votre institution de l'UE. Selon le niveau de risque qu'une activité de traitement peut présenter pour la personne concernée, vous devrez remplir une ou plusieurs des exigences en matière de documentation suivantes:

- **Pour toutes les opérations de traitement:** dossier de vérification de conformité et de traitement
- **Pour les opérations de traitement à haut risque:** analyse d'impact relative à la protection des données (AIPD)
- **Pour les opérations de traitement à haut risque résiduel et les opérations de traitement énumérées à l'article 40, paragraphe 4, du règlement:** consultation préalable

La boîte à outils du CEPD sur la Responsabilisation sur le terrain vous guidera tout au long de ce processus.

Que sont les dossiers?

Un dossier est la documentation de base nécessaire pour toutes vos opérations de traitement. Tous les dossiers alimentent un registre central tenu par votre institution européenne. Ils sont généralement gérés par le délégué à la protection des données (DPD) de l'institution. Il est important de rappeler que, bien que le DPD soit le mieux placé pour gérer ce registre, vous restez responsable du contenu des documents que vous produisez.

Le registre des documents devrait être public. Votre institution est ainsi en mesure de démontrer de manière efficace et transparente qu'elle respecte les règles de protection des données.

Quand devriez-vous procéder à une analyse d'impact relative à la protection des données?

Certaines opérations de traitement risquées exigent davantage qu'un simple dossier. Par exemple:

- le traitement de grandes quantités de données à caractère personnel sensibles, comme les données relatives à la santé;
- le traitement des données relatives aux affaires disciplinaires;
- l'utilisation de techniques de profilage.

Ces cas, comme d'autres, exigent que vous procédiez à une AIPD.

Comment procéder à une analyse d'impact relative à la protection des données?

Les analyses d'impact relatives à la protection des données consistent à analyser en détail les opérations de traitement prévues, afin d'identifier les risques particuliers liés à la protection de la vie privée et d'élaborer des stratégies pour les atténuer. Ce processus devrait mener à la production d'un rapport sur l'AIPD. Cependant, n'oubliez pas que les analyses d'impact relatives à la protection des données sont un processus continu. Vous devriez donc prévoir de procéder à des réexamens réguliers.

Le CEPD fournit des modèles pour la réalisation des AIPD. Ils sont conçus pour vous aider dans ce processus. Toutefois, toute méthodologie conforme aux exigences du règlement ou du RGPD peut être utilisée.

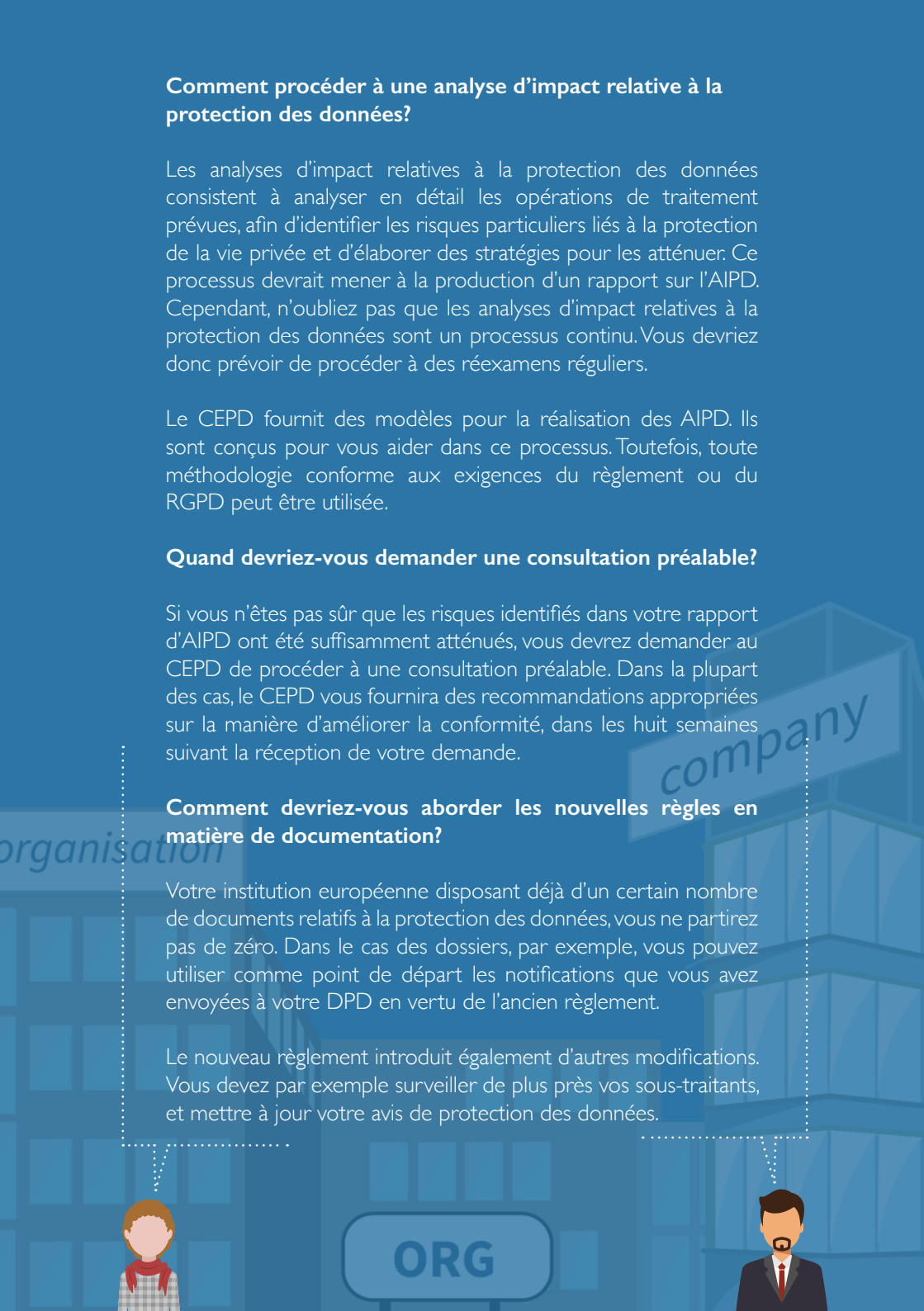
Quand devriez-vous demander une consultation préalable?

Si vous n'êtes pas sûr que les risques identifiés dans votre rapport d'AIPD ont été suffisamment atténués, vous devrez demander au CEPD de procéder à une consultation préalable. Dans la plupart des cas, le CEPD vous fournira des recommandations appropriées sur la manière d'améliorer la conformité, dans les huit semaines suivant la réception de votre demande.

Comment devriez-vous aborder les nouvelles règles en matière de documentation?

Votre institution européenne disposant déjà d'un certain nombre de documents relatifs à la protection des données, vous ne partirez pas de zéro. Dans le cas des dossiers, par exemple, vous pouvez utiliser comme point de départ les notifications que vous avez envoyées à votre DPD en vertu de l'ancien règlement.

Le nouveau règlement introduit également d'autres modifications. Vous devez par exemple surveiller de plus près vos sous-traitants, et mettre à jour votre avis de protection des données.



Comment votre DPD peut-il vous aider?

Dans chaque institution de l'UE, il existe au moins un délégué à la protection des données. Le DPD sert de point de référence pour toutes les questions relatives à la protection des données. Dans certaines grandes institutions de l'UE, comme la Commission européenne, vous aurez également des coordinateurs ou des contacts de la protection des données (CPD). Les DPD et les CPD peuvent vous fournir des conseils sur la façon de produire des dossiers et d'effectuer des AIPD. Vous devez aussi les contacter si vous avez d'autres questions relatives à la protection des données. Gardez à l'esprit qu'en tant que contrôleur des données, il est de votre responsabilité de vous assurer de leur conformité.

Comment le CEPD peut-il vous aider?

Le CEPD est l'autorité de surveillance responsable de la protection des données dans les institutions et organes de l'UE. Notre travail consiste à surveiller et à vérifier que les institutions de l'UE respectent les règles de protection des données. Il peut s'agir d'enquêter sur des plaintes, d'effectuer des inspections, de répondre à des consultations préalables, ou de mener des enquêtes de notre propre initiative. Nous élaborons des lignes directrices et proposons des formations pour vous aider à garantir la conformité et à mettre en œuvre les meilleures pratiques. Tout cela a pour objectif de garantir que les institutions de l'UE sont en mesure de donner l'exemple en matière de protection des données.

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-05-18-173-FR-N

www.edps.europa.eu


@EU_EDPS


EDPS


European Data Protection Supervisor

ISBN: 978-92-9242-386-5