

Dispositions d'application concernant les tâches, les fonctions et les compétences du délégué à la protection des données (article 24, paragraphe 8)

Introduction et champ d'application

L'article 24, paragraphe 8, du règlement n° 45/2001 (ci-après «le règlement») dispose que chaque institution ou organe communautaire adopte des dispositions d'application complémentaires concernant le délégué à la protection des données, conformément aux dispositions figurant à l'annexe du règlement. Ces dispositions complémentaires concernent la mise en œuvre de la fonction du délégué à la protection des données et, en particulier, ses fonctions et ses compétences¹.

Le rôle du responsable du traitement et les règles en vertu desquelles une personne concernée peut exercer ses droits peuvent être intégrés dans le document. Cette approche inclusive est recommandée par le CEPD.

Aux termes de l'article 28, paragraphe 1, du règlement, les institutions et organes communautaires doivent consulter le CEPD lorsqu'ils élaborent des mesures administratives relatives au traitement de données à caractère personnel. Ainsi, **le projet de dispositions d'application et la révision des dispositions d'application doivent être soumis au CEPD à des fins de consultation**. Les présentes lignes directrices sont fondées sur cette pratique de consultation et conçues pour faciliter la rédaction des dispositions d'application qui n'ont pas encore été adoptées.

De manière générale, le document devrait inclure au minimum les principes établis aux articles 24, 25 et 26 et à l'annexe du règlement. Dans la mesure nécessaire, le document adaptera ces principes à l'institution ou à l'organe concerné (taille, pratiques administratives, hiérarchie, etc.). Le document devrait être adopté dans une

¹ Le rôle du délégué à la protection des données a été analysé dans le document du CEPD «Document de référence sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n°45/2001». Les DPD élaborent actuellement un document sur les «normes professionnelles pour les délégués à la protection des données des institutions et organes de l'UE exerçant leurs fonctions en vertu du règlement (CE) n° 45/2001». Une fois adopté, le document sera publié sur le site Internet du CEPD. Ces deux documents fournissent des informations utiles pour la rédaction de dispositions d'application en matière de protection des données.

optique à long terme². Idéalement, le document inclura également les meilleures pratiques, dont certaines sont décrites dans le présent document. Toutefois, d'autres meilleures pratiques pourraient être envisagées, en fonction des caractéristiques de l'institution ou organe concerné et de ses besoins à l'égard des activités de traitement de données.

Contenu

1) **Préambule et définitions**

Le préambule doit à tout le moins faire référence aux textes suivants:

- article 16 du Traité sur le fonctionnement de l'Union européenne;
- règlement (CE) n°45/2001 et en particulier son article 24, paragraphe 8 et son annexe.

Si le document comporte des définitions, le CEPD recommande de ne pas adapter celles déjà prévues dans le règlement. En effet, ceci pourrait être source de confusion quant aux termes utilisés en matière de protection des données et en modifier le sens³.

2) **Désignation et statut du délégué à la protection des données** [article 24, paragraphe 1, point a)]

«1. Chaque institution et organe communautaire désigne au moins une personne comme délégué à la protection des données.»

Les dispositions d'application comportent des informations sur les points suivants:

- la durée du mandat du DPD et les circonstances dans lesquelles il ou elle peut être démis(e) de ses fonctions (article 24, paragraphe 4);
- la communication de sa désignation au CEPD (article 24, paragraphe 5);
- ses qualités professionnelles et ses connaissances spécialisées dans le domaine de la protection des données (article 24, paragraphe 2); le document peut également préciser, le cas échéant, que le DPD doit avoir une bonne connaissance des services de l'institution ou de l'organe;
- des ressources doivent lui être affectées pour l'exécution de ses missions (article 24, paragraphe 6). Dans certains cas, un DPD adjoint peut être nécessaire. Chaque DPD devrait bénéficier de la possibilité de recevoir une formation adéquate et de mettre à jour ses connaissances, principalement sur le droit de la protection des données et les aspects techniques;

² Le document fera également l'objet de révisions en temps voulu. La révision ne devrait pas être menée annuellement, mais plutôt tous les cinq ou dix ans ou dès que l'institution ou l'organe l'estimera nécessaire (modifications du mandat, des activités de base de l'institution, etc.). La révision est soumise à consultation, en application de l'article 28, paragraphe 1.

³ Ceci est particulièrement vrai s'agissant des notions de responsable du traitement et de sous-traitant. Le CEPD recommande également d'éviter toute mention de «sous-traitants au sein de l'agence». Les dispositions d'application devraient de préférence aborder la question du sous-traitant en mettant l'accent sur la sous-traitance externe.

- le fait que sa sélection ne doit pas donner lieu à un conflit d'intérêts entre ses fonctions de DPD et toutes autres fonctions officielles qu'il pourrait exercer (article 24, paragraphe 3), dans la mesure nécessaire, le délégué à la protection des données est déchargé d'autres activités (annexe);
- le fait qu'il ou elle devrait agir de façon indépendante tout en assurant l'application interne des dispositions du règlement [article 24, paragraphe 1, point c)] et ne peut recevoir aucune instruction dans l'exercice de ses fonctions (article 24, paragraphe 7). Dans le cas d'un DPD adjoint, le document doit prévoir les mêmes garanties d'indépendance.

3) Tâches, fonctions et compétences du délégué à la protection des données

L'article 24 comprend également un principe général aux termes duquel le DPD veille à ce que les traitements ne risquent pas de porter atteinte aux droits et libertés des personnes concernées. Dans ce qui suit, le CEPD développe les tâches et les fonctions du DPD qui consistent à veiller à la conformité au règlement des traitements de données, ainsi que les compétences du DPD pour l'exercice de sa fonction de protection des données.

«a) veiller à ce que les responsables du traitement et les personnes concernées soient **informés** de leurs droits et obligations au titre du présent règlement;»

Le DPD **sensibilise** aux questions de protection des données et encourage une **culture** de la protection des données à caractère personnel au sein de son institution ou organe. Les responsables du traitement doivent être informés de leurs obligations (voir le point 6 ci-après) et les personnes concernées doivent être informées de leurs droits (voir le point 7 ci-après). Ceci peut prendre différentes formes:

- Formation des membres du personnel et des responsables du traitement;
- Rendre le registre accessible également sous forme électronique, en tant qu'outil propre à assurer la transparence concernant les traitements de données en place au sein de l'institution ou de l'organe (voir ci-après);
- Assistance apportée par le DPD aux responsables du traitement en matière de notification des traitements, laquelle peut également être officialisée dans les dispositions d'application (voir ci-après);
- Contribution du délégué à la protection des données au **rapport annuel d'activité** de l'institution ou de l'organe, car il s'agit d'un bon outil de sensibilisation aux questions de protection des données en interne mais aussi vis-à-vis de l'extérieur.

«b) répondre aux demandes du contrôleur européen de la protection des données et, dans son domaine de compétence, **coopérer** avec le contrôleur

propre initiative;»

- L'obligation de coopérer avec le CEPD devrait être officialisée dans le document. La coopération peut être décrite de façon plus détaillée: la communication d'informations supplémentaires concernant une notification aux fins d'un contrôle préalable, la coopération dans le cadre d'une plainte, la mise en œuvre des recommandations du CEPD, les réponses aux demandes du CEPD, etc.;

«d) tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 25, paragraphe 2;»

- Le registre peut être tenu sous format électronique et papier (voir ci-dessus);
- Le DPD pourrait tenir un inventaire de toutes les opérations de traitement de données à caractère personnel de l'institution ou de l'organe en vue d'une meilleure identification des traitements de données qui doivent être notifiés. L'expérience a démontré qu'un inventaire des traitements était un outil utile pour assurer le respect de l'article 25 du règlement et pour fournir une base à la poursuite de la mise en œuvre du règlement;
- L'assistance apportée par le DPD aux responsables du traitement en matière de notification des traitements peut également être officialisée dans le document;

«e) notifier au contrôleur européen de la protection des données les opérations de traitement susceptibles de présenter des risques particuliers au sens de l'article 27»

- Le DPD détermine si le traitement de données présente des risques particuliers au sens de l'article 27 et doit donc être soumis au contrôle préalable. Le DPD doit consulter le responsable du traitement de données concerné si nécessaire. La possibilité de consulter le CEPD en cas de doute quant à la nécessité d'un contrôle préalable peut également être mentionnée en faisant référence à l'article 27, paragraphe 3.

«Le délégué à la protection des données peut être consulté directement, sans passer par les voies officielles, sur toute question concernant l'interprétation ou l'application du présent règlement, par l'institution ou l'organe communautaire qui l'a désigné, le responsable du traitement ou le comité du personnel concerné ou encore par toute personne physique. Annexe»

- Le rôle consultatif est important et devrait être officialisé dans l'instrument selon les pratiques administratives de l'institution ou de l'organe;

«de sa propre initiative ou à la demande de l'institution ou l'organe communautaire qui l'a désigné, du responsable du traitement, du comité du personnel concerné ou de toute personne physique, il peut **examiner des questions** et des faits qui sont directement en rapport avec ses attributions et qui ont été portés à sa connaissance et faire rapport à la personne qui a demandé cet examen ou au responsable du traitement. **Annexe.**»

- Le DPD a le devoir d'examiner les questions et les faits qui sont directement en rapport avec ses attributions, et, dès lors, des «pouvoirs d'investigation» devraient être développés dans le document (voir point ci-après);

«D'autres bonnes pratiques en vue de l'amélioration de la conformité au règlement qu'il peut être utile de mentionner dans le document:»

- Le délégué peut tenir un inventaire anonyme des demandes écrites d'exercice des droits visés aux articles 13, 14, 15, 16 et 18 du règlement émanant de personnes concernées. Cette documentation pourrait ensuite être utilisée pour effectuer une analyse visant à mesurer la conformité au règlement et à permettre au DPD d'identifier les faiblesses des systèmes;
- Le DPD peut présenter un **programme de travail annuel** et un **rapport annuel** relatifs à ses activités. Un programme de travail du DPD devrait définir ses priorités et exposer les résultats que le DPD souhaite atteindre en matière de sensibilisation, d'inventaire, de notifications, de contrôle préalable, de registre, etc.;

«Dans l'accomplissement de ses missions, le délégué à la protection des données a **accès**, à tout moment, aux données qui font l'objet des opérations de traitement, à tous les locaux, toutes les installations de traitement de données et tous les supports d'information»

- Bien que ceci ne soit pas explicitement mentionné dans le règlement, le CEPD encourage le traitement des requêtes ou des plaintes par le DPD, le cas échéant. En effet, le traitement des requêtes et des plaintes au niveau local peut contribuer dans la plupart des cas à la résolution des problèmes.
- Il serait conforme aux bonnes pratiques de développer les pouvoirs d'investigation du DPD. Les aspects de procédure devraient être définis: le délai dont dispose le DPD pour répondre à la personne qui a commandé l'enquête (réponse écrite), l'obligation pour le responsable du traitement en cause de répondre au DPD (réponse écrite) et le délai qui lui est imparti pour le faire, l'obligation de confidentialité, l'obligation de mener l'enquête en toute indépendance, etc.;

«Le délégué à la protection des données peut faire, en vue d'améliorer concrètement la protection des données, des recommandations à l'institution ou à l'organe communautaire qui l'a désigné et conseiller ces derniers ainsi que le responsable du traitement concerné sur des questions touchant à l'application des dispositions relatives à la protection des données, **Annexe**»

- Le délégué devrait être impliqué dès que son institution ou organe développe des règles internes relatives à la protection des données à caractère personnel; le DPD devrait être un acteur du cadre institutionnel (voir ci-après).

4) Sources d'information du DPD

Les dispositions d'application constituent également un outil pour officialiser la coopération avec le DPD au sein de l'institution ou organe avec notamment:

- L'auditeur interne, les services informatiques, le responsable local de la sécurité de l'information peuvent demander au DPD de formuler des observations et inversement;
- Le DPD devrait être informé dès que l'institution ou organe consulte le CEPD en vertu de l'article 28, paragraphe 1, de l'article 28, paragraphe 2, ou de l'article 46, point d) (et plus largement, être informé de toute correspondance avec le CEPD), il ou elle devrait être informé des interactions directes entre les responsables du traitement de l'institution ou organe et le CEPD;
- Le DPD devrait être informé ou consulté avant l'adoption par son institution ou organe de tout avis, document ou décision interne sur des questions relatives aux dispositions en matière de protection des données.
- Le DPD devrait être informé de toute réception par le responsable du traitement d'une demande d'accès, de rectification, de suppression, etc., ainsi que de toute plainte liée à des questions de protection des données.

5) Rôle et fonctions des responsables du traitement

«Tout responsable du traitement concerné est tenu d'aider le délégué à la protection des données dans l'exécution de ses missions et de lui fournir les informations qu'il sollicite (**annexe**)»

- Les responsables du traitement devraient informer préalablement le DPD de tout traitement des données. Les informations à fournir sont détaillées à l'article 25, paragraphe 2. Les traitements des données devraient être notifiés suffisamment à l'avance pour permettre un contrôle préalable par le CEPD (au moins deux mois) car l'opération ne peut être mise en œuvre avant que le CEPD n'ait remis son avis;
- Toute modification du traitement impliquant des données à caractère personnel devrait être notifiée sans délai au DPD;

- Les responsables du traitement devraient coopérer avec le DPD en vue de la mise en place de l'inventaire des traitements de données visé à l'article 4, paragraphe 2;
- Le cas échéant, les responsables du traitement devraient consulter le DPD sur la conformité des traitements, en particulier en cas de doute quant à la conformité;
- Les responsables du traitement devraient préparer des notifications au DPD concernant tous les traitements qui n'ont pas encore été notifiés;
- Dans le cas où le responsable du traitement externalise une ou plusieurs parties des traitements de données à un sous-traitant, ceci devrait être fait en conformité avec l'article 23. Idéalement, les extraits pertinents de l'article devraient être cités.

6) Droits de la personne concernée

- Les personnes concernées devraient être correctement informées du traitement de leurs données à caractère personnel, conformément aux articles 11 et 12 du règlement;
- Le document peut également expliquer la manière dont les personnes concernées peuvent exercer leurs droits, en application des articles 13 à 19 du règlement (à qui s'adresser, demande par écrit, délais, etc.).

Observations finales

Le règlement (CE) n°45/2001 prévoit un cadre contraignant et détaillé pour les dispositions d'application concernant les tâches, les fonctions et les compétences du DPD. Néanmoins, le CEPD recommande que l'instrument adopté par chaque institution ou organe comporte également des développements supplémentaires de certaines parties du règlement, en tenant compte des caractéristiques propres de l'institution ou organe.

Le champ d'application de l'instrument devrait être étendu au rôle et aux fonctions du responsable du traitement et aux droits des personnes concernées, comme développé ci-dessus. L'instrument devrait également être l'occasion de mieux intégrer le rôle du DPD dans le cadre institutionnel de chaque institution ou organe.