Conseil de
l'Union européenne

Bruxelles, le 3 octobre 2014
(OR. en)

13772/14

Dossier interinstitutionnel:
2012/0011 (COD)

DATAPROTECT 129
JAI 730
MI 726
DRS 120
DAPIX 137
FREMP 164
COMIX 503
CODEC 1926

NOTE

Origine:	la présidence
Destinataire:	Conseil
Nº doc. préc.:	13212/4/14 REV 4 DATAPROTECT 109 JAI 630 MI 579 DRS 104 DAPIX 109 FREMP 148 COMIX 403 CODEC 1675
Objet:	Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) **[première lecture]** - Chapitre IV

1. Le chapitre IV a fait l'objet de discussions approfondies au sein du groupe "Échange d'informations et protection des données" (DAPIX) pendant le premier semestre de 2013. Si, lors de la session du Conseil des 6 et 7 juin 2013, toutes les délégations ont félicité la présidence irlandaise pour les progrès considérables réalisés à l'égard de ce chapitre, plusieurs questions restaient en suspens, en particulier la nécessité de réduire davantage la charge administrative/les coûts de mise en conformité découlant du présent règlement en affinant l'approche fondée sur les risques.

2. Durant la présidence italienne, les discussions sur le chapitre IV se sont poursuivies lors des réunions du DAPIX des 10 et 11 juillet et des 11 et 12 septembre 2014. Les délégations ont en outre envoyé des observations écrites[1]. Les discussions relatives au chapitre IV se sont ensuite poursuivies lors des réunions des conseillers JAI des 19, 22 et 29 septembre 2014 ainsi que dans le cadre des réunions du Coreper du 25 septembre et du 1er octobre 2014.

3. La présidence tient à exprimer ses sincères remerciements aux délégations pour leur coopération constructive sur ce dossier. Elle est d'avis que cette coopération a donné lieu à une révision équilibrée du chapitre IV.

4. Compte tenu de ce qui précède, la présidence invite le Conseil à adopter une orientation générale partielle sur le texte du chapitre IV figurant en annexe, étant entendu que:
   i. cette orientation générale partielle doit être adoptée sous réserve du principe selon lequel il n'y a d'accord sur rien tant qu'il n'y a pas d'accord sur tout et qu'elle n'exclut pas que des modifications ultérieures soient apportées au texte du chapitre IV en vue d'assurer la cohérence globale du règlement;
   ii. cette orientation générale partielle est sans préjudice des questions horizontales, quelles qu'elle soient;
   iii. cette orientation générale partielle ne charge pas la présidence d'engager des trilogues informels avec le Parlement européen sur le texte.

---

[1] Doc. 12267/2/14 REV 2 DATAPROTECT 107 JAI 625 MI 574 DRS 102 DAPIX 107 FREMP 146 COMIX 395 CODEC 1671. L'Autriche a fait circuler une contribution écrite: doc. 13505/14 DATAPROTECT 124 JAI 700 MI 694 DRS 117 DAPIX 130 FREMP 159 COMIX 482 CODEC 1864.

(60) Il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe en particulier que le responsable du traitement (…) soit tenu de mettre en œuvre les mesures appropriées et soit à même (…) de démontrer la conformité (…) des activités de traitement au présent règlement (...). Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités des traitements ainsi que du risque que ceux-ci présentent pour les droits et les libertés des personnes physiques.

(60 *bis*)Ces risques, aux degrés de probabilité et de gravité variables, peuvent apparaître lorsque les traitements de données sont susceptibles d'entraîner des dommages physiques, matériels ou moraux, en particulier lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, [à une violation du (...) pseudonymat][2] ou à tout autre dommage économique ou social important; ou lorsque les personnes concernées sont susceptibles d'être privées de leurs droits et libertés ou de la maîtrise de l'utilisation qui est faite de leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques, l'appartenance syndicale, ainsi que des données génétiques ou concernant la santé ou la vie sexuelle ou des données relatives à des condamnations ou à des infractions pénales, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse et de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes vulnérables, en particulier des enfants; lorsque le traitement porte sur un volume important de données à caractère personnel et sur un nombre important de personnes concernées; (...).

[2] La mention du recours à la pseudonymisation au chapitre IV devra faire l'objet à l'avenir d'une discussion dans le cadre d'un nouveau débat sur la pseudonymisation des données à caractère personnel.

(60 *ter*) *Il convient de déterminer la probabilité et la gravité du risque en fonction de la nature, de la portée, du contexte et des finalités du traitement de données. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque élevé. On entend par risque élevé un risque particulier*[3] *de porter atteinte aux droits et aux libertés des personnes physiques* (...).

(60 *quater*) Les directives relatives à la mise en œuvre de mesures appropriées par le responsable du traitement [ou le sous-traitant] et à la démonstration de la conformité de ses activités, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et les meilleures pratiques visant à atténuer le risque, pourraient être fournies notamment au moyen de codes de conduite et de certifications approuvés et de lignes directrices du comité européen de la protection des données, ou au moyen des indications données par un délégué à la protection des données. Le comité européen de la protection des données peut également publier des lignes directrices relatives aux opérations de traitement considérées comme peu susceptibles de présenter un risque élevé pour les droits et libertés des personnes physiques et indiquer les mesures qui peuvent suffire dans de tels cas pour faire face à un tel risque. (…)

(61) La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel nécessite de prendre les mesures techniques et organisationnelles appropriées, de sorte que les exigences du présent règlement soient respectées. Afin d'être en mesure de démontrer la conformité au présent règlement, le responsable du traitement devrait adopter des règles internes et appliquer des mesures appropriées, qui répondent en particulier aux principes de la protection des données dès la conception et de la protection des données par défaut. Ces mesures devraient consister notamment à limiter le traitement des données à caractère personnel, (...) à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de superviser le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer. Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui se fondent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il conviendrait d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état d'avancement de la technique, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données.

---

[3] L'emploi du terme "particulier" a été remis en question par BE, CZ, ES et UK, qui estiment que ce terme ne rend pas compte de la gravité du risque en cas de risque "élevé".

(62) La protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et de leurs sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par elles, exige une répartition claire des responsabilités au titre du présent règlement, notamment dans le cas où le responsable du traitement détermine les finalités (…) et les moyens du traitement conjointement avec d'autres responsables, ou lorsqu'un traitement est effectué pour le compte d'un responsable du traitement.

(63) Lorsqu'un responsable du traitement qui n'est pas établi dans l'Union traite des données à caractère personnel concernant des personnes résidant dans l'Union, et que les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, ou à l'observation de leur comportement dans l'Union, (...) il conviendrait que le responsable du traitement désigne un représentant, à moins que (...) *le traitement qu'il effectue soit* **occasionnel et peu susceptible de** *constituer un risque pour les droits et libertés des personnes concernées, compte tenu de la nature, de la portée, du contexte et des finalités du traitement*, **ou** que le responsable du traitement ne soit une autorité ou un organisme public (…). Le représentant devrait agir pour le compte du responsable du traitement et devrait pouvoir être contacté par toute autorité de contrôle. Le représentant devrait être expressément désigné par un mandat écrit du responsable du traitement le chargeant d'agir en son nom pour remplir les obligations qui lui incombent en vertu du présent règlement. La désignation de ce représentant ne modifie pas la responsabilité du responsable du traitement au titre du présent règlement. Ce représentant devrait accomplir ses tâches conformément au mandat reçu du responsable du traitement, y compris en ce qui concerne la coopération avec les autorités de contrôle compétentes pour toute action visant à se conformer au présent règlement. Le représentant désigné devrait faire l'objet de mesures coercitives en cas de non-respect du présent règlement par le responsable du traitement.

(63 *bis*) Afin que les prescriptions du présent règlement soient respectées dans le cadre d'un traitement réalisé par un sous-traitant pour le compte du responsable du traitement, lorsque ce dernier confie des opérations de traitement à un sous-traitant, il ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux prescriptions du présent règlement, y compris en matière de sécurité du traitement. (...) L'adhésion du sous-traitant à un code de conduite approuvé ou un mécanisme de certification approuvé peuvent être utilisés comme moyen de démontrer le respect des obligations incombant au responsable du traitement. La réalisation d'un traitement par un sous-traitant devrait être régie par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et l**es** finalité**s** du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer, ainsi que du risque au regard des droits et des libertés de la personne concernée.

Le responsable du traitement et le sous-traitant peuvent choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence puis par la Commission, ou qui font partie d'une certification délivrée dans le cadre du mécanisme de certification. Après l'exécution du traitement pour le compte du responsable du traitement, le sous-traitant devrait renvoyer ou supprimer les données à caractère personnel, à moins que le droit de l'Union ou celui de l'État membre auquel le sous-traitant est soumis exige la conservation des données.

(64) (…)

(65) Afin d'apporter la preuve qu'il se conforme au présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des registres pour toutes les catégories d'activités de traitement relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à sa disposition sur demande pour qu'ils servent au contrôle des opérations en question.

(66) Afin de préserver la sécurité et de prévenir tout traitement contraire au présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques (...) inhérents au traitement et prenne des mesures pour les atténuer. Ces mesures devraient assurer un niveau de sécurité approprié, y compris en ce qui concerne la confidentialité, compte tenu, d'une part, des technologies disponibles et des coûts de mise en œuvre et, d'autre part, du risque lié au traitement de données à caractère personnel et de la nature des données à protéger. (…) Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient d'apprécier les risques que présente le traitement de données, tels que la destruction, la perte, l'altération, accidentelles ou illicites, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière, qui sont susceptibles d'entraîner des dommages physiques, matériels ou moraux.

(66 *bis*) Afin de mieux garantir le respect du présent règlement dans les cas où les traitements sont susceptibles de comporter un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement [ou le sous-traitant] devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque. Il convient de tenir compte du résultat de l'évaluation pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel est effectué dans le respect du présent règlement. Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'autorité de contrôle soit consultée avant que le traitement n'ait lieu.

(67) Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou moraux tels qu'une perte de maîtrise de leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, [une violation du (...) pseudonymat], une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social. (…). En conséquence, dès que le responsable du traitement apprend qu'une (…) violation de données à caractère personnel susceptible de causer des (...) dommages physiques, matériels ou moraux s'est produite, il conviendrait qu'il en informe l'autorité de contrôle sans retard injustifié et, lorsque c'est possible, dans les 72 heures. Si ce délai ne peut être respecté, la notification devrait être assortie d'une explication concernant ce retard. Les personnes physiques dont les droits et libertés pourraient être gravement affectés par la violation devraient en être averties sans retard injustifié afin qu'elles puissent prendre les précautions qui s'imposent. (…) La notification devra décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne concernée afin d'atténuer les effets négatifs pouvant découler de ladite violation. Il convient que les notifications aux personnes concernées soient effectuées aussi rapidement que possible, en coopération étroite avec l'autorité de contrôle et dans le respect des directives fournies par celle-ci ou par d'autres autorités compétentes (telles que les autorités répressives). Par exemple, vu la nécessité d'atténuer un risque immédiat de dommage, il faudrait adresser rapidement une notification aux personnes concernées, mais la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données ou la survenance de violations similaires pourrait justifier un délai plus long.

(68) **(…)** Il faut vérifier si toutes les mesures de protection technologiques et d'organisation appropriées ont été mises en œuvre pour établir immédiatement si une violation des données est intervenue et pour informer rapidement l'autorité de contrôle et la personne concernée (...). Il convient d'établir que la notification a été faite sans retard injustifié, compte tenu en particulier de la nature et de la gravité de la violation des données et de ses conséquences et effets néfastes pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir, dans le cadre des missions et des pouvoirs qui lui sont confiés par le présent règlement.

(68 *bis*) La communication à la personne concernée d'une violation de ses données à caractère personnel n'est pas nécessaire si le responsable du traitement a mis en œuvre les mesures de protection technologiques appropriées et si ces dernières ont été appliquées aux données concernées par ladite violation. Ces mesures de protection technologiques devraient inclure celles qui rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, notamment en cryptant les données à caractère personnel (...).

(69) Lors de la fixation de règles détaillées concernant la forme et les procédures applicables à la notification des violations de données à caractère personnel, il convient de tenir dûment compte des circonstances de la violation, notamment du fait que les données à caractère personnel étaient ou non protégées par des mesures de protection techniques appropriées limitant efficacement le risque d'usurpation d'identité ou d'autres formes d'abus. Par ailleurs, ces règles et procédures devraient tenir compte des intérêts légitimes des autorités répressives dans les cas où une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation.

(70) La directive 95/46/CE prévoyait une obligation générale de notifier les traitements de données à caractère personnel aux autorités de contrôle. Or cette obligation génère une charge administrative et financière, sans pour autant avoir véritablement amélioré la protection des données. En conséquence, les obligations générales de notification devraient être supprimées et remplacées par des procédures et des mécanismes efficaces ciblant plutôt les types de traitement susceptibles de donner lieu à un risque élevé pour les droits et libertés de personnes physiques, du fait de leur nature, portée, *contexte* et finalités (…). On peut entendre par de tels types de traitement ceux qui, en particulier, passent par le recours aux nouvelles technologies, ou qui sont nouveaux et pour lesquels aucune analyse d'impact relative à la protection des données n'a été effectuée au préalable par le responsable du traitement, ou qui deviennent nécessaires compte tenu du temps écoulé depuis le traitement initial[4].

[4] BE est opposée à la référence temporelle qui est faite dans la dernière partie de la phrase.

(70 *bis*) Dans de tels cas, une analyse d'impact relative à la protection des données devrait être réalisée par le responsable du traitement (…), préalablement au traitement, en vue d'évaluer la probabilité et la gravité particulières de ce risque élevé, compte tenu de la nature, de la portée, *du contexte et* des finalités du traitement et des sources du risque, et devrait porter notamment sur les dispositions, garanties et mécanismes envisagés pour atténuer ce risque et assurer la protection des données à caractère personnel et pour démontrer que le présent règlement est respecté.

(71) Cela devrait s'appliquer en particulier aux opérations de traitement à grande échelle (...), qui servent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational pouvant affecter un nombre important de personnes concernées et qui sont susceptibles de comporter un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, compte tenu de l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle ainsi qu'à d'autres opérations de traitement qui (...) entraînent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces dernières d'exercer leurs droits. Une analyse d'impact relative à la protection des données devrait également être effectuée dans les cas où des données sont traitées en vue d'arrêter des décisions relatives à certaines personnes à la suite d'une évaluation systématique et à grande échelle des aspects personnels propres à une personne physique sur la base du profilage desdites données ou à la suite du traitement de catégories particulières de données à caractère personnel, de données biométriques ou de données se rapportant à des condamnations ou des infractions pénales, ou encore à des mesures de sûreté connexes. Une analyse d'impact relative à la protection des données est en outre requise aux fins de la surveillance à grande échelle des zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques sont utilisés, ou pour toute autre opération pour laquelle l'autorité de contrôle compétente considère que le traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées, en particulier parce qu'elles empêchent ces dernières d'exercer un droit ou de bénéficier d'un service ou d'un contrat, ou parce qu'elles sont effectuées systématiquement à grande échelle. Le traitement (...) *de données à caractère personnel, indépendamment de leur volume ou de leur nature, ne devrait pas être considéré comme étant à grand échelle, si le traitement de ces données est protégé par le secret professionnel* (...)*, comme dans le cas du traitement des données à caractère personnel de patients ou clients par un médecin individuel, un professionnel de la santé, un hôpital ou un avocat. Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire.*

(72) Il existe des cas dans lesquels il pourrait être judicieux et économique d'élargir l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.

(73) Une autorité ou un organisme publics peuvent réaliser une analyse d'impact relative à la protection des données si celle-ci n'a pas déjà été faite au moment de l'adoption de la loi nationale régissant la mission de l'autorité ou de l'organisme publics concernés ainsi que l'opération ou l'ensemble d'opérations de traitement en question.

(74) Lorsqu'il ressort d'une analyse d'impact relative à la protection des données que, malgré les garanties, les mesures de sécurité et les mécanismes envisagés pour atténuer le risque, le traitement comporterait un risque élevé pour les droits et les libertés des personnes physiques (...) et que le responsables du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il y a lieu de consulter l'autorité de contrôle avant le début des opérations de traitement. Certains types de traitements de données, notamment du fait de leur ampleur et de leur fréquence, sont susceptibles d'entraîner un tel risque (...) élevé et peuvent également (...) causer un dommage ou porter atteinte aux droits et libertés de la personne concernée. L'autorité de contrôle devrait répondre à la demande de consultation dans un délai déterminé. Toutefois, l'absence de réaction de l'autorité de contrôle dans le délai imparti devrait être sans préjudice de toute intervention de sa part dans le cadre des missions et des pouvoirs qui lui sont confiés par le présent règlement, y compris le pouvoir d'interdire des opérations de traitement. Dans le cadre de ce processus de consultation, les résultats d'une analyse d'impact relative à la protection des données réalisée en ce qui concerne le traitement visé à l'article 33 peuvent être soumis à l'autorité de contrôle, notamment pour ce qui est des mesures envisagées pour atténuer le risque pesant sur les droits et libertés des personnes physiques.

(74 *bis*) Le sous-traitant devrait aider le responsable du traitement, s'il y a lieu et sur demande, à assurer le respect des obligations découlant des analyses d'impact relatives à la protection des données et de la consultation préalable de l'autorité de contrôle.

(74 *ter*) L'autorité de contrôle devrait également être consultée au stade de la préparation d'une mesure législative ou réglementaire qui prévoit le traitement de données à caractère personnel (...), afin d'assurer que le traitement envisagé est conforme au présent règlement et, en particulier, d'atténuer le risque qu'il comporte pour la personne concernée.

(75) Lorsque le traitement est réalisé dans le secteur public ou lorsque, dans le secteur privé, il est effectué par une grande entreprise ou par une entreprise, quelle que soit sa taille, dont les activités de base impliquent des opérations de traitement exigeant un suivi régulier et systématique, une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données peut aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement. Ces délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et leurs tâches d'une manière indépendante.

(76) Il y a lieu d'encourager les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants à élaborer des codes de conduite, dans le respect du présent règlement, de manière à faciliter sa bonne application, en tenant compte des spécificités des traitements effectués dans certains secteurs et des besoins spécifiques des micro, petites et moyennes entreprises. Ces codes de conduite pourraient en particulier définir les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque auquel le traitement peut exposer les droits et libertés des personnes physiques.

(76 *bis*) Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations.

(77) Afin de favoriser la transparence et le respect du présent règlement, la création de mécanismes de certification, ainsi que de marques et de labels en matière de protection des données, devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.

CHAPITRE IV

RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT[5]

SECTION 1
OBLIGATIONS GÉNÉRALES

Article 22

Obligations incombant au responsable de traitement

1. En tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que de la probabilité et de la gravité des risques au regard des droits et des libertés des personnes physiques, le responsable du traitement (…) met en œuvre les mesures appropriées et est à même de démontrer que le traitement des données à caractère personnel est effectué dans le respect du présent règlement.

2. (…)

2 *bis*. Lorsqu'elles sont proportionnées aux activités de traitement de données[6], les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

2 *ter.* L'adhésion aux codes de conduite approuvés visés à l'article 38 ou un mécanisme de certification approuvé visé à l'article 39 peuvent être utilisés comme moyen de démontrer le respect des obligations incombant au responsable du traitement.

3. (…)

4. (…)

---

[5] SI et UK: réserve d'examen sur l'ensemble du chapitre. BE, DE, NL et UK ne sont pas convaincues par les chiffres fournis par la Commission, selon laquelle la réduction des charges administratives résultant de la suppression de l'obligation générale de notification incombant aux responsables du traitement compenserait les charges administratives et coûts de mise en conformité supplémentaires pouvant découler de la proposition de règlement.

[6] HU, RO et PL considèrent que cette formulation donne une latitude beaucoup trop grande aux responsables du traitement. AT estime que la référence à la proportionnalité pose un problème, en particulier pour ce qui est du respect des délais.

Article 23

Protection des données dès la conception et protection des données par défaut

1. (...) Compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre ainsi que *de la nature, de la portée, du contexte et des finalités du traitement* ainsi que de la probabilité et de la gravité du risque présenté par le traitement au regard des droits et des libertés des personnes physiques, les responsables du traitement appliquent (…) des mesures techniques et organisationnelles appropriées pour l'activité de traitement menée et ses objectifs, [notamment la minimisation et la pseudonymisation[7]], de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et (…) assure la protection des droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures appropriées pour garantir que, par défaut, seules (…) les données à caractère personnel (…) qui sont nécessaires[8] au regard de chaque finalité spécifique du traitement sont traitées; cela s'applique à la quantité de (…) données collectées, à l'étendue de leur traitement, à leur période de conservation et à leur accessibilité. Lorsque le traitement n'a pas pour finalité de fournir des informations au public, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques, sans intervention humaine.

2 *bis*. Un mécanisme de certification approuvé conformément à l'article 39 *peut être utilisé comme moyen* de démontrer le respect des exigences visées aux paragraphes 1 et 2.

3. (…)

4. (…)

---

[7] DE considère que, compte tenu de l'article 5, point c), le principe d'économie et d'évitement des données, ainsi que l'anonymisation et la pseudonymisation devraient figurer parmi les principales options de mise en œuvre. Ce débat devra toutefois avoir lieu dans le cadre des discussions sur la pseudonymisation des données à caractère personnel.

[8] CZ préférerait les termes "ne sont pas excessives". Cette formulation pourrait à nouveau être modifiée à l'avenir dans le cadre du débat sur la formulation de l'article 5, paragraphe 1, point c).

Article 24

Responsables conjoints du traitement[9]

1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement de données à caractère personnel, ils sont les responsables conjoints du traitement. Ils définissent de manière transparente, par voie d'accord, leurs obligations respectives afin de se conformer aux exigences du présent règlement, en ce qui concerne notamment (…) l'exercice des droits de la personne concernée et leurs obligations respectives quant à la communication des informations visées à l'article 14 et à l'article 14 *bis*, sauf si et dans la mesure où les obligations respectives des responsables du traitement sont définies par le droit de l'Union ou la législation de l'État membre à laquelle les responsables des données sont soumis. L'accord précise lequel des responsables conjoints sert de point de contact unique pour que les personnes concernées puissent exercer leurs droits.

2. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard et contre chacun des (...) responsables du traitement.

3. L'accord reflète dûment les rôles effectifs respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées et ses grandes lignes sont mises à disposition de la personne concernée. Le paragraphe 2 ne s'applique pas lorsqu'il a été indiqué à la personne concernée, de manière transparente et sans ambiguïté, lequel des responsables conjoints a procédé au traitement, sauf si cet accord autre qu'un accord déterminé par le droit de l'Union ou la législation d'un État membre est abusif au regard des droits de la personne concernée (...).

---

[9] Réserve de SI; cette délégation met en garde contre les conflits juridiques qui pourraient survenir sur la répartition de la responsabilité et elle estime donc que cet article devra encore être revu dans le cadre du futur débat sur le chapitre VIII. FR considère aussi que la répartition de la responsabilité entre le responsable du traitement et le sous-traitant est très vague et CZ a exprimé des doutes quant à la possibilité de faire appliquer cette disposition dans le secteur privé, en dehors d'accords conclus dans le cadre d'un groupe d'entreprises, et pense qu'elle devrait contenir une clause de sauvegarde contre une externalisation de la responsabilité.

Article 25

Représentants des responsables du traitement qui ne sont pas établis dans l'Union

1. Lorsque l'article 3, paragraphe 2, s'applique, le responsable du traitement désigne par écrit un représentant dans l'Union.

2. Cette obligation ne s'applique pas:

   a) (…);

   b) *au traitement qui est* **occasionnel**[10] **et** *peu susceptible de constituer un* (...) *risque au regard des droits et des libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement* (...);

   c) à une autorité ou à un organisme publics;

   d) (…)

3. Le représentant est établi dans l'un des États membres dans lesquels résident les personnes physiques dont les données à caractère personnel sont traitées dans le contexte de l'offre de biens ou de services qui leur est proposée ou dont le comportement est observé.

3 *bis*. Le représentant est mandaté par le responsable du traitement afin d'être consulté en complément ou à la place du responsable du traitement, notamment par les autorités de contrôle et les personnes concernées, sur toutes les questions relatives au traitement de données à caractère personnel, aux fins d'assurer le respect du présent règlement.

4. La désignation d'un représentant par le responsable du traitement est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement lui-même.

[10] Réserve: HU, SE et UK.

Article 26

Sous-traitant

1. (…)[11]. Le responsable du traitement fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes de mise en œuvre des mesures techniques et organisationnelles appropriées (…), de manière à ce que le traitement soit conforme aux prescriptions du présent règlement (…).

1 *bis*. Le sous-traitant ne recrute pas un autre sous-traitant sans l'accord écrit préalable, spécifique ou général, du responsable du traitement. Dans ce cas, le sous-traitant devrait toujours informer le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements[12].

1 *ter*. (…)[13].

2. La réalisation d'un traitement par un sous-traitant est régie par un contrat ou **un** acte juridique au titre du droit de l'Union ou du droit national liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, les droits du responsable du traitement (...) et prévoyant notamment que le sous-traitant:

   a) ne traite les données à caractère personnel que sur instruction du responsable du traitement (…), à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou de la législation de l'État membre à laquelle le responsable du traitement est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement des données, sauf si la loi interdit une telle information pour des motifs importants d'intérêt public;

---

11 La présidence suggère de compléter l'article 5, paragraphe 2, par les termes "également si des données à caractère personnel sont traitées pour son compte par un sous-traitant". Ce point pourrait aussi nécessiter un examen plus approfondi dans le cadre du futur débat sur la responsabilité dans le contexte du chapitre VIII.

12 LU et FI sont préoccupées par le fait que cette disposition pourrait constituer une ingérence dans la liberté contractuelle.

13 Plusieurs délégations (CZ, AT et LU) ont indiqué qu'un alignement était nécessaire avec les règles visées à l'article 77. La discussion relative à l'exercice des droits conférés à la personne concernée devrait en fait intervenir dans le cadre du chapitre VIII.

b) (…)

c) prend toutes les mesures (…) requises en vertu de l'article 30;

d) respecte les conditions de recrutement d'un autre sous-traitant (…), telles que l'obligation d'une autorisation préalable spécifique du responsable du traitement;

e) (…), compte tenu de la nature du traitement, aide le responsable du traitement à donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;

f) (...) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 30 à 34;

g) renvoie ou supprime les données à caractère personnel, selon le choix du responsable du traitement, au terme des services de traitement des données précisés dans le contrat ou dans un autre acte juridique, à moins que le droit de l'Union ou celui de l'État membre auquel le sous-traitant est soumis exige la conservation des données;

h) met à la disposition du responsable du traitement (…) toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues par le présent article, permettre la réalisation d'audits par le responsable du traitement et contribuer à ces audits.

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou des dispositions de l'Union ou des États membres relatives à la protection des données.

2 *bis*. Lorsqu'un sous-traitant recrute (...) un autre sous-traitant pour exécuter des opérations de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations que celles fixées dans le contrat ou l'autre acte juridique liant le sous-traitant au responsable du traitement, visé au paragraphe 2, s'imposent à cet autre sous-traitant *par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit national*[14], en particulier pour ce qui est de présenter des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

2 bis bis *L'adhésion du sous-traitant à un code de conduite approuvé visé à l'article 38 ou* un *mécanisme de certification* approuvé *visé à l'article 39*[15] peuvent être utilisés comme moyen de démontrer l'existence *des garanties suffisantes visées aux paragraphes 1 et 2 bis*.

2 *bis ter* Sans préjudice d'un contrat particulier entre le responsable du traitement et le sous-traitant, le contrat ou l'autre acte juridique visé aux paragraphes 2 et 2 *bis* peut être fondé, en tout ou en partie, sur les clauses contractuelles types visées aux paragraphes 2 *ter* et 2 *quater* ou sur des clauses contractuelles types qui font partie d'une certification délivrée au responsable du traitement ou au sous-traitant conformément aux articles 39 et 39 *bis*.

---

14 HU suggère de préciser cette référence au droit de l'Union ou au droit national en ajoutant les termes "liant cet autre sous-traitant au sous-traitant initial".

15 Réserve de FR; SK suggère de préciser que, si l'autre sous-traitant ne remplit pas les obligations qui lui incombent en matière de protection des données en vertu du contrat ou d'un autre acte juridique, le sous-traitant demeure pleinement responsable devant le responsable du traitement de la manière dont l'autre sous-traitant s'acquitte de ses obligations. En autorisant le sous-traitant à sous-traiter lui-même et en n'imposant pas au sous-traitant ultérieur d'avoir une relation contractuelle avec le responsable du traitement, il devrait offrir suffisamment de sécurité juridique au responsable du traitement en termes de responsabilité. Le principe de responsabilité du sous-traitant principal pour toute violation commise par le sous-traitant ultérieur est énoncé dans la clause 11 figurant dans la décision 2010/87/UE relative aux clauses types et dans les règles d'entreprises contraignantes pour les sous-traitants, et il constitue donc la norme en vigueur. Il est aussi proposé de supprimer la référence à l'article 2 *bis bis*.

2 *ter*. La Commission peut établir des clauses contractuelles types pour les questions visées aux paragraphes 2 et 2 *bis*, conformément à la procédure d'examen visée à l'article 87, paragraphe 2[16].

2 *quater*. Une autorité de contrôle peut adopter des clauses contractuelles types pour les questions visées aux paragraphes 2 et 2 *bis*, conformément au mécanisme de contrôle de la cohérence visé à l'article 57.

3. Le contrat ou autre acte juridique visé aux paragraphes 2 et 2 *bis* est écrit, y compris en format électronique.

4. (…)

5. (…)[17]

Article 27

Traitement effectué sous l'autorité du responsable du traitement et du sous-traitant

(…)

[16] PL est inquiète à la perspective d'un scénario dans lequel la Commission n'agirait pas. CY et FR sont opposées au fait de confier ce rôle à Cion (FR pourrait éventuellement accepter qu'il soit confié au comité européen de la protection des données).

[17] Cion: réserve sur la suppression.

Article 28

Registre des catégories d'activités de traitement <u>des données à caractère personnel</u>[18]

1. Chaque responsable du traitement et (…), le cas échéant, le représentant du responsable du traitement, tiennent un <u>registre de</u> toutes les <u>catégories d'activités</u> de traitement <u>de données à caractère personnel</u> mises en œuvre sous leur responsabilité. <u>Ce registre</u> comporte (…) les informations suivantes:

   a) le nom et les coordonnées du responsable du traitement et de tout responsable conjoint du traitement (…), du représentant <u>du responsable du traitement</u> et, le cas échéant, du <u>délégué à la protection des données</u>;

   b) (…)

   c) les finalités du traitement, y compris les intérêts légitimes, lorsque le traitement se fonde sur l'article 6, paragraphe 1, point f);

   d) une description des catégories de personnes concernées et des catégories de données à caractère personnel s'y rapportant;

   e) les (…) catégories de destinataires <u>auxquels les données à caractère personnel ont été ou seront communiquées, en particulier lorsque les destinataires sont établis dans des pays tiers</u>;

   f) le cas échéant, <u>les catégories</u> de transferts de données à caractère <u>personnel</u> vers un pays tiers ou à une organisation internationale (…);

   g) <u>dans la mesure du possible</u>, les délais <u>prévus</u> pour l'effacement des différentes catégories de données;

   h) <u>dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 30, paragraphe 1.</u>

[18] AT: réserve d'examen.

2 *bis*. Chaque sous-traitant tient un registre de toutes les catégories de traitements de données à caractère personnel effectués pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du sous-traitant ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, le nom et les coordonnées du représentant du responsable du traitement;

b) le nom et les coordonnées du délégué à la protection des données, le cas échéant;

c) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

d) le cas échéant, les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 30, paragraphe 1.

3 *bis*. Les registres visés aux paragraphes 1 et 2 *bis* se présentent sous une forme écrite, y compris électronique, ou sous une autre forme non lisible pouvant être convertie en forme lisible.

3. Sur demande, le responsable du traitement et le sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement mettent le registre à la disposition (…) de l'autorité de contrôle.

4. Les obligations visées aux paragraphes 1 et 2 *bis* ne s'appliquent pas:

a) (…); ou

b) aux entreprises ou organismes comptant moins de 250 salariés, sauf si le traitement qu'ils effectuent est susceptible de comporter un risque élevé au regard des droits et des libertés des personnes concernées, par exemple (...) une discrimination, un vol ou une usurpation d'identité, [une violation du (...) pseudonymat,] une perte financière, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social pour les personnes concernées, compte tenu de la nature, de la portée, du contexte et des finalités du traitement; ou

5. (…)

6. (…)

Article 29

Coopération avec l'autorité de contrôle

(…)

SECTION 2
SÉCURITÉ DES DONNÉES

Article 30

Sécurité des traitements

1. Compte tenu des techniques disponibles et des coûts liés à la mise en œuvre et prenant en considération la nature, la portée, le contexte et les finalités du traitement ainsi que la probabilité et la gravité du risque pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées[, y compris (...) la pseudonymisation de données à caractère personnel,] afin de garantir un niveau de sécurité approprié au regard du risque.

1 *bis*. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement des données (...), résultant notamment de la destruction accidentelle ou illégale, de la perte, de l'altération, de la divulgation ou de l'accès non autorisé à des données à caractère personnel transmises, stockées ou faisant l'objet d'un autre traitement.

2. (…)

2 *bis*. L'adhésion aux codes de conduite approuvés visés à l'article 38 ou un mécanisme de certification approuvé visé à l'article 39 peuvent être utilisés comme moyen d'*attester du respect des exigences visées au paragraphe 1.*

2 *ter*. Le responsable du traitement et le sous-traitant prennent des mesures pour que toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne puisse les traiter que sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou la législation d'un État membre.

3. (…)

4. (…)

Article 31

Notification à l'autorité de contrôle d'une violation de données à caractère personnel[19]

1. En cas de violation de données à caractère personnel susceptible d'exposer les personnes physiques à un risque élevé au regard de leurs droits et libertés, par exemple une discrimination, un vol ou une usurpation d'identité, une perte financière, [une violation du (...) pseudonymat,] une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important, le responsable du traitement en adresse notification à l'autorité de contrôle compétente conformément à l'article 51, sans retard injustifié et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 72 heures, la notification comporte une motivation.

1 *bis*. La notification visée au paragraphe 1 n'est pas requise si une communication à la personne concernée n'est pas nécessaire aux termes de l'article 32, paragraphe 3, points a) et b)[20].

2. (…) Le sous-traitant informe le responsable du traitement de la violation de données à caractère personnel sans retard injustifié après en avoir pris connaissance.

---

19 AT et SI: réserve d'examen. Réserve de Cion: il convient de préserver la cohérence avec le système institué par la directive relative à la vie privée et aux communications électroniques; SI estime que cet alignement pourrait être obtenu en supprimant le terme "élevé" figurant après le terme "risque" aux articles 31 et 32.

20 BE, AT et PL estiment que ce paragraphe devrait être supprimé.

3. La notification visée au paragraphe 1 doit, à tout le moins:

a) décrire la nature de la violation de données à caractère personnel y compris, si possible et s'il y a lieu, les catégories et le nombre approximatifs de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données concernés;

b) communiquer l'identité et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) (…)

d) décrire les conséquences probables de la violation de données à caractère personnel constatée par le responsable du traitement;

e) décrire les mesures prises ou proposées par le responsable du traitement pour remédier à la violation de données à caractère personnel; et

f) le cas échéant, indiquer des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel.

3 *bis*. Si et dans la mesure où il n'est pas possible de fournir les informations visées au paragraphe 3, points d), e) et f), en même temps que les informations visées au paragraphe 3, points a) et b), le responsable du traitement fournit ces informations sans autre retard justifié.

4. Le responsable du traitement conserve une trace documentaire de toute violation de données à caractère personnel visée aux paragraphes 1 et 2, en indiquant son contexte, ses effets et les mesures prises pour y remédier. La documentation constituée doit permettre à l'autorité de contrôle de vérifier le respect des dispositions du présent article. (…)

5. (…)

6. (…)[21]

[21] Cion: réserve sur la suppression.

Article 32

Communication à la personne concernée d'une violation de données à caractère personnel[22]

1. Lorsque la violation de données à caractère personnel est susceptible d'exposer les personnes physiques à un risque élevé au regard de leurs droits et libertés , par exemple une discrimination, un vol ou une usurpation d'identité, une perte financière, une atteinte à la réputation, [une violation du (...) pseudonymat,] une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important, le responsable du traitement (...) en adresse notification sans retard injustifié à la personne concernée.

2. La communication à la personne concernée prévue au paragraphe 1 décrit la nature de la violation de données à caractère personnel et contient au moins les informations et recommandations prévues à l'article 31, paragraphe 3, points b), e) et f).

3. La communication (…) à la personne concernée (…), visée au paragraphe 1, n'est pas nécessaire si:

   a) le responsable du traitement (…) a mis en œuvre les mesures de protection technologiques et organisationnelles appropriées et que ces dernières ont été appliquées aux données affectées par ladite violation, en particulier celles qui rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, telles que le cryptage; ou

   b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé au regard des droits et des libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser; ou

   c) elle risque d'entraîner des mesures disproportionnées, eu égard notamment au nombre de cas concernés. Dans ce cas, il convient plutôt de procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace; ou

[22] AT: réserve d'examen. Réserve de Cion: il convient de préserver la cohérence avec le système institué par la directive relative à la vie privée et aux communications électroniques.

d) elle risque de porter atteinte à un intérêt public important.

4. (…)

5. (…)

6. (…)[23]

SECTION 3

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES ET CONSULTATION PRÉALABLE

Article 33

Analyse d'impact relative à la protection des données[24]

1. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'exposer les personnes physiques à un risque élevé[25] au regard de leurs droits et libertés, par exemple une discrimination, un vol ou une usurpation d'identité, une perte financière, une atteinte à la réputation, [une violation du (...) pseudonymat,] une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important, le responsable du traitement (…)[26] effectue avant le traitement une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel. (…)

1 *bis*. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

---

23 Cion: réserve sur la suppression.

24 FR, HU, AT et Cion ont exprimé des doutes sur le concept de nouveaux types de traitement, qui est à présent clarifié dans le considérant 70. UK considère que cette obligation ne devrait pas s'appliquer lorsqu'un traitement doit avoir lieu pour des raisons d'intérêt public supérieur (par exemple une situation d'urgence en matière de santé publique).

25 FR, RO, SK et UK ont mis en garde contre les charges administratives considérables résultant de l'obligation proposée. UK considère que l'obligation d'effectuer une analyse d'impact relative à la protection des données devrait être limitée aux cas où un risque élevé pour les droits des personnes concernées a été constaté.

26 Cion: réserve sur la suppression.

2. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est en particulier requise dans les cas suivants:

a) l'évaluation systématique et à grande échelle (…) des aspects personnels propres à (…) des personnes physiques (…), qui est fondée sur le profilage et sur la base de laquelle sont prises des décisions[27] produisant des effets juridiques concernant des personnes concernées ou affectant gravement lesdites personnes;

b) le traitement des catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1 (...)[28], de données biométriques ou de données se rapportant à des condamnations ou des infractions pénales, ou encore à des mesures de sûreté connexes, lorsque les données sont traitées aux fins de l'adoption de (…) décisions à grande échelle visant certaines personnes;

c) la surveillance *à grande échelle* de zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques (…) sont utilisés;

d) (…);

e) (…)[29].

2 *bis*. L'autorité de contrôle établit et publie une liste des types de traitements soumis à l'obligation d'une analyse d'impact relative à la protection des données conformément au paragraphe 1. L'autorité de contrôle communique cette liste au comité européen de la protection des données[30].

---

27 Dans le futur, cette formulation sera alignée sur le libellé final de l'article 20.

28 HU suggère que les données relatives aux enfants soient à nouveau prises en considération.

29 FR: réserve d'examen. PL considère que le comité européen de la protection des données pourrait se voir attribuer un rôle dans l'identification des opérations à haut risque.

30 Réserve de CZ. HU se demande quelles seraient les éventuelles conséquences juridiques de l'inscription sur la liste, par une autorité chargée de la protection des données, d'un type de traitement au regard des traitements en cours, et aussi qu'elle en serait la portée territoriale. La présidence considère que le rôle éventuel du comité européen de la protection des données à cet égard devrait être discuté dans le cadre du chapitre VII.

2 *ter*. L'autorité de contrôle peut aussi établir et publier une liste des types de traitements pour lesquels aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité européen de la protection des données.

2 *quater*. Avant d'adopter les listes visées respectivement aux paragraphes 2 *bis* et 2 *ter*, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence prévu à l'article 57, lorsque ces listes comprennent des traitements liés à l'offre de biens ou de services à des personnes concernées ou à l'observation de leur comportement dans plusieurs États membres, ou susceptibles d'affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union[31].

3. L'analyse contient au moins une description générale des traitements envisagés, une évaluation du risque visé au paragraphe 1, les mesures envisagées pour faire face au risque y compris les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec le présent règlement, en tenant compte des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées[32].

3 *bis*. Le respect, par les responsables du traitement ou sous-traitants compétents, des codes de conduite approuvés visés à l'article 38 est dûment pris en compte lors de l'évaluation de la légalité et de l'impact des opérations de traitement effectuées par lesdits responsables ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données[33].

4. *Le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu*, sans préjudice de la protection des intérêts généraux ou commerciaux ni de la sécurité des traitements (...)[34].

---

31 CZ: réserve.
32 FR: réserve d'examen.
33 HU considère qu'il faudrait déplacer cette disposition dans un considérant.
34 CZ et FR estiment qu'il s'agit d'une obligation totalement irréalisable; IE: réserve.

5. (...) Lorsque le traitement visé à l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans la législation de l'État membre à laquelle le responsable du traitement est soumis, et que cette législation régit l'opération ou l'ensemble des opérations de traitement en question[35], les paragraphes 1 à 3 ne s'appliquent pas, sauf si les États membres estiment qu'une telle analyse est nécessaire avant le traitement.

6. (…)

7. (…)

Article 34

***(…) Consultation préalable*[36]**

1. (…)

2. Le responsable du traitement (…)[37] consulte l'autorité de contrôle avant le traitement de données à caractère personnel lorsqu'une analyse d'impact relative à la protection des données telle qu'elle est prévue à l'article 33 indique que le traitement présenterait un (...) risque élevé si *le responsable du traitement ne devait pas prendre de mesures* pour atténuer le risque.

---

35 BE et SI ont fait savoir que ce texte devra être revu dans le cadre du futur débat sur la manière d'étendre le champ d'application du règlement au secteur public.

36 HU: réserve d'examen; SK: réserve sur le fait de donner ce rôle aux autorités de protection des données, qui pourraient ne pas être en mesure de s'occuper de ces consultations dans tous les cas. ES propose d'exempter les responsables d'un traitement de l'obligation de procéder à une consultation préalable s'ils ont désigné un délégué à la protection des données.

37 Cion et LU: réserve sur la suppression du sous-traitant.

3. Lorsque l'autorité de contrôle est d'avis que le traitement visé au paragraphe 2 ne serait pas conforme au présent règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué *le risque*, elle doit, dans un délai maximum de six semaines suivant la demande de consultation, conseiller le responsable du traitement de données, par écrit, et peut utiliser les pouvoirs visés à[38] l'article 53 (...). Ce délai peut être prolongé de six semaines, compte tenu de la complexité du traitement prévu. En cas de prolongation du délai, le responsable du traitement ou le sous-traitant est informé des raisons du report, dans un délai d'un mois à compter de la réception de la demande.

4. (…)

5. (…)

6. Lorsqu'il consulte l'autorité de contrôle, conformément au paragraphe 2, le responsable du traitement (...) informe l'autorité de contrôle:

a) le cas échéant, des responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants qui interviennent dans le traitement, en particulier pour le traitement au sein d'un groupe d'entreprises;

b) des finalités et des modalités du traitement prévu;

c) des mesures et des garanties prévues afin de protéger les droits et les libertés **des** personne**s** concernée**s** conformément au présent règlement;

d) le cas échéant, des coordonnées du délégué à la protection des données;

e) de l'analyse d'impact relative à la protection des données prévue à l'article 33, et

f) de toute (…) autre information demandée par l'autorité de contrôle (…).

---

38 Réserve de UK; cette délégation considère que le pouvoir d'interdire des traitements ne devrait pas s'appliquer lorsqu'un traitement doit avoir lieu pour des raisons d'intérêt public supérieur (par exemple une situation d'urgence en matière de santé publique). La présidence pense que cette question devrait toutefois être débattue dans le cadre du chapitre VI consacré aux pouvoirs des autorités de protection des données, ces derniers pouvant évidemment être aussi utilisés indépendamment de toute consultation.

7. Les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative qui prévoit le traitement de données à caractère personnel (...)[39].

7 *bis*. Nonobstant le paragraphe 2, la législation des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable pour le traitement de données à caractère personnel effectué par un responsable du traitement dans le cadre d'une mission mené par celui-ci dans l'intérêt public, y compris le traitement de telles données relatives à la protection sociale et à la santé publique[40].

8. (…)

9. (…)

[39] IE: réserve d'examen concernant cette suppression.
[40] SE: réserve d'examen.

SECTION 4
DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Article 35

Désignation du délégué à la protection des données

1. Le responsable du traitement ou le sous-traitant peuvent ou doivent, si le droit de l'Union ou le droit d'un État membre l'exigent[41], désigner un délégué à la protection des données (…).

2. Un groupe d'entreprises peut désigner un délégué à la protection des données unique.

3. Lorsque le responsable du traitement ou le sous-traitant est une autorité ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

4. (…)

5. Le (…) délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données, et de sa capacité à accomplir les tâches énumérées à l'article 37, notamment l'absence de tout conflit d'intérêts. (…)

6. (…)

7. (…) Durant son mandat, sauf motifs graves au regard de la législation de l'État membre concerné justifiant le licenciement d'un employé ou d'un fonctionnaire, le délégué à la protection des données ne peut être démis de ses fonctions que s'il ne remplit plus les conditions requises pour exercer les missions qui lui incombent en vertu de l'article 37.

---

[41] Rendu facultatif à la suite d'une décision du Conseil. AT: réserve d'examen. DE, HU et AT auraient préféré que les cas de désignation obligatoire du DPD soient définis dans le règlement lui-même et peuvent souhaiter revenir sur cette question à un stade ultérieur. Réserve de Cion sur le caractère facultatif et la suppression des points a) à c).

8. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou accomplir ses missions sur la base d'un contrat de service.

9. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle (…).

10. Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de données les concernant et à l'exercice des droits que leur confère le présent règlement.

11. (…)

Article 36

Fonction du délégué à la protection des données

1. Le responsable du traitement ou le sous-traitant veillent à ce que le délégué à la protection des données soit associé d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données à caractère personnel.

2. Le responsable du traitement ou le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 37 en fournissant (…) les ressources nécessaires à l'exécution de ces missions ainsi que l'accès aux données à caractère personnel et aux traitements.

3. Le responsable du traitement ou le sous-traitant veillent à ce que le délégué à la protection des données puisse agir en toute indépendance dans l'accomplissement de ses missions et ne reçoive aucune instruction en ce qui concerne l'accomplissement de celles-ci. Il ne saurait être pénalisé par le responsable du traitement ou le sous-traitant pour l'accomplissement de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé du responsable du traitement ou du sous-traitant.

4. Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant doivent veiller à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

Article 37

Missions du délégué à la protection des données

1. Les missions du (...) délégué à la protection des données (…) sont les suivantes:

a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les salariés traitant des données à caractère personnel sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions de l'Union ou de l'État membre concerné en matière de protection des données (…);

b) contrôler la conformité au présent règlement, à d'autres dispositions de l'Union ou de l'État membre concerné en matière de protection des données et aux règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux traitements, et les audits s'y rapportant;

c) (…)

d) (…)

e) (…)

f) dispenser des conseils, lorsque cela est demandé, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution des tâches conformément à l'article 33;

g) vérifier qu'il a été répondu aux demandes de l'autorité de contrôle et, dans le domaine de compétence du délégué à la protection des données, coopérer avec l'autorité de contrôle, à la demande de celle-ci ou à l'initiative du délégué à la protection des données;

h) faire office de point de contact pour l'autorité de contrôle sur les questions liées au traitement de données à caractère personnel, y compris la consultation préalable visée à l'article 34, et consulter celle-ci, le cas échéant, sur tout autre sujet .

2. (…)

2 *bis*. Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement eu égard à la *nature, à la portée, au contexte et aux finalités* du traitement.

SECTION 5
CODES DE CONDUITE ET CERTIFICATION

Article 38

Codes de conduite[42]

1. Les États membres, les autorités de contrôle, le comité européen de la protection des données et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des différents secteurs de traitement de données et des besoins spécifiques des micro, petites et moyennes entreprises, à la bonne application des dispositions du présent règlement.

1 *bis*. Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou en proroger la validité, afin de préciser les modalités d'application des dispositions du présent règlement, telles que:

a) le traitement loyal et transparent des données;

aa) les intérêts légitimes défendus par les responsables du traitement dans des contextes spécifiques;

b) la collecte des données;

bb) la pseudonymisation des données à caractère personnel;

c) l'information du public et des personnes concernées;

d) l'exercice des droits des personnes concernées;

e) l'information et la protection des enfants et la manière de recueillir le consentement des parents et des tuteurs de l'enfant;

ee) les mesures et les procédures visées aux articles 22 et 23 et les mesures visant à assurer la sécurité du traitement visé à l'article 30;

[42] AT, FI, SK et PL: réserve d'examen.

ef) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication à la personne concernée de ces violations;

f) (…)

1 *bis ter.* Outre l'adhésion du responsable du traitement ou du sous-traitant soumis au règlement, les codes de conduite *approuvés* en application du paragraphe 2 peuvent aussi être appliqués par des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement conformément à l'article 3, afin de fournir les garanties appropriées dans le cadre des transferts de données à caractère personnel à un pays tiers ou à une organisation internationale conformément aux conditions visées à l'article 42, paragraphe 2, point d). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'une autre manière, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

1 *ter*. Ce code de conduite comprend les mécanismes permettant à l'organisme visé à l'article 38 bis , paragraphe 1, de procéder au contrôle obligatoire[43] du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer, sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente au titre de l'article 51 ou de l'article 51 bis .

2. Les associations et les autres organismes visés au paragraphe 1 *bis* qui ont l'intention d'élaborer un code de conduite ou de modifier ou proroger un code de conduite existant soumettent le projet de code à l'autorité de contrôle qui est compétente au titre de l'article 51. L'autorité de contrôle rend un avis sur la conformité au présent règlement du projet de code de conduite, de la modification ou de la prorogation du code existant, et approuve ce projet de code de conduite, cette modification ou cette prorogation du code existant si elle estime qu'il fournit des garanties appropriées suffisantes.

2 *bis*. Lorsque l'avis visé au paragraphe 2 confirme que le code de conduite ou le code modifié ou prorogé est conforme au présent règlement et que le code est approuvé, et s'il ne concerne pas des traitements mis en œuvre dans plusieurs États membres, l'autorité de contrôle enregistre le code de conduite et en publie les références.

[43] CZ préférerait que ce contrôle soit facultatif.

2 *ter*. Si le projet de code de conduite concerne des traitements mis en œuvre dans plusieurs États membres, l'autorité de contrôle compétente au titre de l'article 51 le soumet, avant approbation, suivant la procédure visée à l'article 57, au comité européen de la protection des données, qui donne un avis sur la conformité au présent règlement du projet de code de conduite, de la modification ou de la prorogation du code existant ou, dans la situation visée au paragraphe 1 *bis ter*, sur la fourniture de garanties appropriées[44].

3. Si l'avis visé au paragraphe 2 *ter* confirme que le code de conduite ou le code modifié ou prorogé est conforme au présent règlement ou, dans la situation visée au paragraphe 1 *bis ter*, fournit des garanties appropriées, le comité européen de la protection des données soumet son avis à la Commission .

4. La Commission peut adopter des actes d'exécution afin de constater par voie de décision que les codes de conduite approuvés ainsi que les modifications ou prorogations de codes de conduite existants approuvés qui lui ont été soumis en vertu du paragraphe 3 sont d'application générale sur le territoire de l'Union. Les actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

5. La Commission assure une publicité appropriée aux codes approuvés dont elle a constaté par voie de décision qu'ils étaient d'application générale conformément au paragraphe 4.

5 *bis*. Le comité européen de la protection des données recueille tous les codes de conduite approuvés ainsi que les modifications qui y ont été apportées dans un registre et les met à la disposition du public par tout moyen approprié, comme le portail européen e-Justice.

---

44 FR a proposé un paragraphe 2 *quater* libellé comme suit: "Les codes de conduite approuvés en vertu du paragraphe 2 *bis* constituent un élément de la relation contractuelle entre le responsable du traitement et la personne concernée. Lorsque ces codes de conduite déterminent la conformité au règlement du responsable du traitement ou du sous-traitant, ils sont juridiquement contraignants et exécutoires."

Article 38 bis

Suivi des codes de conduite approuvés[45]

1. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente au titre des articles 52 et 53, le contrôle du respect du code de conduite visé à l'article 38, paragraphe 1 *ter*, peut être effectué par un organisme[46] disposant d'un niveau d'expertise approprié au regard de l'objet du code agréé à cette fin par l'autorité de contrôle compétente.

2. Un organisme visé au paragraphe 1 peut être agréé à cette fin si:

   a) il a prouvé, à la satisfaction de l'autorité de contrôle compétente, son indépendance et l'expertise dont il dispose au regard de l'objet du code;

   b) il a établi des procédures qui lui permettent d'apprécier si les responsables du traitement ou les sous-traitants satisfont aux conditions pour appliquer le code, de contrôler le respect des dispositions dudit code et d'examiner son fonctionnement périodiquement;

   c) il a établi des procédures et des structures pour traiter les réclamations relatives aux violations du code ou à la manière dont le code a été ou est appliqué par un responsable du traitement ou un sous-traitant, et rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public;

   d) il prouve, à la satisfaction de l'autorité de contrôle compétente, que ses tâches et ses missions n'entraînent pas de conflit d'intérêt.

---

[45] AT, LU: réserve d'examen.

[46] CZ, ES et LU sont opposées à ce que l'on donne ce rôle à de tels organismes distincts. Des craintes ont notamment été émises concernant la charge administrative liée à la mise en place de ces organismes. Les codes de conduite sont un mécanisme entièrement volontaire auquel aucun responsable du traitement n'est tenu de participer.

3. L'autorité de contrôle compétente soumet le projet relatif aux critères d'agrément d'un organisme visé au paragraphe 1 au comité européen de la protection des données conformément au mécanisme de contrôle de la cohérence visé à l'article 57.

4. Sans préjudice des dispositions du chapitre VIII, un organisme visé au paragraphe 1 peut, sous réserve des garanties requises, prendre des mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant, y compris suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code. Il informe l'autorité de contrôle compétente de ces mesures et des raisons pour lesquelles elles ont été prises.

5. L'autorité de contrôle compétente révoque l'agrément d'un organisme visé au paragraphe 1 si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme ne sont pas conformes au présent règlement.

6. Le présent article ne s'applique pas au traitement de données à caractère personnel effectué par les autorités et les organismes publics.

Article 39

Certification[47]

1. Les États membres, le comité européen de la protection des données et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de marques et de labels en matière de protection des données, aux fins d'attester de la conformité au présent règlement des traitements effectués par les responsables du traitement et les sous-traitants. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération.

[47] AT, FR, FI: réserve d'examen. FR estime que la terminologie utilisée n'est pas claire et que le DPD devrait être en mesure de vérifier le respect des politiques certifiées en matière de protection des données; ce point devrait être clarifié dans l'article 53.

1 *bis*. Outre l'adhésion des responsables du traitement ou des sous-traitants soumis au présent règlement, les mécanismes de certification, les marques ou les labels en matière de protection des données *approuvés* en application du paragraphe 2 *bis* peuvent aussi être établis aux fins de démontrer l'existence de garanties appropriées fournies par des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement en vertu de l'article 3, dans le cadre des transferts de données à caractère personnel à un pays tiers ou à une organisation internationale conformément aux conditions visées à l'article 42, paragraphe 2, point e). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'une autre manière, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

2. Une certification au titre du présent article ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement et est sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 bis .

2 *bis*. Une certification au titre du présent article est délivrée par *les organismes* de certification *visés à l'article 39 bis ou, le cas échéant, par l'autorité de contrôle compétente* sur la base des critères approuvés par l'autorité de contrôle compétente ou, *en application de l'article 57*, par le comité européen de la protection des données[48].

3. Le responsable du traitement ou le sous-traitant qui soumet son traitement au mécanisme de certification fournit à l'organisme de certification visé à l'article 39 *bis ou, le cas échéant, à l'autorité de contrôle compétente* toutes les informations nécessaires et lui donne accès aux activités de traitement qui sont nécessaires pour mener la procédure de certification.

4. La certification est délivrée à un responsable du traitement ou à un sous-traitant pour une période maximale de trois ans et peut être renouvelée dans les mêmes conditions tant que les exigences applicables continuent d'être respectées. Elle est retirée par les organismes de certification visés à l'article 39 *bis* ou, le cas échéant, par l'autorité de contrôle compétente lorsque les exigences applicables à la certification ne sont pas ou plus respectées.

---

48 Cela est sans préjudice de la future discussion sur les compétences exactes du comité européen de la protection des données. Cette discussion se tiendra dans le cadre du débat sur le mécanisme de guichet unique.

5. Le comité européen de la protection des données recueille dans un registre tous les mécanismes de certification et les marques en matière de protection des données et les met à la disposition du public par tout moyen approprié, comme le portail européen e-Justice.

Article 39 bis

Organisme et procédure de certification[49]

1. Sans préjudice des missions et pouvoirs de l'autorité de contrôle compétente au titre des articles 52 et 53, la certification est délivrée et renouvelée par un organisme de certification disposant d'un niveau d'expertise approprié en matière de protection des données. Chaque État membre prévoit si ces organismes de certification sont agréés par[50]:

   a) l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis*; et/ou

   b) l'organisme national d'accréditation désigné conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis*.

2. L'organisme de certification visé au paragraphe 1 peut être agréé à cette fin seulement si:

   a) il a prouvé, à la satisfaction de l'autorité de contrôle compétente, son indépendance et l'expertise dont il dispose au regard de l'objet de la certification;

[49] AT, FR, LU: réserve d'examen.
[50] BE: réserve d'examen.

aa) il s'est engagé à respecter les critères *visés à l'article 39, paragraphe 2 bis*, et approuvés par l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis* ou, en application de l'article 57, par le comité européen de la protection des données;

b) il a mis en place des procédures en vue de l'émission, de l'examen périodique et du retrait de marques et de labels en matière de protection des données;

c) il a établi des procédures et des structures pour traiter les réclamations relatives aux violations de la certification ou à la manière dont la certification a été ou est appliquée par un responsable du traitement ou un sous-traitant, et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public;

d) il prouve, à la satisfaction de l'autorité de contrôle compétente, que ses tâches et ses missions n'entraînent pas de conflit d'intérêt.

3. L'agrément des organismes de certification visés au paragraphe 1 se fait sur la base de critères approuvés par l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis* ou, *en application de l'article 57*, par le comité européen de la protection des données[51]. *En cas d'agrément en application du paragraphe 1, point b), ces exigences complètent celles prévues dans le règlement (CE) n° 765/2008 et les règles techniques qui décrivent les méthodes et procédures des organismes de certification.*

4. L'organisme de certification visé au paragraphe 1 est chargé de procéder à l'évaluation correcte en vue de la certification [ou du retrait de cette certification], sans préjudice de la responsabilité du responsable du traitement ou du sous-traitant concernant le respect du présent règlement. L'agrément est délivré pour une période maximale de cinq ans et peut être renouvelé dans les mêmes conditions tant que l'organisme respecte les exigences.

5. L'organisme de certification visé au paragraphe 1 communique à l'autorité de contrôle compétente les raisons de la délivrance ou du retrait de la certification demandée.

---

51 Cela est sans préjudice de la future discussion sur les compétences exactes du comité européen de la protection des données. Cette discussion se tiendra dans le cadre du débat sur le mécanisme de guichet unique.

6. *Les* exigences visées au paragraphe 3 et *les* critères visés à l'article 39, paragraphe 2 *bis, sont publiés par l'autorité de contrôle sous une forme aisément accessible*. Les autorités de contrôle les transmettent aussi au comité européen de la protection des données. Le comité européen de la protection des données recueille dans un registre tous les mécanismes de certification et les marques en matière de protection des données et les met à la disposition du public par tout moyen approprié, comme le portail européen e-Justice.

6 *bis*. Sans préjudice des dispositions du chapitre VIII, l'autorité de contrôle compétente ou l'organisme national d'accréditation révoque l'agrément qu'il a délivré à un organisme de certification visé au paragraphe 1 si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme ne sont pas conformes au présent règlement[52].

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 86, aux fins de préciser (…) les critères et exigences à prendre en considération en ce qui concerne les mécanismes de certification en matière de protection des données visés au paragraphe 1, [y compris les conditions d'octroi et de révocation, et les exigences en matière de reconnaissance de la certification ainsi que les exigences relatives à un "label européen de protection des données" au sein de l'Union et dans les pays tiers].

7 *bis*. Le comité européen de la protection des données rend un avis adressé à la Commission sur les critères et les exigences visés au paragraphe 7[53].

8. La Commission peut fixer des normes techniques pour les mécanismes de certification, ainsi que des marques et labels et des mécanismes en matière de protection des données, afin de promouvoir et de reconnaître les mécanismes de certification ainsi que les marques et labels en matière de protection des données. Les actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2[54].

---

52 CZ, FR et HU estiment que l'organisme national d'accréditation devrait toujours consulter l'autorité chargée de la protection des données avant d'agréer un organisme de certification.

53 Cela est sans préjudice de la future discussion sur les compétences exactes du comité européen de la protection des données. Cette discussion se tiendra dans le cadre du débat sur le mécanisme de guichet unique.

54 DE a plaidé en faveur de la suppression des deux derniers paragraphes et suggéré l'ajout d'un nouveau paragraphe libellé comme suit: "Les paragraphes précédents n'affectent pas les dispositions régissant la responsabilité des organismes de certification nationaux, les procédures d'agrément et la spécification des critères de sécurité et de protection des données. La compétence de la Commission pour adopter des actes conformément aux paragraphes 7 et 8 ne s'applique pas aux procédures de certification nationales et internationales menées sur cette base. Les certificats de sécurité délivrés par les organismes responsables ou des organismes agréés par ceux-ci dans le cadre de ces procédures bénéficient d'une reconnaissance mutuelle". ES estime aussi que cet aspect ne devrait pas relever de la compétence exclusive de la Commission.