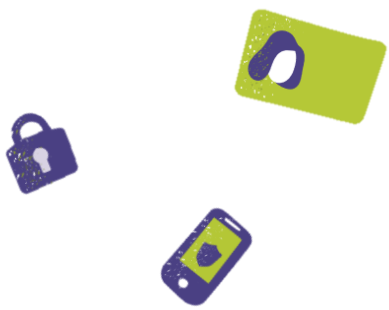
RECOMMANDATION

n° 02/2020 du 31 janvier 2020

La portée de l'obligation de conclure un protocole afin de formaliser les communications de données à caractère personnel en provenance du secteur public fédéral



APD

Autorité de protection des données

I. Le champ d'application matériel de l'article 20 de la LTD ou dans quelles conditions est-il nécessaire de conclure un protocole pour formaliser une communication de données à caractère personnel ? 6

1. Première condition : une « autorité publique fédérale » communique des données à caractère personnel en tant que responsable du traitement 7

2. Deuxième condition : la communication de données à caractère personnel est « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis » (article 6.1.c) du RGPD) ou est « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (article 6.1.e) du RGPD) 8

3. Troisième condition : les modalités de la communication ne sont pas prévues par une norme législative ou règlementaire 15

4. Quatrième condition : la communication présente un caractère systématique ou, si elle est ponctuelle, a lieu vers des personnes ou des institutions qui ne sont pas habilitées à les recevoir en vertu d'une mission légale 16

5. Cinquième condition : le « destinataire » de la communication est situé en Belgique et reçoit les données à caractère personnel en qualité de responsable du traitement 17

II. Le contenu du protocole d'accord 24

III. Éléments de procédure 27

IV. Champ d'application temporel de l'obligation de conclure un protocole d'accord 28

V. Quid si les responsables du traitement n'arrivent pas à conclure un protocole pour formaliser la communication de données à caractère personnel ? 31

1. Principe : délibération de la chambre autorité fédérale du comité de sécurité de l'information 31

2. Exceptions : pas besoin de délibération (ni de protocole) 31

3. Cas particulier concernant les communications en provenance du secteur public fédéral vers des institutions de sécurité sociale appartenant au réseau primaire : délibération des chambres réunies du comité de sécurité de l'information 31

L'objectif principal du présent document est de **clarifier la portée de l'article 20 de la loi du 30 juillet 2018** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après « LTD »). À cette fin, il vise, plus spécifiquement, à éclaircir les points suivants :

- Les **conditions dans lesquelles une autorité publique doit conclure un protocole** pour formaliser une communication de données à caractère personnel à un tiers

- Le **contenu du protocole** formalisant une communication de données en provenance du secteur public fédéral

- Les **exigences procédurales imposées par l'article 20 de la LTD** pour la conclusion d'un protocole

- Le **champ d'application temporel** de l'article 20 de la LTD

- La procédure à suivre **lorsque le responsable du traitement initial et le responsable du traitement destinataire des données ne parviennent pas à un accord**

Entre 2003 et 2018, toute communication électronique de données par un service public fédéral ou par un organisme public relevant de l'autorité fédérale devait, en vertu de l'article 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après « LVP »), être autorisée par le comité sectoriel compétent pour l'Autorité fédérale, lequel avait été institué auprès de l'ancienne Commission de la protection de la vie privée (ci-après « CPVP »). Lors de la procédure d'autorisation, le comité sectoriel pour l'Autorité fédérale vérifiait que la « *communication [était] bien nécessaire à la mise en œuvre des missions confiées, par ou en vertu de la loi, à l'autorité fédérale demanderesse et, d'autre part, que cette communication, en ses divers aspects, [était] compatible avec l'ensemble des normes en vigueur en matière de protection de la vie privée en ce qui concerne le traitement de données personnelles* »[1]. Cette procédure d'autorisation préalable a été abrogée par la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après « LCA »)[2].

L'article 20 de la LTD introduit une nouvelle obligation à charge des autorités publiques fédérales qui transfèrent des données à caractère personnel à des tiers. Chaque communication de données à caractère personnel doit en effet, à présent, être formalisée par un protocole conclu entre l'autorité publique qui transfère les données

[1] Le Comité sectoriel compétent pour l'autorité fédérale rappelait très régulièrement, dans ses autorisations, l'objectif qui était poursuivi par la procédure des autorisations préalable. Cet objectif avait été exprimé très clairement dans la justification de l'amendement n° 12 déposé par le Gouvernement, *Doc. Parl.*, Ch., sess. ord. 2001-2002, n° 50/1940-4, p. 3.

[2] L'article 109 de la LCA dispose que « Les chapitres VII et VIIbis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel sont supprimés »

et le responsable du traitement destinataire des données à caractère personnel, à moins qu'une loi particulière en dispose autrement[3].

Ce changement procédural s'inscrit dans la reconnaissance, par le RGPD, du principe de responsabilité (*accountability*) qui impose aux responsables du traitement de mettre en œuvre des mesures appropriées et effectives pour s'assurer et être en mesure de démontrer la conformité de ces traitements avec le Règlement[4]. En effet, comme les travaux préparatoires de l'article 20 de la LTD le soulignent, l'obligation de conclure un protocole invite les responsables du traitement « *à s'interroger sur la conformité de leurs échanges de données* »[5]. Le protocole conclu entre l'autorité publique fédérale qui transfère des données à caractère personnel et le responsable du traitement destinataire des données constitue un instrument d'*accountability* qui doit amener l'autorité publique à s'assurer que la communication de données respecte la règlementation relative à la protection des données à caractère personnel, y compris le RGPD et la LTD.

Depuis l'entrée en vigueur de l'article 20 de la LTD, les flux de données en provenance du secteur public fédéral ne doivent donc, en principe, plus être autorisés par un organe externe, mais ils doivent être encadrés par un protocole conclu entre le responsable du traitement initial et le responsable du traitement destinataire des données. Toutefois, pour les cas où les responsables du traitement n'arriveraient pas à conclure un protocole formalisant les modalités de la communication, le législateur a prévu une procédure alternative. En effet, l'article 35/1 de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, inséré par l'article 86 de la loi du 5 septembre 2019[6], dispose que « *la communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des tiers autres que les institutions de sécurité sociale […] doit faire l'objet d'une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information […] dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement. […] Dans la mesure où le comité de sécurité de l'information rend une délibération pour la communication de données à caractère*

[3] On pense, par exemple, à l'article 15 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale qui dispose que les communications en provenance d'une institution de sécurité sociale doivent faire l'objet d'une délibération préalable de la chambre sécurité sociale de santé du comité de sécurité de l'information ou des chambres réunies du comité de sécurité de l'information. De même, l'article 11 de la loi prévoit que toute communication de données à caractère personnel par ou à la plate-forme *eHealth* requiert, en principe, une autorisation de principe de la chambre sécurité sociale et santé du comité de sécurité de l'information. Or, l'article 35/1 § 1er de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral dispose que "[…] *Dans la mesure où le comité de sécurité de l'information rend une délibération pour la communication de données à caractère personnel par l'autorité fédérale, cette dernière est, par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dispensée de l'obligation d'établir un protocole y relatif avec le destinataire des données à caractère personnel*".

[4] Article 5 § 2 du RGPD. Voyez également le considérant 74.

[5] Doc. Parl., Ch. Sess. ord., 2017-2018, n° 54-3126/001, p. 421

[6] Loi du 5 septembre 2019 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE, *M.B.*, 10 septembre 2019

personnel par l'autorité fédérale, cette dernière est, par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dispensée de l'obligation d'établir un protocole y relatif avec le destinataire des données à caractère personnel […] ».

*

La présente note cherche à clarifier la portée de l'obligation imposée par l'article 20 de la LTD de conclure des protocoles pour encadrer les flux en provenance du secteur public fédéral. Pour comprendre la portée de cette obligation, il est nécessaire d'interpréter l'article 20 de la LTD dans son contexte normatif, et en particulier de lire cette disposition à la lumière **de l'article 5 de la LTD**, qui définit la notion d'autorité publique fédérale, et **de l'article 35/1 de la loi du 15 août 2012**, qui régit les situations où les responsables du traitement ne parviennent pas à conclure un protocole. Cette lecture de l'article 20 de la LTD à la lumière de cette dernière disposition se justifie d'autant plus que l'article 20 de la LTD lui-même impose que les communications de données à caractère personnel en provenance du secteur public fédéral soient formalisées par un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données, « *sauf autre disposition dans des lois particulières* ».

REMARQUE PRÉALABLE

L'Autorité souligne qu'en utilisant les termes « transmission de données à caractère personnel »[7] ou « communication de données à caractère personnel », elle vise, non seulement les situations où un responsable du traitement envoie des données à caractère personnel à un tiers, mais également celles où un responsable du traitement, sans envoyer directement les données à un tiers, lui permet d'y avoir accès.

[7] L'article 20 de la LTD utilise les termes « l'autorité publique fédérale qui transfert des données à caractère personnel ». L'APD entend toutefois souligner que, dans le RGPD, le terme « transfert » vise les « transferts internationaux », c'est-à-dire les transferts vers des pays « tiers » (hors Espace économique européen). Afin d'éviter toute confusion entre une communication de données au sein de l'EEE et les transferts internationaux de données (vers des pays tiers), l'APD réserve l'utilisation du terme « transfert » aux « transferts internationaux » (au sens du Chapitre V du RGPD)

I. Le champ d'application matériel de l'article 20 de la LTD ou dans quelles conditions est-il nécessaire de conclure un protocole pour formaliser une communication de données à caractère personnel ?

Il se déduit d'une lecture combinée de l'article 20 § 1 de la LTD et l'article 35/1 de la loi du 15 août 2012 que l'obligation de conclure un protocole d'accord est soumise **à la réunion des cinq conditions cumulatives suivantes** :

- ✓ Une « **autorité publique fédérale** » communique des données à caractère personnel en tant que responsable du traitement.

- ✓ La communication de données à caractère personnel est **réalisée en exécution « *d'une obligation légale à laquelle le responsable du traitement est soumis* »** (article 6.1.c) du RGPD) ou est **« *nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* »** (article 6.1.e) du RGPD).

- ✓ Les **modalités de la communication ne sont pas prévues par une norme législative ou règlementaire**.

- ✓ La communication présente un **caractère systématique** ou, **si elle est ponctuelle**, a lieu vers **des personnes ou des institutions qui ne sont pas habilitées** à les recevoir en vertu d'une mission légale.

- ✓ Le « **destinataire** » de la communication est **situé en Belgique** et reçoit les données à caractère personnel **en qualité de responsable du traitement**.

REMARQUE IMPORTANTE

L'article 20 de la LTD, qui impose la conclusion d'un protocole pour encadrer des communications de données en provenance du secteur public fédéral, exécute l'article 6.2 du RGPD, lequel dispose que « *Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX* ». Les dispositions de droit national prises au titre de l'article 6.2 du RGPD ne peuvent toutefois pas dispenser de l'obligation de respecter le RGPD. **Les autorités publiques doivent donc respecter le RGPD, qu'elles soient par ailleurs tenues, ou pas, de conclure un protocole** pour encadrer une transmission de données à caractère personnel.

Il convient, à cet égard, d'attirer l'attention, en particulier, sur le **principe de limitation des finalités** aux termes duquel les données à caractère personnel doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* »[8]. Il s'ensuit que si une communication de données poursuit une ou plusieurs finalités différentes de celles pour lesquelles elles ont été collectées à l'origine, il conviendra de procéder à une **analyse de compatibilité des finalités ultérieures avec les finalités initiales**[9], à moins que le traitement ultérieur soit « *fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1 [du RGPD]*»[10].

1. Première condition : une « autorité publique fédérale » communique des données à caractère personnel en tant que responsable du traitement

L'article 5 de la LTD définit la notion d'autorité publique[11].

Conformément à cette définition[12], la notion d'« autorité publique fédérale » doit se comprendre comme :

1° L'Etat fédéral

Exemples
les différents SPF, le Conseil du contentieux des étrangers, le Commissariat général aux réfugiés et aux apatrides, …

[8] Article 5.1.b) du RGPD

[9] L'article 6.4 du RGPD fournit une liste de critères qui doivent guider le responsable du traitement lors de cette analyse de compatibilité.

[10] Article 6.4 du RGPD.

[11] Le législateur européen a choisi de ne pas définir ce qu'il convenait d'entendre par "autorité publique" dans le cadre de l'application du RGPD. Il a été décidé de laisser les législateurs nationaux définir cette notion. Dans ses lignes directrices concernant les délégués à la protection des données (WP 243 rev.01), le Groupe de travail "Article 29", qui reconnait que la notion d'autorité publique doit être définie par le droit national, recommande l'adoption d'une définition large de la notion englobant les organismes privés chargés d'effectuer des missions de service public ou exerçant l'autorité publique – ce qu'a fait le législateur belge à travers l'adoption de la définition visée à l'article 5 de la LTD.

[12] Dans l'exposé des motifs du projet de loi qui deviendra la LTD, il est indiqué que « La définition d'autorité publique est précisée et est reprise de la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public […] », *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 3126/001, p. 17

2° Les personnes morales de droit public qui dépendent de l'Etat fédéral

Exemples
la Banque nationale, le Bureau fédéral du Plan,…

3° Les personnes quelles que soient leur forme et leur nature qui :

- ✓ ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial ; et
- ✓ sont dotées de la personnalité juridique ; et
- ✓ dont soit l'activité est financée majoritairement par l'Etat fédéral ou une ou plusieurs personnes morales de droit public qui en dépendent, soit la gestion est soumise à un contrôle de l'Etat fédéral ou d'une ou plusieurs personnes morales de droit public qui en dépendent, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par l'Etat fédéral ou une ou plusieurs personnes morales de droit public qui en dépendent ;

L'Autorité attire l'attention sur le caractère cumulatif de ces conditions.

Exemples
bpost [dans l'exercice de ses missions de service public], la SNCB [dans l'exercice de ses missions de service public], skeyes [dans l'exercice de ses missions de service public], Proximus [dans l'exercice de ses missions de service public], La Loterie Nationale

REMARQUE IMPORTANTE

Lorsque les entreprises publiques effectuent des services « purement » commerciaux, et qu'elles n'exercent donc pas leurs missions de service public, elles ne sont pas soumises à l'article 20 de la LTD.

4° les associations formées par une ou plusieurs autorités publiques visées au 1°, 2° ou 3°.

2. Deuxième condition : la communication de données à caractère personnel est « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis » (article 6.1.c) du RGPD) ou est « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (article 6.1.e) du RGPD)

Conformément à l'article 6 du RGPD, une communication de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

- ✓ La personne concernée a consenti à la communication de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

- ✓ La communication est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

- ✓ La communication est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

- ✓ La communication est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

- ✓ La communication est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

- ✓ La communication est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.
  Le RGPD dispose que cette dernière base juridique ne peut pas s'appliquer au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Aux termes de l'article 20 de la LTD, **l'obligation de conclure un protocole** n'existe que lorsque la communication de données à caractère personnel en provenance d'une autorité publique fédérale **est nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis, ou lorsqu'elle est **nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement**, étant entendu que l'obligation légale ou la mission d'intérêt public qui légitime la communication de données à caractère personnel peut exister tant dans le chef du responsable du traitement qui communique les données à caractère personnel que dans le chef du responsable du traitement qui réceptionne ces données.

Cette exigence doit se comprendre à la lumière du principe de l'attribution des compétences administratives, du principe de spécialité des personnes morales ainsi que du principe de légalité qui préside à la définition des conditions auxquelles l'administration peut interférer avec le droit à la protection de la vie privée, lequel inclut le droit à la protection des données à caractère personnel[13]. Aux termes du principe de l'attribution des compétences administratives, qui est consacré par l'article 105 de la Constitution et 78 de la loi spéciale du 8 août 1980 de réformes institutionnelles, les autorités administratives n'ont d'autres pouvoirs que ceux que leur attribuent formellement la Constitution et les lois et décrets portés en vertu de celle-ci. En outre, le principe de

[13] La CPVP l'a déjà souligné dans son avis concernant l'avant-projet de loi qui est ensuite devenu la LTD. Voyez CPVP, Avis n° 33/2018, p. 44.

spécialité des personnes morales dispose que toute institution dotée de la personnalité juridique ne peut agir que pour atteindre le(s) but(s) pour le(s)quel(s) elle a été créé, étant entendu que seule une norme législative peut confier une mission de service public à une personne morale. En outre, comme le Conseil d'Etat l'a rappelé dans son avis sur l'avant-projet de loi "relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel", « *un transfert de données d'une autorité publique à une autre constitue une ingérence dans le droit à la protection de la vie privée des personnes concernées. En vertu de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, tel qu'interprété par une jurisprudence constante de la Cour constitutionnelle, pareille ingérence doit notamment reposer sur une base légale, être proportionnée par rapport à l'objectif poursuivi et être organisée de manière suffisamment précise pour être prévisible pour le citoyen* »[14]. **Ainsi, une autorité publique ne peut traiter – et donc communiquer – des données à caractère personnel que si cette communication est nécessaire au respect d'une obligation imposée par ou en vertu d'une norme législative à l'un des responsables du traitement ou si elle est nécessaire à l'exécution d'une mission d'intérêt public qui a été dévolues à l'un des responsables du traitement par ou en vertu d'une norme législative**. Comme l'a souligné la CPVP dans son avis concernant l'avant-projet de loi "relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel", les communications de données à caractère personnel en provenance du secteur public doivent reposer sur une base légale, étant entendu qu'*« un protocole d'échange ne pourra jamais constituer la base légale d'un traitement de données* »[15].

Cette exigence constitutionnelle implique que, dans l'immense majorité des cas, les communications de données à caractère personnel par des autorités publiques sont « *nécessaire[s] au respect d'une obligation légale à laquelle le responsable du traitement est soumis* » (**A**) ou « *nécessaire[s] à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* » (**B**). Toutefois, on ne peut pas exclure que, dans certaines circonstances, très rares, une communication de données à caractère personnel en provenance du secteur public puisse reposer sur un autre fondement juridique prévus par l'article 6 du RGPD. Aux termes de l'article 20 de la LTD, de telles communications ne doivent pas être formalisées par un protocole (**C**).

A. La communication de données à caractère personnel est nécessaire au respect d'une obligation légale (article 6.1.c) du RGPD)

Pour qu'une autorité publique puisse se prévaloir de l'article 6.1.c) du RGPD pour transférer des données à caractère personnel, il faut que l'autorité publique y soit obligée *par* ou *en vertu* d'une norme législative. Cette obligation doit être juridiquement valable et contraignante et l'autorité publique ne doit donc pas avoir le choix de s'y conformer ou non[16].

[14] Avis du Conseil d'Etat n° 63.192/2 du 19 avril 2018, in *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 421-422.

[15] CPVP, Avis n° 33/2018, p. 44.

[16] Groupe de travail « Article 29 », *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 21.

En outre, l'obligation légale doit être suffisamment claire à propos du traitement de données à caractère personnel qu'elle requiert[17]. La norme qui impose l'obligation légale doit prévoir explicitement l'obligation de communication et ses modalités essentielles. Le responsable du traitement ne devrait donc pas avoir une marge d'appréciation injustifiée quant à la manière de se conformer à cette obligation légale. Conformément à l'article 6.3 du RGPD, cette norme doit définir la ou les finalités du traitement.

B. La communication de données à caractère personnel est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (article 6.1.e) du RGPD)

Pour qu'un responsable du traitement puisse se prévaloir de l'article 6.1.e) du RGPD pour communiquer des données à caractère personnel, il faut que cette communication soit nécessaire à l'exécution d'une mission d'intérêt public ou qu'elle soit nécessaire à l'exercice de l'autorité publique dont il a été investi. Mais, à la différence de la situation visée par l'article 6.1.c) du RGPD, il n'est pas nécessaire que le responsable du traitement soit soumis à une obligation légale de transférer ces données.

Les communications de données à caractère personnel nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement doivent, conformément à l'article 6.3 du RGPD, **avoir une base légale** dans le droit de l'Union ou dans le droit d'un État membre. Cette base légale doit être claire et précise et son application doit être prévisible pour les justiciables. Elle doit, au moins, définir les missions d'intérêt public ou relevant de l'exercice de l'autorité publique qui justifient la nécessité de la communication de données à caractère personnel. La finalité du traitement doit également être déterminée dans cette base juridique[18]. Cette (ou ces) finalité(s) doi(ven)t, comme le rappellent les travaux préparatoires de la loi du 30 juillet 2018, être précise(s) et « *ne pas se limiter à la mention 'exécution des missions légales de l'autorité publique'* »[19]. Par contre, il n'est pas systématiquement requis que la base juridique prescrive spécifiquement un traitement de données ou une transmission de données pour que le responsable du traitement puisse invoquer l'article 6.1.e) du RGPD comme base de légitimité pour fonder son traitement ou la transmission . Il est, par contre, nécessaire que la mission d'intérêt public ne puisse être réalisée autrement qu'en traitant (en transférant) des données[20]. Mais la notion de « traitements nécessaires à l'exécution d'une mission d'intérêt public » a une **portée large** puisqu'elle vise, non seulement les traitements nécessaires à l'exécution de la mission d'intérêt public au sens strict, mais également les traitements nécessaires à l'exécution de missions directement liées à cette mission d'intérêt public, y compris les traitements nécessaires pour la gestion et le fonctionnement des organismes chargés de cette mission d'intérêt public[21].

---

[17] Groupe de travail « Article 29 », *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 22.

[18] Voyez le considérant 45 du RGPD.

[19] *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 45.

[20] *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 45.

[21] Bien que le RGPD ne le prévoit pas explicitement, l'interprétation large de la notion de « traitements nécessaires à l'exécution d'une mission d'intérêt public » trouve un appui dans le Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE

Exemples
✓ Les traitements de données à caractère personnel, y compris les communications de données, effectués par une autorité publique dans le cadre de la gestion de ses ressources humaines [pour autant que les mesures prises soient effectivement nécessaires à la gestion des ressources humaines]. ✓ Les communications, par une autorité publique, de données à caractère personnel nécessaires à la réalisation d'une recherche effectuée à la demande de cette même autorité publique [et qui rentre donc dans le cadre de ses missions d'intérêt public]. ✓ La communication, par le SPF Finance à un autre organisme public ou privé, d'informations relatives à la situation fiscale de personnes physiques avant l'octroi, par l'organisme destinataire des données, d'une prime, d'un subside ou de tout autre avantage consenti directement ou indirectement par l'Etat, une Communauté ou une Région[22]. ✓ Les communications de données à caractère personnel par une autorité publique en exécution de la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public. ✓ Les traitements de données nécessaires pour assurer la sécurité du réseau informatique d'une autorité publique.

REMARQUE IMPORTANTE

Les traitements de données à caractère personnel jugés nécessaires au respect d'une obligation légale et/ou nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement doivent, conformément à l'article 6.3 du RGPD, lu à la lumière du considérant 41, **être encadrés par une règlementation qui soit claire et précise et dont l'application doit être prévisible pour les justiciables.** En outre, aux termes de l'article 22 de la Constitution belge, il est nécessaire que **les « éléments essentiels » du traitement de données soient fixés dans une norme législative formelle** (loi, décret ou ordonnance).

C. Les autres fondements juridiques de l'article 6 du RGPD

Si une communication de données à caractère personnel repose sur un autre fondement juridique que l'exécution d'une obligation légale ou d'une mission d'intérêt public, elle ne tombe pas dans le champ d'application matériel de l'article 20 de la LTD et ne doit donc pas faire l'objet d'un protocole. Bien qu'il soit rare que les autorités publiques puissent fonder leurs traitements de données à caractère personnel sur un des autres fondements de l'article 6 du RGPD, cette situation ne peut pas être complètement exclue.

REMARQUE IMPORTANTE

L'Autorité rappelle qu'aux termes de l'article 5.1.a) du RGPD, les autorités publiques doivent, comme tout responsable du traitement, veiller à la **licéité du traitement** qu'elles entreprennent (en l'occurrence de la communication de données à caractère personnel). Cette exigence implique, en vertu de plusieurs principes constitutionnels et administratifs belges, que **toute communication de données à caractère personnel par une autorité publique doit disposer d'une base légale.**

dont le considérant 22 indique que « […]. Le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et organes de l'Union comprend le traitement de données à caractère personnel nécessaire pour la gestion et le fonctionnement de ces institutions et organes […] ».

[22] L'article 328 du C.I.R dispose que *« Les services administratifs de l'État, les administrations des Communautés, des Régions, des provinces, des agglomérations, des fédérations de communes, et des communes, ainsi que les sociétés, associations, établissements ou organismes de droit public, ne peuvent accorder des crédits, prêts, primes, subsides ou tous autres avantages basés directement ou indirectement sur le montant des revenus ou sur des éléments intervenant dans la détermination de ces revenus, qu'après avoir pris connaissance de la situation fiscale récente du requérant.*

Cette situation est opposable au demandeur pour l'octroi desdits crédits, prêts, primes, subsides ou autres avantages.

Les dispositions des alinéas 1er et 2 sont également applicables aux sociétés, associations, établissements ou organismes de droit privé, mais seulement en ce qui concerne les opérations assorties directement ou indirectement d'un avantage consenti par l'État, par une Communauté ou une Région »

i. La personne concernée a consenti à la communication de ses données à caractère personnel pour une ou plusieurs finalités spécifiques (article 6.1.a) du RGPD)

Sans préjudice des obligations légales et constitutionnelles qui s'imposent aux autorités publiques[23], celles-ci ne pourront avoir recours au consentement pour légitimer un traitement de données à caractère personnel que dans des situations rares et exceptionnelles[24]. En effet, l'exigence d'un consentement « libre » empêche, en principe, les autorités publiques de pouvoir fonder un traitement de données à caractère personnel sur le consentement de la personne concernée. Dès lors que le responsable du traitement est une autorité publique, il existe souvent un déséquilibre manifeste des rapports de force entre le responsable du traitement et la personne concernée. En outre, dans la plupart des cas, la personne concernée n'aura pas de solution alternative réaliste à l'acceptation du traitement par l'autorité publique et des conditions du traitement qu'elle propose. Le consentement ne peut donc pas être donné « librement » au sens du RGPD. D'autres bases juridiques listées à l'article 6 du RGPD sont, en principe, plus adaptées aux activités des autorités publiques. Toutefois, le cadre juridique du RGPD n'exclut pas entièrement le recours au consentement en tant que base juridique du traitement de données par des autorités publiques[25].

Exemples[26]

- ✓ Une école publique demande le consentement de ses étudiants pour utiliser leurs photographies dans une revue étudiante imprimée. Le consentement serait ici le fruit d'un véritable choix dès lors que les étudiants ne se verront pas privés de tout enseignement ou de tout service et pourraient refuser l'utilisation de ces photographies sans aucun préjudice
- ✓ Une municipalité locale prévoit des travaux d'entretien de la voirie. Dès lors que les travaux de voirie pourraient perturber la circulation pendant un certain temps, la municipalité offre à ses citoyens la possibilité de s'inscrire sur une liste d'adresses électroniques afin d'être informés de l'état d'avancement des travaux et des retards prévus. La municipalité indique clairement qu'il n'y a aucune obligation de participation et demande le consentement des personnes concernées pour pouvoir utiliser leurs adresses électroniques (exclusivement) à cette fin. Les citoyens qui ne donnent pas leur consentement ne seront en aucun cas privés d'un service de base de la municipalité ou de l'exercice d'un quelconque droit, et sont donc libres de donner ou de refuser leur consentement à ce traitement de leurs données. Toutes les informations sur les travaux de voirie seront également disponibles sur le site Internet de la municipalité.

[23] L'Autorité renvoie, notamment, aux principes constitutionnels de légalité et d'attribution des compétences administratives qui régissent l'étendue des pouvoirs et compétences des autorités administratives. En outre, l'Autorité souligne le caractère, en principe, inapproprié de cette base de légitimité, étant donné, d'une part, que les usagers sont en droit de recevoir le service public presté par l'autorité publique et, d'autre part, que la soumission à l'*imperium* ne peut pas être conditionné au consentement.

[24] Voyez le considérant 43 du RGPD lequel indique que « Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière […] »

[25] Groupe de travail « Article 29 », *Lignes directrices sur le consentement au sens du Règlement 2016/679,* 28 novembre 2017, p. 7.

[26] Groupe de travail « Article 29 », *Lignes directrices sur le consentement au sens du Règlement 2016/679,* 28 novembre 2017, p. 7.

Par ailleurs, l'Autorité souligne que le consentement peut, dans certaines circonstances, être utilisé par les autorités publiques, non pas comme base juridique du traitement au sens de l'article 6 du RGPD, mais comme une garantie appropriée complémentaire[27]. Le cas échéant, l'Autorité considère que le consentement devra, lui-même être entouré de certaines garanties : la personne concernée doit être informée au préalable et elle doit pouvoir retirer son consentement à tout moment.

ii. La communication est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci (article 6.1.b) du RGPD)

Ce fondement juridique recevra une application limitée dans le secteur public, mais on ne peut pas exclure qu'une autorité publique y fasse recours pour fonder un traitement de données à caractère personnel[28]. C'est le cas lorsque le traitement est strictement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie.

Exemple
L'Autorité de protection des données transfère à une compagnie d'assurance des données à caractère personnel concernant les personnes qui travaillent en son sein afin de conclure un contrat d'assurance hospitalisation à leur profit.

iii. La communication est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique (article 6.1.d) du RGPD)

Ce fondement juridique devrait avoir une application limitée[29]. L'expression « sauvegarde des intérêts vitaux » limite, en effet, l'application de ce motif à des questions de vie ou de mort ou, à tout le moins, à des menaces graves et imminentes quant à l'intégrité physique de la personne concernée ou d'une autre personne physique.

Exemple
Un hôpital public reçoit en urgence un patient dans un état critique (entre la vie et la mort) qui doit être transféré vers un autre hôpital pour recevoir les soins nécessaires (une opération). Il dispose du dossier médical du patient et le transfère à l'autre hôpital en vue de l'opération.

[27] Voyez, par exemple, les avis suivants concernant la mise en place et l'utilisation d'un système d'échange électronique de messages entre instances publiques et entreprises, citoyens ou autre instances publiques (l'eBox) : avis n° 47/2018, avis n° 154/2019, avis n° 165/2019

[28] L'Autorité rappelle, encore une fois, que cela est toujours sans préjudice des obligations légales et constitutionnelles qui s'imposent aux autorités publiques

[29] Groupe de travail « Article 29 », *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 22. Voyez également le considérant 46 du RGPD qui indique que « Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique. Le traitement de données à caractère personnel fondé sur l'intérêt vital d'une autre personne physique ne devrait en principe avoir lieu que lorsque le traitement ne peut manifestement pas être fondé sur une autre base juridique. Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine ».

iv. *La communication est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant (article 6.1.f) du RGPD)*

Le RGPD dispose que la poursuite des intérêts légitimes du responsable du traitement ou d'un tiers **ne peut pas être utilisée pour fonder un traitement effectué par les autorités publiques dans l'exécution de leurs missions de service public**[30]. Le considérant 47 du RGPD indique que cette exclusion a été prévue parce « *qu'il appartient au législateur de prévoir par la loi la base juridique pour le traitement des données à caractère personnel par les autorités publiques* ».

3. Troisième condition : les modalités de la communication ne sont pas prévues par une norme législative ou règlementaire

On peut déduire d'une lecture combinée de l'article 20 de la LTD avec l'article 35/1 de la loi du 15 août 2012 que les communications de données à caractère personnel d'une autorité publique fédérale vers des tiers dont les modalités, c'est-à-dire – au moins – les finalités, les catégories de données et les destinataires, ont été prévues par une norme législative ou règlementaire ne doivent pas être formalisées par un protocole d'accord.

En effet, d'une part, l'article 35/1 de la loi du 15 août 2012 dispose que « *Dans la mesure où le comité de sécurité de l'information rend une délibération pour la communication de données à caractère personnel par l'autorité fédérale, cette dernière est, par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dispensée de l'obligation d'établir un protocole y relatif avec le destinataire des données à caractère personnel* ». Or il dispose également que « *La communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des tiers autres que les institutions de sécurité sociale […] doit faire l'objet une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information […], dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement. Dans les cas mentionnés, la demande est introduite d'office conjointement par les responsables du traitement concernés. La communication, visée dans l'alinéa 1er, ne doit pas faire l'objet d'une délibération préalable dans la mesure où d'autres normes réglementaires précisent les modalités de la communication dont les finalités, les catégories de données et les destinataires […]* »[31].

[30] Article 6.1.f) du RGPD

[31] L'Autorité souligne.

En d'autres termes, lorsqu'une norme prévoit explicitement ***qui*** (destinataire) se voit transmettre ***quoi*** (catégories précises des données communiquées), ***quand*** et ***pourquoi*** (finalités et modalités de la communication), la communication ne doit pas être formalisée par un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données, étant donné que le traitement est déjà encadré de manière suffisante par une règlementation générale.

Exemple
L'article III.31 du Code de droit économique dispose que « *Toute personne physique, morale ou toute entité a accès, via internet, à des données visées à l'article III.29, § 1er, inscrites dans la Banque-Carrefour des Entreprises* [ces données peuvent constituer des données à caractère personnel si elles concernent une personne physique]. *Il est au moins prévu un site internet libre d'accès, sur lequel ces données peuvent se retrouver dans un format lisible. Le Roi détermine les données ainsi accessibles ainsi que leurs modalités de consultation* ». La communication de ces données ne doit pas faire l'objet d'un protocole d'accord entre le SPF Economie, responsable de la Banque-Carrefour des Entreprises, et le responsable du traitement destinataire.
Contre-exemple
La loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules. Bien que cette norme détermine les finalités et conditions auxquelles les données reprises dans la Banque-Carrefour des véhicules peuvent être utilisées, cette norme n'est pas suffisamment précise pour dispenser le SPF Mobilité et Transport de l'obligation qui lui est imposée par l'article 20 de la LTD de conclure un protocole pour formaliser la communication de ces données à un autre responsable du traitement.

4. Quatrième condition : la communication présente un caractère systématique ou, si elle est ponctuelle, a lieu vers des personnes ou des institutions qui ne sont pas habilitées à les recevoir en vertu d'une mission légale

On peut déduire d'une lecture combinée de l'article 20 de la LTD avec l'article 35/1 de la loi du 15 août 2012 que les **communications ponctuelles de données à caractère personnel** d'une autorité publique fédérale **vers des personnes ou institutions qui sont habilitées à les recevoir en vertu d'une mission légale** ne doivent pas être formalisées par un protocole d'accord.

En effet, d'une part, l'article 35/1 de la loi du 15 août 2012 dispose que « *Dans la mesure où le comité de sécurité de l'information rend une délibération pour la communication de données à caractère personnel par l'autorité fédérale, cette dernière est, par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dispensée de l'obligation d'établir un protocole y relatif avec le destinataire des données à caractère personnel* ». Or il dispose également que « *La communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des tiers autres que les institutions de sécurité sociale […] doit faire l'objet*

une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information […], dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement. Dans les cas mentionnés, la demande est introduite d'office conjointement par les responsables du traitement concernés. La communication, visée dans l'alinéa 1er, ne doit pas faire l'objet d'une délibération préalable […] dans la mesure où il s'agit d'une communication ponctuelle de données, en conformité avec le règlement (UE) 2016/679 précité, à des personnes ou institutions habilitées à les recevoir en vertu d'une mission légale »[32].

En d'autres termes, si la communication de données à caractère personnel n'intervient que **de manière ponctuelle** et qu'elle **est nécessaire pour que le responsable du traitement destinataire des données puisse effectuer une mission légale**, elle ne doit pas être formalisée dans un protocole au sens de l'article 20 de la LTD. Elle devra toutefois respecter toute la règlementation en vigueur, en particulier le RGPD et la LTD. Une communication est **ponctuelle** lorsqu'elle n'intervient **qu'une seule fois**.

Une **communication qui est répétée**, même sans régularité fixe, n'est pas, par contre, une communication ponctuelle. Elle devra donc être formalisée par un protocole d'accord. *A fortiori*, **une communication de données systématique** doit aussi être formalisée par un protocole d'accord entre le responsable du traitement fournisseur et le responsable du traitement destinataire des données. De même, une communication de données, même ponctuelle, **vers une personne ou une institution qui n'est pas habilitée à les recevoir en vertu d'une mission légale** doit aussi être encadrée par un protocole conclu entre les responsables du traitement.

5. Cinquième condition : le « destinataire » de la communication est situé en Belgique et reçoit les données à caractère personnel en qualité de responsable du traitement

A. Principe

Pour rappel, l'article 20 de la LTD dispose que « *l'autorité publique fédérale qui transfert des données à caractère personnel sur la base de l'article 6.1.c) et e), du Règlement à toute autre autorité publique ou organisation privée, formalise cette transmission pour chaque type de traitement par un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données* »[33]. On peut en déduire que **le destinataire de la communication**, qui peut donc être une autre autorité publique ou un

[32] L'Autorité souligne.

[33] L'Autorité souligne.

organisme privé, **doit recevoir les données en qualité de responsable du traitement,** et non de sous-traitant.

Cette lecture est d'ailleurs confirmée par l'article 35/1 de la loi du 15 août 2012 qui prévoit que seules les communications vers des « *tiers* », c'est-à-dire « *les instances autres que l'intéressé, le responsable du traitement, le sous-traitant et les personnes autorisées à traiter les données à caractère personnel sous l'autorité directe du responsable du traitement ou du sous-traitant* », doivent faire l'objet d'une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement.

Ainsi, **les communications de données vers un sous-traitant ne doivent pas être formalisées par un protocole au sens de l'article 20 de la LTD**. Mais elles doivent, pour rappel, être « *régi[es] par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit 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, et les obligations et les droits du responsable du traitement* », et ce conformément à l'article 28 du RGPD. Si la communication de données a lieu vers un sous-traitant établi dans un pays tiers (c.-à-d. hors de l'Espace économique européen), il est, en outre, nécessaire que le responsable du traitement respecte les conditions du Chapitre V du RGPD et prévoie, le cas échéant, des « garanties appropriées » pour encadrer le transfert.

REMARQUE CONCERNANT LES COMMUNICATIONS DE DONNÉES ENTRE RESPONSABLES CONJOINTS DU TRAITEMENT

L'Autorité souligne que si deux responsables du traitement « *déterminent conjointement les finalités et les moyens du traitement* », ils sont responsables conjoints du traitement au sens de l'article 26 du RGPD. Dans ce cas, l'article 26 du RGPD leur impose de définir « *de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis* ». Des responsables conjoints du traitement ne doivent pas conclure un protocole au sens de l'article 20 de la LTD pour formaliser les communications de données qui ont lieu dans le cadre du traitement dont ils sont conjointement responsables.

B. Les flux exclus du champ d'application de l'article 20 de la LTD

i. Les flux entre services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police structuré organisé à deux niveaux

L'article 19 de la LTD dispose que les articles 20 à 23 de la LTD s'appliquent aux services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police structuré organisé à deux niveaux et que ces services sont considérés comme une seule autorité publique. Il s'en suit que les communications entre un service de police et un autre ne constituent pas une communication entre deux autorités publiques distinctes. Il s'agit plutôt d'une communication « interne », laquelle ne doit pas être formalisée par un protocole au sens de l'article 20 de la LTD.

ii. Les flux vers les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du Titre 3 de la LTD [34]

L'article 5 de la LTD dispose que « *les définitions du Règlement s'appliquent* ». Or, comme l'a souligné le Conseil d'État dans son avis[35], les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du Titre 3 de la LTD ne sont pas des « destinataires » au sens de l'article 4.9 du RGPD. Les communications de données à ces services ne rentrent donc pas dans le champ d'application de l'article 20 de la LTD lequel s'adresse au « responsable du traitement initial » et au « responsable du traitement destinataire des données »[36].

iii. Les flux vers les institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, b) à f), de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, c'est-à-dire vers des institutions appartenant au réseau secondaire de la sécurité sociale.

L'article 35/1 de la loi du 15 août 2012 dispose que « *la communication de données à caractère personnel par des autorités publiques fédérales à des institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, b) à f), de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale doit faire l'objet d'une délibération préalable des chambres réunies du comité de sécurité de l'information ».* Il ajoute, en outre, que *« dans la mesure où le comité de sécurité de l'information rend une délibération pour la communication de données à caractère personnel par l'autorité fédérale, cette dernière est, par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dispensée de l'obligation d'établir un protocole y relatif avec le destinataire des données à caractère personnel* ».

---

[34] Le sous-titre 3 du Titre 3 est consacré à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité

[35] Avis du Conseil d'Etat n° 63.192/2 du 19 avril 2018, in *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 418.

[36] L'Autorité souligne. Les travaux préparatoires de la LTD le confirment puisqu'il est écrit que « *en ce qui concerne la catégorie de destinataires, il doit être répété, comme le remarque le Conseil d'État dans son avis, page 18, que les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du titre 3 ne sont pas des destinataires, au sens de la définition du Règlement. Le traitement de ces données par ces autorités concorde de la sorte avec les règles applicables en matière de protection des données en fonction des finalités du traitement. Par conséquent, les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du titre 3 sont exclus de la mention dans le protocole* ».

Une lecture combinée de l'article 20 de la LTD avec cette disposition amène à constater que les communications de données à caractère personnel vers des institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, b) à f) de la loi du 15 janvier 1990, c'est-à-dire les **institutions de sécurité sociale appartenant au réseau secondaire**, ne doivent **pas être encadrés par un protocole** au sens de l'article 20 de la LTD. Ces flux doivent, par contre, **être autorisés par le Comité de sécurité de l'information**.

Il s'agit des communications vers les institutions suivantes :

- ✓ les institutions coopérantes de sécurité sociale, c'est-à-dire les organismes de droit privé, autres que les secrétariats sociaux d'employeurs et les offices de tarification des associations de pharmaciens, agréés pour collaborer à l'application de la sécurité sociale ;

- ✓ les fonds de sécurité d'existence institués, en vertu de la loi du 7 janvier 1958, par conventions collectives de travail conclues au sein des commissions paritaires et rendues obligatoires par le Roi, dans la mesure où ils accordent des avantages complémentaires visés au 1°, littera f de la loi du 15 janvier 1990 ;

- ✓ les personnes chargées par les institutions de sécurité sociale visées aux *a), b)* et *c)* de tenir à jour un répertoire particulier des personnes visé à l'article 6, alinéa 2, 2°; de la loi du 15 janvier 1990 ;

- ✓ l'Etat, les Communautés, les Régions et les établissements publics visés à l'article 18 des lois coordonnées relatives aux allocations familiales pour travailleurs salariés, en ce qui concerne leurs missions en matière d'allocations familiales pour leur personnel ;

- ✓ les centres publics d'action sociale dans la mesure où ils sont chargés de l'application de la sécurité sociale au sens de la loi du 15 janvier 1990.

Par contre, la communication de données à caractère personnel par des services publics fédéraux et des institutions publiques de l'autorité fédérale **à des institutions de sécurité sociale appartenant au réseau primaire** de la sécurité sociale doit, en principe[37], être **formalisée dans un protocole** au sens de l'article 20 de la LTD[38].

---

[37] L'article 35/1, § 1, alinéa 3, de la loi du 15 août 2012 dispose que si « *les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou [si] au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement* », la communication sera soumise à la délibération préalable des chambres réunies du comité de sécurité de l'information.

[38] Article 35/1, § 1, alinéa 3, de la loi du 15 août 2012. Le réseau primaire de la sécurité sociale est composé des institutions publiques de sécurité sociale, autres que la Banque-carrefour de la sécurité sociale, et des services publics fédéraux qui sont chargés de l'application de la sécurité sociale

iv. Les flux vers l'étranger

Les travaux préparatoires de l'article 20 de la LTD indiquent que l'obligation de conclure un protocole pour formaliser les communications de données en provenance des autorités publiques fédérales ne peut être imposée pour des flux vers l'étranger. Les travaux préparatoires justifient cette exclusion en renvoyant à l'article 1er du RGPD[39], lequel dispose que « *La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* ». Ainsi**, les communications de données vers des pays de l'Espace économique européen ne peuvent être conditionnées à la conclusion d'un protocole entre le responsable du traitement initial et les destinataires des données.** Mais il n'en demeure pas moins que les responsables du traitement impliqués dans une communication de données à caractère personnel doivent veiller à ce que cette communication respecte toute la règlementation en vigueur, en particulier le RGPD.

Par ailleurs, **si les autorités publiques souhaitent transférer des données à caractère personnel vers un pays tiers (c.-à-d. : hors Espace économique européen) ou vers une organisation internationale, il est nécessaire qu'elles respectent les conditions imposées par le Chapitre V du RGPD** et, le cas échéant, qu'elles prévoient des garanties appropriées.

[39] *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 44.

SCHÉMA RÉCAPITULATIF CONCERNANT LES FORMALITÉS À ACCOMPLIR POUR ENCADRER LES COMMUNICATIONS DE DONNÉES À CARACTÈRE PERSONNEL DANS LE DOMAINE DE LA SÉCURITÉ SOCIALE

Source de la communication	Destinataire de la communication	Délibération préalable ou protocole ?	Chambre compétente au sein du comité de sécurité de l'information	Source
Institution de sécurité sociale ou BCSS	Institution de sécurité sociale	Délibération préalable obligatoire	Chambre sécurité sociale et de santé	Art. 15 § 1er de la loi du 15 janvier 1990
Institution de sécurité sociale ou BCSS	Instance autre qu'un SPF, SPP ou un OIP	Délibération préalable obligatoire	Chambre sécurité sociale et de santé	Art. 15 § 1er de la loi du 15 janvier 1990
Les institutions de sécurité sociale qui appartiennent au réseau primaire ou BCSS	SPF, SPP ou OIP, autre qu'une institution de sécurité sociale	Une délibération n'est obligatoire que si l'instance qui communique, l'instance destinatrice et la BCSS ne parviennent pas à conclure un protocole *ou* si une des parties le demande et en a informé les autres	Chambres réunies	Art. 15 § 2 de la loi du 15 janvier 1990
Les institutions de sécurité sociale, autres que celles appartenant au réseau primaire	SPF, SPP ou OIP, autre qu'une institution de sécurité sociale	Délibération préalable obligatoire	Chambres réunies	Art. 15 § 2 de la loi du 15 janvier 1990
SPF et institutions publiques de l'Autorité fédérale	Les institutions de sécurité sociale qui appartiennent au réseau primaire	Une délibération n'est obligatoire que si l'instance qui communique, l'instance destinatrice et la BCSS ne parviennent pas à conclure un protocole *ou* si une des parties le demande et en a informé les autres	Chambres réunies	Art. 35/1, § 1er, al. 3, de la loi du 15 août 2012
SPF et institutions publiques de l'Autorité fédérale	Les institutions de sécurité sociales, autres que celles appartenant au réseau primaire	Délibération préalable obligatoire	Chambres réunies	Art. 35/1, § 1er, al. 4, de la loi du 15 août 2012

Institution de sécurité sociale : notion définie à l'article 2 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

BCSS : Banque-Carrefour de la Sécurité Sociale

SPF : Service public fédéral

SPP : Service public de programmation

OIP : organisme d'intérêt public

Les institutions de sécurité sociale qui appartiennent au réseau primaire : les institutions publiques de sécurité sociale, autres que la Banque-carrefour de la sécurité sociale, et les services publics fédéraux qui sont chargés de l'application de la sécurité sociale [ONSS, INSATI, INAMI, OCM, Service fédéral des pensions, FAMIFED, FEDRIS, FAT, ONEM, ONVA, SPF Sécurité sociale, SPF Emploi, Travail et Concertation sociale, Collège Intermutualiste national, Service public de programmation Intégration sociale]

REMARQUE GÉNÉRALE IMPORTANTE

Toute communication de données à caractère personnel doit respecter la règlementation en vigueur, en particulier le RGPD et la LTD. Ainsi, les responsables du traitement doivent toujours veiller à ce que la communication respecte cette règlementation, quand bien même cette communication ne doit pas faire l'objet d'un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données en vertu de l'article 20 de la LTD.

Il s'ensuit, notamment, que la communication de données doit être basée sur **l'une des bases juridiques mentionnées à l'article 6 du RGPD** puisque, conformément à l'article 5.1.a) du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. Le responsable du traitement initial doit s'assurer que c'est bien le cas avant de procéder à la communication .

En outre, l'article 5.1.b) du RGPD impose que les données soient collectées pour des **finalités déterminées, explicites et légitimes** et qu'elles ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités. Le responsable du traitement initial doit dès lors également **vérifier que la finalité du traitement ultérieur n'est pas incompatible avec celle du traitement initial.**

Par ailleurs, conformément à l'article 5.1.c) du RGPD, les données à caractère personnel traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Le responsable du traitement initial doit donc s'assurer que les données transférées **répondent au principe de la minimisation des données**.

Enfin, et de manière générale, les responsables du traitement impliqués dans la communication de données doivent mettre en œuvre « *des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au [RGPD]* »[40], y compris en ce qui concerne la sécurité des données transférées[41].

[40] Article 24 du RGPD.

[41] Voyez les développements précédant le projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE , Doc. Parl., Ch., sess. ord. 2017-2018, n° 54-3185/001, p. 63.

II. Le contenu du protocole d'accord

L'article 20 § 1 de la LTD loi mentionne un contenu facultatif et non exhaustif pour le protocole d'accord[42] puisqu'il se lit comme suit « *[…] Ce protocole peut prévoir notamment :*

1° l'identification de l'autorité publique fédérale qui transfère les données à caractère personnel et celle du destinataire;

2° l'identification du responsable du traitement au sein de l'autorité publique qui transfère les données et au sein du destinataire;

3° les coordonnées des délégués à la protection des données concernés au sein de l'autorité publique qui transfère les données ainsi que du destinataire;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° les catégories de données à caractère personnel transférées et leur format;

6° les catégories de destinataires;

7° la base légale du transfert;

8° les modalités de communication utilisée;

9° toute mesure spécifique encadrant le transfert conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut;

10° les restrictions légales applicables aux droits de la personne concernée;

11° les modalités des droits de la personne concernées auprès du destinataire;

12° la périodicité du transfert;

13° la durée du protocole;

14° les sanctions applicables en cas de non-respect du protocole, sans préjudice du titre 6 »[43].

Le caractère facultatif du contenu de l'accord a été critiqué tant par la CPVP[44] que par le Conseil d'Etat[45] dans leurs avis respectifs concernant l'avant-projet de loi "relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel". Le Conseil d'Etat a souligné que le fait que l'avant-projet qui est devenu la LTD « *n'énonce pas, de manière suffisamment précise, les différents éléments sur lesquels doivent porter ces protocoles* » porte atteinte à l'exigence de légalité qui s'impose pourtant en cas d'ingérence avec le droit au respect de la vie privée[46]. L'Autorité a également insisté pour que le législateur prévoie les éléments obligatoires (et non optionnels) du protocole[47]. L'Autorité constate que législateur n'a pas suivi cette recommandation.

---

[42] Par souci de complétude, l'Autorité souligne que ce choix du législateur fédéral en faveur d'un contenu facultatif et non-exhaustif diffère de celui posé par le législateur flamand. En effet, l'article 8 du décret flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives dispose que "*Toute communication électronique de données à caractère personnel par une autorité à une autre autorité ou à une autorité extérieure nécessite un protocole conclu entre les autorités concernées. En tout état de cause, ce protocole prévoit ce qui suit : [liste des différents éléments qui doivent être prévus dans le protocole]*".

[43] L'Autorité souligne

[44] CPVP, Avis n° 33/2018, p. 46.

[45] Avis du Conseil d'Etat n° 63.192/2 du 19 avril 2018, in *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 422.

[46] Avis du Conseil d'Etat n° 63.192/2 du 19 avril 2018, in *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 422.

[47] CPVP, Avis n° 33/2018, p. 46.

Il ne faut toutefois pas en déduire que les responsables du traitement seraient complètement libres de déterminer, sans aucune contrainte juridique, le contenu du protocole qu'ils concluent pour formaliser une communication de données en provenance du secteur public. Les exigences du RGPD et de la LTD quant aux conditions dans lesquelles des données à caractère personnel peuvent être communiquées à des tiers doivent guider les responsables du traitement lors de la conclusion du protocole. Il est important, à cet égard, de rappeler que l'article 24 du RGPD impose au responsable du traitement de mettre en œuvre « *des mesures techniques et organisationnelles appropriées [au regard de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques] pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ». Les responsables du traitement doivent, par l'adoption du protocole, s'assurer que la communication de données à caractère personnel est effectuée conformément au RGPD. Dans ce contexte, l'Autorité recommande que le protocole prévoie, en principe, les éléments suivants :

- ✓ L'**identification** de **l'autorité publique qui transfère** les données à caractère personnel et du **responsable du traitement destinataire** des données ainsi que les coordonnées de leurs délégués à la protection des données ;

- ✓ Les **finalités** précises pour lesquelles **les données ont été collectées à l'origine** par l'autorité publique, les **finalités** pour lesquelles **les données sont transférées** et **l'analyse de la compatibilité de ces finalités** si la communication de données constitue un traitement ultérieur, c'est-à-dire si la communication de données poursuit une ou plusieurs finalités différentes de celles pour lesquelles elles ont été collectées à l'origine. Cette analyse de compatibilité ne sera toutefois pas nécessaire si le traitement ultérieur est « *fondé […] sur le droit d'un Etat membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23.1 [du RGPD]* » et que la règlementation en question est suffisamment claire, précise et prévisible pour les justiciables ;

- ✓ Les **types précis de données** à caractère personnel transférées, afin de permettre aux responsables du traitement de veiller au respect du principe de proportionnalité ;

- ✓ La **base légale qui fonde la communication** des données à caractère personnel par l'autorité publique qui transfère les données **et la base légale qui en fonde la réception** par le responsable du traitement destinataire. Le plus souvent, il s'agira d'indiquer quelle est l'obligation légale et/ou la mission d'intérêt public spécifique poursuivie par le responsable du traitement qui transfère et le responsable du traitement qui reçoit les données à caractère personnel ;

- ✓ Les **modalités de communication** utilisées et une définition fonctionnelles des **mesures de sécurité** adoptées afin de sécuriser la transmission des données ;

- ✓ Le cas échéant, **toute mesure spécifique prise par les responsables du traitement pour encadrer la communication conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut** (choix du format de la communication, journalisation des accès de manière telle que l'on puisse savoir qui a eu accès à quoi quand et pourquoi, mise en place d'un répertoire de références en cas de communication automatique des actualisations des données afin de s'assurer que les données nécessaires soient actualisées pour la durée nécessaire, …) ;

- ✓ La **périodicité de la communication** ;

- ✓ La **durée du protocole** ;

- ✓ Les **sanctions applicables** en cas de non-respect du protocole, sans préjudice du titre 6 de la LTD.

III. Éléments de procédure

L'article 20 de la LTD énonce deux obligations procédurales pour la conclusion des protocoles :

- ✓ **Les DPO doivent être impliqués dans la rédaction du protocole (article 20 § 2 de la LTD)**

L'article 20 § 2 de la LTD dispose que « *Le protocole est adopté après les avis respectifs du délégué à la protection des données de l'autorité publique fédérale détenteur des données à caractère personnel et du destinataire. Ces avis sont annexés au protocole. Lorsqu'au moins un de ces avis n'est pas suivi par les responsables du traitement, le protocole mentionne, en ses dispositions introductives, la ou les raisons pour laquelle ou lesquelles cet ou ces avis n'ont pas été suivis* ».

- ✓ **Les protocoles doivent être publiés sur le site internet des différents responsables du traitement (article 20 § 3 de la LTD)**

L'article 20 § 3 de la LTD dispose que « *Le protocole est publié sur le site internet des responsables du traitement concernés* ». Cette obligation semble faire suite à une remarque formulée tant par la CPVP[48] que par le Conseil d'Etat dans leurs avis respectifs[49], qui ont, chacun, souligné que les protocoles organisent une ingérence dans la vie privée des citoyens et qu'il convient donc qu'ils soient accessible – et donc publiés – pour assurer une prévisibilité des communications de données à caractère personnel.

La CPVP demandait à ce que les protocoles soient publiés au Moniteur belge, mais le législateur a choisi la voie du site internet des responsables du traitement. L'objectif est ainsi de garantir une large visibilité[50].

- ✓ **La possibilité d'adopter des « protocoles types » ou des « protocoles généraux »**

L'Autorité a récemment adopté une recommandation dans laquelle elle détermine les conditions dans lesquelles les responsables du traitement impliqués dans une communication de données à caractère personnel peuvent avoir recours à des « protocoles types » ou à des « protocoles généraux »[51]. Si l'Autorité n'y exclut pas ces possibilités, elle rappelle que ces protocoles doivent nécessairement être conclus dans le respect des exigences légales mentionnées à l'article 20, §§ 2 et 3 de la LTD.

---

[48] CPVP, Avis n° 33/2018, p. 46.

[49] Avis du Conseil d'Etat n° 63.192/2 du 19 avril 2018, in *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 424.

[50] *Doc. Parl.*, Ch., sess. ord. 2017-2018, n° 54-3126/001, p. 46.

[51] APD, Recommandation n° 02/2019 du 18 octobre 2019

IV. Champ d'application temporel de l'obligation de conclure un protocole d'accord

L'article 281 de la LTD dispose que « *La présente loi entre en vigueur le jour de sa publication au Moniteur belge. Par dérogation à l'alinéa 1er, l'article 20 entre en vigueur le premier jour du mois qui suit l'expiration d'un délai de six mois prenant cours le jour suivant la publication de la présente loi au Moniteur belge* ». La LTD a été publiée au Moniteur belge le 5 septembre 2018 et elle est donc entrée en vigueur à cette date, **à l'exception de son article 20 qui est entré en vigueur le 1er avril 2019**.

Dans les travaux préparatoires précédant l'adoption de l'article 281 de la LTD, le législateur justifie l'existence d'un délai supplémentaire pour l'entrée en vigueur de l'article 20 de la LTD en soulignant que *« l'application de [l'article 20 de la LTD] dès l'entrée en vigueur de [la LTD] impliquerait que les administrations publiques qui ne disposeraient pas de protocole pour de nouveaux traitements réalisés directement après l'entrée en vigueur, seraient en violation de la présente loi. Afin de permettre aux administrations publiques d'adopter le protocole pour ces nouveaux traitements, il est prévu un délai raisonnable pour se mettre en conformité* »[52]. Cette justification dévoile qu'aux yeux du législateur ce sont essentiellement **les nouveaux traitements** qui sont soumis à l'obligation de protocole. Ainsi, il ne fait aucun doute que, **depuis le 1er avril 2019**, toutes les **nouvelles communications** de données à caractère personnel, qui rentrent dans le champ d'application de l'article 20 de la LTD, doivent, en principe[53], être formalisées par un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données[54].

Les communications de données à caractère personnel qui ont été mises en place sous l'empire de la loi du 8 décembre 1992 ne doivent, en principe, pas faire l'objet d'un protocole conclu entre le responsable du traitement initial et le responsable du traitement destinataire des données[55]. Aux termes de l'article 36*bis* de la loi du 8

---

[52] L'Autorité souligne.

[53] À moins que les responsables du traitement ne parviennent pas à un accord concernant la communication ou qu'au moins un de ces responsables demande une délibération du comité de sécurité de l'information et en a informé les autres, auquel cas la communication fera l'objet d'une délibération préalable du comité de sécurité de l'information. Dans une telle situation, l'autorité publique est, par dérogation à l'article 20 de LTD, dispensée de l'obligation d'établir un protocole y relatif avec le destinataire des données à caractère personnel (article 35/1 de la loi du 15 août 2012). Par ailleurs, l'article 35/1 de la loi du 15 août 2012 prévoit également d'autres exceptions à l'obligation de conclure un protocole : (1) les communications d'une autorité publique fédérale vers des tiers autres que des institutions de la sécurité sociale ne doivent pas faire l'objet d'une délibération dans la mesure où une norme législative ou règlementaire précise les modalités de la communication dont les finalités, les catégories de données et les destinataire et (2) la communication est ponctuelle, est en conformité avec le RGPD, et a lieu vers des es personnes ou institutions habilitées à les recevoir en vertu d'une mission légale.

[54] Le Comité de sécurité de l'information a considéré que tant que l'article 20 de la LTD n'était pas entré en vigueur, il devait autoriser toutes les communications de données à caractère personnel d'une autorité publique fédérale vers des tiers puisqu'il n'était pas encore possible de formaliser cette communication dans un protocole d'accord (Voyez, par exemple, la délibération n° 19/007 du 5 mars 2019 (dont le § 9 énonce que « *Le Comité souligne que l'article 20 de loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, (ci-après « LTD ») n'entre en vigueur que le 1er avril 2019. Il ne peut dès lors pas encore être satisfait à la condition telle que prévue à l'article 35/1 précité de la loi du 15 août 2012. La communication visée des données par la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports requiert dès lors une délibération sur la base de l'article 35/1 de la loi précitée du 15 août 2012* »).

[55] On peut établir un parallèle avec l'obligation d'effectuer une analyse d'impact relative à la protection des données dont le « Groupe de travail Article 29 » et l'ancienne Commission de la protection de la vie privée ont considéré qu'elle ne s'imposait aux opérations de traitement déjà existantes que si les risques pour les droits et libertés des personnes physiques changent après le 25 mai 2018, par exemple parce qu'une nouvelle technologie est employée ou parce que les données à caractère personnel sont utilisées pour une autre finalité (voyez Groupe de travail « Article 29 », *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière*

décembre 1992, « […] *toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, [exigeait] une autorisation de principe de ce comité sectoriel à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel crée au sein de la Commission pour la protection de la vie privée […]* »[56]. Toutes les **communications existantes** ont donc, en principe, été autorisées par un comité sectoriel institué auprès de l'ancienne Commission de la protection de la vie privée. Or, aux termes de l'article 111 de la loi du 3 décembre 2017, ces autorisations « *gardent leur validité juridique* »[57]. L'article 111 de la loi du 3 décembre 2017 prévoit, en outre, qu'il est **toujours possible d'adhérer à une autorisation générale** qui avait été octroyée par délibération d'un comité sectoriel, à condition que *« celui qui demande l'adhésion [remette] une déclaration d'engagement écrite et signée [au Comité de sécurité de l'information] dans laquelle il confirme adhérer aux conditions de la délibération en question, sans préjudice des pouvoirs de contrôle que peut exercer l'Autorité de protection des données […]* ». Il s'ensuit que les responsables du traitement qui transfèrent des données à caractère personnel selon les modalités qui avaient été **autorisés par un comité sectoriel** de la Commission de la protection de la vie privée avant le 25 mai 2018 **peuvent continuer de se prévaloir de cette autorisation et ne doivent pas encadrer cette communication de données par un protocole au sens de l'article 20 de la LTD**, pour autant qu'il n'y ait pas de modification substantielle des modalités de la communication par rapport à celles qui avaient été prévues dans cette autorisation. En effet, l'article 20 de la LTD prévoit que l'obligation de conclure un protocole ne s'impose qu'à défaut d'« *autre disposition dans des lois particulières* ».

Mais qu'en est-il pour les communications qui auraient dû être autorisées par un comité sectoriel, mais qui ne l'ont pas été parce que le responsable du traitement n'a pas sollicité l'autorisation du comité sectoriel compétent ? À l'évidence, les responsables du traitement impliqués ne peuvent se prévaloir ni d'une autorisation délivrée par les anciens comités sectoriels, ni de l'article 111 de la loi du 3 décembre 2017 qui, en maintenant la validité juridique de ces autorisations, permet de déroger à l'article 20 de la LTD. Il s'ensuit que **ces communications doivent faire l'objet d'un protocole** entre le responsable du traitement initial et le responsable du traitement destinataire des données (à condition, bien entendu, qu'ils rentrent dans le champ d'application matériel de l'article 20 de la LTD).

de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, 4 avril 2017, p. 16 ; CPVP, Recommandation n° 01/2018 du 28 février 2018, p. 37).

[56] Article 36bis de la loi du 8 décembre 1992

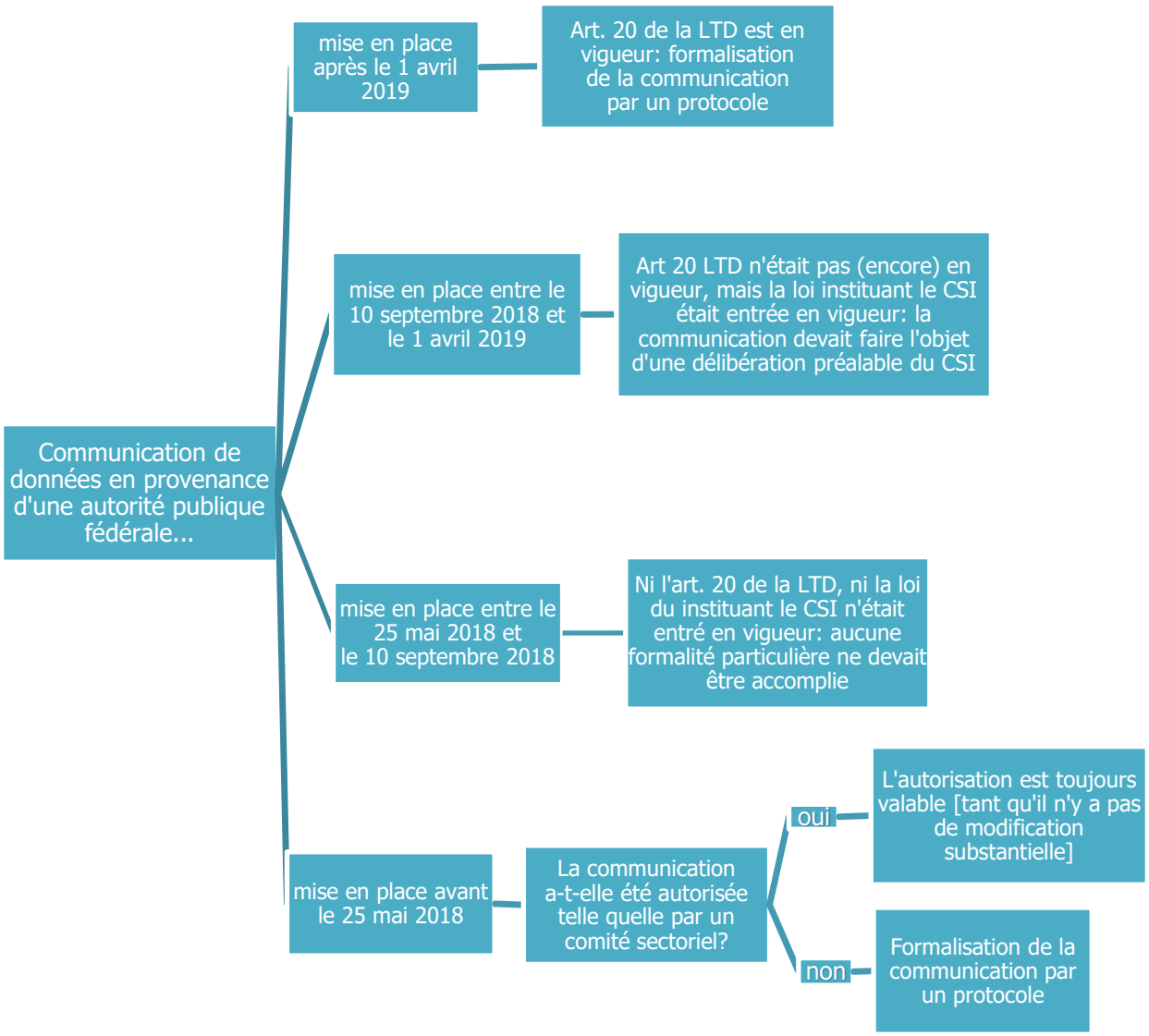
[57] La loi du 3 décembre 2017 est entrée en vigueur le 25 mai 2018.

RÉCAPITULATIF GRAPHIQUE DE L'APPLICATION TEMPORELLE DE L'OBLIGATION DE CONCLURE UN PROTOCOLE POUR FORMALISER LES COMMUNICATIONS DE DONNÉES EN PROVENANCE DES AUTORITÉS PUBLIQUES FÉDÉRALES [QUI RELEVAIENT DU CHAMP D'APPLICATION DE L'ANCIEN ARTICLE 36BIS DE LA LOI DU 8 DÉCEMBRE 1992]

25 mai 2018 : abrogation de la disposition de la loi du 8 décembre 1992 qui instituait le comité sectoriel pour l'autorité fédérale

10 septembre 2018 : entrée en vigueur de la loi instituant le CSI

1er avril 2019 : entrée en vigueur de l'article 20 de la LTD



V. Quid si les responsables du traitement n'arrivent pas à conclure un protocole pour formaliser la communication de données à caractère personnel ?

1. Principe : délibération de la chambre autorité fédérale du comité de sécurité de l'information

Si les responsables du traitement initial et destinataire ne parviennent pas à un accord concernant la communication ***ou*** si, au moins, un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement, l'article 35/1, § 1er, alinéa 1, de la loi du 15 août 2012 prévoit que ladite communication devra faire l'objet **d'une délibération préalable par la chambre autorité fédérale** du comité de sécurité de l'information visé dans la loi du 5 septembre 2018. La communication des données peut dès lors être effectuée sans que le responsable du traitement initial et le responsable du traitement destinataire des données doivent conclure un protocole.

2. Exceptions : pas besoin de délibération (ni de protocole)

L'article 35/1, § 1er, alinéa 2, de la loi du 15 août 2012 prévoit toutefois que la communication ne doit pas faire l'objet d'une délibération préalable :

- ✓ Lorsque des normes réglementaires précisent les modalités de la communication, dont les finalités, les catégories de données et les destinataires, ou
- ✓ Lorsqu'il s'agit d'une communication ponctuelle de données, en conformité avec le règlement (UE) 2016/679 précité, à des personnes ou institutions habilitées à les recevoir en vertu d'une mission légale.

3. Cas particulier concernant les communications en provenance du secteur public fédéral vers des institutions de sécurité sociale appartenant au réseau primaire : délibération des chambres réunies du comité de sécurité de l'information

L'article 35/1, § 1er, alinéa 3, de la loi du 15 août 2012 prévoit que la communication de données à caractère personnel par des autorités publiques fédérales à des institutions de sécurité sociale qui appartiennent au réseau

primaire de la sécurité sociale[58] doit faire l'objet **d'une délibération préalable des chambres réunies** du comité de sécurité de l'information, dans la mesure où les responsables du traitement de l'instance qui communique, de l'instance destinatrice et de la Banque-carrefour de la sécurité sociale ne parviennent pas, en exécution de l'article 20 la LTD, à un accord concernant la communication ou, au moins, un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement.

[58] Il s'agit des institutions visées à l'article 2, alinéa 1er, 2°, a), de la loi du 15 janvier 1990 : "les institutions publiques de sécurité sociale, autres que la Banque-carrefour, ainsi que les services publics fédéraux qui sont chargés de l'application de la sécurité sociale"