



Date	Version	Auteur
06/06/2019	1.1	Laurent GÄRTNER

## DONNÉES À CARACTÈRE PERSONNEL (DCP)

Article 4.1 : «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

Source : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

La nature des informations n'a aucune importance si le lien est établi vers une personne, c'est une donnée à caractère personnel, avec un lien direct ou indirect à la personne

*Une affectation est une donnée à caractère personnelle puisqu'elle est liée à un agent (directement avec le nom ou indirectement avec le « numagt » de la base EPP.*

La loi ne se limite à la capacité du responsable de traitement à identifier la personne physique, mais par n'importe qui dans le monde.

*Une enquête destinée aux directeurs d'école pour laquelle on prélève l'adresse IP de la connexion l'ayant complété. L'IP sera liée soit à l'école d'exercice, soit au domicile de l'agent.*

## DONNÉES SENSIBLES

Article 9 : Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

Source : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Toutefois, attention aux inférences permettant de déterminer des données sensibles par déduction d'autres.

*Par exemple, la déduction d'une opinion religieuse à partir des jours de congés posés dans une application de gestion du temps.*

## TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Article 4.2 : «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

Source : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Un traitement n'est pas forcément une application (un tableau Excel contenant des DCP est un traitement). Il n'a pas besoin d'être automatisé ni numérisé (des fiches manuscrite contenant des DCP est un traitement). Une application peut opérer à plusieurs traitements différents et un traitement peut correspondre aussi à plusieurs applications.

## LICÉITÉ DU TRAITEMENT

Article 5 : 1. Les données à caractère personnel doivent être :

- a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
- b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);
- c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
- d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);
- e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Source : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

La finalité du traitement doit être clairement exposée et énoncée, c'est un élément principal du registre des traitements de données à caractère personnel.

*La finalité du traitement « Affelnet 6ème » est « Affecter les élèves quittant le premier degré dans un collège selon les vœux formulés par les responsables légaux. »*

Les données recueillies par un traitement doivent se limiter au stricte nécessaire.

*Par exemple, le numéro de sécurité sociale ne permet que de réaliser une jointure entre les bases RH académique et le service liaison-rémunération de la TG. Il ne devrait apparaître nulle part ailleurs.*

Article 6 : Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

- a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
- b) le traitement 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;
- c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
- d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
- e) le traitement 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;
- f) le traitement 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 point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Source : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

L'article 8 précise que le consentement d'un mineur de moins de 15 ans doit être doublé du consentement d'un titulaire de l'autorité parentale pour les services de la société de l'information (GAFA en général)

La majorité des traitements opérés par l'Éducation nationale relèvent d'une mission de service publique.

*Par exemple, l'affectation en sixième opérée par l'application Affelnet Lycée correspond à l'arrêté du 17 juillet 2017 - MENE1719988A*

Si le traitement ne correspond à aucune des 5 bases légales, il nécessite le consentement de la personne

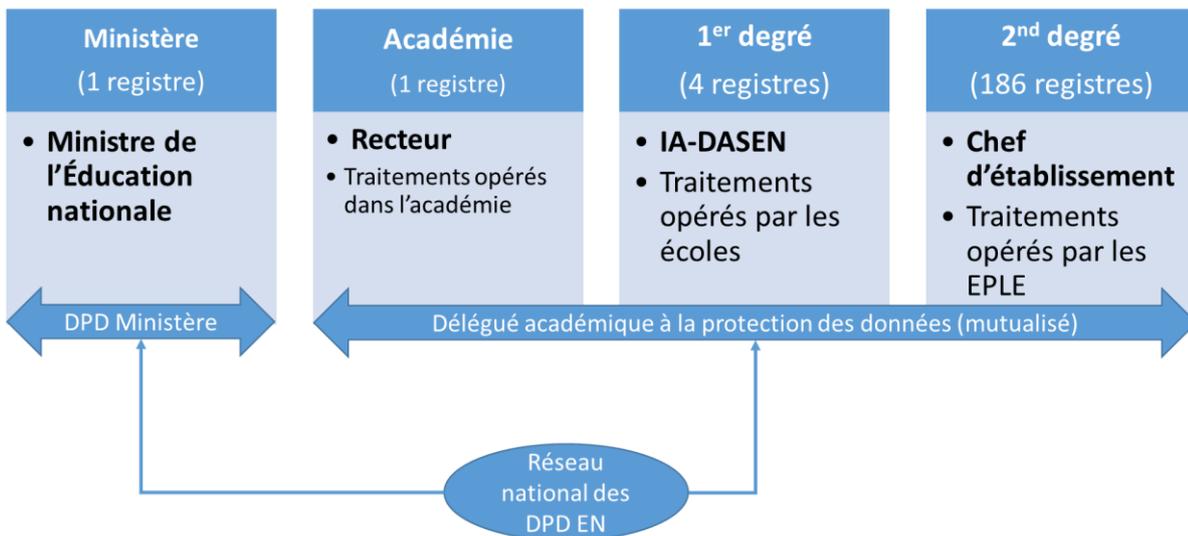
- **Libre** : il ne peut pas être obtenu par la contrainte ou l'obligation ;
- **Éclairé** : il ne peut être obtenu qu'en exposant clairement les enjeux ;
- **Spécifique** : il n'est obtenu que pour un seul et unique traitement ;
- **Univoque** : il doit être le résultat d'un geste positif ;
- Le retrait du consentement doit être tout aussi simple.

Il est nécessaire de garder une trace du consentement des usagers.

## LE RESPONSABLE DE TRAITEMENTS (RT)

Personne morale représentant la structure

- Définir les finalités, moyens et modalités des traitements opérés
- Tenir à jour le registre des traitements opérés dans la structure
- Informer les usagers des traitements opérés
- Contrôler la conformité des sous-traitants
- Coopérer avec les autorités de contrôle (CNIL)
- Mettre en œuvre les mesures de sécurité organisationnelles et techniques appropriées
- Remonter toute violation de données à caractère personnel



## LES DROITS DE L'USAGER

**Droit d'accès** : l'utilisateur doit pouvoir accéder en détail aux données disponibles à son sujet

**Droit d'opposition** : l'utilisateur doit pouvoir s'opposer au traitement de ses données personnelles

**Droit à la limitation** : l'utilisateur doit pouvoir limiter le traitement de ses données personnelles

**Droit de rectification** : l'utilisateur doit pouvoir faire modifier une donnée erronée le concernant

**Droit à l'effacement** : l'utilisateur peut demander la suppression de toutes les données qui le concernent

**Droit à la portabilité** : l'utilisateur peut demander une extraction numérique de ses données

Version	Modifications	Date	Auteurs
1.0	Création du document.	16/01/2019	LG
1.1	Remplacement des textes de référence « loi de 1978 » par les références au RGPD.	06/06/2019	LG