

Projet d'arrêté du Gouvernement de la Communauté française déterminant les catégories de données à caractère personnel faisant l'objet d'un traitement au regard des finalités des espaces numériques et définissant les catégories de données à transmettre par les services du Gouvernement aux écoles en application des articles 6 et 11 du décret du 25 avril 2019 portant sur la gouvernance numérique du système scolaire et à la transmission des données numériques dans l'enseignement obligatoire

Le Gouvernement de la Communauté française,

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu le décret du 25 avril 2019 portant sur la gouvernance numérique du système scolaire et à la transmission des données numériques dans l'enseignement obligatoire, l'article 6 § 1^{er} et l'article 11 § 1^{er}, alinéa 2 ;

Vu le test genre du 8 juin 2020 établi en application de l'article 4, alinéa 2, 1^o, du décret du 7 janvier 2016 relatif à l'intégration de la dimension de genre dans l'ensemble des politiques de la Communauté française ;

Vu le protocole de négociation avec le comité de négociation des organes de représentation et de coordination des Pouvoirs organisateurs de l'enseignement et des centres PMS subventionnés du décret du 20 juillet 2006 relatif à la concertation des organes de représentation et de coordination des Pouvoirs organisateurs de l'enseignement et des Centres PMS subventionnés, conclu en date du 19 mars 2020 ;

Vu le protocole de négociation syndicale au sein du Comité de négociation de secteur IX, du Comité des services publics provinciaux et locaux – section II et du Comité de négociation pour les statuts des personnels de l'Enseignement libre subventionné selon la procédure de l'arrêté royal du 28 septembre 1984 portant exécution de la loi du 19 décembre 1974 organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités, conclu en date du 19 mars 2020 ;

Vu le protocole de négociation avec les organisations représentatives des parents d'élèves au niveau communautaire conformément à l'article 7, §2 du décret du 30 avril 2009 portant sur les associations de parents d'élèves et les organisations représentatives d'associations de parents d'élèves en Communauté française ;

Vu l'avis n° 108/2020 de l'Autorité de protection des données, donné le 5 novembre 2020 en application des articles 23 et 26 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données et en application de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu l'avis X du Conseil d'État, donné le X en application de l'article 84, § 1^{er}, alinéa 1^{er}, 2^o, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, telles que modifiées ;

Sur la proposition de la Ministre de l'Enseignement obligatoire ;

Après délibération,

ARRETE :

Article 1^{er}. – Pour l'application du présent arrêté, il y a lieu d'entendre par :

1° « décret gouvernance numérique » : le décret du 25 avril 2019 relatif à la gouvernance numérique du système scolaire et à la transmission des données numériques dans l'enseignement ;

2° « identification » : le processus de collecte et de validation d'un ensemble d'attributs d'identité visant à identifier une personne physique dans un contexte particulier ;

3° « authentification » : le processus permettant de vérifier qu'un utilisateur est bien le propriétaire d'une identité numérique donnée lors de l'accès à une ressource numérique ; l'utilisateur doit présenter des titres d'authentification qui seront validés dans le processus d'authentification ;

4° « usagers » : les pouvoirs organisateurs, les directeurs, les Fédérations de pouvoirs organisateurs et les membres des personnels de l'enseignement ;

5° « consolidation » : le regroupement de données organisées logiquement ou liées entre elles ;

6° « variable » : propriété représentant une population donnée ou pouvant être comparée à l'ensemble d'une population donnée.

7° « RGPD » : le 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 ;

Article 2. – § 1^{er}. La catégorie de données à caractère personnel, prévue à l'article 6 § 1^{er}, du décret gouvernance numérique et faisant l'objet d'un traitement en application d'une disposition légale, décrétable ou réglementaire et qui est nécessaire au regard des finalités des espaces numériques visés à l'article 4, est relative aux données d'identification et d'authentification des usagers des espaces.

Les données d'identification et d'authentification sont divisées en trois sous-catégories de données nécessaires afin d'assurer la gestion de la fonctionnalité des espaces numériques :

1° les données strictement relatives à l'identification et à l'authentification ;

2° les données relatives à la communication ;

3° les données relatives à la navigation et à la traçabilité.

§ 2. Les données strictement relatives à l'identification et à l'authentification comprennent les données suivantes :

- numéro de Registre national ;
- numéro de matricule de membre des personnels de l'enseignement ;
- numéro de dossier unique ;
- identifiant en ligne ;
- nom et prénom ;
- genre ;
- nationalité ;
- état civil ;
- certificat d'authentification de l'eID ;
- lieu de naissance ;
- pays de naissance ;
- date de naissance ;
- adresse e-mail ;
- lien organisationnel ;
- fonction ;

- adresse professionnelle,
- adresse privée ;
- permissions.

Les données de communication comprennent les données suivantes :

- adresse postale ;
- informations de contact relatives à un moyen de communication ;
- adresse de courrier électronique ;
- contenu des communications, à destination et à l'origine des usagers, relatives aux comptes et aux démarches d'accès aux espaces numériques.

Les données de navigation et de traçabilité comprennent les données suivantes :

- l'adresse IP qui est attribuée lors de la connexion ;
- les dates de création et de modification du compte ;
- le lieu de connexion ;
- la date et l'heure d'accès ;
- les pages consultées et le type de navigateur (browser) utilisé ;
- la plate-forme et/ou le système d'exploitation installé sur le terminal de l'utilisateur ;
- le moteur de recherche ainsi que les mots-clés utilisés pour retrouver le site ;
- les fichiers téléchargés ;
- les informations collectées via les cookies ;
- les informations nécessaires afin d'assurer la sécurité des traitements relatifs aux accès aux espaces numériques, dès lors que ces données permettent de journaliser les accès et de prévoir les procédures de gestion d'éventuels incidents et d'assurer la réalisation de statistique sur le fonctionnement des espaces numériques à des fins d'amélioration de leurs performances.

§ 3. Les données prévues au § 2 ne sont pas systématiquement traitées par le Ministère de la Communauté française. Celui-ci détermine au cas par cas si la collecte de ces données est nécessaire au regard du niveau d'assurance à l'identification et du niveau d'assurance à l'authentification requis par les obligations du responsable de traitement.

Ce niveau est évalué en fonction de critères qui visent, à tout le moins, l'ampleur du traitement concerné, les risques pour les personnes concernées par le traitement ainsi que les mesures organisationnelles et techniques mises en place par le Ministère de la Communauté Française en tant que responsable de traitement au sens du RGPD.

§ 4. Les données décrites au § 2 sont conservées de manière active dans un espace de stockage sécurisé tant que l'utilisateur de la plateforme y possède un compte actif.

Lorsqu'un compte est clôturé, les données prévues à l'article 2 sont conservées de manière passive pendant 6 mois dans un espace de stockage sécurisé.

Au terme du délai de 6 mois, seules les données nécessaires au respect des obligations légales du responsable du traitement en tant qu'autorité publique ou au regard de ses missions, sont archivées sans précision de limitation de durée dans un espace de stockage sécurisé, sans préjudice des réglementations qui s'appliqueraient.

Par exception, les données relatives aux traces d'accès : date, heure, identifiant du compte, adresse IP, URL appelée, navigateur, OS sont conservées 5 ans à partir du moment où ces données sont générées.

Les cookies ont également des durées de conservations spécifiques.

Article 3. – Les bases de données nécessaires à l’exploitation des espaces numériques prévus à l’article 4, § 1er, du décret gouvernance numérique sont les bases de données suivantes du Ministère de la Communauté française :

1° les bases de données créées en application de dispositions décrétales ou réglementaires ;

2° les bases de données créées sur la base des informations fournies par les pouvoirs organisateurs ou Fédérations de pouvoirs organisateurs afin de désigner les personnes physiques placées sous leur autorité qui sont dument habilitées à accéder en leur nom à l’espace numérique, conformément à l’article 4 § 1er, du décret gouvernance numérique ;

3° les bases de données créées sur la base des données de communication et de navigation obtenues dans le cadre de l’exploitation des espaces numériques prévus à l’article 4, § 1er, du décret gouvernance numérique.

Article 4. – §1^{er}. Les catégories de données à transmettre par les services du Gouvernement aux écoles prévues à l’article 11 § 1^{er}, alinéa 2, du décret gouvernance numérique, sont celles nécessaires à la consolidation des informations échangées au moyen de l’espace numérique visé à l’article 4, § 1er, 1°, du décret gouvernance numérique et à la réalisation de ces échanges.

Ces catégories de données comprennent :

1. les catégories de données à caractère personnel mentionnées à l’article 2 ;
2. des données relatives à la structure, à l’encadrement et à la population scolaire, reprenant les éléments tant quantitatifs que qualitatifs décrivant la structure, l’encadrement et la population scolaire de l’école ;
3. des variables relatives aux apprentissages, reprenant l’ensemble de variables prenant en compte les caractéristiques liées aux savoirs et aux compétences de l’élève et aux certifications obtenues ;
4. des variables relatives au climat d’école, prenant en compte des caractéristiques liées au climat de l’école ;
5. des variables relatives à la dynamique collective, reprenant l’ensemble de variables prenant en compte les caractéristiques liées aux personnels de l’école ;
6. des variables relatives au parcours des élèves, reprenant l’ensemble de variables prenant en compte les caractéristiques liées aux trajectoires temporelles des élèves dans leur parcours scolaire ;
7. toute autre information en application de dispositions légales ou décrétales en matière d’enseignement ou d’autres dispositions légales ou décrétales nécessaires pour l’exécution de ces dispositions.

§ 2. Les données visées à l’article 4, § 1, alinéa 2, 2° à 6° ne constituent pas des données à caractère personnel au sens du RGPD.

Article 5. – Le présent arrêté entre vigueur le jour de sa publication au Moniteur belge.

Article 6. – Le Ministre ayant l'Enseignement obligatoire dans ses attributions est chargé de l'exécution du présent arrêté.

Bruxelles, le

Le Ministre-Président,

Pierre-Yves JEHOLET

La Ministre de l'Éducation,

A handwritten signature in blue ink, appearing to be 'CD', with a small blue mark above the 'D'.

Caroline DESIR

Projet d'arrêté du Gouvernement de la Communauté française déterminant les catégories de données à caractère personnel faisant l'objet d'un traitement au regard des finalités des espaces numériques et définissant les catégories de données à transmettre par les services du Gouvernement aux écoles en application des articles 6 et 11 du décret du 25 avril 2019 portant sur la gouvernance numérique du système scolaire et à la transmission des données numériques dans l'enseignement obligatoire

RAPPORT AU GOUVERNEMENT

Dans le cadre du Pacte pour un Enseignement d'excellence, l'avis n°3 du Groupe central (GC) fait de la transition numérique un des objectifs stratégiques de l'amélioration de la qualité du système éducatif.

Depuis les travaux du GC, ont été adoptés :

- la Stratégie numérique pour l'éducation¹ qui constitue un chantier important du Pacte (Chantier 3 : Réussir la transition numérique) et fait de la transition numérique un enjeu transversal à plusieurs chantiers du Pacte ;
- le décret du 25 avril 2019 portant sur la gouvernance numérique du système scolaire et à la transmission des données numériques dans l'enseignement obligatoire (ci-après dénommé « décret gouvernance numérique ») qui offre un cadre juridique à la gouvernance numérique qui tient compte des spécificités de l'enseignement obligatoire.

La gouvernance numérique et la transmission des données constituent, en effet, un enjeu central pour l'amélioration de la qualité de l'enseignement et de son pilotage.

D'une part, la gouvernance numérique agit comme un véritable catalyseur dans un système d'enseignement « décentralisé », composé d'acteurs multiples et où l'échange d'informations constitue un enjeu essentiel. D'autre part, elle est essentielle au sein des établissements, non seulement sur le plan pédagogique, mais également pour la gestion administrative des écoles.

L'approche du décret gouvernance numérique quant à la gestion des flux d'informations est basée sur trois grands principes :

- le développement d'une architecture numérique favorisant le renforcement de la gouvernance administrative et pédagogique et axée sur des espaces numériques au service des utilisateurs ;
- l'optimisation des processus de gestion de l'information afin de favoriser le pilotage du système scolaire et la simplification administrative de la gestion du système et des établissements ;
- la sécurisation des échanges d'informations et la protection stricte des données à caractère personnel.

Basée sur ces principes, l'architecture numérique que le décret régit prend appui sur le développement progressif d'« espaces numériques » destinés à différentes catégories d'intervenants du monde scolaire. A l'instar d'autres systèmes éducatifs, il s'agit, à terme, de permettre à chaque enseignant, à tout élève et leurs parents, à chaque équipe de direction et à leur pouvoir organisateur, etc. de disposer d'un « espace » sécurisé lui étant propre et constituant un point d'entrée unique et sécurisé aux différents services de l'Administration.

¹ Notification de la séance du Gouvernement du 10 octobre 2018.

Quatre « espaces » de cette nature sont envisagés par la Stratégie numérique :

- Un espace destiné aux Directions-PO qui permet à l'équipe de direction et son PO d'accéder aux applications administratives (« applications métiers »), au plan de pilotage/contrat d'objectifs de son établissement scolaire, et, à terme, aux dossiers d'accompagnement des élèves qui y sont scolarisés. Concrètement, cet espace recouvre les applications auxquelles ont accès les pouvoirs organisateurs et les directions d'écoles lorsqu'elles s'identifient dans CERBERE afin de transmettre ou traiter des données.
- Un espace destiné aux Fédérations de pouvoirs organisateurs qui permet d'assurer des échanges d'informations statistiques, ainsi qu'un accès aux informations relatives au pilotage/contrats d'objectifs avec le pouvoir régulateur, tel que prévu par le cadre juridique du nouveau pilotage. Ces informations permettent aux FPO de soutenir les établissements scolaires qui le souhaitent.
- Un espace destiné aux personnels de l'Enseignement qui permettra la communication, à l'ensemble du personnel, des informations administratives qui les concernent, de dossiers administratifs et tout document relatif à la gestion de la carrière. Cet espace personnel permettra également aux enseignants d'accéder aux dossiers d'accompagnement de leurs élèves.
- L'espace destiné aux parents et aux élèves qui assurera, à terme, la communication des informations administrative et scolaire de l'élève, celles contenues dans le dossier d'accompagnement de l'élève, mais aussi celles relatives aux certifications, aux diplômes, aux bourses et aux allocations d'études, aux équivalences et aux attestations de stages qui les concernent.

Seuls les espaces destinés aux Directions/PO, aux Fédérations de PO et aux membres des personnels sont visés par le décret.

Le projet d'arrêté de Gouvernement de la Communauté française exécute deux habilitations du gouvernement prévues par le décret gouvernance numérique du 25 avril 2019.

Le projet d'arrêté a ainsi pour vocation de préciser :

1. En vertu de son article 6, les données ou catégories de données à caractère personnel qui sont nécessaires au regard des finalités des espaces numériques visés à l'article 4, ainsi que les bases de données à caractère personnel qui sont nécessaires à l'exploitation des espaces.
2. En vertu de son article 11, les données ou catégories de données anonymisées ou à caractère personnel nécessaires à l'exécution des dispositions légales, décrétales ou réglementaires qui sont transmises par les services du Gouvernement aux écoles.

Le décret renvoie à d'autres habilitations du gouvernement en vue de préciser les modalités de son exécution. Ces dernières feront l'objet **de projets ultérieurs d'arrêté** du Gouvernement de la Communauté française et portent :

- en vertu de l'article 13§2, sur les cas où peuvent être communiquées à des tiers, les données communiquées à chaque Fédération de pouvoirs organisateurs et au pouvoir organisateur de l'enseignement organisé par la Communauté française, portant sur les informations nécessaires au soutien et à l'accompagnement du pilotage et servant exclusivement au suivi et à l'analyse de la qualité de l'enseignement dispensé dans les écoles relevant des pouvoirs organisateurs

affiliés ou conventionnés à la Fédération de pouvoirs organisateurs ou relevant du pouvoir organisateur de l'enseignement organisé par la Communauté française ;

- en vertu de l'article 14, sur la transmission de données par les services du Gouvernement vers les instances Bassins EFE existantes lorsque la communication de ces données numériques est nécessaire à l'exécution de leurs missions.

Les espaces numériques dont il est question dans le projet d'arrêté et qui sont définis par le décret gouvernance numérique ont des caractéristiques qu'ils convient de préciser.

En effet, **les espaces numériques sont des plateformes d'interface.**

Tout d'abord, au regard de la qualité des parties au regard du Règlement général européen relatif à la protection des données (RGPD), rappelons que les espaces numériques permettent la distinction entre les qualités de responsable de traitement et de sous-traitant en matière de traitement de données à caractère personnel dans le cadre des espaces.

En vertu de l'article 6 § 2 du décret gouvernance numérique, le Ministère de la Communauté française est, à ce titre, responsable du traitement au sens de l'article 4, 7), du RGPD pour les données à caractère personnel traitées au travers des espaces numériques mis à disposition de leurs destinataires. Dans ce cadre, les pouvoirs organisateurs sont alors considérés comme sous-traitants au sens de l'article 4, 8), du RGPD.

Dès lors, au regard de l'article 6 du décret gouvernance numérique, il appartient au Gouvernement, en sa qualité de responsable du traitement, de fixer la liste de données ou les catégories de données à caractère personnel qui font l'objet d'un traitement et qui sont nécessaires aux finalités poursuivies par les espaces numériques. Le Gouvernement identifie également les bases de données existantes créées en application de dispositions décrétales ou réglementaires et qui sont nécessaires à l'exploitation des espaces numériques.

Ensuite, au regard des traitements qui sont nécessaires par rapport aux finalités des espaces numériques visés à l'article 4, il convient de préciser la distinction entre 1) les traitements nécessaires à l'accès et la gestion des espaces numériques et 2) les traitements opérés par les applications auxquelles les espaces numériques donnent accès :

1) Les traitements nécessaires à l'accès et à la gestion des espaces numériques :

Ces traitements portent sur la collecte des données qui relèvent des catégories de données à caractère personnel d'identification, de communication et de navigation. Ces traitements sont les seuls traitements propres aux espaces numériques, qui sont de simples plateformes d'interface.

2) Les traitements opérés par les applications auxquelles les espaces numériques donnent accès :

Ces traitements sont spécifiques à des contextes applicatifs et sont régis par des dispositions décrétales ou réglementaires propres aux finalités de chaque application. Ils sortent du cadre du décret gouvernance numérique et du présent projet d'arrêté. Aucune nouvelle opération n'est réalisée via les espaces numériques et les données collectées dans le cadre des traitements opérés par les applications rendues accessibles via les espaces numériques restent hébergées dans leur contexte applicatif respectif.

En l'espèce, les traitements qui doivent être précisés par le projet d'arrêté conformément aux habilitations données par le Décret du 25 avril 2019, sont les traitements du premier groupe décrit.

Projet d'arrêté du Gouvernement de la Communauté française déterminant les catégories de données à caractère personnel faisant l'objet d'un traitement au regard des finalités des espaces numériques et définissant les catégories de données à transmettre par les services du Gouvernement aux écoles en application des articles 6 et 11 du décret du 25 avril 2019 portant sur la gouvernance numérique du système scolaire et à la transmission des données numériques dans l'enseignement obligatoire.

COMMENTAIRE DES ARTICLES

Article 1

L'article premier définit les termes nécessaires à la compréhension du projet d'arrêté.

Article 2

Définition des catégories de données et des données à caractère personnel

Pour rappel le projet d'arrêté et le traitement de données à caractère personnel explicité à l'article 2 ne concernent que l'accès aux espaces numériques et à leur gestion ; d'autres dispositions règlent les traitements opérés par les applications auxquelles les espaces numériques donnent accès.

L'article 2 fixe à une catégorie de données principales et à trois sous-catégories la liste des catégories de données à caractère personnel qui font l'objet d'un traitement et qui sont nécessaires au regard des finalités des espaces numériques visés à l'article 4. Pour chacune des sous-catégories l'article 2 définit les types de données à caractère personnel présentes dans ces catégories.

La catégorie de données à caractère personnel, prévue à l'article 6 § 1er, du décret gouvernance numérique et faisant l'objet d'un traitement en application d'une disposition légale, décréte ou réglementaire et qui est nécessaire au regard des finalités des espaces numériques est relative aux données d'identification/authentification.

L'identification doit être entendue comme le processus de collecte et de validation d'un ensemble d'attributs d'identité visant à identifier une personne physique dans un contexte particulier.

L'authentification doit être entendue comme le processus permettant de vérifier qu'un utilisateur est bien le propriétaire d'une identité numérique donnée lors de l'accès à un espace numérique ; l'utilisateur doit présenter des titres d'authentification qui seront validés dans le processus d'authentification.

Les données décrites ci-dessous sont demandées lors des procédures d'identification et d'authentification. Elles ne sont pas systématiquement traitées par le responsable de traitement : elles constituent le périmètre **maximal** des données collectées. Celui-ci détermine au cas par cas si la collecte de ces données est nécessaire au regard du niveau d'assurance à l'identification et du niveau d'assurance à l'authentification requis par les obligations du responsable de traitement.

Ce niveau est évalué en fonction de critères qui visent, à tout le moins, l'ampleur du traitement concerné, les risques pour les personnes concernées par le traitement ainsi que les mesures organisationnelles et techniques mises en place par le responsable de traitement.

Les données d'identification/authentification pures sont :

- numéro de Registre national ;
- numéro de matricule ;
- numéro de dossier unique ;
- identifiant en ligne ;
- nom et prénom ;
- genre ;
- nationalité ;
- état civil ;
- certificat d'authentification de l'eID ;

- lieu de naissance ;
- pays de naissance
- date de naissance ;
- adresse e-mail ;
- lien organisationnel ;
- fonction ;
- adresse professionnelle,
- adresse privée ;
- permissions.

Les données de communication sont :

- adresse postale ;
- informations de contact relatives à un moyen de communication ;
- adresse de courrier électronique ;
- contenu des communications relatives aux accès aux espaces numériques.

Les données de navigation et de traçabilité :

- l'adresse IP qui est attribuée lors de la connexion ;
- les dates de création et de modification du compte ;
- le lieu de connexion ;
- la date et l'heure d'accès ;
- les pages consultées et le type de navigateur (browser) utilisé ;
- la plate-forme et/ou le système d'exploitation installée sur le terminal de l'utilisateur ;
- le moteur de recherche ainsi que les mots-clés utilisés pour retrouver le site ;
- les fichiers téléchargés ;
- les informations collectées via les cookies ;
- les informations nécessaires afin d'assurer la sécurité des traitements relatifs aux accès aux espaces numériques, dès lors que ces données permettent de journaliser les accès et de prévoir les procédures de gestion d'éventuels incidents.

Les données à caractère personnel décrites ci-dessus se rapportent aux usagers des espaces numériques qui sont définis à l'article 1 du décret numérique de la façon suivante : les pouvoirs organisateurs, les directeurs, les Fédérations de pouvoirs organisateurs et les membres des personnels de l'enseignement. Dès lors les catégories de données personnelles concernant les élèves et leurs parents ne sont pas concernées par cet article, étant donné que les parents et les élèves ne figurent pas parmi les usagers ciblés par les espaces numériques.

Fondement légal et finalité du traitement

Le traitement des données à caractère personnel décrites ci-dessus trouve son fondement légal (licéité) en ce qu'il 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 et qui est décrite à l'article 4 du décret gouvernance numérique.

En effet les catégories de données et les données reprises ci-dessus sont nécessaires aux finalités décrites à l'article 4 du décret gouvernance numérique qui stipule notamment que :

Les espaces numériques visés au paragraphe 1^{er} poursuivent comme finalités générales de :

1. collecter et traiter des données et les rendre accessibles au sein des espaces visés aux paragraphes 3 à 5 ;
2. mettre aisément à disposition des usagers des documents administratifs ;
3. permettre aux usagers d'opérer des démarches administratives et d'en assurer le suivi en ligne ;

4. créer un canal de communication privilégié entre l'utilisateur et les services du Gouvernement en mettant à disposition des utilisateurs des documents officiels ;
5. améliorer la diffusion de l'information et l'accessibilité aux démarches administratives.

Le traitement de ces catégories de données sera réalisé dans le respect des principes décrits à l'article 5 du RGPD, dont notamment le principe de limitation des finalités et de minimisation des données. Cela implique que le traitement des catégories de données décrites à l'article 2 du projet d'arrêté sera strictement limité à ce qui est nécessaire pour répondre aux finalités décrites à l'article 4 du décret gouvernance.

Afin d'apporter toute clarté au sujet du fondement légal et des finalités relatives aux catégories de données à caractère personnel qui font l'objet d'un traitement et qui sont nécessaires au regard des finalités des espaces numériques visés à l'article 4, le projet d'arrêté de gouvernement apporte explicitement cette précision dans le texte de son article 2.

Durées de conservation des données

Le RGPD pose pour principe la limitation de la conservation des données à caractère personnel.

Les données décrites à l'article 2 du projet d'arrêté sont conservées de manière active dans un espace de stockage sécurisé tant que l'utilisateur de la plateforme y possède un compte actif.

Lorsqu'un compte est clôturé, les données prévues à l'article 2 sont conservées de manière passive pendant 6 mois dans un espace de stockage sécurisé.

Au terme du délai de 6 mois, seules les données qui sont nécessaires au respect des obligations légales du responsable du traitement en tant qu'autorité publique ou au regard de ses missions, sont archivées sans précisions de limitation de durée dans un espace de stockage sécurisé sans préjudice des réglementations qui s'appliqueraient notamment en matière d'archivage.

Par exception, les données relatives aux traces d'accès : date, heure, identifiant du compte, adresse IP, URL appelée, navigateur, OS sont conservées 5 ans à partir du moment où ces données ont été générées. Ce délai de 5 ans correspond au délai relatif dans l'applicatif « Cerbere ».

Les cookies ont également des durées de conservations qui leurs sont spécifiques.

Afin d'explicitier les éléments de mise en œuvre du présent principe du RGPD, le projet d'arrêté de gouvernement apporte cette précision à la fin de son l'article 2, comme suit :

« Les données à caractère personnel issues des catégories décrites au paragraphe 1, sont conservées de manière active dans un espace de stockage sécurisé tant que l'utilisateur de la plateforme y possède un compte actif.

Lorsqu'un compte n'est plus actif, les données sont conservées de manière passive dans un espace de stockage sécurisé et ce afin de respecter les obligations légales en vigueur et d'assurer les besoins du métier. »

Article 3

L'article 3 définit les bases de données nécessaires aux finalités des espaces numériques visés par le décret, à savoir les espaces destinés aux Directions/PO, aux Fédérations de PO et aux membres des personnels de l'enseignement.

Afin de garantir le bon fonctionnement des espaces décrits et des applicatifs/actifs de données auxquels ces derniers donnent accès, l'ETNIC a mis en place, dans le cadre de ses missions et de son rôle de sous-traitant, l'infrastructure dénommée « CERBERE » qui assure la sécurisation, notamment par l'identification des utilisateurs, de l'écosystème informatique du Ministère de la Fédération Wallonie-Bruxelles (MFWB). En vertu de l'article 3, § 1, 1a), du Décret relatif à l'Entreprise publique des Technologies Numériques de l'Information et de la Communication de la Communauté française (ETNIC) du 16 novembre 2018, l'ETNIC est en charge du développement, de la maintenance, de

l'hébergement et/ou de l'exploitation d'applications existantes ou à développer pour les services de la FWB. C'est dans ce cadre que l'infrastructure IAM dite « CERBERE » a été mise en place.

Les données d'identification récoltées au travers des espaces numériques alimentent donc la base de données dite « CERBERE » afin de garantir l'identification et l'authentification, selon le niveau d'assurance jugé nécessaire par le Ministère, et ce sans équivoque quant à l'identité de l'utilisateur.

Dans le cadre de l'infrastructure « CERBERE » et la création des comptes relatifs, la collecte de données personnelles d'identification et d'authentification vise notamment à permettre la réalisation de contrôles lorsque des données sont manquantes, c'est le cas notamment des données relatives à l'adresse privée et l'état civil. Cependant, ces données ne sont pas systématiquement traitées par le Ministère de la Communauté Française dans le cadre des finalités décrites à l'article 4 du décret gouvernance numérique. Celui-ci détermine au cas par cas si la collecte de ces données est nécessaire au regard du niveau d'assurance à l'identification et du niveau d'assurance à l'authentification requis par les obligations du responsable de traitement.

Ce niveau est évalué en fonction de critères qui vise, à tout le moins, l'ampleur du traitement concerné, les risques pour les personnes concernées par le traitement ainsi que les mesures organisationnelles et techniques mises en place par le Ministère de la Communauté française en tant que responsable de traitement au sens du RGPD.

Cette identification passe également, par la désignation par les pouvoirs organisateurs et Fédérations de pouvoirs organisateurs, des personnes placées sous leur autorité dûment habilitées à accéder aux espaces et applications en leur nom. Le terme « autorité » a une signification générale et ne se limite pas à l'autorité hiérarchique établie par une relation de travail. Cette désignation nécessite la transmission, d'une part, des données d'identification du demandeur, à savoir en l'espèce l'utilisateur, le responsable PO ou toute personne agissant en son nom (le directeur d'établissement, par exemple) et, d'autre part, des données d'identification du bénéficiaire, à savoir, en l'espèce, l'utilisateur qui agira au nom du PO dans ses interactions avec le MFWB. Ces données servent à alimenter le processus et la base de données permettant de réguler l'accès aux différents espaces.

La gestion des espaces numériques visés par le décret gouvernance numérique nécessite la récolte des données de communication qui alimentent les bases de données qui les supportent, afin de permettre la transmission des informations d'identification à l'utilisateur. Ces données de communication servent également à notifier l'utilisateur de tout changement en lien avec son compte ou avec ses démarches. Les données de communication peuvent être éditées à tout moment par l'utilisateur soit en se connectant à son espace soit en passant par l'outil d'édition de comptes « CERBERE ».

La gestion des espaces numériques visés par le décret gouvernance numérique nécessite également la récolte des données de navigation et de traçabilité.

Ces informations permettent à l'ETNIC :

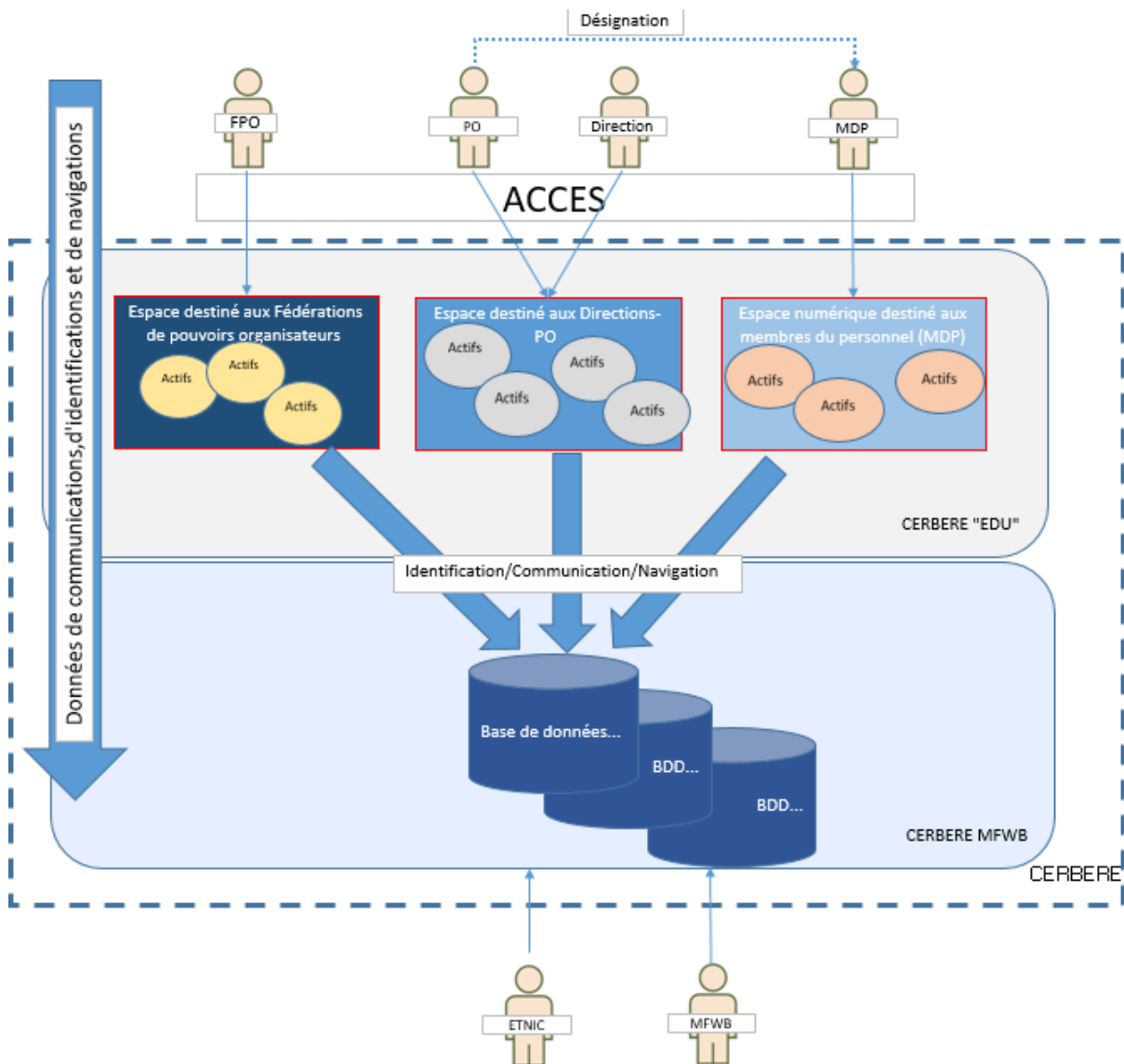
- d'assurer le support à l'usager et l'évaluation de l'accessibilité et la diffusion de l'information présente dans les espaces numériques en conformité avec les finalités décrites à l'article 4 du décret gouvernance et, si nécessaire, d'ajuster le service offert ;
- d'assurer la sécurité des traitements relatifs aux accès aux espaces numériques, dès lors que ces données permettent de journaliser les accès et de prévoir les procédures de gestion d'éventuels incidents afin de pouvoir réagir en cas, par exemple, de violation de données.

Ces informations permettent aux usagers :

- d'avoir un suivi de leurs démarches dans les espaces.

L'ensemble des bases de données identifiées dans le cadre de la gestion des espaces numériques et de leur utilisation est sécurisé par l'infrastructure « CERBERE ». Leur accès est limité aux personnes travaillant au sein du MFWB et de son sous-traitant l'ETNIC qui y accède afin de permettre leur gestion et leur maintenance. Les accès sont personnels, soumis au respect du principe de proportionnalité et accessibles uniquement aux fins de répondre aux finalités exposées dans le présent décret et dans toute autre disposition légale.

La figure ci-dessous schématise les processus fonctionnels en lien avec les bases de données se rapportant aux catégories de données à caractère personnel mentionnées à l'article 2 du présent projet d'arrêté.



Afin d'explicitier les processus fonctionnels en lien avec les bases de données se rapportant aux catégories de données à caractère personnel mentionnées à l'article 2 du présent projet d'arrêté, le projet d'arrêté de gouvernement propose l'article 3 suivant :

Les bases de données nécessaires à l'exploitation des espaces numériques prévus à l'article 4, § 1er, du décret gouvernance numérique, sont les bases de données suivantes du Ministère de la Communauté française :

1. les bases de données créées en application de dispositions décrétales ou réglementaires ;

2. les bases de données créées sur la base des informations fournies par les pouvoirs organisateurs ou Fédérations de pouvoirs organisateurs afin de désigner les personnes physiques placées sous leur autorité qui sont dûment habilitées à accéder en leur nom à l'espace numérique, conformément à l'article 4 § 1^{er}, du décret gouvernance numérique ;
3. les bases de données créées sur base des données de communication et de navigation obtenues dans le cadre de l'exploitation des espaces numériques prévus à l'article 4, § 1^{er}, du décret gouvernance numérique.

Le choix de ne pas citer nominativement les bases de données dans le projet d'arrêté résulte du caractère évolutif des espaces numériques et du besoin de disposer d'une formulation de l'arrêté du Gouvernement de la Communauté française qui rende possible l'absorption de l'évolution des espaces numériques.

Article 4

L'article définit les données ou catégories de données anonymisées ou à caractère personnel nécessaires à l'exécution des dispositions légales, décrétales ou réglementaires qui sont transmises par les services du Gouvernement aux écoles organisées ou subventionnées au moyen de l'espace numérique visé à l'article 4, § 1^{er}, 1^o.

L'article 4 porte donc exclusivement sur la transmission par les services du Gouvernement de données ou catégories de données au travers de l'espace numérique destiné aux écoles.

Ainsi, les données ou catégories de données listées, accessibles depuis l'espace numérique destiné aux écoles, peuvent être des données à caractère personnel ou non.

Les seules données à caractère personnel auxquelles l'article 4 fait référence, sont celles qui relèvent des catégories de données d'identification, de communication et de navigation décrites à l'article 2 de l'arrêté.

Les autres catégories de données proviennent de la série d'indicateurs transmise à chaque école en vue d'établir leur diagnostic, conformément à l'article 3 de l'arrêté du Gouvernement de la Communauté française du 24 octobre 2018 portant application de l'article 67, §§ 2 à 6, du décret du 24 juillet 1997 définissant les missions prioritaires de l'enseignement fondamental et de l'enseignement secondaire et organisant les structures propres à les atteindre. Ledit article définit ces indicateurs rassemblés en cinq rubriques dans lesquelles les données qui s'y retrouvent sont les suivantes :

- données relatives à la structure, l'encadrement et la population scolaire, reprenant les éléments tant quantitatifs que qualitatifs décrivant la structure, l'encadrement et la population scolaire de l'école ;
- variables relatives aux apprentissages, reprenant l'ensemble de variables prenant en compte les caractéristiques liées aux savoirs et compétences de l'élève et aux certifications obtenues ;
- variables relatives au climat d'école, prenant en compte des caractéristiques liées au climat de l'école ;
- variables relatives à la dynamique collective, reprenant l'ensemble de variables prenant en compte les caractéristiques liées aux personnels de l'école ;
- variables relatives au parcours des élèves, reprenant l'ensemble de variables prenant en compte les caractéristiques liées aux trajectoires temporelles des élèves dans leur parcours scolaire.

Ces données sont des indicateurs et donc, par définition, des données statistiques informant sur l'état ou l'évolution au cours du temps d'un phénomène jugé important. En éducation, le recueil d'indicateurs vise à informer sur la santé et la qualité du système éducatif. Ces données ne sont pas des données à caractère personnel et les traitements de données, ayant amené à la collecte des données personnelles à l'origine

des indicateurs et la création de ceux-ci, sont encadrés par d'autres dispositions légales, décrétales ou réglementaires, dont notamment :

- la loi du 29 juin 1983 concernant l'obligation scolaire ;
- le code de l'enseignement fondamental et de l'enseignement secondaire du 3 mai 2019 ;
- le décret du 24 juillet 1997 définissant les missions prioritaires de l'enseignement fondamental et de l'enseignement secondaire et organisant les structures propres à les atteindre ;
- le décret du 27 mars 2002 relatif au pilotage du système éducatif de la Communauté française ;
- le décret du 21 novembre 2013 organisant divers dispositifs scolaires favorisant le bien-être des jeunes à l'école, l'accrochage scolaire, la prévention de la violence à l'école et l'accompagnement des démarches d'orientation scolaire ;
- l'arrêté Royal relatif à l'organisation de l'enseignement secondaire du 29 juin 1984 ;
- l'arrêté du Gouvernement de la Communauté française relatif aux attestations, rapports, certificats et brevets délivrés au cours des études secondaires de plein exercice du 11 mai 2016 ;
- l'arrêté du Gouvernement de la Communauté française fixant les modèles des attestations et certificats sanctionnant les études dans l'enseignement secondaire en alternance du 11 mai 2016 ;
- l'arrêté du Gouvernement de la Communauté française du 29 octobre 2018 portant application de l'article 67, §§ 2 à 6, du décret du 24 juillet 1997 définissant les missions prioritaires de l'enseignement fondamental et de l'enseignement secondaire et organisant les structures propres à les atteindre ;
- l'arrêté royal du 20 août 1957 portant coordination des lois sur l'enseignement primaire ;
- Etc.

Observations complémentaires relatives à la sécurité juridique des échanges de données à caractère personnel

L'article 8 du décret gouvernance numérique balise, par ailleurs, le cadre de sécurité des échanges de données à caractère personnel relatifs aux espaces numériques visés par le décret en se référant aux politiques de sécurité des services du Ministère de la Communauté française.

Les traitements de données concernés par le décret gouvernance numérique, et les projets d'arrêtés du Gouvernement de la Communauté française en exécution dudit décret, s'inscrivent dès lors dans le cadre plus général de la mise en conformité avec les prescrits du RGPD de l'ensemble des services du Ministère de la Communauté française.

Parmi les mesures d'ensemble mises en place à l'échelle du Ministère de la communauté française en matière de protection des données, citons :

- la mise en place de principes et/ou de procédures spécifiques en matière de sécurité des données, notamment en application des articles 7 et 8 du décret du 25 octobre 2018 relatif au cadre de gouvernance de la politique du numérique et de l'informatique en Communauté française ;
- l'identification des traitements et l'établissement du registre des traitements du Ministère de la Communauté française ;
- la réalisation des analyses d'impact RGPD et des analyses de risques sécurité nécessaires, sur la base des analyses préalables et des recommandations des relais RGPD et du Délégué à la Protection des Données (DPD) ;

- la mise en place des documents légaux nécessaires à la conformité des traitements, tels que les contrats de sous-traitances, les notices vie privée, etc. En ce qui concerne les traitements concernés par les espaces numériques, une notice reprenant l'ensemble des informations reprises aux articles 13 et 14 du RGPD sera disponible au niveau de chacun des espaces ;
- l'implémentation de procédures relatives à la prise en charge des incidents de sécurité et des demandes des personnes concernées quant à l'exercice de leurs droits.