MINISTÈRE
DE L'ÉDUCATION
NATIONALE
Liberté
Égalité
Fraternité

Direction générale
de l'enseignement
scolaire

Cahier des charges

Nom de l'application

Application : Nom de l'application Version de référence : Date de livraison souhaitée :

Demandeur : Prénom Nom – DGESCO XX-X Demande stabilisée par la MOA : OUI/NON

Description synthétisée du besoin

Analyse de la valeur (en référence aux grilles de valeur de la feuille de route SI)
Valeur Métier (MOA) : Valeur pour le SI (MOE) :

Acteurs
MOA : MOE :

Historique

Version	Date	Objet	Auteur	Validation
v 1.00		Initialisation		
v 1.01		Rédaction		
v 1.02		Modifications suite au comité utilisateurs		
v 1.03		Rédaction		
v 2.00		Finalisation		
v 3.00				
v 3.01				

Table des matières

1. Présentation du projet 4
   1.1 Le contexte 4
   1.2 Les enjeux et objectifs du projet 4
   1.3 Le périmètre du projet 4
   1.4 Les chiffres clés 4
   1.5 Le calendrier du projet 4
2. Processus metier 4
   2.1 Processus A 4
   2.2 Processus B 4
   2.3 Processus C 4
   2.4 Processus N 4
3. Expression du besoin 4
   3.1 Les fonctionnalités 4
   3.2 L'ergonomie 5
4. Conditions d'utilisation 6
   4.1 Droits d'accès 6
   4.2 Sauvegarde et archivage 6
   4.3 Qualité de service 6
5. Reprise de l'existant 6
   5.1 Données 7
   5.2 Calendrier 7
6. Conduite du changement 7
   6.1 Périmètre 7
   6.2 Besoins de communication 7
   6.3 Besoins de formation 7
   6.4 Ressources d'accompagnement à produire 7
7. Annexes 7
   7.1 Glossaire 7
   7.2 Documents de références 7
   7.3 Protection des données (RGPD) 7

1. PRESENTATION DU PROJET

1.1 Le contexte

1.2 Les enjeux et objectifs

1.3 Le périmètre

1.4 Les chiffres clés

- *Chiffres du métier (ex. : N bourses traitées annuellement)*
- *Nombre d'utilisateurs*

1.5 Le calendrier

2. PROCESSUS METIER

Ce chapitre vise à décrire le métier sous forme de diagramme (ou d'un tableau) compréhensible par un acteur métier, indépendamment de toute informatique.

Autant de parties "Nom du processus" que de processus métiers à outiller ou à mieux outiller *(répondre aux questions : qui fait quoi ? à quel moment ? dans quel but ? quels sont les éléments d'entrée ? quels sont les éléments de sortie ?).*

La description porte sur la cible et non sur l'existant.

2.1 Processus A

2.2 Processus B

2.3 Processus C

….

2.4 Processus N

Une matrice des flux peut utilement compléter ce chapitre pour matérialiser l'information qui circule dans et en dehors des processus identifiés.

3. EXPRESSION DU BESOIN

3.1 Les fonctionnalités

Le niveau de détail de ce chapitre dépend de la maturité du projet.

Chaque fonctionnalité identifiée donnera lieu à un sous-chapitre comportant :

- *la description du service à rendre ;*

- *l'évènement déclencheur (le terme d'une échéance, la réception d'un flux de données, une action utilisateur, etc.) ;*
- *les données nécessaires en entrée, tout en veillant à ne pas traiter plus de données que nécessaires (principe de minimisation des données exigé par le RGPD), car cela augmente inutilement l'exposition de données personnelles et le risque de violation de données. Lorsque les données d'entrée proviennent d'une autre application du MEN ou bien d'une autre administration, ou encore d'un logiciel externe, le préciser (flux entrants) ;*
- *les règles de gestion métier qui s'appliquent ;*
- *les données produites en sortie. Préciser si elles doivent être transmises à des applications, et s'il s'agit d'applications tierces internes ou externes au MEN (flux sortants).*

Au-delà des fonctionnalités métier, il convient de décrire celles directement liées aux obligations du règlement général à RGPD (voir annexe chapitre 7.3 pour en savoir plus), afin de couvrir :

- *l'information des personnes concernées par le traitement de données personnelles (prévoir l'édition de mentions informatives ou leur affichage dans le cas d'un service en ligne) ;*
- *l'exercice des droits des personnes concernées :*
  - *le droit d'accès (prévoir l''édition d'un relevé des données traitées concernant un élève, un responsable de l'élève, un agent, etc.) ;*
  - *le droit de rectification de données inexactes (qui peut modifier, quelles données, via quels écrans, avec quelle traçabilité) ;*
  - *le droit à la limitation du traitement (empêcher temporairement tout traitement ou réutilisation des données concernées) ;*
  - *le droit d'opposition (identifier la base légale de chaque traitement et permettre de désactiver le traitement contesté, sans affecter les traitements relevant de l'obligation légale).*

3.2 L'ergonomie

Description des parcours utilisateurs et des écrans types en référence à une charte d'ergonomie (Design System de l'Etat – DSFR – pour les services en ligne, ou un équivalent pour les applications de gestion – charte Siecle Intégré, DSMEN – en cours d'élaboration).

La présence de champs libres doit être limitée au strict nécessaire, au profit de listes déroulantes et cases à cocher.

En effet, les champs libres ouvrent la porte à la collecte non maîtrisée de données, y compris sensibles (art. 9) ou excessives, en contradiction avec la minimisation (art. 5, paragraphe 1, c). Les valeurs prédéfinies limitent les risques d'abus et facilitent la maîtrise des catégories de données traitées. Lorsque des champs libres sont indispensables, un message d'information ou d'avertissement doit rappeler ce qu'il est possible d'y saisir (et ce qu'il ne faut pas saisir).

La sensibilisation des utilisateurs fait partie des mesures organisationnelles pour garantir un traitement conforme (art. 24 et 32). Un message contextuel permet de réduire le risque de saisie de données non pertinentes, sensibles ou portant atteinte aux droits et libertés des personnes.

Des contrôles doivent être mis en place pour limiter les abus (longueur maximale, filtrage de certains contenus, revue régulière du contenu saisi, etc.) ?

Ce chapitre peut être utilement complétée par des maquettes d'écran à valeur illustrative (dans un document annexe, le cas échéant), de même que par une cartographie des documents édités (bilan, relevés, courriers, exports PDF, etc.).

Les documents édités sont un vecteur majeur de diffusion des données. Ils doivent respecter les mêmes principes de minimisation et de finalité (art. 5, paragraphe 1, b et c). Une cartographie des éditions peut aider à repérer celles contenant des données excessives, ou inadaptées à leur destinataire. Des mesures techniques doivent limiter le risque de fuite via ces documents (format non modifiable, masquage de données sensibles, messages d'avertissement avant impression ou téléchargement, etc.) ? L'article 32 impose des mesures de sécurité appropriées, y compris pour les supports de sortie (PDF, impressions). Une édition peut être facilement diffusée à des tiers non autorisés, ce qui génère des violations de données (art. 33 et 34).

4. CONDITIONS D'UTILISATION

4.1 Droits d'accès

Recensement des différents profils utilisateurs afin de limiter l'accès des fonctionnalités et des données aux seules personnes légitimes au titre de leurs missions.

Pour chacun des profils utilisateurs identifié, liste des fonctionnalités susceptibles d'être mobilisées au titre de l'activité, description du périmètre de gestion ou d'exercice (nature d'établissement ou liste d'établissements scolaires, département, académie, national, etc.) et précision de la profondeur de l'historique accessible.

Des habilitations mal conçues peuvent conduire à des accès trop larges, contraires aux principes de confidentialité et de sécurité.

4.2 Sauvegarde et archivage

La conservation des données doit être limitée à ce qui est strictement nécessaire en gestion.

Afin de garantir cette limitation de la conservation des données, des mécanismes de purge (suppression des données) et/ou d'archivage (versement de données qui n'ont plus d'utilité en gestion dans des archives intermédiaires) sont à prévoir.

4.3 Qualité de service

Exigences en termes de performance (temps de réponse acceptable en seconde, temps de traitement en différé/ mise en file d'attente acceptable ou pas avec information de l'utilisateur lorsque sa demande a abouti, invitation de l'utilisateur à se déconnecter en cas dégradation du service, etc.) et de disponibilité de l'application (précision du délai de remise en service en cas d'indisponibilité de l'application, affichage d'un message à l'utilisateur lui indiquant sous quel délai l'application sera à nouveau opérationnelle, etc.).

5. REPRISE DE L'EXISTANT

En fonction de l'application, cette partie peut faire l'objet d'un cahier des charges à part entière.

5.1 Données

Liste des données reprises, l'application source ainsi que les règles de gestion de la migration des données de l'application d'origine à l'application cible (existante ou à développer).

5.2 Calendrier

Calendrier de la reprise des données, veiller à la cohérence avec le calendrier de gestion des processus métier

6. CONDUITE DU CHANGEMENT

6.1 Périmètre

Couverture de tout ou partie du projet ?

6.2 Besoins de communication

Publics cibles, calendrier, canal de communication, format de la communication

6.3 Besoins de formation

Publics cibles, calendrier, modalités (en autonomie ou pas), etc.

6.4 Ressources d'accompagnement à produire

Liste des ressources envisagées et précision du format attendu pour chacune.

7. ANNEXES

7.1 Glossaire

7.2 Documents de références

Textes réglementaires notamment

7.3 Protection des données (RGPD)

L'article 25 du RGPD impose de prendre en compte, dès la conception de l'application les obligations du règlement général relatif à la protection des données.

Le principe de minimisation des données

La liste des données collectées a-t-elle été revue pour vérifier que chaque champ est « adéquat, pertinent et limité à ce qui est nécessaire » au regard des finalités ?

Le principe de minimisation est un des principes de base du RGPD (art. 5, paragraphe 1, c). Collecter plus de données que nécessaire augmente inutilement les risques de violation de données.

Des profils d'habilitation sont-ils définis pour limiter l'accès aux seules personnes qui ont « besoin d'en connaître » (par fonction, établissement, type de données) ?

La minimisation ne concerne pas que la collecte, mais aussi l'accès. Seules les personnes autorisées à en connaître dans le cadre de leurs missions doivent pouvoir gérer les données ou pouvoir y accéder (art. 5, paragraphe 1, c, et art. 32 sur la sécurité). Des habilitations mal conçues peuvent conduire à des accès trop larges, contraires aux principes de confidentialité et de sécurité (art. 32).

Le périmètre de visibilité a-t-il été réfléchi (données visibles selon le profil ; profondeur historique accessible, …) ?

La conservation et l'accès doivent être limités à ce qui est strictement nécessaire (art. 5, paragraphe 1, c et e). Permettre l'accès illimité à tout l'historique, alors que seuls les événements récents sont utiles, est contraire à la minimisation et à la limitation de conservation.

L'information des personnes dont les données personnelles sont traitées

Le principe de transparence impose d'informer les personnes de manière claire, complète et accessible, au moment où leurs données sont collectées. En effet, c'est une obligation centrale du RGPD mentionnée aux articles 12 à 14 (modalités de l'information, contenu minimal des mentions, collecte directe / indirecte). En pratique, si l'application ne permet pas de produire ou d'afficher ces mentions, le responsable de traitement se retrouve en difficulté pour respecter ses obligations.

L'information ne doit pas être cachée ou difficile à trouver. Le RGPD insiste sur le caractère « aisément accessible » et « compréhensible » de l'information (articles 12 et 13). Retenez bien que l'ergonomie de l'application conditionne la conformité. Si l'information est peu visible, l'obligation de transparence n'est pas remplie en pratique.

Dans le cas d'un service en ligne, ces mentions doivent être facilement accessibles depuis l'interface (lien « Protection des données », ou encore « Vie privée », notamment sur les espaces familles/élèves par exemple).

En cas de collecte indirecte, l'article 14 exige une information spécifique sur la source des données. Les personnes doivent comprendre qui collecte, à quel moment, et pour quelles finalités (art. 13 et 14). Pour ces collectes indirectes, la documentation et/ou l'interface renvoient-elles vers les bonnes mentions d'information de l'application source ?

En cas de réutilisation de données, il faut vérifier que la nouvelle finalité est compatible avec la finalité pour laquelle les données ont été collectées (art. 5, paragraphe 1, b et art. 6, paragraphe 4). Un renvoi clair aux mentions de l'application d'origine évite les ruptures de transparence.

L'exercice des droits des personnes concernées

Un mécanisme existe-t-il pour s'assurer que l'exercice des droits n'est pas empêché par les choix de conception (comme des données non exportables, une absence de journalisation, ou autre) ?

Le droit d'accès (art. 15) impose au responsable de traitement de fournir une copie des données. Sans fonctionnalité d'extraction ou d'édition, répondre aux demandes devient matériellement très difficile, voire impossible dans les délais (un mois, art. 12), ce qui expose le responsable de traitement (RT) à un risque de non-conformité.

L'outil propose-t-il une fonctionnalité permettant d'extraire ou d'éditer facilement un relevé des données qui y sont traitées concernant un élève ou une famille (par exemple, édition « Bilan des données ») pour répondre au droit d'accès ?

Le droit de rectification (art. 16) impose que les données inexactes soient corrigées. Si l'application ne permet la modification de ces données, le RT ne peut pas respecter ce droit. La

différence « scolarisé / plus scolarisé » renvoie aussi aux règles de conservation (art. 5, paragraphe 1, e) et à la gestion des archives. Une fois en archives intermédiaires, la rectification doit être encadrée mais possible, ou compensée par des mécanismes adaptés.

En conséquence, la rectification des données doit être possible lorsque l'élève est scolarisé et lorsqu'il ne l'est plus (données archivées, profils restreints, etc.).

Le droit à la limitation (art. 18) permet à la personne concernée d'obtenir que ses données personnelles soient conservées mais non traitées activement, le temps du traitement d'une contestation par exemple. Pendant la période de limitation, l'application doit suspendre toute modification, transmission ou réutilisation des données de la personne concernée, tout en en conservant leur traçabilité. A l'issue de cette période, l'application doit permettre la levée de la restriction.

Le droit d'opposition (art. 21) permet à toute personne concernée de s'opposer, à tout moment, à un traitement de ses données personnelles, pour des raisons tenant à sa situation particulière. L'exercice de ce droit dépend de la base légale du traitement retenue au sens de l'article 6, paragraphe 1 du RGPD. La base légale s'apprécie pour chaque finalité de l'application (elle peut en effet différer d'une finalité à l'autre) et vaut pour l'ensemble des traitements attachés à la finalité. L'application doit tenir compte du régime d'opposition qui découle de la base légale.

Lorsque celle-ci relève :

- du consentement (art. 6, paragraphe 1, a) : le droit d'opposition ne s'applique pas en tant que tel ; toutefois, la personne concernée dispose du droit de retirer son consentement à tout moment (art. 7, paragraphe 3), avec *in fine* un effet équivalent à celui d'une opposition accordée. L'application doit donc permettre le retrait du consentement et prévoir en conséquence l'arrêt de tout traitement des données attaché à la finalité ;
- de l'obligation légale (art. 6, paragraphe 1, c) : le droit d'opposition ne s'applique pas ;
- de la mission d'intérêt public (art. 6, paragraphe 1, e) : le droit d'opposition s'applique. La personne peut s'opposer « pour des raisons tenant à sa situation particulière », mais le responsable de traitement peut poursuivre le traitement s'il démontre des motifs légitimes et impérieux qui prévalent sur les intérêts, droits et libertés de la personne, ou si le traitement est nécessaire à la constatation, l'exercice ou la défense de droits en justice ;
- de l'intérêt légitime (art. 6, paragraphe 1, f) : même régime que pour la mission d'intérêt public : opposition possible « pour des raisons tenant à sa situation particulière », sauf motifs légitimes et impérieux démontrés par le responsable de traitement, ou nécessité liée à un contentieux.

L'application doit permettre de prendre en compte l'exercice du droit d'opposition par une personne concernée en désactivant, pour celle-ci, les traitements (ou fonctionnalités) pour lesquels le droit d'opposition s'applique, sans impacter les autres traitements.

La conservation des données/archives

Des durées de conservation sont-elles définies pour chaque catégorie de données et intégrées au paramétrage applicatif ?

L'article 5 du RGPD, paragraphe 1, e prévoit que les données ne doivent pas être conservées sous une forme permettant l'identification au-delà de ce qui est nécessaire. Sans durée définie ni paramétrage correspondant, le ministère risque de conserver indéfiniment des données, en contradiction avec le principe de limitation de la conservation.

Un mécanisme de purge ou d'archivage est-il prévu (versement en archives intermédiaires, purge définitive, anonymisation/ pseudonymisation, journalisation des opérations) ?

La simple « décision » de limiter la conservation ne suffit pas, il faut des mesures techniques effectives (art. 24 et 25). Les mécanismes de purge/archivage participent au respect du principe de minimisation et de limitation de conservation (art. 5, paragraphe 1, c et e) et à la sécurité (art. 32).

Le sort des données à l'expiration de la durée d'utilité en gestion (suppression, anonymisation, transfert vers archives) est-il documenté avec la fiche de registre et, le cas échéant, l'AIPD ?

La fiche de registre (art. 30) et l'AIPD (art. 35) doivent refléter la réalité opérationnelle. Si l'application ne respecte pas ce qui est prévu dans ces documents, le RT ne peut pas démontrer sa conformité (art. 5, paragraphe 2, et 24).