



**MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE**

*Liberté
Égalité
Fraternité*

OUTILS D'AIDE A LA DECISION PARCOURSUP

**Analyse d'impact relative à la protection des
données :**

Outil d'aide à la sélection des candidats IFSI





Analyse d'impact relative à la protection des données

Suivi du document	Référence	Auteur	Validation	Date de validation
	REF : 5706.1	Julien Bracq Sabine Robardet	Sabine Robardet	
	Blue médi IFSI			

Sommaire

1.	Contexte	4
1.1.	Contexte général	4
1.2.	L'outil d'aide à la décision dans la procédure Parcoursup	4
1.3.	Vue d'ensemble.....	8
1.3.1.	Traitement considéré	8
1.3.2.	Textes applicables	9
1.4.	Données, processus et supports	10
1.4.1.	Description des données	10
1.4.2.	Description des destinataires	11
1.4.3.	Description de la durée de conservation	12
1.5.	Identification des actifs sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier)	12
2.	Principes fondamentaux.....	12
2.1.	Mesures garantissant la proportionnalité et la nécessité du traitement	12
2.1.1.	Finalités	13
2.1.2.	Fondement	13
2.1.3.	Minimisation des données	Erreur ! Signet non défini.
2.1.4.	Qualité des données.....	25
2.1.5.	Durées de conservation.....	25
2.1.6.	Evaluation des mesures.....	26
2.2.	Évaluation des mesures protectrices des droits des personnes concernées.....	26
2.2.1.	Mesures pour l'information des personnes	26
2.2.2.	Mesures pour les droits d'accès et de rectification	27
2.2.3.	Mesures pour la sous-traitance.....	27
2.2.4.	Evaluation des mesures.....	28
3.	Etude des risques liés à la sécurité des données	28
3.1.	Évaluation des mesures.....	28



3.1.1.	Mesures contribuant à traiter des risques liés à la sécurité des données	29
3.1.2.	Mesures générales de sécurité.....	29
3.1.3.	Mesures organisationnelles (gouvernance)	31
3.2.	Appréciation des risques : les atteintes potentielles aux droits et libertés	33
3.2.1.	Echelle de gravité	34
3.2.2.	Echelle de vraisemblance	34
3.2.3.	Analyse, estimation des risques par sources et description des mesures	36
4.	Validation de l'analyse d'impact	41
4.1.	Éléments utiles à la validation.....	41
4.1.1.	Synthèse relative à la conformité au RGPD.....	41
4.1.2.	Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données.....	41
4.1.3.	Cartographie des risques liés à la sécurité des données.....	42
4.1.4.	Plan d'action.....	42
4.2.	Validation formelle.....	42
5.	Annexes	42
5.1.	Présentation de l'écosystème numérique local et des échanges d'information avec le SI Parcoursup	43
5.2.	Convention de sous-traitance	44
5.3.	Etapes juridiques du déploiement de Parcoursup	45
5.4.	Liste des principales mesures de sécurité pouvant être prises.....	46



1. Contexte

1.1. Contexte général

Dans l'objectif de favoriser la réussite des étudiants dans les formations post-baccalauréat et apporter une réponse structurelle et durable au taux d'échec particulièrement élevé des étudiants au cours du premier cycle de l'enseignement supérieur, l'article 1^{er} de la loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants (dite loi ORE) a modifié l'article L. 612-3 du code de l'éducation qui fixe les modalités d'accès aux formations initiales du premier cycle de l'enseignement supérieur.

Cet article prévoit que toute demande d'admission dans une formation du premier cycle de l'enseignement supérieur dispensée par un établissement public se fait via une procédure nationale de préinscription. A cette fin, la plateforme numérique Parcoursup¹ a été créée par le ministère de l'enseignement supérieur, de la recherche et de l'innovation (MESRI)².

Cette plateforme permet aux candidats, d'une part, de constituer un dossier et de formuler leurs vœux et, d'autre part, de consulter l'offre de formation du premier cycle de l'enseignement supérieur et les données afférentes à chaque formation intégrée à Parcoursup (caractéristiques, capacités d'accueil, attendus, critères, données en termes de réussite, de tension et d'insertion le cas échéant).

Les informations enregistrées dans Parcoursup sont celles issues des différents fichiers de gestion scolaire ainsi que celles transmises par les candidats eux-mêmes voire, pour les lycéens et étudiants en recherche d'une réorientation, par les personnels des établissements du second degré d'enseignement dans lequel ils sont scolarisés.

Ces informations sont accessibles aux établissements d'enseignement supérieur auprès desquels les candidats ont formulé une demande. C'est au regard de ces informations ainsi que des attendus et critères qu'ils ont préalablement établis que les établissements d'enseignement supérieur renseignent sur la plateforme une décision sur la candidature.

Parcoursup permet également l'application des « quotas » que les recteurs peuvent introduire (candidats boursiers, candidats de l'académie), conformément aux dispositions de l'article L. 612-3 du code de l'éducation nationale.

Enfin, la plateforme permet la gestion des réponses des candidats aux propositions d'admission formulées par les établissements d'enseignement supérieur.³

1.2. L'outil d'aide à la décision dans la procédure Parcoursup

L'inscription dans un établissement (ou dans une formation) peut être subordonnée :

- à l'acceptation par le candidat d'un dispositif d'accompagnement pédagogique ou à un parcours de formation spécialisée⁴. Il est tenu compte, à cette fin, des aménagements et des adaptations dont bénéficient les candidats en situation de handicap ;

¹ Plateforme Parcoursup qui a succédé à Admission-Post-bac – APB – en vigueur jusqu'à la rentrée universitaire 2017 incluse

² Le MESRI est responsable de traitement au sens du règlement général sur la protection des données (RGPD)

³ Les modalités par lesquelles l'algorithme national Parcoursup effectue ces opérations sont détaillées dans un [document synthétique rendu public et accessible](#) en ligne.

⁴ Article L. 612-3 du code de l'éducation



- au respect, pour certaines formations, des modalités fixés par le ministre chargé de l'enseignement supérieur⁵ ;
- à la capacité d'accueil d'une formation⁶ .

Dans ce dernier cas, la décision doit tenir compte des caractéristiques de la formation, de la cohérence du projet du candidat et de ses acquis et compétences.

- **« Obligations relatives aux traitements de données destinés à l'ordonnement des candidatures »**

A cet effet, les établissements réunissent, pour chaque formation ayant enregistré des vœux, **une commission d'examen des vœux** dont la composition est arrêtée par le chef d'établissement. Cette commission définit, dans le respect des informations générales portées à la connaissance des candidats dès l'ouverture de la procédure nationale de préinscription en application de l'article D. 612-1-5 du code de l'éducation (attendus, critères généraux d'examen des vœux), les modalités et les critères d'examen des candidatures. Cette commission propose ensuite au chef d'établissement, après examen des dossiers de candidature, les réponses à apporter aux candidats (deuxième alinéa de l'article D. 612-1-13 du code de l'éducation).

Pour les aider dans leurs travaux préparatoires, en particulier pour le classement des candidatures, ces commissions peuvent choisir de s'appuyer sur un traitement de données à caractère personnel. Dès lors que l'établissement décide librement des modalités et critères d'examen des candidatures reçues ainsi que du dispositif utilisé pour permettre le traitement de ces informations en vue du classement des candidatures, il est « responsable de traitement ⁷ » au sens du RGPD.

A ce titre, l'établissement doit veiller au respect des dispositions de la réglementation en matière de protection des données personnelles (RGPD et loi « informatique et libertés » du 6 janvier 1978 modifiée).

Les établissements qui procèdent à un ordonnancement des dossiers via l'utilisation d'un traitement de données sont notamment tenus de réaliser une analyse d'impact sur la protection des données (AIDP) en application de l'article 35 du RGPD qui prévoit qu'une telle analyse est obligatoire pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes physiques⁸.

- **L'outil d'aide à la décision proposé par le MESRI**

Pour accompagner les établissements dans l'accomplissement de leurs missions, le ministère a développé un outil d'aide à la décision (ci-après « OAD ») mis à la disposition des établissements via la plateforme Parcoursup.

Cet outil d'aide à la décision, dont l'utilisation n'est ni obligatoire ni systématique, permet aux commissions d'examen des vœux de disposer d'une première analyse globale des candidatures.

Ainsi que la CNIL l'a rappelé, les établissements qui recourent à l'OAD du ministère demeurent responsable de traitement dans la mesure où « *d'une part, ils choisissent librement de l'utiliser ou non et, d'autre part, ils décident de le paramétrer en fonction de leurs besoins ou de l'utiliser tel que proposé par Parcoursup* ».

⁵ Article L. 612-3 du code de l'éducation

⁶ Article L. 612-3 du code de l'éducation

⁷ Définition du responsable de traitement (article 4 du RGPD) : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ».

⁸ Au regard des critères établis par le G29, la CNIL a considéré que chacun des traitements mis en œuvre par les établissements d'enseignement supérieur pour classer les candidatures dans ses différentes filières nécessitait la réalisation d'une AIDP (<https://www.cnil.fr/fr/parcoursup-et-les-etablissements-denseignement-superieur>).



Dans ces conditions, le ministère intervient en tant que sous-traitant de l'établissement puisqu'il est amené à traiter des données en son nom et pour son compte. Conformément à l'article 28 du RGPD⁹, la relation entre chaque établissement utilisateur de l'outil d'aide à la décision et le ministère de l'enseignement supérieur, de la recherche et de l'innovation est régie par une convention de sous-traitance¹⁰.

- **Analyse d'impact cadre pour les traitements reposant sur l'OAD du ministère**

Pour aider les établissements à répondre à leur obligation de réaliser d'une analyse d'impact¹¹, et compte tenu des caractéristiques du dispositif Parcoursup, le ministère a souhaité mutualiser certains éléments de l'AIPD entre plusieurs unités de formation et de recherche (UFR) d'une université ou entre établissements.

Le RGPD prévoit à cet égard qu'« *une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires* ».

La CNIL, consciente des difficultés à conduire des travaux d'une telle ampleur, notamment eu égard au grand nombre de formations post-baccalauréat existantes, a notamment considéré que le fait que les données traitées ne soient pas toutes les mêmes et que les critères de pondération soient distincts entre les formations, n'impliquait pas la réalisation d'une AIPD par formation, dans la mesure où les données traitées étaient toutes prévues par l'arrêté du 28 mars 2018 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup ».

C'est la raison pour laquelle le ministère s'est engagé dans l'élaboration d'un cadre commun pour la réalisation de cette AIPD avec le concours de la CNIL et dans le cadre d'une concertation avec des membres du réseau SupDPO, des chefs d'établissement du second degré et des responsables de la sécurité des systèmes d'information au sein des établissements.

L'analyse réalisée concerne le traitement des données à partir de l'OAD proposé par le ministère. Toutefois, ce document cadre pourra également servir de base de travail pour les établissements qui utiliseraient un autre outil pour l'examen des candidatures ou qui procèderaient à une extraction de tout ou partie des données accessibles via l'OAD afin de les transférer dans un autre système d'information visant à permettre des traitements de données spécifiques ou complémentaires.

Ces établissements, en s'inscrivant dans une démarche nouvelle, pourront donc reprendre le cadre de cette étude tout en l'adaptant à leur situation. Il sera notamment nécessaire de définir le dossier d'architecture et le dossier d'exploitation du système d'information d'accueil des données ainsi que les mesures de sécurité des systèmes d'information existantes afin de déboucher, comme dans le présent document, sur une étude de risques et, en fin de procédure, à une réduction des risques qui seront acceptés par l'autorité responsable du traitement.

En cas de demande d'information par la CNIL ou en cas d'incident de divulgation d'information, l'AIPD produite par l'établissement pourra être sollicitée et constituera un des éléments de réponse pour attestation de la démarche préventive initiée par l'établissement.

⁹ Le traitement par un sous-traitant est régi 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.

¹⁰ Une convention cadre est mise à la disposition des établissements d'enseignement supérieur depuis février 2019 - Convention jointe en Annexe X.

¹¹ Conformément au RGPD, le sous-traitant doit aider le responsable du traitement à effectuer l'AIPD.



Attention ! Une AIPD cadre à adapter à chaque contexte particulier

Le ministère a souhaité que les établissements disposent d'un document-cadre le plus complet et opérationnel possible pour faciliter leurs travaux. Chaque établissement devra néanmoins le compléter et l'adapter afin de tenir compte de ses propres besoins, des modalités de traitements qu'il a effectivement mis en œuvre ainsi que des spécificités liées à la sécurité (techniques et organisationnels).

A cet égard, la CNIL a rappelé en particulier que « chaque établissement devra néanmoins veiller à adapter ou compléter une éventuelle AIPD commune à sa situation propre si des risques étaient spécifiques à ses traitements afin de tenir compte, par exemple, de la nature des données traitées ou de la spécificité des mesures de sécurité devant être mises en œuvre ».

Pour rappel, une AIPD repose sur une évaluation **des risques inhérents au traitement pour mettre œuvre des mesures pour les atténuer.**

L'AIPD se décompose en trois parties¹² :

- **Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels ;**
- **L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;**
- **L'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.**

Or, il était impossible tenir compte des spécificités de l'ensemble des établissements pour réaliser une analyse d'impact qui soit le reflet exact du traitement mis en œuvre. Bien que le moyen utilisé soit identique (OAD du ministère), l'environnement et les besoins diffèrent.

Exemples :

1) les données traitées pour l'examen des candidatures correspondent à celles collectées et traitées dans le cadre de Parcoursup et listées dans l'arrêté du 31 décembre 2020. Pour autant, l'ensemble de ces données n'ont pas vocation à être systématiquement et automatiquement traitées, seules celles strictement nécessaires pour répondre aux critères de la formation le seront.

Aussi, bien que l'AIPD cadre mentionne l'intégralité des données de Parcoursup ainsi que les justifications, il appartiendra à chaque établissement d'opérer une sélection des données nécessaires par rapport à sa situation/besoin et de l'indiquer dans son AIPD modifiée.

2) De la même manière, l'évaluation des mesures prises pour garantir la sécurité et la confidentialité des données implique de réaliser une évaluation des mesures existantes au préalable, ce qui ne peut raisonnablement pas être réalisé dans le cadre des travaux relatifs à l'AIPD cadre. Concernant l'évaluation des risques, ils diffèrent également d'un établissement à un autre selon son environnement, les mesures prises, etc. Il en est de même pour les mesures permettant d'atténuer les éventuels risques identifiés.

Néanmoins, afin de faciliter ce travail, le groupe de travail constitué pour l'élaboration de ce document cadre a réalisé un inventaire des différents aléas les plus courants (ou les plus probables) afin de détecter les risques pour la vie privée et d'identifier les mesures pouvant être prises pour réduire ces risques à un niveau acceptable afin de garantir le respect de la vie privée et la sécurité des systèmes.

¹² Sources : site de la CNIL, <https://www.cnil.fr/fr/ce-qui-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>



Ainsi, il a été constaté qu'un certain nombre de préalables à une bonne gestion des risques doivent ainsi être réalisés, tels que l'information et la formation des personnels (ou des différents acteurs concernés).

Ce point, qui est central, et qui a été relevé par le comité éthique et scientifique Parcoursup dans son rapport au parlement 2020 doit ainsi conduire à la diffusion de consignes de sécurité qui doivent atteindre effectivement l'intégralité des autres acteurs finaux concernés dans ces milieux variés et hétérogènes : professeurs, jurys de formations et autres personnels concernés se trouvant au bout de chaînes parfois complexes – eux-mêmes souvent peu au fait des questions informatiques et en particulier de celles posées par la sécurité. **Ce risque est particulièrement pris en compte dans cette AIPD-cadre et il appartiendra aux établissements de prendre les mesures adaptées pour réduire ce dernier.**

Pour les accompagner dans l'élaboration de l'analyse d'impact, les établissements devront enfin veiller à consulter leur délégué à la protection des données, conformément au RGPD.

1.3. Vue d'ensemble

Cette partie doit permettre de présenter le traitement de manière synthétique : sa finalité, le contexte dans lequel il s'inscrit, le processus des données, le ou les responsables de traitement, les sous-traitants auxquels l'établissement fait appel et les textes applicables. Veuillez compléter les éventuels éléments manquants correspondant à votre situation.

1.3.1. Traitement considéré

Description du traitement	<p>Les commissions d'examen des vœux (CEV) des établissements d'enseignement supérieur déterminent, dans le cadre des critères généraux d'examen des vœux définis et affichés sur le site parcoursup.fr, les modalités et les critères d'examen des candidatures qu'elles reçoivent ainsi que, le cas échéant, le paramétrage de l'outil d'aide à la décision en fonction de leurs besoins et des choix pédagogiques qu'elles ont faits dans le respect des dispositions issues de la loi du 8 mars 2018.</p> <p>La procédure d'examen des candidatures se décompose en plusieurs étapes, qui peuvent être prises en charge directement par la plateforme nationale, par l'OAD ou encore par un outil qu'on qualifiera d'outil « maison » :</p> <ul style="list-style-type: none">- le recueil et le traitement des vœux des candidats ;- l'analyse et classement des vœux par les commissions d'examen des vœux de chaque établissement – avec, le cas échéant, un outil d'aide à la décision ;- le retour du classement et la prise en compte par la plateforme nationale Parcoursup des exigences légales (comme le pourcentage minimal de bacheliers retenus bénéficiaires d'une bourse nationale de lycée) ;- la récupération des données des candidats retenus dans Parcoursup pour leur inscription dans chaque établissement. <p>Il est à noter que l'inscription des étudiants dans chaque établissement relève d'un traitement totalement distinct lié à la gestion administrative de la scolarité des étudiants.</p>
Finalités du traitement	<p>L'OAD a pour finalité de faciliter l'analyse et l'examen des candidatures effectués par la commission d'examen des vœux de la formation, compte tenu des modalités et critères d'examen pédagogique qu'elle a déterminés en amont.</p> <p>En effet, pour les aider dans leurs travaux et non se substituer à eux, ces commissions peuvent choisir de s'appuyer sur des traitements de données dont elles ont, seules, défini le paramétrage. Ces outils d'aide à la décision, dont l'utilisation n'est donc ni obligatoire ni systématique, permettent aux</p>



	commissions d'examen des vœux de disposer d'une première analyse globale des candidatures. Ce travail de pré-classement permet de nourrir les échanges et la délibération collective des membres des commissions d'examen des vœux et d'identifier les examens particuliers à conduire en amont de la délibération finale.
Responsable du traitement	La collecte et le traitement des informations sont sous la responsabilité de l'établissement.
Sous-traitant(s)	Le ministère de l'enseignement supérieur, de la recherche et de l'innovation traite les données personnelles nécessaires au classement des candidatures pour le compte de l'établissement.
Faites-vous appel à un autre sous-traitant ?	Non

1.3.2. Textes applicables

Textes applicables au traitement	
Textes internationaux (collecte de données)	
Règlement UE 2016/679 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 (RGPD)	
Textes législatifs et réglementaires	
Article L. 612-3 du code de l'éducation	
Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés	
Articles D. 612-1 et suivants jusqu'à l'article D. 612-1-35 inclus	
Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels	
Arrêté du 31 décembre 2020 portant création d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup »	
Arrêté du 19 juin 2018 relatif à la création du service à compétence nationale dénommé « Parcoursup »	
Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques	
Jurisprudence et autres	
C.C., 3 avril 2020, n° 2020-834 QPC	
CE, 15 juillet 2020, n° 433296 et 433297 mentionnées aux tables	
Textes relatifs aux dispositifs techniques	
Cahier des charges synthétique de la plateforme Parcoursup	
Document de présentation des algorithmes de Parcoursup	
Étude de risques du système d'information Parcoursup	
Instruction de tri et de conservation pour les archives reçues et produites par les services et établissements	



concourant à l'éducation nationale
Décision du 30 novembre 2018 désignant le SCN Parcoursup comme opérateur de service essentiel du secteur de l'éducation
Arrêté du 18 mai 2020 portant homologation du téléservice Parcoursup

1.4. Données, processus et supports

1.4.1. Description des données

Le tableau suivant décrit les catégories de données collectées et traitées. Pour chaque donnée ou catégorie de données, vérifiez que celles-ci font bien l'objet d'un traitement, et dans l'affirmative, que celui-ci se justifie au regard de la formation concernée. Supprimez les informations que vous ne traitez pas. Le cas échéant, corrigez ou complétez les destinataires ainsi que la durée de conservation.

		Données
X	Données relatives au candidat à une formation post-baccalauréat	Données d'identification (numéro d'inscription, numéro d'identifiant élève ou étudiant, numéro campus études en France)
X		Identité : civilité, en principe pas de visibilité des nom, prénoms, date de naissance, sexe dans les cas et conditions fixées par l'article D. 612-1-13 du code de l'éducation
<input type="checkbox"/>		Etat civil (département et commune de naissance)
<input type="checkbox"/>		Coordonnées personnelles (adresse postale, coordonnées téléphoniques, académie ou bassin de résidence, adresse courriel) dans les cas et conditions fixées par l'article D. 612-1-13 du code de l'éducation
<input type="checkbox"/>		Version en format pdf d'un justificatif d'identité pour les candidats sollicitant une formation dans un lycée militaire
		Données relatives à la fraude ou tentative de fraude commise à l'occasion de la procédure de préinscription dans une formation initiale du premier cycle de l'enseignement supérieur.
X	Informations relatives aux candidats boursiers	Statut de boursier du second degré (oui/non) Pour une formation de CPGE disposant d'un internat : revenu brut global, avis d'imposition de l'année précédente, nombre de frères et sœurs à charge, nombre de frères et sœurs scolarisés dans l'enseignement supérieur, avis conditionnel d'attribution de bourse.
X	Données relatives aux agents bénéficiant d'un accès à l'application Parcoursup	Civilité, nom, prénom, téléphone (portable et fixe), adresse courriel, identifiant de connexion, mot de passe et profil d'habilitation.
<input type="checkbox"/>	Données relatives au parcours du candidat	Curriculum vitae
X		Projet de formation motivé
X		Attestations de formations, de titres ou qualifications divers
X		Informations relatives aux expériences et engagements divers
X		Informations relatives aux activités sportives et artistiques (niveau de pratique, inscription sur une liste de sportifs de haut niveau, discipline, résultat, performance, prix obtenus, personnes référentes dans l'institution sportive ou artistique)
X	Données relatives à la scolarité du candidat	Parcours scolaire (informations relatives à l'établissement scolaire, niveaux, cursus suivis, enseignements de spécialité, enseignements optionnels, langues vivantes)
X		Résultats scolaires (notes, moyennes, classements, appréciations des professeurs)
X		Avis d'orientation du conseil de classe dans le cadre de l'expérimentation de modalités d'admission dans une section de techniciens supérieurs pour les titulaires d'un baccalauréat professionnel
X		Proposition de l'équipe pédagogique et avis du chef de l'établissement lorsque le candidat, bachelier professionnel ou

		technologique, a suivi une formation complémentaire de type « classe passerelle » lui permettant d'acquérir les connaissances et compétences attendues pour la réussite dans la spécialité de section de techniciens supérieurs
X		Données relatives à la fiche « AVENIR » (éléments d'appréciation du professeur principal, des professeurs de la classe dans laquelle sont scolarisés les candidats, avis et éléments d'appréciation du chef d'établissement)
X	Données relatives au parcours du candidat étudiant en réorientation ou mise à niveau	Informations relatives à l'établissement, niveaux, cursus suivis, options
X		Résultats obtenus
X		Fiche de suivi le cas échéant
X	Données relatives au parcours du candidat non scolarisé souhaitant reprendre des études	Informations relatives au parcours scolaire, universitaire et professionnel
X		Résultats, diplômes et qualification obtenus
<input type="checkbox"/>	Information sur le paiement des frais de dossier et d'inscription	Type de paiement
<input type="checkbox"/>		Paieement effectué
<input type="checkbox"/>		Montant du paiement
<input type="checkbox"/>		Date du paiement
X	Informations relatives au baccalauréat	Académie et centre d'examen
X		Série, dominante, enseignements de spécialité, spécialités et enseignements optionnels
X		Date d'obtention
X		Numéro d'inscription
X		Liste des épreuves, résultat et moyenne générale par épreuve
X		Mention obtenue au baccalauréat ou diplôme équivalent
X		Groupe de passage à l'oral, le cas échéant
X		Fiche de suivi, le cas échéant
X		Niveau de langue française (tests et résultats, dispense éventuelle)
<input type="checkbox"/>	Données relatives aux justificatifs à produire par le candidat	Possession du certificat médical (Oui, Non)
<input type="checkbox"/>		Pour les candidats à une inscription dans un établissement relevant du ministère des armées : visite médicale effectuée (O/N) et date de rendez-vous
<input type="checkbox"/>	Données liées aux vœux et sous-vœux des vœux multiples (éléments pour chaque vœu/sous-vœu)	Pour une formation de CPGE disposant d'une internat : demande d'accueil en internat
<input type="checkbox"/>		Pour une formation de CPGE disposant d'une internat : distance entre le domicile et l'établissement de formation demandé
<input type="checkbox"/>		Libellé du groupe, le cas échéant
<input type="checkbox"/>		Date de formulation et de confirmation du vœu
	Autres catégories de données collectées par l'établissement	Pièces complémentaires demandées par la formation dans le cadre de la procédure de candidature Attestation (pour les licences de Droit et de Sciences)

1.4.2. Description des destinataires

Le cas échéant, corrigez ou complétez la liste des destinataires.

Les destinataires des données de ce traitement sont, dans les établissements dispensant des formations du premier cycle de l'enseignement supérieur dans lesquels les candidats sollicitent une préinscription en première année d'une formation post-baccalauréat et dans les structures chargées de la mutualisation de la gestion des candidatures : **le chef d'établissement et des personnes habilitées par ce dernier en fonction dans les services et commissions chargés de traiter les dossiers des candidats ou d'examiner les candidatures, ou le cas échéant, les personnes habilitées dans les structures chargées de la mutualisation de la gestion des candidatures.**

1.4.3. Description de la durée de conservation

Au terme de la prestation de services relative au traitement de ces données, les informations et données à caractère personnel relatives aux candidats sont conservées pendant une durée de deux ans. Les données relatives à la traçabilité des accès de chaque campagne sont conservées pendant un an. Les données à caractère personnel hébergées par le sous-traitant sont détruites et les données de paramétrage sont restituées au responsable de traitement.

Les données utilisées dans le cadre de l'examen des vœux fait l'objet d'une conservation (tableur excel propre à la CEV de l'établissement – candidat et évaluation (note), le temps nécessaire au processus de classement des vœux (environ 7 mois). Ce tableur est centralisé au niveau de la direction de l'IFSI. Les notation sont reportés dans Parcoursup après validation CEV.

1.5. Identification des actifs sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier)

Le tableau ci-dessous doit être complété ou modifié selon votre situation en cochant les cases correspondantes.

Systèmes informatiques sur lesquels reposent les données (matériels, dont supports de données électroniques), logiciels et canaux informatiques	Autres supports (personnes, supports papier et canaux de transmission papier).
<input checked="" type="checkbox"/> Smartphone/tablette/ordinateur professionnel	<input checked="" type="checkbox"/> Utilisateurs
<input checked="" type="checkbox"/> Application mobile/navigateur	<input type="checkbox"/> Locaux de l'utilisateur
<input checked="" type="checkbox"/> Réseau Wifi-Internet	<input checked="" type="checkbox"/> Supports papier
<input checked="" type="checkbox"/> Serveurs	<input checked="" type="checkbox"/> Tableur Excel propre à la CEV du Groupement permettant l'évaluation du dossier selon les critères propres des IFSI du Groupement. Les notations sont ensuite reportées dans le dossier du candidat dans parcourusup. => Conservation Dossier partagé IFSI Direction sur les serveurs du CHANGE, Accès restreint données de notation du candidats identifiés par un numéro de dossier (uniquement)
<input type="checkbox"/> Cloud	

2. Principes fondamentaux

2.1. Mesures garantissant la proportionnalité et la nécessité du traitement

Cette partie doit permettre :

- *D'explicitier et de justifier les choix effectués pour respecter les exigences suivantes :*
 - *finalité(s) : déterminée, explicite et légitime (art. 5.1b du RGPD) ;*
 - *fondement: licéité du traitement, interdiction du détournement de finalité (art. 6 du RGPD) ;*
 - *minimisation des données : adéquates, pertinentes et limitées (art. 5.1c du RGPD) ;*
 - *qualité des données : exactes et tenues à jour (art. 5.1d du RGPD) ;*
 - *durées de conservation: limitées (art. 5.1e du RGPD).*
- *De vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément au RGPD.*

Le cas échéant, proposer des mesures complémentaires.

Seules les parties surlignées doivent être complétées.

2.1.1. Finalités

Finalités	Légitimité
<p>Faciliter l'analyse des candidatures effectuée par la commission d'examen des vœux de la formation compte tenu des modalités et critères d'examen pédagogique qu'elle a déterminés.</p>	<p>Conformément à l'article L. 612-3, l'inscription dans une formation du premier cycle dispensée par un établissement public est précédée d'une procédure nationale de préinscription qui permet aux candidats de bénéficier d'un dispositif d'information et d'orientation qui, dans le prolongement de celui proposé au cours de la scolarité du second degré, est mis en place par les établissements d'enseignement supérieur. Cette inscription est prononcée par le président ou le directeur de l'établissement ou, dans les cas prévus aux VIII et IX de l'article susmentionné, par l'autorité académique.</p> <p>Aux termes de l'article D. 612-1-13 du même code, il appartient aux établissements dispensant des formations initiales du premier cycle de l'enseignement supérieur proposées sur la plateforme Parcoursup d'examiner les dossiers de candidature des candidats.</p> <p>L'OAD a pour finalité de faciliter cet examen.</p> <p>Au regard de ces éléments, la finalité du traitement apparaît comme déterminée, explicite et légitime conformément au b de l'article 5 du RGPD.</p>

2.1.2. Fondement

Pour être licite, un traitement doit se fonder sur l'une des six bases légales prévues par le RGPD (fondement juridique).

Critères de licéité	Justification
<p>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 (cette analyse a été confirmée par la CNIL, cf. FAQ)</p>	<p>Aux termes de l'article D. 612-1-13 du code de l'éducation, il appartient aux établissements dispensant des formations initiales du premier cycle de l'enseignement supérieur proposées sur la plateforme Parcoursup d'examiner les dossiers de candidature des candidats.</p> <p>Pour procéder à cet examen, les établissements réunissent, pour chaque formation ayant enregistré des vœux, une commission d'examen des vœux dont la composition est arrêtée par le chef d'établissement. Cette commission définit, dans le respect des critères généraux fixés en application de l'article D. 612-1-5, les modalités et les critères d'examen des candidatures et propose au chef d'établissement les réponses à faire aux candidats.</p> <p>Lorsque le nombre de candidatures excède les capacités d'accueil de la formation à la date de confirmation des vœux prévue par le calendrier mentionné à l'article D. 612-1-2, elle ordonne également les candidatures.</p> <p>Pour procéder à l'examen des dossiers de candidature pour l'accès aux formations relevant du VI de l'article L. 612-3, les établissements mettent en œuvre les modalités d'examen des candidatures prévues par les dispositions législatives et réglementaires les concernant.</p> <p>Le traitement est ainsi nécessaire à l'exécution d'une mission d'intérêt public au sens des dispositions du e de l'article 6 du RGPD.</p>

2.1.3. . Minimisation des données

Le RGPD prévoit que seules peuvent être traitées des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données).

Les données traitées pour le pré-classement des vœux varient en fonction des modalités et des critères préalablement définis. Aussi, ne peuvent être traitées que les données strictement nécessaires à l'examen des vœux selon les choix préalablement opérés.

Pour celles qui ne seraient pas visées ci-après, justifiez leur traitement, en illustrant dans la mesure du possible.

Le respect du principe de minimisation participe à la réduction la gravité des risques dans la mesure où les données traitées seront limitées au strict nécessaire.

	Données	Justification du besoin et de la pertinence des données	Mesures de minimisation
Données relatives au candidat à une formation post-baccalauréat	Données d'identification (numéro d'inscription, numéro d'identifiant élève ou étudiant, numéro campus études en France)	Ces données sont nécessaires au fonctionnement du service mis en œuvre pour le bénéfice des utilisateurs.	
	Identité (civilité, nom, prénoms, date de naissance, sexe) dans les cas et conditions fixées par l'article D. 612-1-13 du code de l'éducation	<p>Ces données sont nécessaires au fonctionnement du service mis en œuvre pour le bénéfice des utilisateurs.</p> <p>Le service offert par Parcoursup est un service individualisé. Le recueil de ces données est nécessaire afin que les services en charge du suivi du déroulement de la procédure et du fonctionnement de la plateforme puissent assurer un accompagnement efficace des candidats.</p>	<p>Conformément à l'article D. 612-1-13 du code de l'éducation, les dossiers de candidature ne mentionnent pas le nom, le prénom, l'adresse du domicile et l'âge du candidat, sauf si ces renseignements figurent dans des documents produits par le candidat ou par l'établissement scolaire dans lequel il est inscrit et s'ils ne peuvent être supprimés par les moyens techniques mis en œuvre par la plateforme.</p> <p>La plateforme signale aux candidats de ne pas faire apparaître ces données dans les rubriques à texte libre qu'ils sont amenés à compléter (projet de formation motivé; activités et centres d'intérêt). Par ailleurs, la plateforme conduit une politique de limitation des données demandées aux candidats, réduisant ainsi ce risque. Lorsque cela est possible, les pièces demandées aux candidats sont gérées par la plateforme garantissant ainsi l'anonymat (fiche de suivi; attestation de saisie des questionnaires des</p>

		<p>licences de Sciences et de Droit).</p> <p>Ces informations normatives (nom, prénom, adresse du domicile et âge du candidat) ne font l'objet d'une communication aux établissements que lorsque celle-ci est nécessaire pour l'attribution d'une place d'hébergement en internat, pour la convocation du candidat aux épreuves écrites/ou orales de sélection ou pour l'accompagnement du candidat dans la signature d'un contrat d'apprentissage.</p> <p>Par principe, les données nominatives ne sont pas accessibles (sauf si ces renseignements figurent dans des documents produits par le candidat ou par l'établissement scolaire dans lequel il est inscrit et s'ils ne peuvent être supprimés par les moyens techniques mis en œuvre par la plateforme)</p>
Etat civil (département et commune de naissance)	Ces données sont nécessaires au fonctionnement du service mis en œuvre pour le bénéfice des usagers.	Pas d'accès
Coordonnées personnelles (adresse postale, coordonnées téléphoniques, académie ou bassin de résidence, adresse courriel) dans les cas et conditions fixées par l'article D. 612-1-13 du code de l'éducation	<p>Ces données sont nécessaires au fonctionnement du service mis en œuvre pour le bénéfice des utilisateurs.</p> <p>Le service offert par Parcoursup est un service individualisé. Le recueil de ces données est nécessaire afin que les services en charge du suivi du bon déroulement de la procédure de préinscription et du fonctionnement de la plateforme puissent assurer un accompagnement efficace des candidats. Les coordonnées renseignées leurs permettent notamment de bénéficier de nombreux services</p>	<p>Pour mémoire, conformément à l'article D. 612-1-13 du code de l'éducation, les dossiers de candidature ne mentionnent pas le nom, le prénom, l'adresse du domicile et l'âge du candidat, sauf si ces renseignements figurent dans des documents produits par le candidat ou par l'établissement scolaire dans lequel il est inscrit et s'ils ne peuvent être supprimés par les moyens techniques mis en œuvre par la plateforme.</p> <p>La plateforme signale aux candidats de ne pas faire apparaître ces données dans les rubriques à</p>

		<p>(ex : envoi de mels et SMS les informant de différentes actions à mener et étapes à suivre pour le bon traitement de leur dossier). En outre la connaissance de leur adresse postale, de leur académie d'appartenance ou bassin de résidence est nécessaire afin de mettre en œuvre la possibilité qui leur est offerte dans certaines situations de postuler dans certaines formations en dehors de leur académie ou lieu de résidence.</p> <p>Bien sûr, ces données peuvent être mises à jour par le candidat qui le souhaite au cours de la procédure.</p>	<p>texte libre qu'ils sont amenés à compléter (projet de formation motivé ; activités et centres d'intérêt). Par ailleurs, la plateforme conduit une politique de limitation des données demandées aux candidats, réduisant ainsi ce risque. Lorsque cela est possible, les pièces demandées aux candidats sont gérées par la plateforme garantissant ainsi l'anonymat (fiche de suivi ; attestation de saisie des questionnaires des licences de Sciences et de Droit).</p> <p>Ces informations normatives (nom, prénom, adresse du domicile et âge du candidat) ne font l'objet d'une communication aux établissements que lorsque celle-ci est nécessaire pour l'attribution d'une place d'hébergement en internat, pour la convocation du candidat aux épreuves écrites/ou orales de sélection ou pour l'accompagnement du candidat dans la signature d'un contrat d'apprentissage.</p>
	Version en format pdf d'un justificatif d'identité pour les candidats sollicitant une formation dans un lycée militaire	Nécessaire à la justification, par ces candidats, de la nationalité française.	L'information n'est collectée que pour les candidats formulant un vœu sur une formation dans un lycée militaire.
	Données relatives à la fraude ou tentative de fraude commise à l'occasion de la procédure de préinscription dans une formation initiale du premier cycle de l'enseignement supérieur	Données nécessaires à la mise en œuvre de l'article D. 612-1-36 du code de l'éducation	Pas d'accès
Informations relatives aux candidats boursiers	Statut de boursier du second degré Pour une formation de CPGE disposant d'un internat : revenu brut global, avis d'imposition de l'année précédente,		Ces données ne sont collectées que si le candidat a expressément formulé un vœu en internat.

OAD PARCOURSUP - Analyse d'impact relative à la protection des données

	nombre de frères et sœurs à charge, nombre de frères et sœurs scolarisés dans l'enseignement supérieur, avis conditionnel d'attribution de bourse.		
Données relatives aux agents bénéficiant d'un accès à l'application Parcoursup	Civilité, nom, prénom, téléphone (portable et fixe), adresse courriel, identifiant de connexion, mot de passe et profil d'habilitation.	Ces données sont nécessaires au fonctionnement du service par les fournisseurs de ressources au service des utilisateurs En outre, elles sont nécessaires au contrôle des droits d'accès et des habilitations.	
Données relatives au parcours du candidat	Curriculum vitae	Nécessaire à la mise en œuvre de la procédure de préinscription : nécessaire à l'examen de la candidature par les formations	
	Projet de formation motivé	Nécessaire à la mise en œuvre de la procédure de préinscription : nécessaire à l'examen de la candidature par les formations.	Le candidat est guidé pour la rédaction de son projet de formation motivé de manière à ce qu'il ne fasse figurer que les éléments attendus par les formations d'affectation.

Données relatives au parcours du candidat	Attestations de formations, de titres ou qualifications divers	Nécessaire à l'examen des candidatures, notamment afin de déterminer l'adéquation du profil d'un candidat à la formation demandée.	
	Informations relatives aux expériences et engagements divers	Nécessaire à l'examen des candidatures, notamment afin de déterminer l'adéquation du profil d'un candidat à la formation demandée.	Le candidat est guidé pour la rédaction de la rubrique de manière à ce qu'il ne fasse figurer que les éléments utiles. La rubrique « activités et centres d'intérêt » a un caractère facultatif.
	Informations relatives aux activités sportives et artistiques (niveau de pratique, inscription sur une liste de sportifs de haut niveau ou une autre liste	Nécessaire à l'examen de la candidature, notamment afin de déterminer l'adéquation du profil du candidat à la formation demandée.	La rubrique a un caractère facultatif. Elle est saisie à la discrétion du candidat.

	<p>de sportifs identifiés par le ministère chargé des sport, discipline, résultat, performance, prix obtenus, personnes référentes dans l'institution sportive ou artistique)</p>	<p>En outre, certaines de ces informations sont nécessaires à la mise en œuvre des dispositifs bénéficiant aux sportifs de haut niveau sur le fondement du IX de l'article L. 612-3 du code de l'éducation</p> <p>L. 612-3 : (...) « IX.- Lorsque la situation d'un candidat justifie, eu égard à des circonstances exceptionnelles tenant (...) à son inscription en tant que sportif de haut niveau sur la liste mentionnée au premier alinéa de l'article L. 221-2 du code du sport ou à ses charges de famille, son inscription dans un établissement situé dans une zone géographique déterminée, l'autorité académique, saisie par ce candidat, peut procéder au réexamen de sa candidature dans des conditions fixées par décret. En tenant compte de la situation particulière que l'intéressé fait valoir, des acquis de sa formation antérieure et de ses compétences ainsi que des caractéristiques des formations, l'autorité académique prononce, avec son accord, son inscription dans une formation du premier cycle.</p>	
<p>Données relatives à la scolarité du candidat</p>	<p>Parcours scolaire (informations relatives à l'établissement scolaire, niveaux, cursus suivis, enseignements de spécialité, enseignements optionnels, langues vivantes, y compris pour les bacheliers, la participation aux dispositifs d'accompagnement mis en place entre les établissements d'enseignement pour garantir l'égalité des chances)</p>	<p>Nécessaire à l'examen de la candidature, notamment afin de déterminer l'adéquation du profil du candidat à la formation demandée. Nécessaire également à la mise en œuvre d'autres dispositifs facilitant notamment l'accès à certaines formations pour les titulaires d'un baccalauréat professionnel ou technique (STS et IUT) permettant de favoriser la promotion de l'égalité des chances (article L. 612-3 du code de l'éducation).</p>	
	<p>Résultats scolaires (notes, moyennes,</p>	<p>Nécessaire à l'examen de la candidature,</p>	

	classements, appréciations des professeurs)	notamment afin de déterminer l'adéquation du profil du candidat à la formation demandée.	
	Avis d'orientation du conseil de classe dans le cadre de l'expérimentation de modalités d'admission dans une section de techniciens supérieurs pour les titulaires d'un baccalauréat professionnel	Nécessaire à la mise en œuvre de l'expérimentation qui permet aux bacheliers professionnels d'être admis en section de techniciens supérieurs après avis du conseil de classe de l'établissement d'origine (article 40 de la loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté).	
	Proposition de l'équipe pédagogique et avis du chef de l'établissement lorsque le candidat, bachelier professionnel ou technologique, a suivi une formation complémentaire de type « classe passerelle » lui permettant d'acquérir les connaissances et compétences attendues pour la réussite dans la spécialité de section de techniciens supérieurs	Données nécessaires à la mise en œuvre du dispositif « classe passerelle » (Décret n° 2019-215 du 21 mars 2019).	
	Données relatives à la fiche « AVENIR » (éléments d'appréciation des professeurs qui assurent les enseignements pour les candidats ou qui les accompagnent dans leur orientation, avis et éléments d'appréciation du chef d'établissement)	Nécessaire à l'examen de la candidature, notamment afin de déterminer l'adéquation du profil du candidat à la formation demandée.	
Données relatives au parcours du candidat étudiant en réorientation ou mise à niveau	Informations relatives à l'établissement, niveaux, cursus suivis, options	Nécessaire à l'examen de la candidature, notamment afin de déterminer l'adéquation du profil du candidat à la formation demandée.	
	Résultats, diplômes et qualification obtenus	Nécessaire à l'examen de la candidature, notamment afin de déterminer l'adéquation du profil du candidat à la formation demandée.	

OAD PARCOURSUP - Analyse d'impact relative à la protection des données

	Fiche de suivi permettant de préciser son projet d'orientation le cas échéant	Nécessaire à la mise en œuvre de l'article D. 612-1-9-1 : « Pour tenir compte de la situation particulière des candidats inscrits sur la plateforme Parcoursup dans le cadre d'une réorientation ou d'une reprise d'études, une fiche de suivi est mise à la disposition de ceux d'entre eux qui le souhaitent par la plateforme Parcoursup. Cette fiche de suivi a pour objet de valoriser auprès d'un service d'orientation la démarche de réflexion dans laquelle le candidat s'est engagé afin que ce service l'accompagne dans sa démarche et formule un avis sur son projet de réorientation ou de reprise d'études. »	Le candidat est guidé pour la rédaction de cette fiche de suivi de manière à ce qu'il ne fasse figurer que les éléments utiles. La fiche de suivi a un caractère facultatif.
Données relatives au parcours du candidat non scolarisé souhaitant reprendre des études	Informations relatives au parcours scolaire, universitaire et professionnel	Nécessaire afin de proposer aux candidats déjà titulaires du baccalauréat une offre de formations en adéquation avec le besoin exprimé sur le fondement de l'article D. 612-1 du code de l'éducation : (...) II.- La plateforme Parcoursup assure aux candidats déjà titulaires du baccalauréat ou d'un diplôme équivalent et qui s'inscrivent sur la plateforme Parcoursup pour reprendre des études, une information sur l'offre de formation professionnelle tout au long de la vie et le conseil en évolution professionnelle.	
	Résultats, diplômes et qualification obtenus	Nécessaire afin de proposer aux candidats déjà titulaires du baccalauréat une offre de formations en adéquation avec le besoin exprimé sur le fondement de l'article D. 612-1 du code de l'éducation : (...) II.- La plateforme Parcoursup assure aux candidats déjà titulaires du baccalauréat ou d'un diplôme équivalent et qui s'inscrivent sur la plateforme Parcoursup pour reprendre des études, une	

		information sur l'offre de formation professionnelle tout au long de la vie et le conseil en évolution professionnelle.	
	Fiche de suivi permettant de préciser son projet d'orientation le cas échéant et informations relatives aux expériences et engagements divers	<p>Nécessaire afin de proposer aux candidats déjà titulaires du baccalauréat une offre de formations en adéquation avec le besoin exprimé sur le fondement de l'article D. 612-1 du code de l'éducation : (...) II.- La plateforme Parcoursup assure aux candidats déjà titulaires du baccalauréat ou d'un diplôme équivalent et qui s'inscrivent sur la plateforme Parcoursup pour reprendre des études, une information sur l'offre de formation professionnelle tout au long de la vie et le conseil en évolution professionnelle.</p> <p>Egalement nécessaire à la mise œuvre des dispositions du D612-1-9-1 : (...) II.- Pour tenir compte de la situation particulière des candidats inscrits sur la plateforme Parcoursup dans le cadre d'une réorientation ou d'une reprise d'études, une fiche de suivi est mise à la disposition de ceux d'entre eux qui le souhaitent par la plateforme Parcoursup. Cette fiche de suivi a pour objet de valoriser auprès d'un service d'orientation la démarche de réflexion dans laquelle le candidat s'est engagé afin que ce service l'accompagne dans sa démarche et formule un avis sur son projet de réorientation ou de reprise d'études.</p>	<p>Le candidat est guidé pour la rédaction de cette fiche de suivi de manière à ce qu'il ne fasse figurer que les éléments utiles.</p> <p>La fiche de suivi a un caractère facultatif</p>
Information sur le paiement des frais de dossier et d'inscription	Type de paiement	Pour certaines formations, le paiement de frais est une condition de validation de la candidature ou de l'inscription. L'information confirmant que le candidat a effectivement payé ces frais est	
	Paiement effectué		

OAD PARCOURSUP - Analyse d'impact relative à la protection des données

	Montant du paiement	nécessaire à la suite du déroulement du processus d'examen du dossier ou d'inscription du candidat (même si aucun paiement n'est effectué sur Parcoursup).	
	Date du paiement		
Informations relatives au baccalauréat	Académie et centre d'examen	Nécessaire pour l'admission dans les formations ainsi que pour la bonne gestion de la procédure. Les notes d'examen sont remontées directement dans Parcoursup par les académies et les centres d'examen. Il est donc nécessaire de pouvoir les identifier savoir dans quel centre d'examen et dans quelle académie les candidats ont passé leur examen.	
	Série, dominante, enseignements de spécialité, spécialités et enseignements optionnels	Nécessaire à l'inscription dans l'enseignement supérieur et à la mise en application des dispositions relatives aux meilleurs bacheliers (article D612-1-31)	
	Date d'obtention	Nécessaire au bon déroulement de la procédure (prendre en compte la situation des candidats encore en cours d'examen du baccalauréat) ainsi qu'à la mise en application des dispositions relatives aux meilleurs bacheliers (article D612-1-31)	
	Numéro d'inscription	Données d'identification nécessaires à la mise en œuvre du traitement	
	Liste des épreuves, résultat et moyenne générale par épreuve	Nécessaire à l'examen des candidatures ainsi qu'à la mise en application des dispositions relatives aux meilleurs bacheliers (article D612-1-31)	
	Mention obtenue au baccalauréat ou diplôme équivalent	Nécessaire à l'examen des candidatures ainsi qu'à la mise en application des dispositions	

		relatives aux meilleurs bacheliers (article D612-1-31)	
	Groupe de passage à l'oral, le cas échéant		
	Niveau de langue française (tests et résultats, dispense éventuelle)	Nécessaire à l'examen de la candidature	
	Possession du certificat médical (Oui, Non)	<p>Pour l'accès à certaines formations (notamment militaire) la possession d'un certificat médical est nécessaire.</p> <p>Nécessaire également afin de justifier pouvoir bénéficier du dispositif prévu à l'article D612-1-29 (accompagnement individuel par la commission d'accès à l'enseignement supérieur) : « Lorsque la demande est présentée en raison de la situation de handicap du candidat ou de son état de santé, la commission régionale d'accès à l'enseignement supérieur tient notamment compte, pour l'examen de cette demande, des besoins d'accompagnement, de compensation, de soins, de transport du candidat, de la situation de l'élève ou de l'étudiant, d'une reconnaissance, le cas échéant, de sa situation de handicap et des modalités de prise en compte de sa situation en matière d'accessibilité par les établissements qui délivrent les formations souhaitées. »</p>	
	Libellé du groupe, le cas échéant	Nécessaire à l'examen de la candidature ainsi qu'au bon déroulement de la procédure car des quotas d'admission peuvent être définis en fonction des différents groupes de bac existants (pro, techno...)	
	Date de formulation et de confirmation du vœu	Nécessaire au bon déroulement des phases de la procédure dans le respect du calendrier défini	

OAD PARCOURSUP - Analyse d'impact relative à la protection des données

		chaque année par arrêté. L'alinéa 2 de l'article D612-1-2 prévoit, à titre d'exemple que : « (...) Le candidat est averti via la plateforme Parcoursup de la fin du délai pouvant entraîner l'annulation de ses vœux et des propositions d'admission reçues via la plateforme. Il est également informé via cette plateforme des périodes au cours desquelles il doit confirmer la proposition d'admission qu'il a acceptée ou les placements sur liste d'attente dont il bénéficie, sous peine d'être réputé y avoir renoncé ».	
Autres catégories de données collectées par l'établissement	Pièces complémentaires demandées par la formation dans le cadre de la procédure de candidature		NA
	Attestation (pour les licences de Droit et de Sciences)		NA

2.1.4. Qualité des données

Le tableau ci-dessous doit être complété en indiquant les modalités d'information des personnes, notamment par rapport à l'adresse mail de contact pour l'exercice des droits.

Le responsable de traitement doit veiller à ce que les données qu'il traite soient exactes et, si nécessaires, mises à jour. Il doit également permettre aux personnes de demander la rectification de leurs données, en les invitant par exemple à vérifier leur exactitude. Veuillez compléter le tableau ci-dessous en précisant notamment la personne ou le service auprès duquel les droits peuvent être exercés.

Mesures pour la qualité des données	Modalités de mise en œuvre
<p><u>Les données traitées sont celles issues du traitement Parcoursup.</u></p> <p>Les personnes voient les données les concernant. Les modifications peuvent être opérées par l'utilisateur lui-même ou via interaction avec les services centraux ou académiques qui pilotent la plateforme.</p> <p>Tout au long de la procédure Parcoursup, un accompagnement des usagers est organisé de manière à les aider à la saisie des données, et à recueillir les demandes de modification : le numéro vert, la messagerie « contact » de Parcoursup permettent des interactions à tout moment au cours de la procédure.</p> <p>Au moment de leur inscription, les candidats peuvent saisir ou corriger (lorsque les informations sont pré-remplies) les données les concernant.</p> <p>Au moment de la remontée des notes par les établissements scolaires, les lycéens peuvent faire corriger les données les concernant.</p>	<p>Les modifications peuvent être opérées par le candidat lui-même ou via une interaction avec les services centraux ou académiques qui pilotent la plateforme.</p> <p>Les droits de rectification susvisée s'exercent auprès de : de la plateforme ou du DPO du ministère</p> <p>Pour les éléments relevant de l'IFSI (remontée de note) : au près du chef d'établissement ou du dpo@ch-annecygenevois.fr.</p> <p>En cas de difficultés dans l'exercice de leurs droits, les candidats ont la possibilité de saisir le délégué à la protection des données personnelles de la manière suivante : auprès de la plateforme ou du DPO du ministère</p> <p>Pour les éléments relevant de l'IFSI (notamment s'agissant des remontées de note) : au près du chef d'établissement ou du dpo@ch-annecygenevois.fr.</p>

2.1.5. Durées de conservation

Le tableau ci-dessous doit être complété en indiquant les mécanismes de suppression des données à la fin de la durée de conservation fixée. Il convient également de s'assurer que les durées de conservation mentionnées dans ce tableau à titre indicatif sont exactes et, le cas échéant, de les adapter.

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données enregistrées lors de l'inscription sur la plateforme Parcoursup et données issues des traitements de données	Deux ans	Les données sont conservées durant deux ans dans le cadre du dispositif national	Suppression directement effectuée sur la plateforme Parcoursup (suppression de l'accès à ces données). Mesures complémentaires de l'établissement : - tableau consolidé reprenant les notations des candidats, pendant la période d'examen des vœux jusqu'à la fin de la période des admissions définitives (environ 7 mois). - les données des candidats devenus élèves sont conservées pendant la scolarité + Candidat non retenu pendant 1 an - Les durées de conservations sont celles résultant notamment de l'Instruction DPACI/RES/2005/007 du 28 avril 2005

2.1.6. Evaluation des mesures

Procédez à l'évaluation des mesures prises pour respecter les principes fondamentaux relatifs à la protection des données et précisez la justification du caractère acceptable ou pas de ces mesures.

Enfin, le cas échéant, précisez les mesures correctives ou préventives envisagées.

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorable	Justifications et, le cas échéant, mesures correctives / préventives
Finalités : déterminées, explicites et légitimes	Acceptable - Cf. tableau 2.1.1	
Fondement : licéité du traitement	Acceptable – Cf. Tableau 2.1.2	
Minimisation des données : adéquates, pertinentes et limitées	Acceptable – Cf. tableau 2.1.3	
Qualité des données : exactes et tenues à jour	Acceptable – Cf. tableau 2.1.4	
Durées de conservation : limitées	Acceptable – Cf. tableau 2.1.5	

2.2. Évaluation des mesures protectrices des droits des personnes concernées

Cette partie doit permettre de décrire et d'évaluer les mesures prises pour garantir aux personnes la possibilité d'exercer leurs droits de manière effective.

2.2.1. Mesures pour l'information des personnes

Rappel : L'information des personnes en pratique (fiche thématique « L'utilisation du module d'aide à la décision : les obligations CNIL »)

Cette information pourra être diffusée, pour chaque traitement de données créé, au moyen d'affiches apposées dans les établissements ou du site internet de ces derniers. Des dispositions techniques seront prises pour qu'un accès à cette information puisse également être visible sur la plateforme parcoursup.fr.

Cette information devra comporter les mentions légales suivantes :

Conformément au règlement général européen sur la protection des données (RGPD), je vous informe que vos données à caractère personnel font l'objet d'un traitement informatique mis en œuvre par **(fonction de l'autorité responsable du traitement, au sein de l'établissement. Ex : président de l'Université X et adresse)**, pour l'exécution d'une mission d'intérêt public au sens des dispositions du RGPD.

Ces données sont collectées dans le but de faciliter l'analyse des candidatures effectuée par la commission d'examen des vœux de la formation **xxx** dans le strict cadre des modalités et critères d'examen pédagogique des vœux qu'elle a déterminés.

Les données relatives à **(catégorie de données à caractère personnel recueillies pour l'analyse des vœux. Ex : données relatives au parcours scolaire du candidat, données relatives à la scolarité. Voir l'arrêté Parcoursup en ce sens)** peuvent provenir du traitement automatisé dénommé « Parcoursup » (cf. arrêté du 28 mars 2018 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup »).

Les informations recueillies sont conservées pour une durée de **(à compléter)**

Les destinataires de ces données sont **(à compléter)**

Vous pouvez accéder aux données vous concernant et exercer les droits que vous tenez des articles 38, 39, 40 et 40-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés à l'adresse suivante : (**adresse générique**)

Pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter le délégué à la protection des données de l'établissement à l'adresse suivante : (**adresse générique**). Si vous estimez, après nous avoir contactés, que vos droits ne sont pas respectés ou que ce dispositif n'est pas conforme aux règles de protection des données, vous pouvez adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

L'ensemble des mentions informatives prévues par les dispositions des articles 13 et 14 du RGPD et de l'article 85 de la loi du 6 janvier 1978 sont portées à la connaissance des personnes concernées sur le site internet de l'établissement, accessible à l'adresse suivant : <https://www.hopitauxduleman.fr>

2.2.2. Mesures pour les droits d'accès et de rectification

Mesures pour le droit d'accès	Modalités de mise œuvre
<p>Mention sur le site internet : Mention dédiée à Parcoursup + Charte de protection de données élèves étudiants + Mention dans le Règlement interieur + Affiche dédiée Parcoursup lors de portes ouvertes à compter de 2024</p>	<p>Les personnes objet du traitement disposent d'un droit d'accès et de rectification au traitement de leurs données.</p> <p>Ces droits s'exercent à l'adresse suivante : dpo@ch-hopitauxduleman.fr ou secrétariat de l'ifsi : IFSI-Sec@ch-hopitauxduleman.fr</p> <p>Pour toute question sur le traitement des données dans ce dispositif ou en cas de difficultés dans l'exercice de leurs droits, les personnes objet du traitement peuvent contacter le délégué à la protection des données à : dpo@ch-hopitauxduleman.fr</p> <p>Si les personnes objet du traitement estiment que leurs droits ne sont pas respectés ou que ce dispositif n'est pas conforme aux règles de protection des données, elles peuvent adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).</p>

2.2.3. Mesures pour la sous-traitance

Nom du sous-traitant	Finalité	Référence du contrat	Conformité art.28
Ministère de l'enseignement supérieur, de la recherche et de l'innovation	<ul style="list-style-type: none"> - mise à disposition et la gestion de l'outil d'aide à la décision et des données du traitement Parcoursup utilisées par les commissions d'examen des vœux ; - hébergement, pendant une durée de deux ans, des données relatives aux critères définis par les commissions d'examen des vœux et nécessaires aux opérations de pré-classement effectuées par ces commissions (critères paramétrés dans l'outil d'aide à la décision) ; - hébergement, pendant une durée de deux ans, des données à caractère personnel résultant des 	Convention de sous-traitance conclue le 2023 lors de l'inscription sur la plateforme pour le paramétrage selon modeler du ministère (absence de date))	Oui

	opérations de pré-classement effectuées par l'outil d'aide à la décision.		
Sous-traitants ultérieurs	Le ministère de l'enseignement supérieur, de la recherche et de l'innovation n'effectue aucune sous-traitance ultérieure dans le cadre du traitement Parcoursup.		

2.2.4. Evaluation des mesures

Mesures protectrices des droits des personnes concernées	Acceptable / Améliorable ?	Mesures correctives
Information des personnes concernées (traitement loyal et transparent)	Acceptable	Prévoir affichage lors des prochaines portes ouvertes
Recueil du consentement	Le consentement n'est pas recueilli dans le cadre du traitement	Sans objet
Exercice des droits d'accès et à la portabilité	Le droit à la portabilité ne s'applique pas. Sur le droit d'accès : Acceptable	Sans objet
Exercice des droits de rectification	Acceptable	
Exercice des droits de limitation du traitement et d'opposition	Acceptable	
Sous-traitance : identifiée et contractualisée	Acceptable	Révision annuelle de la convention de sous-traitance
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	Aucun transfert hors UE	Sans objet

3. Etude des risques liés à la sécurité des données

3.1. Évaluation des mesures

- Identifier ou déterminer les mesures existantes ou prévues (déjà engagées), qui peuvent être de trois natures différentes :
 - Mesures portant spécifiquement sur les données du traitement : chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, etc. ;
 - Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre : sécurité de l'exploitation, sauvegardes, sécurité des matériels, etc. ;
 - Mesures organisationnelles (gouvernance) : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, etc.
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité.
- Le cas échéant, préciser leur description ou proposer des mesures complémentaires.

Certaines des mesures de sécurité énoncées ci-après sont directement mises en œuvre au niveau de la plateforme nationale Parcoursup.

Dans ces conditions, le ministère garantit, notamment en sa qualité de sous-traitant, la mise en œuvre de ces mesures et, par conséquent, un niveau de risques acceptable. C'est la raison pour laquelle certaines de ces colonnes ont d'ores et déjà été complétées. En revanche, il appartient à l'établissement de définir les mesures de sécurité qui relèvent de son champ de compétence et d'évaluer le niveau d'acceptabilité des risques après mise en œuvre de ces mesures. Enfin, dans certains cas, les mesures de sécurité sont mises en œuvre à la fois par la plateforme Parcoursup et par l'établissement.

3.1.1. Mesures contribuant à traiter des risques liés à la sécurité des données

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Mesures correctives
Chiffrement	Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance).	Acceptable	Sans objet
Anonymisation	Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance).	Acceptable	Sans objet <i>(parfois nom prénom à différents endroits non spécifique , cependant des mentions d'information et recommandation sont prévues)</i>
Contrôle d'intégrité	Les notes remontées font l'objet d'une vérification par le chef d'établissement	Acceptable	Sans objet
Archivage	Les données font l'objet d'une conservation pendant 2 ans sur la plateforme Dans l'établissement les données ne sont conservées que le temps nécessaire au processus, puis les données des candidats sont conservées et archivées en tenant comptes des règles et instructions applicables.	Acceptable	Sans objet
Sécurité des documents papier	Sans objet	Sans objet	Sans objet

3.1.2. Mesures générales de sécurité

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Mesures correctives
Sécurité de l'exploitation	Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance).	Acceptable	Sans objet

Sécurité des canaux informatiques (réseaux)	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Mesures de sécurité de l'établissement en lien avec la PSSI</p>	<p>Acceptable</p> <p>Acceptable</p>	
Surveillance	Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance).	Acceptable	Sans objet
Contrôle d'accès physique	<p>La gestion des accès physique par badges se fait par badges sécurisés. Le contrôle d'accès est confié à un ensemble de lecteurs de badges connectés à un logiciel de gestion des accès. Les accès sont nominatifs.</p> <p>+ système de vidéoprotection surveillance de l'établissement</p> <p>De plus, les salles serveurs sont équipées d'alarme anti-intrusion.</p>	Acceptable	Rédaction en cours d'une procédure visant à définir le processus de destruction des badges
Sécurité des matériels		Acceptable	
Éloignement des sources de risques	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Mesures établissements : 2 salles serveurs avec Sécurité incendie et électrique Accès restreint et sécurisé</p>	Acceptable	
Protection contre les sources de risques non humaines	Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)	Acceptable	

3.1.3. Mesures organisationnelles (gouvernance)

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Mesures correctives
Organisation	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Le RSSI est chargé du pilotage, de la coordination de la mise en œuvre, de l'application et de l'évolution de la politique de sécurité de l'information.</p>	<p>Acceptable</p> <p>Acceptable</p>	

	<p>Le DPO (Délégué à la Protection des Données) est chargé de veiller à la confidentialité et à l'intégrité des données.</p>		<p>Le DPO du GHT est actuellement en cours de recrutement (novembre 2023)</p>
<p>Politique (gestion des règles)</p>	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>PSSI établissement Charte d'usage et charte prestataire.</p>	<p>Acceptable</p>	
<p>Gestion des risques</p>	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Mesures de sécurité de l'établissement en lien avec la PSSI</p> <p>Continuité d'activité et plans de secours : Afin de réagir efficacement en cas de sinistres informatiques et notamment en cas de cyberattaque, le Centre Hospitalier a démarré les travaux suivants :</p> <ul style="list-style-type: none"> - Formalisation du plan blanc volet Cyber sécurité (décrit l'organisation face à la crise) - Formalisation du plan de Continuité d'activité (décrit la conduite à tenir par les métiers pendant la crise) - Formalisation du Plan de continuité et reprise du système informatique (décrit les étapes et procédures de redémarrage des Services SI) 	<p>Acceptable</p>	
<p>Gestion des projets</p>	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Méthode projet- fiche de conformité RGPD déployée pour prise en compte dans les projets</p>	<p>Acceptable</p>	
<p>Gestion des incidents et des violations de données</p>	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p>	<p>Acceptable</p>	

	<p>Mesures de sécurité de l'établissement en lien avec la PSSI</p> <p>Procédure de gestion des incidents et procédure de gestion des violations de données en cours de rédaction.</p>		
Gestion des personnels	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Mesures de sécurité de l'établissement en lien avec la PSSI</p> <p>- L'ensemble du personnel est sensibilisé et est conditionné par une clause de confidentialité (charte informatique) contenu dans les contrats de travail signés lors de l'embauche.</p> <p>Il existe un plan de sensibilisation et de formation en matière de sécurité et de confidentialité mené par le RSSI. Une sensibilisation est faite lors de la journée d'accueil des nouveaux arrivants.</p>	Acceptable	
Relations avec les tiers	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Mesures de sécurité de l'établissement en lien avec la PSSI</p> <p>Les prestataires de la DSI sont sensibilisés et sont conditionnés par une clause de confidentialité (charte prestataire) pour les achats réalisés au sein du GHT .</p>	Acceptable	Charte prestataire à inclure dans les contrats de maintenance achetés directement par les Hôpitaux du Léman.
Supervision	<p>Mesures de sécurité prises directement en charge par la plateforme Parcoursup (cf. convention de sous-traitance)</p> <p>Projet de mise en place de supervision prévu pour 2024</p>	Acceptable	

3.2. Appréciation des risques : les atteintes potentielles aux droits et libertés

Le tableau ci-après synthétise pour chaque événement redouté (un accès illégitime à des données, une modification non désirée de données et une disparition de données) les menaces qui pourraient mener à cet événement redouté en fonction des sources de risques qui pourraient en être à l'origine accompagné de leur vraisemblance ainsi que les impacts potentiels sur la vie privée des personnes concernées s'ils survenaient ainsi que leur gravité.

Il pourrait par exemple s'agir du vol de l'ordinateur d'un examinateur d'une commission d'examen des vœux, qui n'aurait pas été verrouillé et qui aurait pour conséquence la visualisation et le téléchargement de données à caractère personnel relatives à un candidat ou encore la modification de l'ensemble du classement des candidatures. De tels événements pourraient avoir pour conséquences

une fuite massives sur internet de données à caractère personnel ou encore une perte de chance pour l'ensemble des candidats dont les classements auraient été modifiés.

Ce tableau est le résultat du travail effectué en collaboration avec des représentants de la CNIL, du réseau « Supdpo », des chefs d'établissement du second degré, des responsables de la sécurité des systèmes d'information en fonction au sein des établissements, des délégués à la protection des données ainsi que des membres des commissions d'examen des vœux.

Il n'a pas vocation à être exhaustif.

Pour chaque événement redouté, il vous appartient de déterminer les mesures de sécurité existantes ou déjà engagées qui permettront de rendre ces risques acceptables (colonne « mesures ») en évaluant au regard de ces mesures, la vraisemblance des menaces ainsi que la gravité des impacts sur la vie privée des personnes. Les colonnes « vraisemblance » et « gravité » figurant dans le tableau ont été pré-remplies dans le cadre des travaux collaboratifs mentionnés ci-dessus. Elles doivent toutefois faire l'objet d'une révision de votre part. Ainsi, par exemple, la vraisemblance d'une menace relative aux catastrophes naturelles ne pourra pas être identique d'un territoire à l'autre.

Vous pourrez trouver en annexe un tableau récapitulant les principales mesures qui peuvent être mises en œuvre pour réduire les risques.

Dans le cas où les risques ainsi identifiés ne pourraient pas être jugés acceptables compte tenu des mesures existantes ou prévues, il conviendra de proposer des mesures complémentaires et de ré-estimer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels (tableau 2).

3.2.1. Echelle de gravité

Niveaux	Descriptions génériques des impacts (directs et indirects)
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté.
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés
3. Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives.
4. Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter

3.2.2. Echelle de vraisemblance

Niveaux de vraisemblance	Description générique du niveau de vraisemblance d'une menace donnée
1. Négligeable	Il ne semble pas possible que les sources de risques retenues puissent réaliser la menace

2. Limité	Il semble difficile pour les sources de risques retenues de réaliser la menace
3. Important	Il semble possible pour les sources de risques retenues de réaliser la menace
4. Maximal	Il semble extrêmement facile pour les sources de risques retenues de réaliser la menace

3.2.3. Analyse, estimation des risques par sources et description des mesures

	Type	Sources de risque	Principales menaces	Impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Vraisemblance de l'évènement au regard de la source de risque	Gravité
ACCES ILLEGITIME	Sources humaines internes	Agents	Utilisation de clés USB ou de disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles Vol ou perte du matériel Utilisation d'un réseau non sécurisé en cours de déplacement (ou à domicile, voire dans l'établissement) et/ou d'espaces de stockage partagés (type Dropbox) Exposition accidentelle des données sur internet Sensibilisation aux enjeux de la sécurité informatique insuffisante (mot de passe, verrouillage de sessions,...)	Diffamation donnant lieu à des représailles physiques ou psychiques Décès (ex. : meurtre, suicide, accident mortel) Perte de temps pour réitérer des démarches ou pour attendre de les réaliser Réception de courriers non sollicités (ex. : spams) Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux, réutilisation pour un mailing papier) Publicité ciblée pour des produits de consommation courants Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) Réception de courriers ciblés non sollicités susceptibles de nuire à la réputation des personnes concernées Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel Opportunités ciblées, uniques et non récurrentes, perdues (ex. : refus d'études, de stages ou d'emploi)	Ensemble des mesures mises en œuvre pour la plateforme par le ministère Authentifier les utilisateurs Gérer les habilitations Tracer les accès et gérer les incidents Sécuriser les serveurs + Sensibiliser les utilisateurs Sécuriser les postes de travail Sécuriser l'informatique mobile Protéger le réseau informatique interne Sécuriser les sites web Sauvegarder et prévoir la continuité d'activité Protéger les locaux	Maximale	Maximale
	Sources humaines externes	Destinataires des DCP		Perte d'emploi Simple contrariété par rapport à l'information reçue ou demandée			
	Sources humaines externes	Prestataires	Tentatives d'accès par des sociétés commerciales en vue de réaliser des démarches publicitaires auprès des étudiants (cf. proposition de formations etc.) Politique d'accès aux données par les prestataires insuffisantes				Limité

	Sources humaines externes	Pirates informatiques	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données Rançongiciel	Peur de perdre le contrôle de ses données Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale)		Maximale	Maximale
	Sources humaines externes	Anciens employés	Absence ou insuffisance de politique de gestion des habilitations	Perte de temps pour paramétrer ses données Affection psychologique mineure mais objective (diffamation, réputation)		Maximale	Limité
	Sources humaines externes	Délinquant	Accès aux locaux, vol de matériel pendant une éventuelle occupation des locaux par des personnes extérieures à l'établissement	Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance)		Négligeable	Négligeable
	Sources non humaines	Codes malveillants d'origine inconnue (virus, vers...)	Phishing, keylogger...	Sentiment d'atteinte à la vie privée sans préjudice irrémédiable		Maximale	Maximale
	Sources humaines	Télétravail	Accès de tiers (conjoint, enfant, colocataire) aux données	Intimidation sur les réseaux sociaux		Limité	Limité
	Sources non humaines	Epidémies	Confinement entraînant la nécessité d'un travail à domicile, avec accès de tiers (conjoint, enfant, colocataire) aux données	Sentiment d'atteinte à la vie privée et de préjudice irrémédiable Victime de chantage Cyberbullying et harcèlement moral Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)		Négligeable	Négligeable
MODIFICATION NON DESIREE	Sources humaines internes	Salariés	Utilisation de clés USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles Vol ou perte du matériel Utilisation de réseaux non sécurisés en cours de déplacement et/ou d'espaces de stockage partagé (type Dropbox) - Exposition accidentelle des données sur internet Sensibilisation aux enjeux de la sécurité informatique insuffisante (mot de passe, verrouillage de sessions,...)	Décès (ex. : meurtre, suicide, accident mortel) Perte de temps pour réitérer des démarches ou pour attendre de les réaliser Données non mises à jour (ex. : poste antérieurement occupé) Opportunités ciblées, uniques et non récurrentes, perdues (ex. : refus d'études, de stages ou d'emploi) Perte d'emploi Simple contrariété par rapport à l'information reçue ou demandée Peur de perdre le contrôle de ses données	Ensemble des mesures mises en œuvre pour la plateforme par le ministère Gérer les habilitations Tracer les accès et gérer les incidents Sauvegarde + Sensibiliser les utilisateurs – et guide sur usage plateforme Centralisation de la gestion des comptes utilisateurs	Maximale	Maximale
	Sources humaines internes	Administrateurs informatiques	Partage de comptes Absence ou mauvaise gestion des habilitations	Perte de temps pour paramétrer ses données Affection psychologique mineure mais objective	Sécuriser les postes de	Maximale	Maximale

Sources humaines externes	Destinataires des DCP	Utilisation de clés USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles Vol ou perte du matériel Utilisation de réseaux non sécurisés en cours de déplacement et/ou d'espace de stockage partagé (type Dropbox) Exposition accidentelle des données sur internet Sensibilisation aux enjeux de la sécurité informatique insuffisante (mot de passe, verrouillage de sessions,...)	(diffamation, réputation) Affection psychologique grave (ex. : dépression, développement d'une phobie) Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression)	travail Sécuriser l'informatique mobile Protéger le réseau informatique interne Sécuriser les sites web Sauvegarder et prévoir la continuité d'activité	Maximale	Maximale
	Sources humaines externes	Pirates informatiques	Risques d'intrusion sur le réseau de l'établissement pour modifier les données Piratage de boîtes mails (compromission du mot de passe d'accès) ou d'espaces de stockage partagés contenant des données		Maximale	Maximale
	Sources humaines externes	Visiteurs	Modifications accidentelles des données		Limitée	Négligeable
	Sources humaines externes	Anciens employés	Absence ou insuffisance de politique de gestion des habilitations		Maximale	Négligeable
	Sources humaines externes	Maintenance	Modification accidentelle dans le cas d'une opération de maintenance sur les serveurs ou les ordinateurs		Limitée	Négligeable
	Sources humaines externes	Délinquant	Accès aux locaux et vol de matériel ou dégradation pendant l'occupation des locaux par des personnes extérieures à l'établissement autre qu'étudiants et employés		Négligeable	Négligeable
	Sources humaines externes	Activités industrielles environnantes	Accident industriel entraînant la destruction des serveurs/ ordinateurs		Négligeable	Négligeable
	Sources non humaines	Codes malveillants d'origine inconnue (virus, vers...)	Phishing, keylogger...		Maximale	Maximale
	Sources non humaines	Télétravail	Accès de tiers (conjoint, enfant, colocataire) aux données et modifications accidentelles		Limitée	Limitée
	Sources non humaines	Eau (canalisations, cours d'eau...)	Inondation qui détruirait l'infrastructure réseau et système d'une composante		Négligeable	Négligeable
	Sources non humaines	Catastrophes naturelles	Destruction des serveurs et des ordinateurs		Négligeable	Négligeable
	Sources non humaines	Animaux	Suppression accidentelle des données par un animal (télétravail)		Négligeable	Négligeable

DISPARITION DE DONNEES	Sources humaines internes	Salariés	Utilisation de clés USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles Vol ou perte du matériel Utilisation de réseaux non sécurisés en cours de déplacement et/ou d'espace de stockage partagé (type Dropbox) Exposition accidentelle des données sur internet Sensibilisation aux enjeux de la sécurité informatique insuffisante (mot de passe, verrouillage de sessions,...)	Perte de temps pour réitérer des démarches ou pour attendre de les réaliser	Ensemble des mesures mises en œuvre pour la plateforme par le ministère Gérer les habilitations Tracer les accès et gérer les incidents Sauvegarde + Sensibiliser les utilisateurs – et guide sur usage plateforme	Négligeable	Maximale
	Sources humaines internes	Administrateurs informatiques	Partage de comptes Absence ou mauvaise gestion des habilitations		Négligeable	Maximale	
	Sources humaines externes	Destinataires des DCP	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles Vol ou perte du matériel Utilisation de réseaux non sécurisés en cours de déplacement et/ou d'espace de stockage partagé (type Dropbox) Exposition accidentelle des données sur internet Sensibilisation aux enjeux de la sécurité informatique insuffisante (mot de passe, verrouillage de sessions,...)		Négligeable	Maximale	
	Sources humaines externes	Pirates informatiques	Intrusion sur le réseau de l'établissement pour effacer les données		Limitée	Maximale	
	Sources humaines externes	Visiteurs	Effacement accidentel des données		Limitée	Négligeable	
	Sources humaines externes	Anciens employés	Absence ou insuffisance de politique de gestion des habilitations		Limitée	Négligeable	
	Sources humaines externes	Personnels d'entretien	Nettoyage sur un poste dont la session n'a pas été bloquée		Limitée	Négligeable	
	Sources humaines externes	Maintenance	Suppression accidentelle dans le cas d'une opération de maintenance sur les serveurs ou les ordinateurs		Limitée	Négligeable	
	Sources humaines externes	Délinquant	Accès aux locaux et vol de matériel ou dégradation pendant l'occupation des locaux par des personnes extérieures à l'établissement autre qu'étudiants et employés.		Limitée	Négligeable	
	Sources humaines externes	Activités industrielles environnantes	Accident industriel entraînant la destruction des serveurs/ ordinateurs		Négligeable	Négligeable	

	Sources non humaines	Codes malveillants d'origine inconnue (virus, vers...)	Phishing, keylogger...		Sensibilisation des personnels- charte télétravail	Limitée	Maximale
	Sources non humaines	Télétravail	Accès de tiers (conjoint, enfant, colocataire) aux données qui efface les données accidentellement			Négligeable	Négligeable
	Sources non humaines	Eau (canalisations, cours d'eau...)	Inondation qui détruirait l'infrastructure réseau et système d'une composante			Négligeable	Négligeable
	Sources non humaines	Animaux	Effacement accidentel des données par un animal (télétravail)			Négligeable	Négligeable

Risques	Acceptable / améliorable	Mesures correctives	Risque résiduel
ACCES ILLEGITIME	Acceptable	Na	
MODIFICATION NON DESIREE	Acceptable	Na	
DISPARITION DE DONNEES	Acceptable	na	

4. Validation de l'analyse d'impact

4.1. Eléments utiles à la validation

4.1.1. Synthèse relative à la conformité au RGPD

Finalités	Evaluation Acceptable / améliorable
Mesures garantissant la proportionnalité et la nécessité du traitement	
Finalités : déterminées, explicites et légitimes	Acceptable
Fondement : licéité du traitement, interdiction du détournement de finalité	Acceptable
Minimisation des données : adéquates, pertinentes et limitées	Acceptable
Qualité des données : exactes et tenues à jour	Acceptable
Durées de conservation : limitées	Acceptable
Mesures protectrices des droits des personnes des personnes concernées	
Information des personnes concernées (traitement loyal et transparent)	Améliorable (voir affiche 2024)
Recueil du consentement	Sans objet
Exercice des droits d'accès et à la portabilité	Acceptable
Exercice des droits de rectification	Acceptable
Exercice des droits de limitation du traitement et d'opposition	Acceptable
Sous-traitance : identifiée et contractualisée	Acceptable
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	Sans objet

4.1.2. Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données

Finalités	Evaluation Acceptable / améliorable
Mesures portant spécifiquement sur les données du traitement	
Chiffrement	Acceptable
Anonymisation	Acceptable
Cloisonnement des données (par rapport au reste du système d'information)	Acceptable
Contrôle des accès logiques des utilisateurs	Acceptable
Traçabilité (journalisation)	Acceptable
Contrôle d'intégrité	Acceptable
Archivage	Acceptable
Sécurité des documents papier	Acceptable
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	
Sécurité de l'exploitation	Acceptable
Lutte contre les logiciels malveillants	Acceptable
Gestion des postes de travail	Acceptable
Sécurité des sites web	Acceptable
Sauvegardes	Acceptable
Maintenance	Acceptable
Sécurité des canaux informatiques (réseaux)	Acceptable
Surveillance	Acceptable
Contrôle d'accès physique	Acceptable

Sécurité des matériels	Acceptable
Éloignement des sources de risques	Acceptable
Protection contre les sources de risques non humaines	Acceptable
Mesures organisationnelles (gouvernance)	
Organisation	Acceptable
Politique (gestion des règles)	Acceptable
Gestion des risques	Acceptable
Gestion des projets	Acceptable
Gestion des incidents et des violations de données	Acceptable
Gestion des personnels	Acceptable
Relations avec les tiers	Acceptable
Supervision	Acceptable

4.1.3. Cartographie des risques liés à la sécurité des données

4.1.4. Plan d'action

Mesures complémentaires demandées	Responsable	Jalon
Insertion information sur site internet	IFSI	immédiatement
Réalisation affichage porte ouverte 2024	IFSI	2024

4.2. Validation formelle

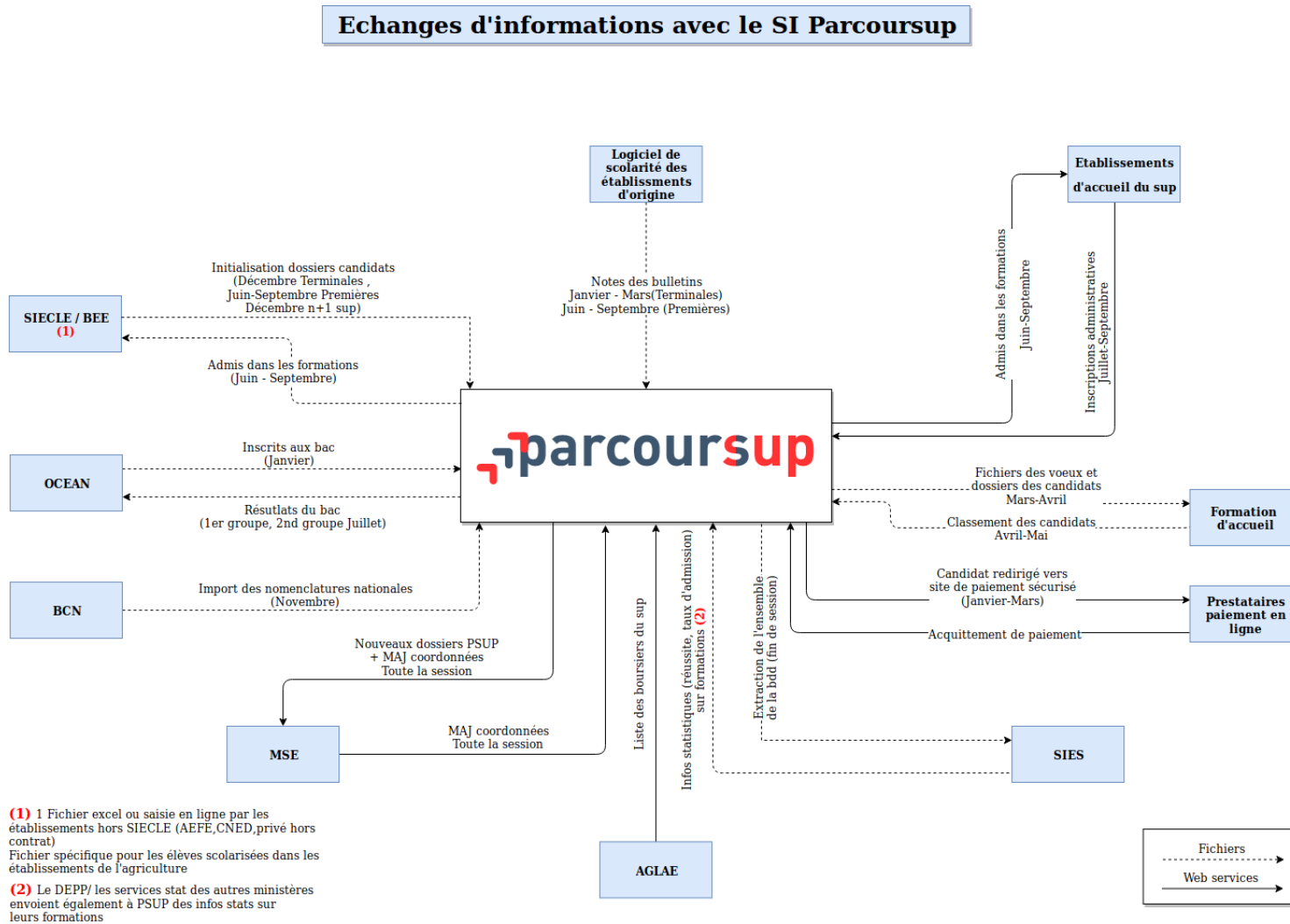
Avis du délégué ministériel à la protection des données : FAVORABLE (AIPD CADRE)

Avis du délégué à la protection des données de l'établissement : FAVORABLE

5. Annexes

- Présentation de l'écosystème numérique local et des échanges d'information avec le SI Parcoursup
- Convention de sous-traitance
- Etapes juridiques du déploiement de Parcoursup
- Liste des principales mesures de sécurité pouvant être prises

5.1. Présentation de l'écosystème numérique local et des échanges d'information avec le SI Parcoursup



5.2. Convention de sous-traitance

Voir convention signée via plateforme

5.3. Etapes juridiques du déploiement de Parcoursup

- Demande d'avis sur projet d'arrêté autorisant la mise en œuvre du traitement de données à caractère personnel dénommé Parcoursup déposé auprès de la CNIL ;
- Délibération de la CNIL n° 2018-011 du 18 janvier 2018 portant avis sur un projet d'arrêté ;
- Arrêté du 19 janvier 2018 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup » ayant pour finalité le recueil des vœux des candidats dans le cadre de la gestion de la procédure nationale de préinscription dans une formation du premier cycle de l'enseignement supérieur ;
- Loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants (dite loi ORE) modifiant l'article L. 612-3 du code de l'éducation qui fixe les modalités d'accès aux formations initiales du premier cycle de l'enseignement supérieur. L'ensemble des textes législatifs et réglementaires applicables sont recensés sur le [site ministériel](#) ;
- Demande d'avis sur modification du projet d'arrêté autorisant la mise en œuvre du traitement de données à caractère personnel dénommé Parcoursup déposé auprès de la CNIL ;
- Délibération n° 2018-119 de la Commission nationale de l'informatique et des libertés en date du 22 mars 2018 ;
- Arrêté du 28 mars 2018 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup » ayant pour finalité le recueil et le traitement des vœux des candidats dans le cadre de la gestion de la procédure nationale de préinscription dans une formation du premier cycle de l'enseignement supérieur ;
- Décision du 30 novembre 2018 désignant le SCN Parcoursup comme opérateur de service essentiel du secteur de l'éducation
- Etablissement d'une convention cadre de sous-traitance entre le service à compétence nationale Parcoursup et les établissements d'enseignement supérieur utilisant l'outil d'aide à la décision (février 2019) ;
- Inscription du traitement Parcoursup sur le registre des traitements du ministère de l'enseignement supérieur et de la recherche (fiche n° MESRI/DGESIP/002) ;
- Arrêté du 18 mai 2020 portant homologation du téléservice Parcoursup ;
- Rédaction d'une AIPD Parcoursup et d'une AIPD cadre relative aux traitements réalisés par les établissements d'enseignement supérieur.

5.4. Liste des principales mesures de sécurité pouvant être prises

1 Sensibiliser les utilisateurs	
1	Informez et sensibilisez les personnes manipulant les données
2	Rédigez une charte informatique et lui donner une force contraignante
2 Authentifier les utilisateurs	
3	Définissez un identifiant (login) unique à chaque utilisateur
4	Adoptez une politique de MdP utilisateur conforme aux recommandations CNIL (1)
5	Obligez l'utilisateur à changer son mot de passe après réinitialisation
6	Limitez le nombre de tentatives d'accès à un compte
3 Gérer les habilitations	
7	Définissez des profils d'habilitation
8	Supprimez les permissions d'accès obsolètes
9	Réaliser une revue annuelle des habilitations
4 Tracer les accès et gérer les incidents	
10	Prévoyez un système de journalisation
11	Informez les utilisateurs de la mise en place du système de journalisation
12	Protégez les équipements de journalisation et les informations journalisées
13	Prévoyez les procédures pour les notifications de violation de données à caractère personnel
5 Sécuriser les postes de travail	
14	Prévoyez une procédure de verrouillage automatique de session
15	Utilisez des antivirus régulièrement mis à jour
16	Installez un « pare-feu » (firewall) logiciel
17	Recueillez l'accord de l'utilisateur avant toute intervention sur son poste
6 Sécuriser l'informatique mobile	
18	Prévoyez des moyens de chiffrement des équipements mobiles
19	Faites des sauvegardes ou synchronisations régulières des données
20	Exigez un secret pour le déverrouillage des smartphones
7 Protéger le réseau informatique interne	
21	Limitez les flux réseau au strict nécessaire
22	Sécurisez les accès distants des appareils informatiques nomades par VPN
23	Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
8 Sécuriser les serveurs	
24	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées
25	Installez sans délai les mises à jour critiques
26	Assurez une disponibilité des données
9 Sécuriser les sites web	
27	Utilisez le protocole TLS et vérifiez sa mise en œuvre
28	Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url
29	Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu
30	Mettez un bandeau de consentement pour les cookies non nécessaires au service
10 Sauvegarder et prévoir la continuité d'activité	
31	Effectuez des sauvegardes régulières
32	Stockez les supports de sauvegarde dans un endroit sûr
33	Prévoyez des moyens de sécurité pour le convoyage des sauvegardes
34	Prévoyez et testez régulièrement la continuité d'activité
11 Archiver de manière sécurisée	
35	Mettez en œuvre des modalités d'accès spécifiques aux données archivées
36	Détruisez les archives obsolètes de manière sécurisée
12 Encadrer la maintenance et la destruction des données	
37	Enregistrez les interventions de maintenance dans une main courante
38	Encadrez par un responsable de l'organisme les interventions par des tiers

39	Effacez les données de tout matériel avant sa mise au rebut
13	Gérer la sous-traitance
40	Prévoyez une clause spécifique dans les contrats des sous-traitants
41	Prévoyez les conditions de restitution et de destruction des données
42	Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
14	Sécuriser les échanges avec d'autres organismes
43	Chiffrez les données avant leur envoi
44	Assurez-vous qu'il s'agit du bon destinataire
45	Transmettez le secret lors d'un envoi distinct et via un canal différent
15	Protéger les locaux
46	Restreignez les accès aux locaux au moyen de portes verrouillées
47	Installez des alarmes anti-intrusion et vérifiez-les périodiquement
16	Encadrer les développements informatiques
48	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux
49	Évitez les zones de commentaires ou encadrez-les strictement
50	Testez sur des données fictives ou anonymisées
17	Utiliser des fonctions cryptographiques
51	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues
52	Conservez les secrets et les clés cryptographiques de manière sécurisée