MINISTÈRE DE LA JUSTICE
Liberté
Égalité
Fraternité

ÉNAP
ÉCOLE NATIONALE
D'ADMINISTRATION PÉNITENTIAIRE



MINISTÈRE DE LA JUSTICE

ÉCOLE NATIONALE D'ADMINISTRATION PÉNITENTIAIRE (Énap)

Secrétariat Général
Département des Systèmes d'Information
Délégué à la protection des données

Contrat de sous-traitance relatif à la protection des données à caractère personnel portant sur le service de restauration collective et de prestations annexes sur le site de l'ÉNAP

Marché 2026-11

Table des matières :

CONTRAT DE SOUS-TRAITANCE RELATIF A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL 1

PORTANT SUR : 1

1. OBJET 4

2. DÉFINITIONS 4

3. QUALIFICATION JURIDIQUE DES PARTIES 5

4. DUREE DU CONTRAT 5

5. IDENTIFICATION DES TRAITEMENTS (..... 6

6. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DE L'Énap 8

7. DROITS ET OBLIGATIONS DE l'Énap 8

8. INSTRUCTIONS DE L'Énap 9

9. DÉCLARATION DU PRESTATAIRE 9

10. SOUS - TRAITANCE ULTÉRIEURE 9

11. FLUX TRANSFRONTIÈRES 10

12. CONFIDENTIALITÉ RENFORCÉE 10

13. OBLIGATION DE SÉCURITÉ 10

14. DROIT D'INFORMATION DES PERSONNES CONCERNEES 11

15. EXERCICE DES DROITS DES PERSONNES CONCERNEES 11
15.1. Droit d'information des personnes concernées 11
15.2. Exercice des droits des personnes 11

16. VIOLATION DE DONNÉES 11

17. AIDE ET ASSISTANCE DE l'ÉNAP 12
17.1 AIDE ET ASSISTANCE CONCERNANT LE DROIT DE PERSONNES 12
17.2 AIDE ET ASSISTANCE CONCERNANT LA SÉCURITÉ DU TRAITEMENT 13
17.3 AIDE ET ASSISTANCE CONCERNANT LA NOTIFICATION DE VIOLATIONS DE DONNÉES 13
17.4 AIDE ET ASSISTANCE CONCERNANT L'ANALYSE D'IMPACT 13

18. CONTRÔLE DE LA CNIL 14

19. SORT DES DONNÉES À LA FIN DU CONTRAT 14

20. REGISTRE DES OPÉRATIONS DE TRAITEMENT 14

21. DOCUMENTATION 15

22. AUDIT 15
23. RESPONSABILITÉ 16
24. RÉPARATION DU PRÉJUDICE 16
25. ASSURANCE RESPONSABILITE CIVILE 17
26. RÉVISION 17
27. DÉSIGNATION D'UN REPRÉSENTANT 17
28. DÉLÉGUÉ À LA PROTECTION DES DONNÉES POUR L'ÉNAP 17
29. DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU SOUS-TRAITANT 17
30. ANNEXES 18
..... 19
ENGAGEMENT DE CONFIDENTIALITE 19
MESURES DE SECURITE MISE EN ŒUVRE PAR LE PRESTATAIRE 21
1. Gestion de la sécurité 21
2. Protection antivirale 22
4. Sauvegardes et restauration 22
5. Authentification 23
6. Confidentialité et intégrité des flux 23
7. Imputabilité, traçabilité 24
8. Personnels en charge des prestations 24
9. Qualifications et expérience, formations et sensibilisation dans le domaine de la SSI des personnels en charge des prestations 24
10. Exigences de sécurité concernant les personnels extérieurs (maintenance, entretien…). 25
TABLEAU DES SOUS-TRAITANTS ULTERIEURS 26

1. OBJET

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les éventuelles opérations de traitement de données à caractère personnel rendues nécessaires dans l'exécution du marché 2026-11.

La société XXXXXX est sous-traitant au sens de l'article 28 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après « RGPD »). Elle est désignée en qualité de prestataire, dans le présent contrat. Le prestataire est informé que le respect de la règlementation en matière de protection des données à caractère personnel est un élément fondamental pour l'Énap..

Le prestataire déclare présenter les garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et de la réglementation actuelle et future.

Le prestataire s'engage à respecter, sans réserve, à l'ensemble des obligations prévues dans la présente annexe afin de se conformer aux dispositions de l'article 28 et de l'article 32 du règlement général de protection des données applicable en France et dans l'Union européenne dans le domaine de la protection des données à caractère personnel.

Le contrat de sous-traitance est composé des éléments indivisibles suivants :

1. Le présent contrat de sous-traitance ;
2. l'engagement de confidentialité (annexe 1) ;
3. les mesures de sécurité mise en œuvre par le prestataire (annexe 2) ;
4. tableau des sous-traitances ultérieures (annexe 3) ;

2. DÉFINITIONS

Pour le présent contrat, les termes ci-dessous ont entre les parties la signification suivante :

- « *destinataire* », la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

- « *données à caractère personnel* » : désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

- « *finalité* » : désigne les objectifs principaux assignés au traitement et aux fonctions substantielles mises en œuvre.

- « *personne concernée* » : désigne les personnes physiques identifiables ou identifiées dont les données à caractère personnel sont collectées et intégrées dans le traitement de données à caractère personnel.

- « *traitement de données à caractère personnel* » : désigne toute opération ou ensemble d'opérations portant sur des données à caractère personnel, quel que soit le procédé utilisé telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

- « *violation de données à caractère personnel* » : désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

- « *sous-traitant* », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

- « *responsable du traitement* », 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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

- « *RGPD* » : désigne le Règlement Général de la protection des données, règlement UE 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

3. QUALIFICATION JURIDIQUE DES PARTIES

Au sens du RGPD et pour la bonne application des présentes :

- L'Énap a la qualité de responsable de traitement ;

- Le prestataire XXXXXX a la qualité de sous-traitant.

4. DUREE DU CONTRAT

Le présent contrat démarre à compter du 05 juin 2027 et s'achève le 04 juin 2028.
Il est reconduit tacitement par période d'un an, sans pouvoir excéder une durée maximale de 5 ans et sauf dénonciation par l'une des parties par courrier recommandé avec réception respectant un préavis de trois mois.

5. IDENTIFICATION DES TRAITEMENTS (Article 28 § 3 du RGPD)

Les éléments d'identification du traitement couverts par le présent contrat de sous-traitance sont les suivants :

TRAITEMENT DES DONNEES POUR LA FACTURATION DE LA RESTAURATION DES USAGERS DU RESTAURANT DE L'ENAP MARCHE 2026-11	
Objet et Finalité du traitement	Traitement de la facturation des repas des usagers du restaurant de l'Enap
Fondement juridique du traitement (art.6 du RGPD)	Art 6 B : exécution d'un contrat
Durée du traitement	La même durée que l'article 4 du CCAP du marché 2026-11.
Transfert de données hors pays adéquate.	Pas de transfert hors UE ou pays adéquate au sens de l'article 45 du RGPD
Mesure(s) juridique(s) mise(nt) en place pour le transfert hors pays adéquate.	Sans objet
Nature du traitement	○ Enregistrement ○ Conservation ○ Consultation ○ Utilisation ○ Effacement ○ Destruction
Types de données	• Données d'identité : (tels que nom, prénom, identifiant Csn (Id Enap), • Données vie personnelle : type et nombre de repas pris • Données ordre économique : type de droits sur les repas, subvention

Durée de conservation des données	• Conservation des données 5 ans pour ce qui concerne les données de facturation
Catégories de personnes concernées	• Personnels de l'ENAP • Apprenants de l'Enap • Intervenants de l'Enap
Destinataire des données	• Les personnels habilités du prestataire • Les gestionnaires financiers pour la personne publique
Coordonnées du DPO du sous-traitant	○ A compléter par le prestataire
AIPD obligatoire	○ Non

6. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DE L'Énap

Le sous-traitant s'engage à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance,

2. traiter les données conformément aux instructions documentées du responsable de traitement figurant au présent contrat de sous-traitance. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public,

3. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat,

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
   - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
   - reçoivent la formation nécessaire en matière de protection des données à caractère personnel,

5. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut, article 25 du RGPD. (privacy by design, privacy by default.).

7. DROITS ET OBLIGATIONS DE l'Énap (Article 28 § 3 du RGPD)

L'Énap s'engage à :

- fournir au prestataire toutes les informations et instructions documentées nécessaires à la bonne exécution du traitement ;
- indiquer au prestataire toute évolution des traitements ;
- fournir au prestataire les coordonnées de son interlocuteur ou, le cas échéant, de son délégué à la protection des données ;
- notifier les violations de données auprès de l'autorité compétente ;
- respecter ses obligations en matière de protection des données.

L'Énap dispose du droit de :

- demander au prestataire, la communication de tout élément, pièce ou documentation permettant de garantir qu'il respecte les exigences du RGPD et du présent avenant ;
- formuler des objections et des réserves sur un sous-traitant ultérieur recruté par le prestataire ;
- réaliser des audits ou des inspections auprès du prestataire afin de s'assurer du respect par ce dernier des exigences du RGPD et de l'avenant ;
- demander l'assistance du prestataire sur la mise en œuvre d'une étude d'impact (AIPD), article 35 du RGPD et la mise en œuvre de l'exercice des droits des personnes concernées,

sur la coopération avec la CNIL, sur la mise en œuvre des moyens de sécurité du traitement article 32 du RGPD ou encore sur la mise en œuvre des notifications de violations de données auprès de la CNIL ou des personnes concernées.

8. INSTRUCTIONS DE L'Énap (Article 28 du RGPD)

Le prestataire s'engage à ne traiter les données à caractère personnel dans le cadre du contrat que dans le respect des instructions documentées, communiquées par l'Énap au fur et à mesure de l'exécution de la prestation.

Les instructions documentées sont communiquées au prestataire par écrit, ou sous toute forme choisie par l'Énap telle que par document, courrier électronique ou compte rendu de réunion, sans que cette liste ne soit exhaustive.

Le prestataire informe immédiatement l'Énap si, selon lui, une instruction de l'Énap constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données. Cette information doit être adressée par écrit et dans un temps compatible avec sa prise en compte par l'Énap.

9. DÉCLARATION DU PRESTATAIRE (Article 28 § 1 du RGPD)

Le prestataire est informé que le respect de la règlementation en matière de protection des données à caractère personnel est un élément fondamental pour l'Énap.

À ce titre, le prestataire déclare :

- présenter toutes les garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée ;
- disposer d'une politique informatique et libertés conforme au RGPD.

10. SOUS - TRAITANCE ULTÉRIEURE (Article 28 § 2 du RGPD)

Le prestataire est autorisé par l'Énap à recruter d'autres sous-traitants dans le cadre du traitement.

Les autres sous-traitants recrutés par le prestataire sont listés en annexe 3 du présent avenant.

Dans tous les cas, le prestataire s'engage à :

- recruter un sous-traitant présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et du présent avenant mais également garantisse la protection des droits de la personne concernée ;
- signer avec l'autre sous-traitant un contrat faisant référence au présent avenant, et imposant à son sous-traitant les mêmes obligations en matière de protection des données à caractère personnel que celles fixées dans le présent avenant et au contrat ;
- tenir à la disposition l'Énap la liste, annexées au présent avenant, des autres sous-traitants recrutés dans le cadre du contrat ayant accès à des données à caractère personnel ;
- informer l'Énap de tout changement prévu concernant l'ajout ou le remplacement des autres sous-traitants, donnant ainsi à l'Énap la possibilité d'émettre des objections et des réserves.

Le prestataire demeure pleinement responsable vis-à-vis l'Énap et des tiers des actes de son propre sous-traitant. Il appartient donc au prestataire de prendre toutes les mesures nécessaires afin de garantir le respect par son sous-traitant des dispositions du RGPD, l'Énap n'ayant aucun contrôle sur les autres sous-traitants.

Si le prestataire souhaite changer un ou plusieurs des autres sous-traitants, il doit en aviser préalablement l'Énap avec un préavis minimum d'un (1) mois durant lequel l'Énap peut émettre des « *objections* ».

En cas d'objections aux changements demandés, les parties s'engagent à se réunir et en discuter de bonne foi.

Si, à l'issue de cette réunion, l'Énap maintien ses objections, il peut procéder à la résiliation du contrat moyennant un préavis de six (6) mois et ce, sans indemnité, lorsque :

- l'Énap est en précontentieux ou contentieux avec l'autre sous-traitant ;
- l'Énap apporte la preuve que le fait d'accepter l'autre sous-traitant lui ferait courir un risque de conflit d'intérêt ou un risque économique ou juridique ou de réputation.

11. FLUX TRANSFRONTIÈRES (Article 44 du RGPD)

Aucun transfert de données à caractère personnel ne peut intervenir en dehors de l'Union européenne ou d'un pays adéquat au sens de l'article 45 du RGPD sans l'accord préalable, exprès et spécial de l'Énap.

En cas d'accord formalisé de l'Énap, le prestataire s'engage à respecter l'ensemble des obligations en matière de transfert de données à caractère personnel vers un pays tiers et notamment à conclure un acte juridique contraignant avec le destinataire des données comme des clauses contractuelles types ou des BCR (règles d'entreprise contraignantes ou Binding Corporate Rule), (article 47 du RGPD), et d'en justifier auprès de l'Énap.

12. CONFIDENTIALITÉ RENFORCÉE (Article 28 §3 b) du RGPD)

Le prestataire s'engage à faire signer par toutes les personnes susceptibles d'accéder aux données à caractère personnel de l'Énap un engagement individuel de confidentialité conforme à l'annexe 1.

Le prestataire doit être en mesure de confirmer le respect de cette obligation auprès de l'Énap, à première demande, en communiquant la liste des personnes susceptibles d'accéder aux données à caractère personnel, accompagnée des annexes signées par lesdites personnes.

Le prestataire s'engage à former les personnes susceptibles d'accéder aux données à caractère personnel de l'Énap sur les mesures de sécurité à mettre en œuvre. Le plan de formation annuel est communiqué à l'Énap.

Le prestataire s'engage à ce que ses éventuels sous-traitants ultérieurs soient également tenus par ces obligations spécifiques et soient en mesure d'en justifier auprès de l'Énap, à sa première demande.

13. OBLIGATION DE SÉCURITÉ (Article 28 §3 c) du RGPD)

Le prestataire est tenu de mettre en œuvre les mesures organisationnelles et techniques de nature à lutter contre la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

À ce titre, le prestataire met en œuvre les mesures techniques et organisationnelles définies en annexe 2.

L'annexe 2 doit être maintenue à jour et tenir compte des évolutions technologiques. Aucune modification ne peut être apportée à l'annexe 2 qui n'ait été préalablement portée à la connaissance de l'Énap et approuvée par elle.

14. DROIT D'INFORMATION DES PERSONNES CONCERNEES (Article 12 du RGPD)

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

15. EXERCICE DES DROITS DES PERSONNES CONCERNEES (Article 15 du RGPD)

15.1. Droit d'information des personnes concernées

De manière générale, il appartient au Responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Toutefois et lorsque l'exécution du Contrat nécessite une collecte de données à la charge du Sous-traitant, ce dernier doit, au moment de la collecte des données par ses soins, fournir aux personnes l'information relative aux traitements de données qu'il réalise pour le compte du Responsable de traitement. En pareil cas, la formulation et le format de l'information doivent être convenus avec le Responsable de traitement avant la collecte de données.

15.2. Exercice des droits des personnes

Le Sous-traitant s'engage, dans la mesure du possible, à aider le Responsable de traitement à donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit à ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage), droit au retrait du consentement. Le Sous-traitant met à la disposition du Responsable de traitement les moyens techniques ou procédures nécessaires pour répondre aux demandes précitées.

Lorsque les personnes concernées exercent leurs droits auprès du Sous-traitant, celui-ci doit faire suivre ces demandes, dès réception et dans un délai maximum de soixante-douze (72) heures par courrier électronique au Responsable de traitement, aux coordonnées DPO indiquées à l'article 3 de la présente Annexe. Dans le cas où l'exercice des droits des personnes est sous-traité au Sous-traitant, les modalités seront à convenir dans une annexe dédiée.

16. VIOLATION DE DONNÉES (Article 33 du RGPD)

Il appartient à l'Énap, et à elle seule, de notifier les éventuelles violations de sécurité à la CNIL.

Le prestataire s'engage à notifier à l'Énap, dans les meilleurs délais et, si possible au plus tard 24 heures après en avoir pris connaissance, toute violation de donnée à caractère personnel qu'il aurait subi.

En cas de retard dans la communication de la violation, le prestataire doit accompagner sa notification des motifs expliquant ce retard.

Le prestataire devra en tout état de cause respecter les attendus de l'article 33 du RGPD.

La violation de données est communiquée aux interlocuteurs désignés par à l'Énap ou, à défaut, au délégué à la protection des données désigné par à l'Énap.

La notification doit, au minimum, préciser :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

Si le prestataire est dans l'incapacité de fournir l'ensemble de ces informations au même moment, cela ne l'exonère pas de son obligation de notifier à l'Énap la violation des données accompagnée de l'ensemble des informations à sa disposition, le reste devant être communiqué dès prise de connaissance.

En cas de violation de données, le prestataire prend, dès que possible, toutes les mesures nécessaires pour remédier et diminuer l'impact de la violation et informe l'Énap des mesures prises et des résultats attendus et constatés.

Le prestataire s'engage à collaborer activement avec l'Énap pour qu'elle soit en mesure de répondre à ses obligations réglementaires et contractuelles et notamment pour répondre aux interrogations de la CNIL.

17. AIDE ET ASSISTANCE DE l'ÉNAP (Article 28 § 3 e) f) h) du RGPD)

17.1 AIDE ET ASSISTANCE CONCERNANT LE DROIT DE PERSONNES

Le prestataire s'engage à aider et assister l'Énap par l'intermédiaire de mesures techniques et organisationnelles appropriées et en tenant compte de la nature du traitement à s'acquitter de l'obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits.

17.2 AIDE ET ASSISTANCE CONCERNANT LA SÉCURITÉ DU TRAITEMENT

Le prestataire est tenu d'aider et d'assister l'Énap dans le cadre de la mise en œuvre des mesures techniques et organisationnelles appropriées de nature à satisfaire aux obligations de protection et de sécurisation des traitements.

Afin d'apporter une aide appropriée à l'Énap, le prestataire doit s'appuyer sur l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les personnes concernées.

L'Énap reste le seul responsable de la mise en œuvre des propositions formulées par le prestataire.

Le prestataire informe sans délai, par écrit, l'Énap en cas d'identification d'une vulnérabilité technique ou d'une défaillance organisationnelle.

17.3 AIDE ET ASSISTANCE CONCERNANT LA NOTIFICATION DE VIOLATIONS DE DONNÉES

Le prestataire s'engage à assister et aider l'Énap en cas de violation de données afin que l'Énap soit en capacité de communiquer l'ensemble des informations demandées par le RGPD dans le délai imparti, qu'il s'agisse de la notification à la CNIL ou aux personnes concernées. (Articles 33 et 34 du RGPD)

Pour ce faire, le prestataire s'engage à fournir l'ensemble des informations qu'il dispose et toutes les informations demandées par le RGPD concernant le traitement et la violation de données.

En outre, le prestataire s'engage à apporter toute aide ou assistance technique dont pourrait bénéficier l'Énap afin de limiter les effets de la violation de données ou d'interrompre ladite violation.

17.4 AIDE ET ASSISTANCE CONCERNANT L'ANALYSE D'IMPACT

Le prestataire informe l'Énap dès lors qu'il a connaissance d'un type de traitement qui, compte tenu de sa nature, du contexte et des finalités, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Le prestataire s'engage à aider et assister l'Énap dans la mise en œuvre de l'analyse d'impact en fournissant, à première demande, l'ensemble des informations dont l'Énap a besoin pour réaliser cette analyse d'impact, conformément aux articles 35 et 36 du RGPD.

Le prestataire s'engage à aider et assister l'Énap lorsque ce dernier décide de consulter la CNIL à la suite d'une analyse d'impact ayant indiqué que le traitement présenterait un risque élevé si le traitement ne fait pas l'objet d'une modification.

Le prestataire s'engage à fournir toutes les informations qu'il dispose ainsi qu'une aide et assistance technique afin de proposer des mesures d'atténuation des risques pour les droits et libertés des personnes physiques.

18. CONTRÔLE DE LA CNIL (Article 31 du RGPD)

L'Énap et le prestataire sont tenus de coopérer avec la CNIL, à la demande de celle-ci,

- Dans le cas où le contrôle mené auprès du prestataire concernerait les traitements mis en œuvre au nom et pour le compte de l'Énap, le prestataire s'engage à en informer immédiatement l'Énap et à ne prendre aucun engagement pour elle.
- En cas de contrôle de la CNIL auprès de l'Énap portant notamment sur les prestations délivrées par le prestataire, ce dernier s'engage à coopérer avec l'Énap et à lui fournir toute information dont la CNIL pourrait avoir besoin.
- Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le prestataire en tant que responsable du traitement, ce dernier fait son affaire du contrôle et s'interdit de communiquer ou de faire état des données à caractère personnel de l'Énap
- Dans tous les cas, si le prestataire fait l'objet d'une mise en demeure, d'un avertissement ou d'une condamnation de la CNIL, même dispensée de publication, ce dernier est tenu d'en informer l'Énap sans délai et au plus tard dans les 48h de la décision.

19. SORT DES DONNÉES À LA FIN DU CONTRAT

À l'expiration du contrat et au plus tard le dernier jour du contrat, le prestataire a pour obligation de restituer l'ensemble de ses données à l'Énap.

Il ne saurait y avoir de rétention de la part du prestataire pour quelque raison que ce soit.

Concomitamment à la restitution des données, le prestataire adresse à une attestation de destruction à l'Énap de toutes les copies, sauvegardes, existantes des données détenues par lui ou ses sous-traitants s'ils en existent.

20. REGISTRE DES OPÉRATIONS DE TRAITEMENT (Article 30 §2 du RGPD)

Le prestataire se doit de tenir un « registre des opérations de sous-traitance » et le maintenir à jour.

Pour ce faire, l'Énap communique au prestataire les éléments et informations qui lui seront demandés par le prestataire pour la bonne tenue de son registre.

Le prestataire est tenu de justifier de l'existence de son registre à la première demande de l'Énap ou dans le cadre d'un audit.

Le registre doit comporter à minima les informations suivantes :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
  - la pseudonymisation et le chiffrement des données à caractère personnel ;
  - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le registre est tenu à la disposition de la CNIL.

21. DOCUMENTATION

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

22. AUDIT (Article 28 § 3 h) du RGPD)

L'Énap se réserve le droit de procéder à toute vérification qui lui paraitrait utile pour constater le respect des obligations précitées en procédant à un audit de sécurité auprès du prestataire ou directement auprès d'un de ses sous-traitants.

Le prestataire s'engage à répondre aux demandes d'audit de l'Énap ou d'un tiers de confiance que l'Énap aura sélectionné, reconnu en tant qu'auditeur indépendant, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à l'Énap.

Les audits doivent permettre une analyse du respect par le prestataire de ses obligations au titre des présentes, ainsi qu'au titre de la règlementation applicable en matière de la protection des données à caractère personnel.

L'Énap doit aviser le prestataire par écrit de son intention de faire procéder à un audit moyennant le respect d'un préavis minimum de trente (30) jours. L'Énap ne peut réaliser un audit qu'une fois par an.

L'Énap communique de la manière la plus précise et exhaustive possible le périmètre envisagé, la liste des opérations de contrôle et des outils de mesure qu'il envisage utiliser.

Le déploiement d'un outil est fait sous l'entière responsabilité de l'Énap Le prestataire a le droit de faire analyser l'outil. Si un risque est identifié pour le système d'information et les données du prestataire, ce dernier est en droit de refuser l'utilisation d'un tel outil.

L'Énap communique, le cas échéant, le nom de l'auditeur. Le prestataire a le droit de refuser l'auditeur pour un motif légitime. En cas de désaccord après une troisième proposition, le choix de l'auditeur est fixé par le tribunal compétent. L'Énap est responsable des dommages causés par l'auditeur.

Le prestataire peut refuser l'accès aux zones confidentielles, sécurisées et mutualisées et effectue, dans ce cas, l'audit et en communique les résultats à l'Énap.

Les résultats de l'audit sont formalisés dans un rapport qui doit être adressé au prestataire pour qu'il puisse y insérer ses observations et réserves. Le rapport final doit nécessairement comprendre les observations du prestataire.

Si un désaccord survient concernant des écarts de conformité, l'Énap est en droit de demander une mise en conformité. L'Énap pourra invoquer la non-réalisation de la mise en conformité pour suspendre ses engagements après un délai de deux (2) mois sans indemnité ni pénalité. Ce délai

commencera à courir après réception par le prestataire d'une lettre Recommandée avec Accusé de Réception transmise par l'Énap. Ce courrier contiendra le rapport de l'audit mentionnant les écarts de conformités identifiés qui devront faire l'objet d'une correction.

Cette période peut faire l'objet d'une ou plusieurs prorogations, si l'Énap donne son accord par écrit au prestataire.

La procédure d'audit se termine par la remise par l'Énap d'une lettre clôturant l'audit même en cas d'audit favorable pour le prestataire.

23. RESPONSABILITÉ

Aux termes de l'article 82 du RGPD, le prestataire est tenu pour responsable du dommage causé par le traitement dès lors :

- qu'il n'a pas respecté les obligations prévues dans le RGPD qui incombent spécifiquement aux sous-traitants ou ;
- qu'il a agi en-dehors des instructions licites de l'Énap ou ;
- qu'il a agi contrairement aux instructions licites de l'Énap.

À ce titre, le prestataire est tenu à une obligation de résultat sur :

- le respect de l'article 32 du RGPD et de l'annexe « *mesures de sécurité* » si existante ;
- l'aide et l'assistance qu'il doit à l'Énap ;
- sa réaction en cas de violation de sécurité ;
- ses obligations au titre du droit d'audit de l'Énap ;
- l'assistance due à l'Énap en cas de contrôle de la part de la CNIL.

24. RÉPARATION DU PRÉJUDICE

Lorsque l'une des parties est individuellement responsable d'un dommage du fait du traitement, il est individuellement tenu responsable de ce dommage dans sa totalité afin de garantir aux personnes concernées une réparation effective.

Lorsque les parties sont conjointement responsables d'un dommage causé par le traitement, les parties sont également conjointement responsables du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

En cas de condamnation de l'Énap à une amende administrative ou à toute autre décision lui créant préjudice, le prestataire s'engage à la dédommager à hauteur des condamnations ou préjudices exposés.

25. ASSURANCE RESPONSABILITE CIVILE

Le prestataire devra fournir une attestation d'assurance en responsabilité civile prouvant sa capacité de couverture en cas de sanction financière émise par une autorité de contrôle ou une juridiction compétente.

26. RÉVISION

Toute évolution de la jurisprudence, décision de la CNIL ou toute nouvelle règlementation en matière de protection des données à caractère personnel, qui modifieraient l'une des dispositions du présent avenant implique nécessairement sa révision.

La révision doit emporter l'accord des deux parties.

En cas de désaccord sur la révision de l'avenant qui exposerait l'Énap à un risque technique, économique ou juridique, le contrat peut être résilié sans indemnité ni pénalité par lettre RAR sous réserve de respecter un délai maximum de six (6) mois à compter de l'envoi de la demande de résiliation.

27. DÉSIGNATION D'UN REPRÉSENTANT (Article 27 du RGPD)

Dans le cas où le prestataire ne serait pas localisé sur le territoire de l'Union européenne, il s'engage, dans le respect de la réglementation applicable, à désigner par écrit un représentant au sein de l'Union européenne.

Les coordonnées de ce représentant doivent être communiquées à l'Énap à sa première demande.

28. DÉLÉGUÉ À LA PROTECTION DES DONNÉES POUR L'ÉNAP

L'Énap, en sa qualité d'organisme public, a désigné un délégué à la protection.

Il peut être joint par voie postale à :

École nationale d'administration pénitentiaire
Le délégué à la protection des données
440 Avenue Michel Serres
CS 10028
47916 Agen Cedex 9

ou par voie électronique à : dpo.enap@justice.fr

29. DÉLÉGUÉ À LA PROTECTION DES DONNÉES DU SOUS-TRAITANT.

Si le prestataire désigne un délégué à la protection des données, les deux délégués se voient communiquer pour information le présent contrat. Par ailleurs les délégués à la protection des données se réunissent au moins une fois par an pour évoquer les améliorations pouvant être apportées au présent contrat.

30. ANNEXES

Le présent contrat est complété des annexes suivantes :

- Annexe 1 - « *Engagement de confidentialité* » ;
- Annexe 2 - « *Mesures de sécurité mise en œuvre par le prestataire* » ;
- Annexe 3 - « *Liste des sous-traitants ultérieurs au jour de la signature du contrat* » ;

Fait à le Pour le prestataire,	Fait à AGEN le Pour l'Énap, La directrice, Sophie BONDIL

Annexe 1

Engagement de confidentialité

Les supports informatiques, papiers et informations fournis ou mis à disposition par l'Énap et tous les documents de quelque nature qu'ils soient résultant de leur traitement par le prestataire restent la propriété exclusive de l'Énap.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal). Conformément aux articles 32 ; 33 et 34 du Règlement Général sur la Protection des Données Règlement UE 2016/679 du 27 avril 2016, le prestataire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquer à des personnes non autorisées ;

Le prestataire s'engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel ou ses sous-traitants, c'est-à-dire notamment à ;

- Ne prendre, à d'autres fins que la bonne exécution du marché, aucune copie des documents et supports d'information confiés par l'Énap pour les besoins de l'exécution de sa prestation, objets du présent marché ;
- Ne pas utiliser pour son propre compte ou pour le compte de tiers (personnes privées ou publiques, physiques ou morales) les informations auxquelles il aurait pu avoir accès dans le cadre de la prestation ;
- Ne pas utiliser les informations d'une manière qui soit préjudiciable à l'Énap ;
- Ne pas communiquer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- Prendre toutes les mesures permettant d'éviter toute utilisation détournée ou frauduleuse des informations en cours d'exécution de la prestation ainsi que toute forme d'usage ou de traitement illicite ;
- Prendre toutes les mesures, notamment de sécurité matérielle, pour assurer la confidentialité des informations et des traitements traités tout au long de la durée de la prestation ;
- Mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les informations contre la destruction accidentelle ou illicite, la perte accidentelle ou l'altération et cela concernant toute ressource utilisée par la société pour les besoins de l'exécution de sa prestation ;
- Former l'ensemble de ses collaborateurs ou sous-traitants à la protection des données à caractère personnel et à la sécurité des systèmes d'information.

Le titulaire s'oblige à procéder à la destruction des informations dont il a connaissance dès lors qu'elles ne sont plus nécessaires à la bonne exécution de la prestation. Sauf indication contraire de l'Énap, cette destruction doit être totale à l'issue du contrat, prestation ou marché.

Il est rappelé que, en cas de non-respect des dispositions précitées, la responsabilité du prestataire peut également être engagé sur la base des dispositions des articles 226-17 et 226-22 du nouveau code pénal.

Fait à le Pour le prestataire,	Fait à AGEN le Pour l'Énap, La directrice Sophie BONDIL

Annexe 2

Mesures de sécurité mise en œuvre par le prestataire

1. Gestion de la sécurité

Les mesures de sécurité édictées dans le présent document sont les règles et mesures à **respecter à minima**.

Ce document se fonde sur l'article 32 du RGPD et les recommandations de l'ANSSI.

Le prestataire dans le cadre de son obligation de conseil envers l'Énap, pourra les renforcer s'il estime que cela soit nécessaire.

Sa responsabilité en tant que prestataire l'oblige à mettre en œuvre la notion d'«accountability» ou démontrabilité prouvant qu'il s'inscrit dans une démarche d'amélioration continu de la sécurité de son système d'information pour assurer la protection des données à caractère personnel et l'hébergement des applicatifs, tant sur le plan matériel que logiciel.

Cette démarche devra être documentée et communiqué à l'Énap à sa demande.

Pour s'aider dans cette tâche, le prestataire pourra utiliser la méthode de gestion de la qualité PDCA (Plan-Do-Check-Act) :

- phase de préparation ;
- phase de réalisation ;
- phase de vérification :
- phase d'ajustement (mesures correctives suite aux insuffisances constatées lors de la vérification).

Le prestataire devra s'il en dispose fournir son Plan d'assurance Sécurité (PAS) à l'Énap.

Le gestionnaire devra fournir une base line de l'ensemble de l'infrastructure interagissant avec le traitement de données (Configuration machine et éléments actifs réseaux, version et définition des composants machines et logiciels).

Cette baseline devra être fournie en début de contrat et après chaque correctif de sécurité faisant l'objet d'un CERT-FR ou à la demande du responsable de traitement en cas de risque avéré sur la sécurité des données.

2. Protection antivirale

Une politique antivirale stricte devra être mise en place au niveau des serveurs et des postes. La mise à jour des signatures sera réalisée lors des opérations de maintenance.

Un contrôle de non contamination des serveurs et des postes dédiés à la télémaintenance de production devra être effectué périodiquement et avant toute maintenance.

3. Mises à jour, correctifs de sécurité

Le prestataire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERT-FR (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), le correctif doit être appliqué dans un délai de 24 heures sur les infrastructures de l'ENAP.

Lorsqu'aucun correctif n'est pas disponible, le prestataire doit suivre les recommandations de l'éditeur ou du CERT-FR dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le prestataire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenance .

Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient .

En cas d'alerte donnée par les équipes d'experts du prestataire, par l'administration ou le CERT-FR, l'Énap sera notifié par téléphone et courrier électronique avant toutes opérations. La décision de l'action ne pourra être prise que par des personnels de l'Énap désignés par écrit. En particulier, le responsable sécurité des systèmes d'information (RSSI) de l'Énap sera le correspondant privilégié pour le suivi des opérations.

Le prestataire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (H24, heures ouvrables, …) permettant à l'Énap de suivre le traitement d'une alerte.

Le sous-traitant devra appliquer les correctifs de sécurités dans un délai d'un mois permettant de remédier aux failles de sécurité qui pourrait être mise en lumière lors d'un audit de sécurité effectué par ou pour le compte du responsable de traitement.

4. Sauvegardes et restauration

Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé.

Le prestataire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :

- confidentialité des flux lors des opérations de sauvegardes ;
- stockage sécurisé des sauvegardes.

En cas de sauvegarde externalisée, les sauvegardes doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du prestataire et de l'Énap.

Dans le cadre de plans de sécurité gouvernementaux, l'Énap pourra imposer une augmentation de la fréquence des sauvegardes.

5. Authentification

Les interfaces d'accès aux fonctionnalités bas niveau (exemple : configuration du BIOS) doivent impérativement authentifier un utilisateur (mise en place d'un mot de passe pour l'utilitaire de configuration du BIOS).

Les identifiants des comptes d'accès sont nominatifs. L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifiant est acceptée par l'Énap. Dans ce cas, le prestataire présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité.

L'utilisation de mots de passe constructeur ou par défaut est interdite.

L'utilisation de protocoles dont l'authentification est en clair ou qui s'appuie sur des composants ou protocoles obsolètes (réputés non sécurisés) est interdite

Les mots de passe doivent satisfaire aux contraintes de complexité tel que défini dans la délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017

- Avoir une longueur minimale de 12 caractères (sauf limitation technique) ;
- Comporter au minimum une majuscule, une minuscule, un chiffre et un caractère spécial ;
- Ne pas être vulnérables aux attaques par dictionnaire.et avoir un niveau minimal générique de 80 bits d'entropie.

6. Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, IP sec, etc.), garantissant la confidentialité et l'intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties.

Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.

Le prestataire tiendra à disposition de l'Énap l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

7. Imputabilité, traçabilité

Les informations suivantes devront être enregistrées :

- entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ;
- actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet,
- type de la tentative d'accès, réussite ou échec de la tentative ;
- création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
- actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure,
- identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

L'intégralité de ce registre sera à la disposition de l'Énap sur simple demande.

Aucune purge ne devra avoir lieu sur la période contractuelle.

A la fin du contrat, ces données devront transmises dans un format standard, facilement exploitable à l'Énap puis faire l'objet d'une destruction dès que l'Énap accusera réception de ces données.

8. Personnels en charge des prestations

Le prestataire s'engage à la demande de l'Énap à fournir une liste, régulièrement mise à jour, des personnels autorisés à accéder aux informations transmise par l'Énap ainsi que leur niveau d'habilitation (types d'accès et ressources concernées du client).

Le prestataire tiendra à disposition de l'Énap les moyens mis en œuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l'expérience professionnelle des futurs employés.

Dans le cadre de plans de sécurité gouvernementaux, l'Énap pourra imposer un renforcement des contrôles d'accès physiques et logiques à ces équipements.

Toute personne intervenant sur des données à caractère personnel concernant le présent contrat devra avoir signée préalablement à toute intervention l'engagement de confidentialité de l'annexe2 du présent contrat.

9. Qualifications et expérience, formations et sensibilisation dans le domaine de la SSI des personnels en charge des prestations

Le prestataire :

- S'assurera que les qualifications, diplômes ainsi que le niveau d'expérience des personnels retenus pour la réalisation des prestations d'infogérance sont compatibles avec le niveau d'exigence de l'Énap ;
- S'assurera que la fréquence et le contenu des actions de formation et de sensibilisation de ses personnels aux enjeux de sécurité et de protection des données soit constant pour rester en conformité avec les exigences présentes et à venir.

10. Exigences de sécurité concernant les personnels extérieurs (maintenance, entretien…)

Le prestataire précisera en cas de demande de l'Énap les moyens de contrôle mis en œuvre pour s'assurer du respect des exigences de sécurité de l'Énap par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre du support et de la maintenance sur le système du client.

Fait à le Pour le prestataire,	Fait à AGEN le Pour l'Énap, La directrice Sophie BONDIL

,

Annexe 3

MINISTÈRE DE LA JUSTICE
Liberté
Égalité
Fraternité

ÉNAP
ÉCOLE NATIONALE D'ADMINISTRATION PÉNITENTIAIRE

TABLEAU DES SOUS-TRAITANTS ULTERIEURS

Nom du traitement	Nom du sous-traitant	Lieu de traitement des données	Lieu de stockage des données	Données ou périmètres sous traités	Date d'accord de l'ÉNAP	Date de la mise en œuvre de la sous-traitance	Date de retrait de l'habilitation

Fait à le Pour le prestataire, Sous-traitant de niveau 1,	Fait à AGEN le Pour l'Énap, La directrice Sophie BONDIL