LEXING

Lexing certification RGPD – Critères

(Publication RGPD 2016/679 art.43 § 6)

V5.0

LEXING

SOMMAIRE

1. Approche générale

1.1 Préambule

1. Le présent dossier a pour objet de soumettre, au titre de l'article 42 du RGPD, à l'approbation de la Cnil un mécanisme de certification national.

1.2 Contexte

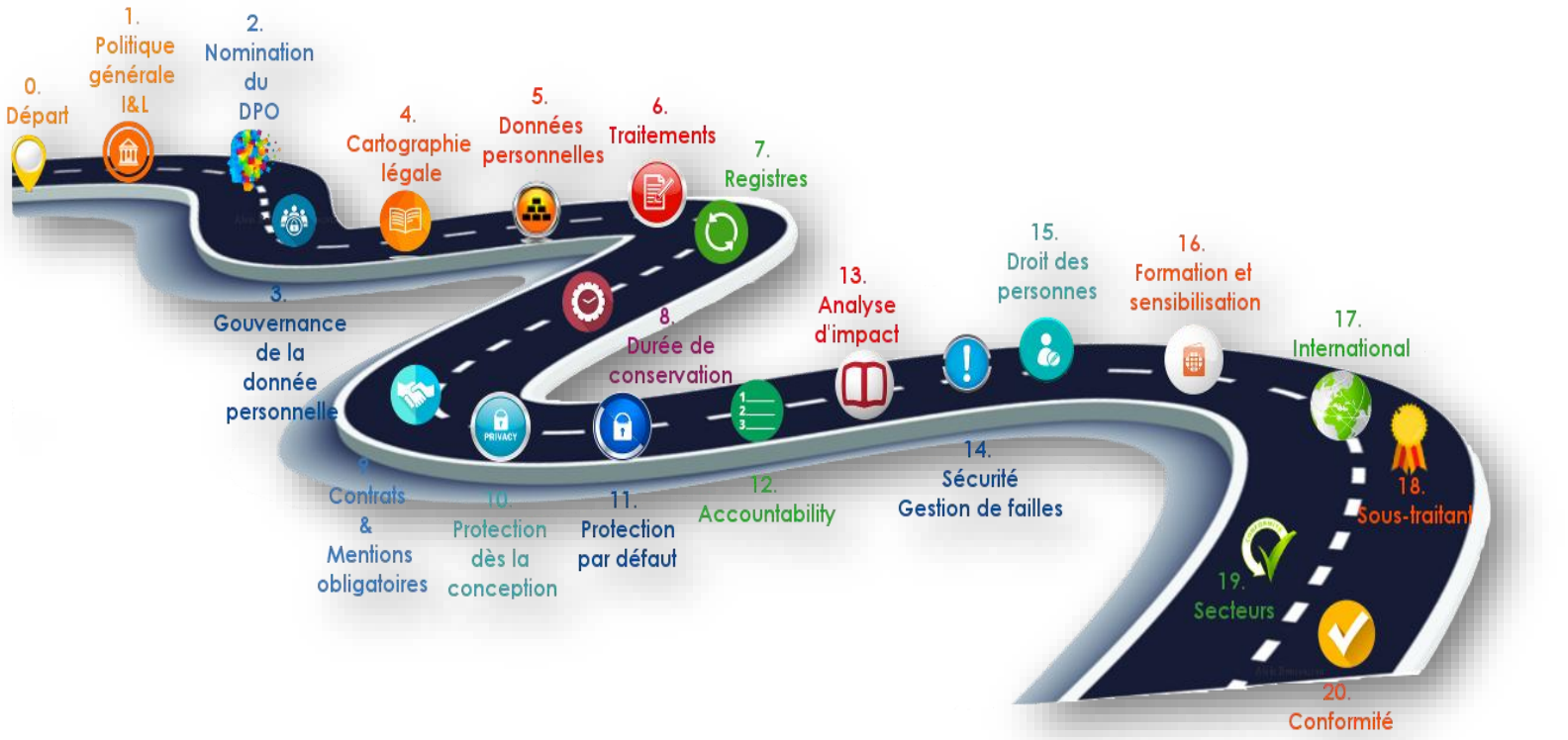
2. Lexing a conçu un mécanisme de certification ayant pour objet d'évaluer la conformité des organismes privés et publics aux exigences issues de la réglementation sur la protection des données personnelles[1].

3. Ce mécanisme de certification, déployé à ce jour auprès de plusieurs centaines d'organismes privés et publics, comprend 20 exigences[2].

4. Ces 20 exigences sont représentées sous la forme d'une route de la conformité :

[1] RGPD, loi Informatique et libertés.

[2] Chaque exigence est représentée par la lettre « E » (cf. « Annexe 3 : Sigles » figurant dans le document « Lexing certification RGPD – Guide d'évaluation »).



5. C'est dans ce contexte que Lexing soumet, au titre de l'article 42 du RGPD, ce mécanisme de certification national de la conformité à l'approbation de la Commission.

1.3 Référentiel documentaire

6. Le présent dossier est constitué sur la base du référentiel suivant :
   - Article 42 du RGPD ;
   - CEPD, Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement, Version 3.0, 4 juin 2019 ;
   - Addendum aux lignes directrices 1/2018 : Guide sur l'évaluation des critères de certification (Version du 06-04-2021 pour consultation publique du 14 avril au 26 mai 2021) ;
   - CEPD, Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données ;
   - Cnil, Comment faire approuver un mécanisme de certification ?, 17 février 2021.

1.4 Démarche

7. L'ensemble des obligations découlant de la réglementation sur la protection des données personnelles est décliné sous forme d'exigences représentées par le sigle « E ». Par exemple, l'obligation de protection des données dès la conception est visée au sein du paragraphe intitulé « Exigences relatives à la protection des données dès la conception (E10) ».

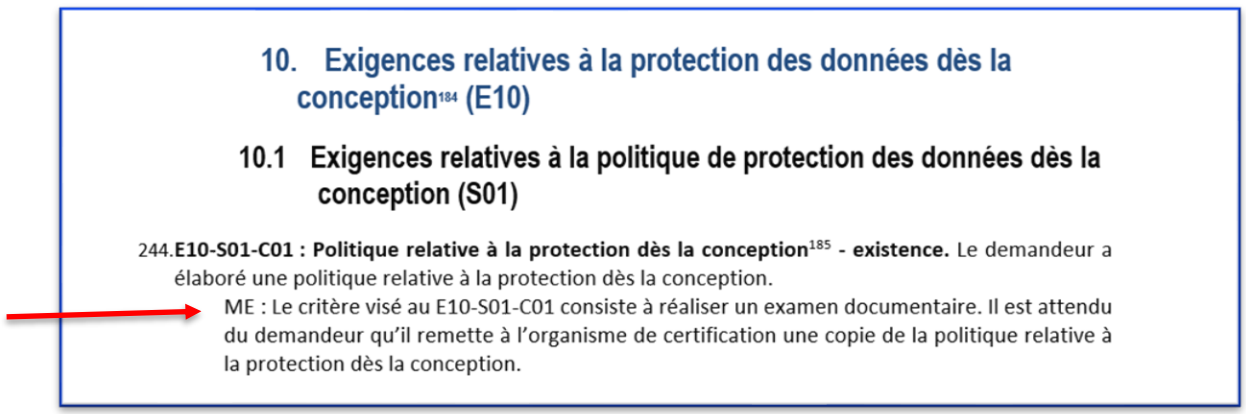
8. Ces exigences font ensuite, pour chacune, l'objet de sous exigences représentées par le signe « S ». Ainsi par exemple, on trouve sous le paragraphe consacré aux « Exigences relatives à la protection dès la conception (E10) », une première sous exigence intitulée « Exigences relatives à la politique de protection des données dès la conception (S01) ».

9. Chacune des sous exigences fait l'objet de déclinaison en critères représentés par le sigle « C », comme le montre l'exemple ci-dessous.

> **10. Exigences relatives à la protection des données dès la conception[184] (E10)**
>
> **10.1 Exigences relatives à la politique de protection des données dès la conception (S01)**
>
> 244.**E10-S01-C01 : Politique relative à la protection dès la conception[185] - existence.** Le demandeur a élaboré une politique relative à la protection dès la conception.

10. Enfin, pour chaque critère est renseigné la modalité d'évaluation représentée sous le signe «ME »[3] qui sera appliquée par l'organisme de certification, comme le montre l'exemple ci-dessous.

[3] Les modalités d'évaluation associées à chaque critère figurent dans le document « Lexing Certificaiton RGPD - Guide d'évaluation ».



10. Exigences relatives à la protection des données dès la conception[184] (E10)

10.1 Exigences relatives à la politique de protection des données dès la conception (S01)

244. **E10-S01-C01 : Politique relative à la protection dès la conception[185] - existence.** Le demandeur a élaboré une politique relative à la protection dès la conception.

ME : Le critère visé au E10-S01-C01 consiste à réaliser un examen documentaire. Il est attendu du demandeur qu'il remette à l'organisme de certification une copie de la politique relative à la protection dès la conception.

1.5 Composition du dossier

11. Le présent dossier est composé :
- d'une approche générale comprenant un contexte, le référentiel documentaire, la démarche et la composition du dossier ;
- d'un préambule ;
- des vingt exigences, sous exigences et critères associés.

1.6 Plan

12. Le présent dossier est divisé en trois parties :
- approche générale ;
- préambule ;
- les vingt exigences, sous exigences et critères associés.

Préambule

13. Sont exclus de la cible d'évaluation et ne sont pas soumis au processus d'évaluation les traitements de données à caractère personnel mis en œuvre par le demandeur :
    - en sa qualité de sous-traitant ;
    - sa qualité de responsable conjoint ;
    - qui n'est pas établi dans l'Union européenne, même si ses activités de traitement sont liées à l'offre de biens ou de services à des personnes concernées dans l'Union ou au suivi d'un comportement de ces personnes qui a lieu dans l'Union.

14. Le présent référentiel n'est pas un outil de transfert au titre de l'article 46 du RGPD.

15. La cible d'évaluation comprend tous les traitements de données à caractère personnel soumis à la certification par le demandeur pour l'activité[4]; cette activité et la liste associée des traitements de données à caractère personnel sont intégrées dans la liste visée au critère E04-S02-C02.
    Remarque : les traitements de données à caractère personnel inclus et ceux exclus sont précisés de manière formelle dans la cible d'évaluation.

16. En cas de non applicabilité d'un des critères du présent référentiel, le demandeur précise :
    - la non applicabilité ;
    - les raisons associées.

17. D'éventuelles conditions de non applicabilité d'un critère sont définies dans ses modalités d'évaluation (ME), tout en permettant au demandeur de justifier les raisons pour lesquelles il estime que le critère n'est pas applicable (l'organisme de certification appréciera lors de son évaluation). Tel est le cas par exemple du critère E01-S02-C05 qui précise dans ses modalités d'évaluation que le demandeur doit démontrer le respect de ce critère « si les traitements mis en œuvre dans le cadre du système d'information Ressources Humaines font partie du périmètre de la certification » ou du critère E14-S19-C03 où un réseau dit DMZ n'est pas requis si l'environnement du traitement ne permet aucun accès depuis internet.

18. Les critères relatifs à la cible d'évaluation sont dans la partie E21.

19. Des critères ont été élaborés pour exiger des politiques (information générale des métiers concernés) et des procédures (implémentation détaillée desdites politiques).

20. Lorsque les critères imposent la disponibilité d'une politique et d'une procédure associée, le demandeur doit démontrer la présence :
    - de politiques rédigées sous la forme d'énoncés ou de règles ;
    - de procédures associées qui précisent, sous la forme d'instructions à suivre selon un ordre logique et des étapes déterminées, comment mettre en œuvre les politiques par des actions concrètes.

21. Lorsqu'un critère requiert une politique, cela peut prendre la forme de plusieurs politiques et/ou d'une partie d'une politique plus large, du moment que l'exigence relative à la politique générale de protection des données à caractère personnel est respectée (E01-S02-C03).

[4] Le terme « activité » désigne les services et processus pour lesquels le demandeur fait la demande de certification.

22. Les critères faisant référence à des procédures requièrent une procédure documentée/formalisée et pas uniquement un processus formalisé.

23. Lorsque les critères exigent des procédures sans politique, cela signifie que des actions ou des processus spécifiques sont définis pour être suivis, mais sans qu'il y ait de cadre stratégique ou d'orientation générale (la politique) pour guider ces actions. Par exemple, la procédure relative au contrôle de l'accès physique (R14-S03-C01) n'a pas besoin d'être encadrée par une politique générale.

24. Lorsque les critères exigent des politiques sans procédures associées, cela signifie qu'une orientation ou une ligne directrice est définie au niveau stratégique, mais que les actions spécifiques pour la mettre en œuvre sont laissées ouvertes. Tel est le cas par exemple de la politique interne de protection des données à caractère personnel visée au E01-S02-C05.

25. Les certifications sont délivrées pour une durée de 3 ans.

1. Exigences de Politique générale (E01)

1.1 Exigences relatives aux engagements de la Direction Générale dans le domaine de la protection des données à caractère personnel (S01)

26. **E01-S01-C01 : Orientation**[5]**.** Le demandeur a adressé à ses collaborateurs une communication personnalisée par courrier électronique émanant de la Direction Générale définissant la posture, les axes et la stratégie poursuivis dans le cadre de l'application de la réglementation sur la protection des données à caractère personnel. Le demandeur prévoit que cette communication personnalisée soit réitérée tous les trois ans. En cas de mise à jour substantielles[6] des orientations, une nouvelle communication intervient avant le terme des trois ans dans le mois suivant cette mise à jour.

27. **E01-S01-C02 : Nouveaux collaborateurs.** Le demandeur a intégré dans le kit d'arrivée des nouveaux collaborateurs la copie de la communication visée au E01-S01-C01[7].

1.2 Exigences relatives aux politiques de protection des données à caractère personnel (S02)

28. **E01-S02-C01 : Politique générale de protection des données à caractère personnel**[8] **- existence.** Le demandeur dispose d'une politique générale de protection des données à caractère personnel à destination des personnes extérieures[9].

29. **E01-S02-C02 : Politique générale de protection des données à caractère personnel – communication aux personnes concernées.** La politique en matière de protection des données à caractère personnel visée au E01-S02-C01 est aisément accessible[10] aux personnes extérieures via le site internet du demandeur.

30. **E01-S02-C03 : Politique générale de protection des données à caractère personnel - forme.** La politique en matière de protection des données à caractère personnel visée au E01-S02-C01 est portée à la connaissance des personnes extérieures dans un format compréhensible[11].

---

[5] Le terme « demandeur » désigne l'organisme à l'origine de la demande de certification ainsi que l'organisme qui a obtenu la certification. Ce terme est également défini dans le glossaire visé en annexe 4 figurant dans le document « Lexing certification RGPD – Guide d'évaluation ».

[6] Exemples : introduction de nouvelles technologies, intelligence artificielle, capteurs intelligents, vidéo comportementale.

[7] Cette exigence vise à s'assurer que les nouveaux collaborateurs prendront connaissance, dès leur arrivée, de la communication adressée initialement par la Direction Générale sans attendre que le délai de réitération de 3 ans soit écoulé.

[8] Cette exigence était imposée par la Cnil dans délibération n° 2014-500 du 11 décembre 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et libertés.

[9] L'expression « personnes extérieures » désigne les contacts personnes physiques au sein des sociétés clientes personnes morales, des prospects personnes morales, des sociétés fournisseurs personnes morales…

[10] RGPD, Art. 12-1 vise l'exigence d'accessibilité aisée de l'information.

[11] RGPD, Art. 12-1.

31. **E01-S02-C04 : Politique générale de protection des données à caractère personnel - contenu.** La politique en matière de protection des données à caractère personnel visée au E01-S02-C01 indique[12] :
- l'identité et les coordonnées du responsable du traitement ;
- les coordonnées du délégué à la protection des données ;
- les finalités du ou des traitement(s) ;
- la base juridique du ou des traitement(s) ;
- lorsque le traitement est fondé sur l'intérêt légitime, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
- les destinataires ou les catégories de destinataires des données à caractère personnel ;
- le cas échéant les transferts de données à caractère personnel vers un pays tiers et les outils utilisés pour les encadrer ;
- la durée de conservation des données à caractère personnel ou lorsque ce n'est pas possible les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, une limitation du traitement relatif à la personne concernée, le droit de s'opposer au traitement et le droit à la portabilité des données à caractère personnel, le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données à caractère personnel ;
- l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;
- lorsque le traitement de données à caractère personnel repose sur le consentement de la personne concernée - qu'il s'agisse d'un consentement au traitement de données à caractère personnel ou d'un consentement explicite requis pour le traitement de catégories particulières de données - que cette dernière a le droit de retirer son consentement à tout moment[13] ;
- que lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées et que le test de compatibilité mentionné au E05-S04-C02 permet de justifier cette évolution de finalité, le demandeur fournit au préalable à la personne concernée des informations au sujet de cette autre finalité[14] ;
- le référentiel visé au E19-S01-C01 précisant la réglementation sectorielle que le demandeur est tenu de suivre.

32. **E01-S02-C05 : Politique interne de protection des données à caractère personnel[15] - existence.** Le demandeur dispose d'une politique interne de protection des données à caractère personnel à destination de son personnel.

[12] RGPD, Art. 13-1 et 13-2.

[13] RGPD, Art. 13-2 c).

[14] RGPD, Art. 13-3.

[15] Cette exigence était imposée par la Cnil dans délibération n° 2014-500 du 11 décembre 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et libertés. La politique est l'un des moyens d'information des personnes.

33. **E01-S02-C06 : Politique interne de protection des données à caractère personnel – communication aux personnes concernées.** La politique interne[16] en matière de protection des données à caractère personnel visée au E01-S02-C05 est aisément accessible aux personnes concernées[17] et communiquée sur le site intranet du demandeur et/ou par affichage et/ou par courrier électronique personnalisé et/ou dans le kit d'arrivée.

34. **E01-S02-C07 : Politique interne de protection des données à caractère personnel - forme.** La politique interne en matière de protection des données à caractère personnel visée au E01-S02-C05 est portée à la connaissance du personnel dans un format compréhensible[18].

35. **E01-S02-C08 : Politique interne de protection des données à caractère personnel - contenu.** La politique interne en matière de protection des données à caractère personnel visée au E01-S02-C05 indique[19] :
- l'identité et les coordonnées du responsable du traitement ;
- le cas échéant les coordonnées du délégué à la protection des données ;
- les finalités du ou des traitement(s) ;
- la base juridique du ou des traitement(s) ;
- lorsque le traitement est fondé sur l'intérêt légitime, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
- les destinataires ou les catégories de destinataires des données à caractère personnel ;
- le cas échéant les transferts de données à caractère personnel vers un pays tiers et les outils utilisés pour les encadrer ;
- la durée de conservation des données à caractère personnel ou lorsque ce n'est pas possible les critères utilisés pour déterminer cette durée ;l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, une limitation du traitement relatif à la personne concernée, le droit de s'opposer au traitement et le droit à la portabilité des données à caractère personnel, le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données à caractère personnel ;
- l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;
- lorsque le traitement de données à caractère personnel repose sur le consentement de la personne concernée - qu'il s'agisse d'un consentement au traitement de données à caractère personnel ou d'un consentement explicite requis pour le traitement de catégories particulières de données - que cette dernière a le droit de retirer son consentement à tout moment[20] ;

---

[16] Le terme « interne » vise le personnel du demandeur. Cette politique a pour objet d'informer les employés des traitements de données à caractère personnel mis en œuvre par le demandeur qui les concernent (gestion administrative du personnel, de la paye, de la formation, des congés, de l'évaluation annuelle…).

[17] RGPD, Art. 12-1.

[18] RGPD, Art. 12-1.

[19] RGPD, Art. 13-1 et 13-2.

[20] RGPD, Art. 13-2 c).

- que lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées et que le test de compatibilité mentionné au E05-S04-C02 permet de justifier cette évolution de finalité, le demandeur fournit au préalable à la personne concernée des informations au sujet de cette autre finalité[21].

36. **E01-S02-C09 : Politique de protection des données à caractère personnel vis-à-vis des tiers. - existence.** Le demandeur dispose d'une politique de protection des données à caractère personnel vis-à-vis des tiers[22].

37. **E01-S02-C10 : Politique de protection des données à caractère personnel vis-à-vis des tiers – communication aux personnes concernées.** La politique de protection des données à caractère personnel visée au E01-S02-C09 est portée à la connaissance des tiers concernés.

38. **E01-S02-C11 : Politique de protection des données à caractère personnel vis-à-vis des tiers - contenu.** La politique en matière de protection des données à caractère personnel visée au E01-S02-C09 indique[23]. :
- l'identité et les coordonnées du responsable du traitement ;
- le cas échéant les coordonnées du délégué à la protection des données ;
- les finalités du ou des traitement(s) ;
- la base juridique du ou des traitement(s) ;
- lorsque le traitement est fondé sur l'intérêt légitime, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
- les destinataires ou les catégories de destinataires des données à caractère personnel ;
- le cas échéant les transferts de données à caractère personnel vers un pays tiers et les outils utilisés pour les encadrer ;
- la durée de conservation des données à caractère personnel ou lorsque ce n'est pas possible les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, une limitation du traitement relatif à la personne concernée, le droit de s'opposer au traitement et le droit à la portabilité des données à caractère personnel, le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données à caractère personnel ;
- l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;
- lorsque le traitement de données à caractère personnel repose sur le consentement de la personne concernée - qu'il s'agisse d'un consentement au traitement de données à

[21] RGPD, Art. 13-3.

[22] Les « tiers » visés par cette politique sont les personnes en assistance technique, les intérimaires, les visiteurs, les commissaires aux comptes… Il s'agit de tiers « contractuels ». Ces « tiers contractuels » se différencient des « tiers autorisés » au sens de l'article 4-10 du RGPD (administration fiscale, organismes de sécurité sociale, administrations de la justice, de la police et de la gendarmerie, commissaires de justice...) pour lesquels le critère E01-S02-C11 impose au demandeur de disposer d'une liste.

[23] RGPD, Art. 13-1 et 13-2.

caractère personnel ou d'un consentement explicite requis pour le traitement de catégories particulières de données - que cette dernière a le droit de retirer son consentement à tout moment[24] ;
- que lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées et que le test de compatibilité mentionné au E05-S04-C02 permet de justifier cette évolution de finalité, le demandeur fournit au préalable à la personne concernée des informations au sujet de cette autre finalité[25].

Cette politique prévoit également que le demandeur établit la liste des « tiers autorisés »[26] qui, en vertu de dispositions législatives et réglementaires, sont susceptibles d'exiger la transmission de documents ou de renseignements pouvant comprendre des données à caractère personnel.

39. **E01-S02-C12 : Politique de protection des données à caractère personnel vis-à-vis des tiers - contenu.** Les politiques de protection de protection des données à caractère personnel visées au E01-S02 formalisées par le demandeur comprennent des dispositions communes ainsi que des contenus spécifiques selon les personnes concernées.

1.3 Exigences transverses (S03)

40. **E01-S03-C01 : Historique des versions.** Le demandeur dispose de l'historique des versions de la documentation[27] visée par le présent référentiel.

41. **E01-S03-C02 : Communication aux métiers impliqués dans le traitement[28].** La documentation visée par le présent référentiel est portée à la connaissance des métiers impliqués dans le traitement.

42. **E01-S03-C03 : Conseil du délégué (DPO)[29].** La documentation visée par le présent référentiel a été transmise au délégué (DPO), avant sa diffusion, pour lui permettre d'exercer son rôle de conseil.

43. **E01-S03-C04 : Audits annuels.** Les audits visés par le présent référentiel sont, sauf circonstances critiques nécessitant leur déclenchement en urgence[30], réalisés annuellement en interne ou en externe par des personnes justifiant d'une compétence et d'une expérience dans la réalisation d'audits ainsi qu'une compétence en matière de protection des données à caractère personnel. Au cas où l'audit porterait sur la tâche d'une personne, celui-ci devra être réalisé par une personne différente.

---

[24] RGPD, Art. 13-2 c).

[25] RGPD, Art. 13-3.

[26] Il s'agit des tiers autorisés au sens de l'article 4-10 du RGPD.

[27] Politiques, procédures, listes, tables, programme de formation...

[28] L'expression « métiers impliqués dans le traitement » fait référence au personnel impliqué dans la mise en œuvre du traitement (le service en charge de la paye, de la comptabilité, du marketing… qui traitent les données à caractère personnel au quotidien).

[29] RGPD, Art. 38-1.

[30] Il s'agit de circonstances critiques où la conformité de l'organisation à la réglementation sur la protection des données pourrait être compromise : par exemples en cas de violation de données rendant nécessaire de déclencher un audit immédiat afin d'identifier les actions correctives à déployer en urgence, en cas de plainte de personnes concernées un audit doit être lancé pour évaluer la conformité des pratiques de l'organisation…

2. Exigences relatives au Délégué à la Protection des données[31] (E02)

2.1 Exigences relatives à la désignation du Délégué à la protection des données (S01)

44. **E02-S01-C01 : Désignation d'un délégué (DPO)[32].** Le demandeur a procédé à la nomination d'un délégué (DPO) interne choisi parmi les membres de son personnel ou d'un délégué (DPO) externe.

2.2 Exigences relatives à la définition des missions du Délégué à la protection des données (S02)

45. **E02-S02-C01 : Formalisation des missions du délégué (DPO) interne ou externe[33].** Le demandeur a formalisé les missions confiées au délégué (DPO) interne ou externe.

46. **E02-S02-C02 : Définition des missions du délégué (DPO) interne ou externe[34].** Le document visé au E02-S02-C01 dans lequel les missions confiées au délégué (DPO) interne ou externe sont formalisées détaille ces missions de la manière suivante[35] :
- informer et conseiller l'organisme qui l'a désigné ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la réglementation relative à la protection des données à caractère personnel ;
- contrôler le respect de cette réglementation ainsi que le respect des politiques du demandeur ;
- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données à caractère personnel et vérifier l'exécution de celle-ci ;
- rendre compte au niveau le plus élevé de la direction ;
- coopérer avec l'autorité de contrôle ;
- faire office de point de contact pour l'autorité de contrôle.

47. **E02-S02-C03 : Acceptation des missions**. Le demandeur dispose de la lettre d'acceptation de mission signée par le délégué (DPO) interne ou du contrat de prestation de service conclu avec le délégué (DPO) externe.

48. **E02-S02-C04 : Indépendance[36]**. Le demandeur veille à ce que le délégué (DPO) ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions.

49. **E02-S02-C05 : Protection[37]**. Le document visé au E02-S02-C01 dans lequel les missions confiées au délégué (DPO) sont formalisées précise que le délégué (DPO) ne peut être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions.

---

[31] Le Délégué à la protection des données est désigné sous l'acronyme « DPO ».

[32] RGPD, Art. 37-6, Cnil « Le guide du délégué à la protection des données » 6 avril 2022.

[33] RGPD, Art. 39-1.

[34] Cnil « Le guide du délégué à la protection des données » 6 avril 2022.

[35] Cnil « Le guide du délégué à la protection des données » 6 avril 2022.

[36] RGPD, Art. 38-3.

[37] RGPD, Art. 38-3.

2.3 Exigences relatives à la compétence du Délégué à la protection des données (S03)

50. **E02-S03-C01 : Expertise**[38]. Le demandeur désigne le délégué (DPO) sur la base de ses qualités professionnelles (connaissance du secteur d'activité, connaissance de l'organisation interne, compréhension des opérations de traitement, compréhension des systèmes d'information et des exigences en matière de sécurité), en prenant en considération :
- ses connaissances juridiques spécialisées ;
- ses pratiques en matière de protection des données à caractère personnel.

51. **E02-S03-C02 : Maintien des compétences.** Le demandeur permet au délégué (DPO) d'entretenir ses connaissances spécialisées.

2.4 Exigences relatives aux liens avec la Direction générale (S04)

52. **E02-S04-C01 : Interventions devant la Direction générale**[39]**.** Le demandeur prévoit que le délégué (DPO) fait rapport directement au niveau le plus élevé de la direction.

53. **E02-S04-C02 : Bilan annuel d'activité**[40]**.** Le demandeur prévoit que le délégué (DPO) établit un bilan annuel de ses activités.

2.5 Exigences relatives au budget et aux moyens du Délégué à la protection des données (S05)

54. **E02-S05-C01 : Budget**[41]**.** Le demandeur accorde chaque année au délégué (DPO) un budget dédié pour exercer ses missions et maintenir et actualiser ses connaissances spécialisées[42].

55. **E02-S05-C02 : Actualisation du budget.** Le demandeur élabore chaque année, en concertation avec le délégué (DPO), un bilan de l'utilisation du budget sur l'année N et le prévisionnel sur l'année N+1. La nature des dépenses réalisées sur le budget de l'année N sont précisées dans le bilan.

2.6 Exigences relatives à l'information et la diffusion des coordonnées du Délégué à la protection des données (S06)

56. **E02-S06-C01 : Information de la Cnil**[43]**.** La désignation du délégué (DPO) a fait l'objet d'une notification auprès de la Cnil via le téléservice dédié.

57. **E02-S06-C02 : Information des instances représentatives du personnel**[44]**.** La désignation du délégué (DPO) a fait l'objet d'une information auprès des instances représentatives du personnel.

---

[38] RGPD, Art. 37-5.

[39] RGPD, Art. 38-3.

[40] Cnil « Le guide du délégué à la protection des données » 6 avril 2022.

[41] RGPD, Art. 38-2.

[42] RGPD, Art. 38-2.

[43] Cnil « Le guide du délégué à la protection des données » 6 avril 2022.

[44] Cnil « Le guide du délégué à la protection des données » 6 avril 2022.

58. **E02-S06-C03 : Information générale**[45]**.** Les coordonnées du délégué (DPO) figurent dans la politique générale de protection des données à caractère personnel visée à l'exigence E01-S02-C01**.**

59. **E02-S06-C04 : Information du personnel.** La désignation du délégué (DPO) a fait l'objet d'une information auprès du personnel du demandeur.

2.7 Exigences relatives à la confidentialité (S07)

60. **E02-S07-C01 : Secret professionnel ou obligation de confidentialité**[46]**.** Le délégué (DPO) désigné par le demandeur doit être soumis au secret professionnel ou à une obligation de confidentialité.

2.8 Exigences relatives aux autres tâches (S08)

61. **E02-S08-C01 : Affectation des tâches**[47]**.** Le demandeur s'assure que le délégué (DPO) dispose du temps nécessaire à l'exercice de ses missions, en particulier lorsque d'autres tâches que celles relevant de la fonction de délégué (DPO) s'impose à lui au titre de son contrat de travail.

62. **E02-S08-C02 : Absence de conflit d'intérêts**[48]**.** Le demandeur s'assure le délégué (DPO) n'est pas impliqué dans des tâches :
- susceptibles d'entrainer un conflit d'intérêt, en particulier lorsque d'autres tâches que celles relevant de sa fonction de délégué (DPO) s'imposent à lui au titre de son contrat de travail ;
- qui le conduirait à déterminer les finalités et les moyens d'un traitement de données à caractère personnel.

3. Exigences relatives à la Gouvernance de la donnée à caractère personnel (E03)

3.1 Exigences relatives au programme de conformité (S01)

63. **E03-S01-C01 : Directeur de programme de la conformité (Chief Compliance Officer)**[49]. Si le demandeur a désigné un Directeur de programme de la conformité[50] (Chief Compliance Officer) ce dernier doit être distinct du délégué (DPO). Le rôle du Directeur de programme de la conformité (Chief Compliance Officer) est défini dans une lettre de mission. La conformité à la réglementation sur la protection des données à caractère personnel fait partie du domaine d'intervention du Directeur de programme de la conformité (Chief Compliance Officer).

[45] Cnil « Le guide du délégué à la protection des données » 6 avril 2022.

[46] Le « Directeur de programme de la conformité » est responsable de la posture Informatique et libertés au sein de l'organisme. En fonction du type d'organisation, il est membre du comité exécutif ou directement rattaché à la Direction générale.

[47] RGPD, Art. 38-6.

[48] RGPD, Art. 38-6.

[49] Le rôle du Chief Compliance Officier ne peut pas empiéter sur les tâches du DPO visées au E02-S02.

[50] RGPD, Art. 38-6.

64. **E03-S01-C02 : Collaboration avec le délégué (DPO).** Le demandeur prévoit expressément que le Directeur de programme de la conformité (Chief Compliance Officer) et le délégué (DPO) coopéreront dans l'exercice de leurs fonctions.

65. **E03-S01-C03 : Relais du délégué (DPO).** Le demandeur a constitué un réseau de relais[51] du délégué (DPO) dont il a défini les règles de dimensionnement, le profil des membres, leur mission ainsi que la répartition des tâches entre leur fonction de relais et leurs autres fonctions.

3.2 Exigences relatives à la politique de gouvernance de la donnée à caractère personnel (S02)

66. **E03-S02-C01 : Politique de gouvernance - existence.** Le demandeur a formalisé la gouvernance de la donnée à caractère personnel au sein de son organisme dans une politique.

67. **E03-S02-C02 : Politique de gouvernance - contenu.** La politique de gouvernance de la donnée à caractère personnel décrit la gouvernance permettant d'atteindre les objectifs de protection des données à caractère personnel définis par la Direction Générale dans sa communication visée au E01-S01-C01, lesquels portent sur la conception et la mise en œuvre des traitements de données à caractère personnel.

68. **E03-S02-C03 : Comité de gouvernance - réunion.** Le demandeur a constitué un Comité qui se réunit régulièrement afin de piloter l'atteinte des objectifs de la politique de gouvernance de la donnée à caractère personnel visée au E03-S02-C01. Le délégué (DPO) et le Directeur de programme de la conformité (Chief Compliance Officer) (dans le cas où un Directeur de programme de la conformité (Chief Compliance Officer) a été désigné) participent à ce Comité.

69. **E03-S02-C04 : Comité de gouvernance – ordre du jour.** Le demandeur établit, avant la réunion du comité de gouvernance de la donnée à caractère personnel, un ordre du jour qu'il transmet aux participants.

70. **E03-S02-C05 : Comité de gouvernance – plan d'action.** Le demandeur établit un plan d'action à l'issue de chaque comité de gouvernance de la donnée à caractère personnel qu'il transmet aux participants.

71. **E03-S02-C06 : Comité de gouvernance – suivi du plan d'action.** Le demandeur effectue un suivi de la réalisation du plan d'action définit dans le cadre du comité de gouvernance de la donnée à caractère personnel.

72. **E03-S02-C07 : Règlement du comité de gouvernance.** Le demandeur dispose d'un règlement du comité de gouvernance de la donnée à caractère personnel qui précise le fonctionnement de ce comité dont la prise en compte et l'application systématique des critères E03-S02-C03 à E03-S02-C08 (réunion régulière, ordre du jour, plan d'action et suivi du plan d'action). Le

[51] Le relais du DPO :
- contribue à la diffusion de la culture de protection des données à caractère personnel au sein de son service ou de sa direction ;
- remonte les informations utiles (incidents, nouveaux projets, besoins d'accompagnement…) ;
- veille à la bonne application des procédures internes en matière de données personnelles ;
- sensibilise ses collègues aux bons réflexes à adopter.

demandeur dispose également de l'historique des versions dont ce règlement a fait l'objet. Le règlement doit prévoir d'associer le délégué (DPO) au comité de gouvernance[52].

3.3 Exigences relatives aux relations avec la Cnil (S03)

73. **E03-S03-C01 : Membre de la Direction Générale.** Le demandeur désigne un membre de la Direction générale en charge des relations avec la Cnil. Cette désignation est sans préjudice du rôle du délégué (DPO) vis-à-vis de la Commission visé au E02-S02-C02.

4. Exigences relatives à la cartographie légale (E04)

4.1 Exigences relatives au référentiel (S01)

74. **E04-S01-C01 : Code(s) de conduite et référentiel(s) sectoriel.** Le demandeur identifie, pour les traitements de données à caractère personnel propres à son secteur d'activité, les codes de conduite approuvés par la Cnil et/ou les référentiels publiés par la commission applicables à son secteur d'activité. Le demandeur actualise cette liste dès l'adoption de nouveaux codes de conduite et/ou de nouveaux référentiels publiés par la Cnil applicables à son secteur d'activité.

4.2 Exigences relatives au recensement (S02)

75. **E04-S02-C01 : Procédure de recensement des traitements - existence.** Le demandeur établit une procédure de recensement des traitements de données à caractère personnel mis en œuvre pour l'activité[53].

76. **E04-S02-C02 : Liste des traitements.** Le demandeur établi et tient à jour, en suivant la procédure visée au E04-S02-C01, la liste des traitements de données à caractère personnel mis en œuvre dans le cadre de son activité[54]. Cette liste permet, dans un second temps, de constituer le registre des traitements visé au E07-S01-C04 qui présente les caractéristiques (finalités, du traitement, catégories de personnes concernées, catégories de données à caractère personnel selon la classification visée au E05-C01-S01, catégories de destinataires, transferts de données à caractère personnel, durée de conservation des données à caractère personnel, sécurité de chacun des traitements recensés dans la liste visée au E04-S02-C04.

77. **E04-S02-C03 : Liste des catégories de personnes concernées.** Le demandeur établi et tient à jour la liste des catégories de personnes concernées par les traitements mis en œuvre dans le cadre de son activité.

78. **E04-S02-C04 : Procédure de vérification des listes - existence.** Le demandeur établit une procédure prévoyant un examen régulier de la liste des traitements, de la liste des logiciels visée au E21-C03, de la liste des technologies visée au critère E21-C04 et de la liste des catégories de personnes concernées.

---

[52] Invitation aux réunions, réception de l'ordre du jour, accès à la documentation associée aux plans d'action…

[53] Sur cette base, le demandeur propose une cible d'évaluation (E21-C01) qui sera définie avec l'aide de l'organisme certificateur.

[54] Le terme « activité » désigne les services et processus pour lesquels le demandeur fait la demande de certification.

5. Exigences relatives aux données à caractère personnel (E05)

5.1 Exigences relatives aux catalogues des types de données à caractère personnel (S01)

79. **E05-S01-C01 : Classification des types de données à caractère personnel.** Le demandeur classifie les types de données à caractère personnel qu'il traite dans le cadre de son activité en cinq catégories :
- catégories particulières de données à caractère personnel[55] ;
- données à caractère personnel relatives aux condamnations et infractions[56].

Les catégories suivantes viennent en complément :
- données sensibles ou données à caractère hautement personnel[57] ;
- données à caractère personnel soumises à des réglementations nationales particulières[58] ;
- autres données à caractère personnel[59].

80. **E05-S01-C02 : Justification de la collecte et du traitement des types de catégories particulières de données à caractère personnel[60].** Le demandeur justifie, en lien avec la définition de la cible d'évaluation, le besoin de collecter et traiter des types de catégories particulières de données à caractère personnel.

81. **E05-S01-C03 : Catalogue des types de catégories particulières de données à caractère personnel.** Compte tenu de la cible d'évaluation, le demandeur dispose et tient à jour un catalogue des types de catégories particulières de données à caractère personnel.

82. **E05-S01-C04 : Politique relative aux types de catégories particulières de données à caractère personnel. - existence.** Le demandeur établit une politique définissant les règles de collecte et de traitement des types de catégories particulières de données à caractère personnel.

83. **E05-S01-C05 : Justification de la collecte et du traitement des types données à caractère personnel relatives aux condamnations et infractions[61].** Le demandeur justifie, en lien avec la définition de la cible d'évaluation, le besoin de collecter et traiter des types de données à caractère personnel relatives aux condamnations, aux infractions ou aux mesures de sureté connexes, étant précisé que le traitement de ce type de données ne peut être effectué que

---

[55] RGPD, Art. 9 (Traitement portant sur des catégories particulières de données à caractère personne).

[56] RGPD, Art. 10 (Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions).

[57] Il s'agit de données autres que celles visées à l'article 9 ou 10 du RGPD.

Cf. CEPD, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, adoptées le 4 avril 2017, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017.

[58] Exemple : numéro de sécurité sociale.

[59] Exemples : nom, prénom, adresse électronique, adresse postale, téléphone, fonction…

[60] L'expression « catégories particulières de données à caractère personnel » vise les données à caractère personnel mentionnées à l'article 9-1 du RGPD à savoir celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

[61] Il s'agit des données visées à l'article 10 du RGPD.

sous le contrôle de l'autorité publique ou que s'il est autorisé par le droit de l'Union ou par le droit d'un Etat membre.

84. **E05-S01-C06 : Catalogue des types de données à caractère personnel relatives aux condamnations et infractions.** Compte tenu de la cible d'évaluation, le demandeur dispose d'un catalogue des types de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sureté connexe.

85. **E05-S01-C07 : Politique relative aux condamnations et infractions - existence.** Le demandeur établit une politique définissant les règles de collecte et de traitement des types de données à caractère personnel relatives aux condamnations, infractions et mesures de sureté connexes.

86. **E05-S01-C08 : Justification de la collecte et du traitement des types données sensibles ou données à caractère hautement personnel[62].** Le demandeur justifie, en lien avec la définition de la cible d'évaluation, le besoin de collecter et traiter des types de données sensibles ou données à caractère hautement personnel.

87. **E05-S01-C09 : Catalogue des types de données sensibles ou données à caractère hautement personnel.** Compte tenu de la cible d'évaluation, le demandeur dispose d'un catalogue des types de données sensibles ou données à caractère hautement personnel utilisées dans le cadre de son activité.

88. **E05-S01-C10 : Politique relative aux types de données sensibles ou données à caractère hautement personnel - existence.** Le demandeur établit une politique définissant les règles de collecte et de traitement des types de données sensibles ou données à caractère hautement personnel.

89. **E05-S01-C11 : Justification de la collecte et du traitement des types de données à caractère personnel soumises à des réglementations nationales particulières[63].** Le demandeur justifie, en lien avec la définition de la cible d'évaluation, le besoin de collecter et traiter des types de données à caractère personnel soumises à des réglementations nationales particulières.

90. **E05-S01-C12 : Catalogue des types de données à caractère personnel soumises à des réglementations nationales particulières.** Compte tenu de la cible d'évaluation, le demandeur dispose d'un catalogue des types de données à caractère personnel soumises à des réglementations nationales particulières utilisées dans le cadre de son activité.

91. **E05-S01-C13 : Politique relative aux types de données à caractère personnel soumises à des réglementations nationales particulières - existence.** Le demandeur établit une politique définissant les règles de collecte et de traitement des types de données à caractère personnel soumises à des réglementations nationales particulières.

[62] Une donnée hautement personnelle est une donnée personnelle dont le traitement augmente les risques d'atteinte aux droits et libertés fondamentaux d'une personne, ou dont la violation suppose une incidence réelle sur la vie quotidienne d'une personne concernée. Il s'agit du terme utilisé par le CEPD dans les lignes directrices WP 248 rev.01.

[63] Il s'agit des données faisant l'objet d'une réglementation spéciale telle que le NIR.

92. **E05-S01-C14 : Catalogue des autres types de données à caractère personnel**[64]**.** Le demandeur dispose et tient à jour un catalogue des autres types de données à caractère personnel qu'il traite dans le cadre de son activité.

93. **E05-S01-C15 : Politique relative aux autres types de données à caractère personnel - existence.** Le demandeur établit une politique définissant les règles de collecte et de traitement des autres types de données à caractère personnel.

5.2 Exigences relatives à la licéité (S02)

94. **E05-S02-C01 : Politique relative à la licéité - existence.** Le demandeur dispose d'une politique qui pose comme règle que les données à caractère personnel doivent être traitées de manière licite[65] et que pour pouvoir être mis en œuvre, tout traitement de données à caractère personnel doit se fonder sur l'une des bases légales prévues par la réglementation applicable[66]. Cette politique est complétée par la procédure relative à la licéité des traitements de données à caractère personnel visée au E06-S02-C02 qui indique comment mettre en œuvre cette règle.

5.3 Exigences relatives à la loyauté et à la transparence (S03)

95. **E05-S03-C01 : Politique relative à la loyauté et à la transparence. - existence.** Le demandeur dispose d'une politique qui pose comme règle que les données à caractère personnel doivent être traitées de manière loyale[67] et transparente[68] à l'égard des personnes concernées.

96. **E05-S03-C02 : Politique relative à la loyauté et à la transparence - contenu.** La politique visée au E05-S03-C01 précise a minima que :
- pour le demandeur, la transparence contribue à un traitement loyal des données à caractère personnel et permet d'instaurer une relation de confiance avec les personnes concernées ;
- cette transparence est également assurée par la politique générale de protection des données à caractère personnel visée au E01-S02-C04 qui permet aux personnes concernées de connaître la raison de la collecte des données à caractère personnel les concernant, de comprendre le traitement qui sera fait de leurs données à caractère personnel et d'assurer la maîtrise de leurs données à caractère personnel, en facilitant l'exercice de leurs droits.

La politique visée au E05-S03-C01 précise également que pour le demandeur, la loyauté se traduit par les principaux éléments suivants :
- autonomie : le demandeur permet aux personnes concernées de déterminer l'utilisation de leurs données à caractère personnelles et de connaître la portée et les conditions de cette utilisation ;
- interaction : les personnes concernées peuvent facilement communiquer avec le demandeur et exercer leurs droits sur les données à caractère personnel traitées par ce dernier ;
- attentes : le traitement des données à caractère personnel répond aux attentes raisonnables des personnes concernées ;

[64] L'expression « autres données à caractère personnel » vise les nom, prénom, numéro de téléphone, adresse postale, adresse électronique…

[65] RGPD, Art. 5-1-a).

[66] RGPD, Art.6-1.

[67] RGPD, Art. 5-1-a).

[68] RGPD, Art. 5-1-a).

- non-discrimination : le demandeur s'engage à ne pas discriminer injustement les personnes concernées ;
- non-exploitation : le demandeur veille à ne pas exploiter les besoins ou vulnérabilités des personnes concernées ;
- choix des consommateurs : le demandeur ne doit pas contraindre de manière déloyale les utilisateurs à s'engager dans l'utilisation des services ;
- équilibre de pouvoir : les relations entre le demandeur et les personnes concernées sont équilibrées et les déséquilibres de pouvoir sont minimisés ;
- absence de transfert des risques : le demandeur ne doit pas transférer les risques commerciaux aux personnes concernées ;
- absence de tromperie : les informations relatives au traitement des données à caractère personnel sont fournies de manière claire, objective et neutre, sans manipulation ni tromperie ;
- respect des droits : Le demandeur respecte les droits fondamentaux des personnes concernées et met en place des mesures de protection adéquates pour éviter toute atteinte, sauf justification légale ;
- éthique : Le traitement des données à caractère personnel est effectué de manière éthique, en tenant compte de l'impact sur la dignité et les droits des personnes concernées ;
- véracité : le demandeur s'assure que les informations sur le traitement des données à caractère personnel sont exactes, complètes et mises à jour ;
- intervention humaine : pour les décisions automatisées, une intervention humaine qualifiée est prévue pour traiter les biais ou erreurs éventuelles ;
- loyauté des algorithmes : les algorithmes utilisés pour le traitement les données à caractère personnel sont régulièrement vérifiés pour garantir leur conformité avec les finalités définies et le respect du principe de loyauté.

5.4 Exigences relatives aux finalités (S04)

97. **E05-S04-C01 : Politique relative aux finalités déterminées, explicites, légitimes et aux traitements ultérieurs - existence.** Le demandeur dispose d'une politique qui pose comme règle que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités[69].

98. **E05-S04-C02 : Politique relative aux finalités déterminées, explicites et légitimes et aux traitements ultérieurs - contenu.** La politique visée au E05-S04-C01 précise a minima que le demandeur met en œuvre des mesures pour :
- avant d'envisager la mise en œuvre d'un traitement de données à caractère personnel, déterminer les finalités du traitement ;
- s'il est envisagé une évolution du traitement, déterminer si cette évolution concerne les finalités du traitement ;
- prévenir un détournement de finalité.

La politique précise également[70] que, lorsque le traitement de données à caractère personnel envisagé poursuit une finalité différente de celle initialement prévue, et qu'il ne repose ni sur le consentement de la personne concernée ni sur une obligation légale, le demandeur effectue un test de compatibilité de l'évolution de la finalité et évalue la compatibilité de cette nouvelle finalité au regard de plusieurs critères. Cette évaluation prend notamment en compte :

[69] RGPD, Art. 5-1-b).

[70] RGPD, Art. 6-4.

- l'existence d'un lien entre les finalités initiales et celles du traitement de données à caractère personnel ultérieur envisagé ;
- le contexte dans lequel les données ont été collectées, en particulier la nature de la relation entre les personnes concernées et le demandeur ;
- la nature des données à caractère personnel concernées ;
- les conséquences possibles pour les personnes concernées ;
- l'existence de garanties appropriées, telles que le chiffrement ou la pseudonymisation.

La politique précise également qu'en cas d'évolution positive de la finalité, dès lors que les résultats demeurent compatibles avec la finalité initiale, le demandeur en informe les personnes concernées.

99. **E05-S04-C03 : Politique relative au caractère adéquat, pertinent et à la minimisation des données à caractère personnel - existence.** Le demandeur dispose d'une politique qui pose comme règle que les données à caractère personnel répondant à la classification visée au E05-C01-S01 doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données à caractère personnel)[71].

100. **E05-S04-C04 : Politique relative au caractère adéquat, pertinent et à la minimisation des données à caractère personnel – mise en œuvre.** La mise en œuvre par le demandeur de la politique visée au E05-S04-C03 se matérialise par la justification de la nécessité, pour les finalités poursuivies, de chaque donnée inscrite dans les catalogues référencés aux E05-S01-C01, E05-S01-C02, E05-S01-C05, E05-S01-C11 et E05-S01-C08.

101. **E05-S04-C05 : Politique relative à l'exactitude et la mise à jour des données à caractère personnel - existence.** Le demandeur dispose d'une politique relative au fait que les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour[72].

102. **E05-S04-C06 : Politique relative à l'exactitude et la mise à jour des données à caractère personnel - contenu.** La politique relative au fait que les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour visée au E05-S04-C05 précise que :
- le demandeur sollicite tous les deux ans la personne concernée pour vérifier si les données qu'il détient sont toujours exactes dans le cas où il n'a pas eu de contact avec cette personne à une autre occasion pendant 12 mois au moins ;
- en cas de contacts réguliers, la personne concernée dispose d'un outil lui permettant d'actualiser ses données par elle-même.

103. **E05-S04-C07 : Politique relative à l'exactitude et la mise à jour des données à caractère personnel – mise en œuvre.** La mise en œuvre par le demandeur de la politique visée au E05-S04-C05 se matérialise par :
- la sollicitation tous les deux ans de la personne concernée pour vérifier si les données qu'il détient sont toujours exactes dans le cas où il n'a pas eu de contact avec cette personne à une autre occasion pendant 12 mois au moins.
- en cas de contacts réguliers, la mise à disposition à la personne concernée d'un outil lui permettant d'actualiser ses données par elle-même.

104. **E05-S04-C08 : Politique relative à la durée de conservation des données à caractère personnel - existence.** Le demandeur dispose d'une politique qui pose comme règle que les données à

[71] RGPD, Art. 5-1-c).

[72] RGPD, Art. 5-1-d).

caractère personnel doivent être conservées pendant une durée[73] n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

105. **E05-S04-C09 : Politique relative à la durée de conservation des données à caractère personnel - contenu.** La politique relative à la durée de conservation des données à caractère personnel visée au E05-S04-C08 précise :
- son objectif ;
- son champ d'application ;
- les principes généraux applicables ;
- l'existence d'une procédure associée visée au E08-S03-C01 ;
- l'existence d'une table des durées de conservation des données à caractère personnel visée au E08-S02-C01.

106. **E05-S04-C010 : Politique relative à la durée de conservation des données à caractère personnel - mise en œuvre.** La mise en œuvre par le demandeur de la politique visée au E05-S04-C08 est décrite au sein de l'exigence E08.

6. Exigences relatives aux traitements de données à caractère personnel (E06)

6.1 Exigences relatives aux traitements génériques de données à caractère personnel mis en œuvre dans le cadre d'un système d'information (S01)

107. **E06-S01-C01 : Procédure relative aux traitements génériques - existence.** Le demandeur dispose d'une procédure relative aux traitements génériques de données à caractère personnel qui décrit les étapes à suivre pour veiller à leur conformité à la réglementation sur la protection des données à caractère personnel. Cette procédure s'applique dans tous les cas, indépendamment des procédures dont chaque traitement spécifique fait l'objet.

108. **E06-S01-C02 : Procédure relative aux traitements génériques - contenu.** La procédure relative aux traitements génériques visée au E06-S01-C01 précise les principales règles à respecter préalablement à la mise en œuvre d'un traitement générique de données à caractère personnel en termes d'enjeux, de finalité, de données à caractère personnel, de collecte, de liste des opérations à réaliser, de durée de conservation et de règles générales de sécurité.

109. **E06-S01-C03 : Procédure relative aux traitements génériques - application**. Le demandeur met en œuvre la procédure relative aux traitements génériques, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative aux traitements génériques -est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

6.2 Exigences relatives à la procédure de licéité des traitements de données à caractère personnel (S02)

110. **E06-S02-C01 : Procédure relative à la licéité des traitements de données à caractère personnel**[74]**- existence.** Le demandeur dispose d'une procédure relative à la licéité des

[73] RGPD, Art. 5-1-e).

[74] RGPD, Art. 6.

traitements de données à caractère personnel applicable préalablement à la mise en œuvre d'un nouveau traitement ou avant la modification substantielle d'un traitement existant.

111. **E06-S02-C02 : Procédure relative à la licéité des traitements de données à caractère personnel - contenu.** Le demandeur dispose d'une procédure relative à la licéité des traitements de données à caractère personnel qui permet de déterminer sur laquelle des six bases légales suivantes repose le traitement :
- le consentement : la personne a consenti au traitement de ses données à caractère personnel ;
- le contrat : le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ;
- l'obligation légale : le traitement est imposé par des textes légaux ;
- la mission d'intérêt public : le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
- l'intérêt légitime : le traitement est nécessaire à la poursuite d'intérêts légitimes du demandeur ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données à caractère personnel sont traitées ;
- la sauvegarde des intérêts vitaux : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'une autre personne physique.

La procédure précise également que :
- la base légale appropriée doit être déterminée par le responsable du traitement de manière adaptée à la situation et au type de traitement, au cas par cas ;
- lorsqu'un même traitement de données à caractère personnel poursuit plusieurs finalités, une base légale doit être définie pour chacune de ces finalités. En revanche, il n'est pas possible de « cumuler » des bases légales pour une même finalité : il faut en choisir une seule ;
- le choix de la base légale est documenté.

112. **E06-S02-C03 : Procédure relative à la licéité des traitements de données à caractère personnel - application.** Le demandeur met en œuvre la procédure relative à la licéité des traitements de données à caractère personnel, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative à la licéité des traitements de données à caractère personnel est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

6.3 Exigences relatives au choix des bases légales (S03)

113. **E06-S03-C01 : Choix documenté.** Le demandeur met en œuvre la procédure prévue au critère E06-S02-C02 et documente le choix de la base légale de chacun des traitements de données à caractère personnel mis en œuvre dans le cadre de son activité.

114. **E06-S03-C02 : Conditions propres au consentement.** Le demandeur vérifie, lorsqu'il envisage de retenir le consentement comme base légale, que ses conditions spécifiques sont remplies, à savoir que le consentement est libre, spécifique, éclairé et univoque. Il s'assure également :
- que le consentement a été recueilli préalablement à la mise en œuvre du traitement ;
- que le consentement est demandé pour une finalité déterminée ;
- que le consentement soit donné par une déclaration ou tout autre acte positif clair et exprès[75] ;

[75] Par exemple, par le biais d'une case à cocher.

- que les informations contenues dans la demande de consentement sont compréhensibles pour les personnes concernées ;
- que si le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions ;
- que la personne concernée a la possibilité de retirer son consentement à tout moment sans conséquences négatives suite à ce retrait, par le biais d'une modalité simple et équivalente à celle utilisée pour recueillir le consentement[76] ;
- qu'il n'existe pas un déséquilibre manifeste entre la personne concernée et le demandeur, en particulier lorsque le demandeur est une autorité publique ou l'employeur de la personne concernée ;
- lorsque la personne concernée est un enfant, que le consentement requis[77] dans le cadre de l'offre directe de services de la société de l'information est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, si celui-ci est âgé de moins de 15 ans[78],'. En pareil cas, le demandeur vérifie ' que ce consentement est effectivement donné ou autorisé par le titulaire de la responsabilité parentale, compte tenu des moyens technologiques disponibles[79] ;
- dans les cas où il existe un risque sérieux sur la protection des données qui nécessitent un plus haut degré de contrôle de l'individu[80], qu'il dispose d'une déclaration expresse de la part de la personne concernée[81] ;
- être en mesure de démontrer à tout moment que la personne a bien consenti et de conserver les traces et preuves du consentement ;
- de documenter les conditions de recueil du consentement.

115. **E06-S03-C03 : Conditions propres au contrat.** Le demandeur retient le contrat comme base légale lorsque le traitement est nécessaire à l'exécution d'un contrat entre le demandeur et les personnes concernées.

116. **E06-S03-C04 : Conditions propres à l'obligation légale.** Le demandeur retient l'obligation légale comme base légale lorsque la mise en œuvre d'un traitement lui est imposée par des textes européens ou nationaux.

117. **E06-S03-C05 : Conditions propres à l'intérêt légitime.** Le demandeur retient l'intérêt légitime comme base légale si les intérêts qu'il poursuit ne créent pas de déséquilibre au détriment des droits et intérêts des personnes dont les données à caractère personnel sont traitées et sont compatibles avec les « attentes raisonnables » de ces personnes et si le droit national ou de l'Union européenne n'impose pas une autre base juridique que l'intérêt légitime.

118. **E06-S03-C06 : Conditions propres à la mission d'intérêt public.** Le demandeur justifie le recours à cette base légale :

---

[76] Par exemple, si le consentement a été recueilli en ligne, il doit pouvoir être retiré en ligne également.

[77] RGPD, Art. 6-1 a).

[78] Loi Informatique et libertés modifiée, Art. 45.

[79]RGPD, Art. 8-2.

[80] Par exemples pour le traitement des données sensibles ou pour permettre la prise de décision entièrement automatisée.

[81] Pour s'assurer d'un consentement explicite, le demandeur peut par exemple prévoir une case de recueil du consentement spécifiquement dédiée au traitement des données sensibles, demander une déclaration écrite et signée par la personne concernée ou l'envoi d'un courriel indiquant que la personne accepte expressément le traitement de certaines catégories de données…

- s'il est un organisme public, pour les traitements mis en œuvre aux fins d'exécuter ses missions ;
- s'il est un organisme privé, par la poursuite d'une mission d'intérêt public ou le fait qu'il soit doté de prérogative de puissance publique.

119. **E06-S03-C07 : Conditions propres à la sauvegarde des intérêts vitaux.** Le demandeur retient la sauvegarde des intérêts vitaux comme base légale uniquement lorsqu'un intérêt vital est en jeu et que la personne concernée est dans l'incapacité physique ou juridique de donner son consentement pour le traitement.

6.4 Exigences relatives au dossier de conception du traitement de données à caractère personnel (S04)

120. **E06-S04-C01 : Dossier de conception du traitement - existence.** Le demandeur a élaboré un modèle de dossier de conception du traitement dont la procédure visée au E10-S02-C02 fait référence. Ce modèle est utilisé pour les nouveaux traitements de données à caractère personnel à compter de la date où le demandeur a mis en place ce dossier.

121. **E06-S04-C02 : Dossier de conception du traitement - contenu.** Le modèle de dossier de conception du traitement comprend :
- les finalités détaillées du traitement ;
- les catégories de données à caractère personnel traitées et classifiées selon les catégories visées au E05-S01-C01 ;
- les personnes concernées ;
- la description des acteurs impliqués dans le traitement et leur rôle ;
- les flux de données à caractère personnel ;
- la durée de conservation envisagée ;
- les mécanismes d'information des personnes et, le cas échéant, de recueil du consentement ;
- les mesures de sécurité et de confidentialité envisagées ;
- les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (ces mesures correspondent à celles définies, le cas échéant, par les codes de conduite approuvés par la Cnil et les référentiels publiés par la Commission) ;
- l'étude des risques en l'absence de réalisation d'analyse d'impact ;
- le cas échéant, les transferts de données à caractère personnel hors UE ;
- le cas échéant, les références réglementaires ou sectorielles à respecter.

122. **E06-S04-C03 : Dossier de conception du traitement - application.** Le demandeur établit, pour chaque traitement concerné, le dossier de conception du traitement visé au critère E06-S04-C01, réalise un audit annuel dans le respect du critère E01-S03-C03 afin de s'assurer que le dossier de conception du traitement est élaboré par les métiers et rédige un rapport à l'issu de l'audit.

7. Exigences relatives aux registres (E07)

7.1 Exigences relatives au registre des activités de traitement (S01)

123. **E07-S01-C01 : Politique relative au registre des activités de traitement - existence.** Le demandeur dispose d'une politique relative au registre des activités de traitement qui lui

impose de constituer un registre en sa qualité de responsable du traitement, même s'il n'est pas légalement soumis à cette obligation.

124. **E07-S01-C02 : Procédure relative au registre des activités de traitement - existence**. Le demandeur dispose d'une procédure relative au registre des activités de traitement applicable préalablement à la mise en œuvre d'un nouveau traitement ou avant la modification substantielle d'un traitement existant.

125. **E07-S01-C03 : Procédure relative au registre des activités de traitement – contenu.** La procédure visée au E07-S01-C02 décrit la méthodologie à suivre pour constituer le registre, en assurer la complétude et le mettre à jour à savoir :
- rassembler les informations disponibles en identifiant et rencontrant les responsables opérationnels des différents services susceptibles de traiter des données à caractère personnel ;
- élaborer la liste des traitements visée au critère E04-S02-C02 en listant, par finalité, les différentes activités du demandeur nécessitant le traitement de données à caractère personnel ;
- inscrire au fil de l'eau les nouveaux traitements ainsi que les modifications substantielles des traitements existants ;
- effectuer une revue annuelle de ce registre.

126. **E07-S01-C04 : Procédure relative au registre des activités de traitement -application**. Le demandeur met en œuvre la procédure relative au registre des activités de traitement, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative au registre des activités de traitement est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

127. **E07-S01-C05 : Contenu du registre des activités de traitement**[82]**.** Le registre des activités de traitements constitué par le demandeur indique :
- le nom et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement et du délégué à la protection des données ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel répondant à la classification visée au E05-C01-S01 ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale (y compris leur identification) ainsi que les documents attestant de l'existence de garanties appropriées ;
- les délais prévus pour l'effacement des différentes catégories de données à caractère personnel ;
- une description générale des mesures de sécurité techniques et organisationnelles.

7.2 Exigences relatives au registre des traitements de données à caractère personnel confiés à des sous-traitant (S02)

128. **E07-S02-C01 : Politique relative au registre des traitements confiés à des sous-traitants - existence.** Le demandeur dispose d'une politique qui lui impose de constituer un registre des

[82] RGPD, Art. 30-1.

traitements de données à caractère personnel qu'il confie, en sa qualité de responsable du traitement, à des sous-traitants.

129. **E07-S02-C02 : Procédure relative au registre des traitements confiés à des sous-traitants - existence.** Le demandeur dispose d'une procédure relative au registre des traitements de données à caractère personnel confiés à des sous-traitants applicable préalablement à la mise en œuvre d'un nouveau traitement confié à un sous-traitant ou avant la modification substantielle d'un traitement existant faisant intervenir un sous-traitant.

130. **E07-S02-C03 : Procédure relative au registre des traitements confiés à des sous-traitants – contenu.** La procédure visée au E07-S02-C02 décrit la méthodologie à suivre pour constituer le registre, en assurer la complétude et le mettre à jour.

131. **E07-S02-C04 : Procédure relative au registre des traitements confiés à des sous-traitants - application.** Le demandeur met en œuvre la procédure relative au registre des traitements confiés à des sous-traitants, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative au registre des traitements confiés à des sous-traitants est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

132. **E07-S02-C05 : Contenu du registre des traitements confiés à des sous-traitants.** Le registre des traitements de données à caractère personnel confiés à des sous-traitants précise :
- le nom et les coordonnées des sous-traitants ;
- les catégories de traitements effectués par les sous-traitants pour le compte du demandeur en sa qualité de responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers, y compris l'identification de ce pays tiers et les documents attestant de l'existence de garanties appropriées ;
- une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre par les sous-traitants.

7.3 Exigences relatives au registre des violations de données à caractère personnel (S03)

133. **E07-S03-C01 : Contenu du registre des violations de données à caractère personnel[83].** Le registre des violations de données à caractère personnel constitué par le demandeur indique :
- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif d'enregistrements concernés ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- les violations notifiées auprès de la Cnil et/ou ayant fait l'objet d'une communication aux personnes concernées ;
- le cas échéant, la justification de l'absence de notification auprès de la Cnil ou d'information aux personnes concernées. ;
- le descriptif des incidents de sécurité ayant fait l'objet d'une qualification[84].

[83] RGPD, Art. 33-5.

[84] Exemples : sans violation de données, tentative avérée mais sans succès…

8. Exigences relatives à la durée de conservation des données à caractère personnel (E08)

8.1 Exigences relatives à la politique de durée de conservation des données à caractère personnel (S01)

134. **E08-S01-C01 : Politique de durée de conservation des données à caractère personnel.** Le demandeur met en œuvre la politique de durée de conservation des données à caractère personnel visée au E05-S04-C08.

8.2 Exigences relatives à la table des durées de conservation des données à caractère personnel (S02)

135. **E08-S02-C01 : Table des durées de conservation[85] - existence.** Le demandeur établit et met régulièrement à jour une table identifiant les durées applicables à la conservation des données à caractère personnel traitées dans le cadre de son activité.

136. **E08-S02-C02 : Table des durées de conservation - contenu.** La table des durées de conservation des données à caractère personnel précise, pour chaque traitement de données à caractère personnel :
- la durée de conservation des données à caractère personnel en base active[86] ;
- la durée de conservation des données à caractère personnel en archivage intermédiaire[87] ;
- la durée de conservation des données à caractère personnel en archivage définitif[88] ;
- les fondements/textes de référence ;
- la date de mise à jour : il s'agit de la date de dernière vérification des fondements/textes de référence.

137. **E08-S02-C03 : Table des durées de conservation - application.** Le demandeur met en œuvre la table des durées de conservation, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la table des durées de conservation est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

8.3 Exigences relatives à la procédure en matière de durée de conservation des données à caractère personnel (S03)

138. **E08-S03-C01 : Procédure de durée de conservation des données à caractère personnel - existence.** Le demandeur dispose d'une procédure permettant le respect des durées de conservation des données à caractère personnel telles que définies dans la table visée au E08-S02-C01.

---

[85] Cnil, « Guide pratique les durées de conservation », 07 2020.

[86] Il s'agit de la durée pendant laquelle les données personnelles sont accessibles dans le cadre d'une utilisation courante par les services opérationnels chargés du traitement. Il s'agit de la durée nécessaire à la réalisation de l'objectif (finalité du traitement) ayant justifié la collecte/enregistrement des données. En pratique, les données seront alors facilement accessibles dans l'environnement de travail immédiat pour les services opérationnels qui sont en charge de ce traitement (ex : le service des ressources humaines pour les opérations de recrutement).

[87] C'est la durée prédéfinie pendant laquelle, une fois la finalité atteinte, il est possible, sous conditions, de maintenir les données accessibles à des personnes habilitées.

[88] Il s'agit des données qui sont archivées sans limitation de durée.

139. **E08-S03-C02 : Procédure de durée de conservation des données à caractère personnel - contenu.** La procédure relative à la durée de conservation des données personnelles visée au E08-S03-C01 prévoit :
- les modalités d'accès spécifiques aux données à caractère personnel archivées ;
- les modalités de destruction des archives obsolètes de manière sécurisée ou de versement, le cas échéant, des documents présentant un intérêt historique, scientifique ou statistique aux archives publiques dans les conditions fixées par le code du patrimoine ;
- les modalités de versement aux archives intermédiaires visées au E08-S04-S01 et définitives visées au E08-S05-C01 ;
- le processus de suppression qui doit être appliqué en base active suite au versement ;
- les processus et les rôles de gestion des archives : distinguer les processus de versement, stockage, gestion des données à caractère personnel descriptives, consultation /communication et administration (relation avec les services producteurs, veille technologique et juridique, projets d'évolution et migration des supports et des formats) ;
- comment vérifier que les mesures prises permettent de garantir, si besoin, l'identification et l'authentification de l'origine des archives, l'intégrité des archives, l'intelligibilité et la lisibilité des archives, la durée de conservation des archives, la traçabilité des opérations effectuées sur les archives (versement, consultation, migration, élimination), la disponibilité et l'accessibilité des archives, les compléter si ce n'est pas le cas.

Le fait de suivre cette procédure permet de garantir que des moyens de protection de la confidentialité des données à caractère personnel archivées (selon les risques identifiés) seront appliqués.

140. **E08-S03-C03 : Procédure de durée de conservation des données à caractère personnel - application.** Le demandeur met en œuvre la procédure relative au respect des durées de conservation, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure de durée de conservation des données à caractère personnel est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

8.4 Exigences relatives à la procédure d'archivage intermédiaire (S04)

141. **E08-S04-C01 : Procédure d'archivage intermédiaire - existence.** Le demandeur dispose une procédure relative à l'archivage intermédiaire des données à caractère personnel qui doivent être conservées pour répondre à une obligation légale ainsi que pour constituer des éléments de preuve dans le cadre d'un contentieux. Cette procédure s'applique lorsque les données à caractère personnel ne sont plus utilisées pour atteindre l'objectif fixé[89] initialement (finalité du traitement) ayant justifié la collecte des données à caractère personnel, mais présentent encore un intérêt administratif pour l'organisme (exemple : gestion d'un éventuel contentieux) ou doivent être conservées pour répondre à une obligation légale.

142. **E08-S04-C02 : Procédure d'archivage intermédiaire - contenu :** La procédure visée au E08-S04-C01 précise :
- les objectifs de l'archivage intermédiaire ;
- les critères de sélection du type de données à caractère personnel devant faire l'objet d'un archivage intermédiaire ;
- les modalités de préparation des données à caractère personnel, c'est-à-dire les étapes à suivre pour préparer les données à caractère personnel à être archivées, y compris leur

[89] « Dossier Clos ».

nettoyage, leur anonymisation, leur compression éventuelle, leur regroupement par catégories et le lieu de stockage ;
- la méthode d'archivage, c'est-à-dire la description de la méthode utilisée pour l'archivage intermédiaire (système d'archivage électronique, supports physiques ou combinaison des deux) ;
- la méthode d'indexation des métadonnées, c'est-à-dire la définition des informations à conserver en tant que métadonnées associées à chaque ensemble de données à caractère personnel archivées, permettant ainsi une recherche et une récupération efficaces ultérieures ;
- les mesures de sécurité à mettre en place pour protéger les données à caractère personnel archivées contre tout accès non autorisé ;
- les durées de conservation des données à caractère personnel visées au E08-S02-C02 ;
- les modalités d'accès et de récupération des données à caractère personnel, c'est-à-dire les procédures à suivre pour permettre un accès et une récupération appropriés des données à caractère personnel archivées lorsque cela est nécessaire, en précisant les autorisations requises et les processus d'approbation ;
- les modalités de destruction des données à caractère personnel archivées, c'est-à-dire les mesures à prendre lorsque les données à caractère personnel archivées atteignent la fin de leur durée de conservation, y compris les méthodes de destruction sécurisée des supports physiques ou l'effacement définitif des données électroniques ;
- les modalités de suivi et d'audit, c'est-à-dire les modalités de suivi et de vérification régulière de l'intégrité des données à caractère personnel archivées, ainsi que des audits périodiques pour s'assurer de la conformité aux politiques et aux procédures d'archivage.

143. **E08-S04-C03 : Procédure d'archivage intermédiaire - application.** Le demandeur met en œuvre la procédure relative à l'archivage intermédiaire, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure d'archivage intermédiaire est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

8.5 Exigences relatives à la procédure d'archivage définitif (S05)

144. **E08-S05-C01 : Procédure d'archivage définitif - existence.** Le demandeur dispose d'une procédure relative à l'archivage définitif des données à caractère personnel qui en raison de leur intérêt historique doivent être archivées de manière définitive et pérenne. Les traitements à des fins archivistiques dans l'intérêt public sont visés par cette procédure. Cette procédure s'applique à l'expiration de la durée relative à l'archivage intermédiaire.

145. **E08-S05-C02 : Procédure d'archivage définitif - contenu :** La procédure visée au E08-S05-C01 précise :
- les objectifs de l'archivage définitif ;
- les critères de sélection du type de données à caractère personnel devant faire l'objet d'un archivage définitif ;
- les modalités de préparation des données à caractère personnel, c'est-à-dire les étapes à suivre pour préparer les données à caractère personnel à être archivées, y compris leur nettoyage, leur anonymisation en application de E14-S04, leur compression éventuelle, leur regroupement par catégories et le lieu de stockage ;
- la méthode d'archivage, c'est-à-dire la description de la méthode utilisée pour l'archivage définitif (système d'archivage électronique, supports physiques ou combinaison des deux) ;
- la méthode d'indexation des métadonnées, c'est-à-dire la définition des informations à conserver en tant que métadonnées associées à chaque ensemble de données à caractère

personnel archivées, permettant ainsi une recherche et une récupération efficaces ultérieures ;
- les mesures de sécurité à mettre en place pour protéger les données à caractère personnel archivées contre tout accès non autorisé ;
- les modalités d'accès et de récupération des données à caractère personnel, c'est-à-dire les procédures à suivre pour permettre un accès et une récupération appropriés des données à caractère personnel archivées lorsque cela est nécessaire, en précisant les autorisations requises et les processus d'approbation ;
- les modalités de destruction, élimination ou anonymisation des données à caractère personnel conformément à E14-S04, c'est-à-dire un descriptif des mesures à prendre pour empêcher toute destruction ou modification accidentelle des données à caractère personnel archivées de manière définitive, et pour assurer leur préservation même en cas de changement de technologie ou de support de stockage ;
- les modalités de suivi et d'audit, c'est-à-dire les modalités de suivi et de vérification régulière de l'intégrité des données à caractère personnel archivées, ainsi que des audits périodiques pour s'assurer de la conformité aux politiques et aux procédures d'archivage.

146. **E08-S05-C03 : Procédure d'archivage définitif - application.** Le demandeur met en œuvre la procédure relative à l'archivage définitif, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure d'archivage définitif est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

8.6 Exigences relatives à la procédure de purge (S06)

147. **E08-S06-C01 : Procédure de purge - existence.** Le demandeur dispose d'une procédure relative à la purge des données à caractère personnel. Cette procédure est applicable aux données à caractère personnel en base active et mise en œuvre à l'expiration de la durée relative à l'archivage intermédiaire.

148. **E08-S06-C02 : Procédure de purge - contenu :** La procédure visée au E08-S06-C01 précise :
- les objectifs de la purge ;
- les critères de sélection du type de données à caractère personnel devant faire l'objet d'une purge ;
- les procédures de validation et d'approbation pour la suppression des données à caractère personnel, en s'assurant que toutes les exigences légales, réglementaires ou internes sont respectées avant de procéder à la purge ;
- les méthodes spécifiques utilisées pour supprimer les données à caractère personnel de manière sécurisée et irréversible, telles que l'effacement sécurisé des disques durs, la destruction physique des supports de stockage, l'utilisation de techniques de suppression de données conformes aux normes reconnues, l'anonymisation selon les modalités visées au E14-S04-C02 ;
- l'enregistrement précis des données à caractère personnel purgées, y compris les détails de leur identification, les motifs de leur suppression, les autorisations associées ;

- les modalités de contrôle qualité permettant de s'assurer de l'efficacité et de l'intégrité du processus de purge des données à caractère personnel, y compris la vérification de l'exhaustivité et de la précision des enregistrements, la validation de la suppression effective des données ;
- les procédures de communication internes et externes liées à la purge de données à caractère personnel ;

- les modalités de suivi et de vérification régulière de l'efficacité du processus de purge des données à caractère personnel, ainsi que des audits périodiques pour s'assurer de la conformité aux politiques et aux procédures de purge.

149. **E08-S06-C03 : Procédure de purge - application.** Le demandeur met en œuvre la procédure de purge, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure de purge est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

8.7 Exigences relatives à la procédure de remise à zéro des matériels (S07)

150. **E08-S07-C01 : Procédure de remise à zéro des matériels - existence.** Le demandeur dispose, en cas de revente, destruction ou réaffectation du matériel, départ d'un collaborateur d'une procédure de remise à zéro des matériels utilisés pour réaliser les traitements de données à caractère personnel qui se trouvent dans la cible d'évaluation, laquelle distingue quatre grandes catégories de matériaux :
- les équipements des collaborateurs[90] ;
- les serveurs ;
- les disques ;
- les baies de sauvegarde.

Pour chaque catégorie de matériel, le demandeur définit la procédure, les documents associés et établit les procès-verbaux. En cas de sous-traitance de ces opérations, un contrat fixera le respect de ces procédures et le sous-traitant devra adresser au fur et à mesure de l'exécution des prestations selon la nécessité définie par le demandeur, des attestations de destruction des données à caractère personnel confiées.

151. **E08-S07-C02 : Procédure de remise à zéro des matériels – contenu.** La procédure visée au E08-S07-C01 précise :
- les modalités de remise en main propre du matériel ;
- les modalités d'inspection du matériel pour s'assurer que toute donnée a bien été effacée ;
- les modalités de stockage du matériel dans un local sécurisé en attendant qu'il quitte l'organisme ;
- de faire signer un accord de confidentialité dans le cas où la remise à zéro du matériel est réalisée par un tiers ;
- d'émettre un PV de remise à zéro du matériel et de le conserver pendant 10 ans ;
- le matériel concerné par la remise à zéro ;
- les obligations des salariés en matière de purge des données contenues dans le matériel ;
- les modalités de remise à zéro et de réinitialisation du matériel ;
- les modalités de conservation des traces des opérations d'effacement des données contenues dans le matériel.
- d'utiliser un dispositif d'effacement sécurisé sur les données à caractère personnel stockées sur les disques durs ou la mémoire intégrée ou détruire physiquement le matériel si ce n'est pas possible.

152. **E08-S07-C03 : Procédure de remise à zéro des matériels - application.** Le demandeur met en œuvre la procédure de remise à zéro des matériels, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure de remise à zéro des matériels est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

[90] PC, téléphone portable...

8.8 Exigences relatives à la durée de conservation des traitements de données à caractère personnel papiers (S08)

153. **E08-S08-C01 : Procédure de durée de conservation des traitements papiers**[91] **- existence.** Le demandeur dispose d'une procédure relative à de durée de conservation des données à caractère personnel figurant dans traitements papiers. Cette procédure précise :
- comment les documents papier sont imprimés, stockés, détruits et échangés ;
- les modalités de récupération des documents imprimés, notamment s'ils doivent être récupérés immédiatement ou imprimés à partir d'une imprimante sécurisée ;
- les conditions de diffusion des documents papier contenant des données à caractère personnel, notamment les limitations de diffusion à appliquer ;
- les modalités de stockage les documents papier contenant des données à caractère personnel dans un meuble sécurisé ;
- les modalités de destruction des documents papier contenant des données à caractère personnel et qui ne sont plus utiles à l'aide d'un broyeur approprié ;
- les modalités visant à sécuriser leur transport : sensibiliser les personnes transportant les documents papier aux risques s'ils appartiennent à l'organisme, prévoir des clauses relatives à la protection de la disponibilité, de l'intégrité et de la confidentialité des documents papier dans le contrat établi avec un transporteur tiers, contrôler l'identité du transporteur, envoyer les documents sous double enveloppe en recommandé, apposer une marque « Confidentiel » sur les enveloppes.

154. **E08-S08-C02 : Procédure de durée de conservation des traitements papiers - application.** Le demandeur met en œuvre la procédure de durée de conservation des traitements papiers, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que cette procédure est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

9. Exigences relatives aux mentions obligatoires et contrats (E09)

9.1 Exigences relatives aux contrats conclus avec les sous-traitants (S01)

155. **E09-S01-C01 : Modèle de contrat**[92]**.** Dans le cadre de la procédure visée au E18-S01-C01 qui encadre le recours à des sous-traitants, le demandeur a constitué un modèle de contrat, définissant l'objet, la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées, les obligations et droits du demandeur. Le modèle de contrat précise que le sous-traitant :
- ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement ;
- veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- prend toutes les mesures requises pour assurer la sécurité des données à caractère personnel ;
- obtient une autorisation écrite spécifique ou générale pour recruter un autre sous-traitant ;

[91] Il s'agit des traitements de données à caractère personnel dans la cible d'évaluation qui sont basés sur un fichier papier organisé.

[92] RGPD, Art. 28.

- doit informer, si l'autorisation a une portée générale, le responsable de traitement de la liste de ses sous-traitants ultérieurs, ainsi que de tout ajout ou remplacement dans cette liste, afin de lui permettre d'y objecter s'il le souhaite ;
- demeure responsable devant le responsable du traitement si le sous-traitant recruté ne remplit pas ses obligations ;
- aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits ;
- aide le responsable du traitement à établir les analyses d'impacts compte tenu de la nature du traitement et des informations à la disposition du sous-traitant et à garantir le respect des obligations relatives à la sécurité des données à caractère personnel compte tenu de la nature du traitement et des informations dont il dispose (par exemples en mettant en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ou en notifiant les violations de données à caractère personnel aux personnes concernées) ;
- selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes ;
- met à la disposition du responsable du traitement toutes les informations nécessaires 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 ;
- informe le responsable du traitement si une instruction constitue une violation des règles applicables en matière de protection des données à caractère personnel ;
- s'engage contractuellement à informer le responsable du traitement qu'il est tenu de procéder à un traitement de données à caractère personnel en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, sauf si la loi le lui interdit pour des motifs importants d'intérêt public.

Le modèle de contrat prévoit une annexe permettant au demandeur de documenter les instructions données au sous-traitant quant au traitement des données à caractère personnel.

156. **E09-S01-C02 : Suivi des contrats conclus avec les sous-traitants.** Le demandeur dispose d'une liste de sous-traitants qui précise si les contrats conclus avec les sous-traitants intègrent des clauses répondant au critère E09-S01-C01.

9.2 Exigences relatives aux mentions d'information (S02)

157. **E09-S02-C01 : Modèle de mention d'information en cas de collecte directe.** Le demandeur dispose d'un modèle de mention d'information en cas de collecte directe[93] ainsi que de l'historique des versions dont ce modèle a fait l'objet. Ce modèle d'information intègre, comme pour la politique visée au E01-S02-C01, les éléments suivants :
- identité et coordonnées du demandeur (responsable du traitement) ;
- finalités ;
- base légale du traitement des données à caractère personnel ;
- caractère obligatoire ou facultatif du recueil des données à caractère personnel et conséquences
- pour la personne en cas de non-fourniture des données à caractère personnel ;
- destinataires ou catégories de destinataires des données à caractère personnel ;
- durée de conservation des données (ou critères permettant de la déterminer) ;

[93] RGPD, Art.13.

- droits des personnes concernées ;
- coordonnées du délégué à la protection des données s'il a été désigné ou d'un point de contact sur les questions de protection des données à caractère personnel ;
- droit d'introduire une réclamation auprès de la Cnil.

Selon les cas, les informations suivantes figurent également dans ce modèle :

- les intérêts légitimes poursuivis par le demandeur en sa qualité de responsable du traitement ;
- le fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat ;
- l'existence d'un transfert des données à caractère personnel vers un pays hors union européenne (ou vers une organisation internationale), les garanties associées à ce transfert et la faculté d'accéder aux documents autorisant ce transfert ;
- l'existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée ;
- le droit au retrait du consentement à tout moment, si la base légale du traitement est le consentement des personnes ;
- les autres droits applicables au traitement de données à caractère personnel, en fonction de sa base légale : droit d'opposition et droit à la portabilité.

Le demandeur fournit ces informations au moment du recueil des données à caractère personnel.

158. **E09-S02-C02 : Modèle de mention d'information en cas de collecte indirecte.** Le demandeur dispose d'un modèle de mention d'information en cas de collecte indirecte[94] ainsi que de l'historique des versions dont ce modèle a fait l'objet. Ce modèle d'information intègre, comme pour la politique visée au E01-S02-C01, les éléments suivants :

- identité et coordonnées du demandeur (responsable du traitement) ;
- finalités ;
- base légale du traitement des données à caractère personnel ;
- caractère obligatoire ou facultatif du recueil des données à caractère personnel et conséquences
- pour la personne en cas de non-fourniture des données à caractère personnel ;
- destinataires ou catégories de destinataires des données à caractère personnel ;
- durée de conservation des données (ou critères permettant de la déterminer) ;
- droits des personnes concernées ;
- coordonnées du délégué à la protection des données s'il a été désigné ou d'un point de contact sur les questions de protection des données à caractère personnel ;
- droit d'introduire une réclamation auprès de la Cnil.

Selon les cas, les informations suivantes figurent également dans ce modèle :

- les intérêts légitimes poursuivis par le demandeur en sa qualité de responsable du traitement ;
- le fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat ;
- l'existence d'un transfert des données à caractère personnel vers un pays hors union européenne (ou vers une organisation internationale), les garanties associées à ce transfert et la faculté d'accéder aux documents autorisant ce transfert ;
- l'existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée ;

[94] RGPD, Art.14.

- le droit au retrait du consentement à tout moment, si la base légale du traitement est le consentement des personnes ;
- les autres droits applicables au traitement de données à caractère personnel, en fonction de sa base légale : droit d'opposition et droit à la portabilité.

Enfin, les Informations suivantes sont communiquées :

- catégories de données à caractère personnel recueillies répondant à la classification visée au E05-C01-S01 ;
- source des données (en indiquant notamment si elles sont issues de sources accessibles au public).

Le demandeur fournit ces informations dès que possible (notamment lors du premier contact avec la personne concernée) et, au plus tard, dans le délai d'un mois (sauf exceptions).

159. **E09-S02-C03 : Recueil des mentions d'information.** Le demandeur dispose d'un recueil des mentions d'information fournies aux personnes concernées.

160. **E09-S02-C04 : Revue des modèles et du recueil des mentions d'information.** Le demandeur établit une procédure prévoyant un examen régulier des modèles de mentions d'information ainsi que des mentions d'information fournies aux personnes concernées intégrées au recueil visé au E09-S02-C03. La fréquence de l'examen régulier est définie par le demandeur.

161. **E09-S02-C05 : Modalités d'information des personnes.** Le demandeur délivre aux personnes concernées, en application du critère E01-S02-C03, une information en utilisant un vocabulaire simple, adapté au public visé, en rédigeant des phrases courtes et lisibles et en permettant aux personnes concernées de voir immédiatement comment et où accéder à l'information. Il leur garantit l'accessibilité de l'information en adaptant les méthodes choisies en fonction du contexte et des modalités d'interaction avec les personnes concernées (site intranet et/ou affichage et/ou courrier électronique personnalisé et/ou kit d'arrivée et/ou documentation papier ou électronique et/ou encart dédié apposé en bas des formulaires).

10. Exigences relatives à la protection des données à caractère personnel dès la conception[95] (E10)

10.1 Exigences relatives à la politique de protection des données à caractère personnel dès la conception (S01)

162. **E10-S01-C01 : Politique relative à la protection dès la conception - existence.** Le demandeur a élaboré une politique qui impose de mettre en œuvre des mesures techniques et organisationnelles dès les premières étapes de la conception des opérations de traitement, de manière à préserver en amont les principes en matière de protection des données à caractère personnel.

10.2 Exigences relatives à la procédure de protection dès la conception (S02)

163. **E10-S02-C01** : **Procédure relative à la protection dès la conception - existence.** Le demandeur dispose d'une procédure relative à la protection dès la conception qui s'applique aux nouveaux traitements de données à caractère personnel et aux modifications appliquées aux traitements de données à caractère personnel qui sont dans le périmètre de la certification. ’’’’’

[95] RGPD, Art.25-1.

164. **E10-S02-C02 : Procédure relative à la protection dès la conception - contenu.** La procédure relative à la protection dès la conception précise :
- le moment où elle doit être déclenchée ;
- ses objectifs (prendre en compte toutes les exigences légales en début de phase de conception, garder opérationnelles ces exigences pendant le cycle de vie, mobiliser les métiers au respect de la protection des données à caractère personnel) ;
- les étapes de la procédure à respecter lors de la conception d'un nouveau traitement (dossier de conception du traitement visé au E06-S04-C01, analyse de la conformité aux exigences légales, plan d'action visé au E03-S02-C05, mise en œuvre du plan d'action et calendrier visé au E03-S02-C06) ;
- que le délégué (DPO) doit être associé suffisamment tôt dans la conception des traitements pour que ses conseils puissent être pris en considération dès le cahier des charges.
- les mécanismes à mettre à œuvre pour l'ajustement continu des mesures techniques et organisationnelles adoptées, afin de garantir que celles-ci restent appropriées et effectives tout au long du cycle de vie du traitement de données à caractère personnel.

165. **E10-S02-C03 : Procédure relative à la protection dès la conception - application.** Le demandeur met en œuvre la procédure relative à la protection dès la conception, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que cette procédure est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

10.3 Exigences relatives au dossier de conception du traitement (S03)

166. **E10-S03-C01 : Dossier de conception du traitement - existence.** Le demandeur a élaboré le dossier de conception du traitement dont le critère E06-S04-C01 fait référence.

167. **E10-S03-C02 : Dossier de conception du traitement - contenu.** Le contenu du dossier de conception est défini au E06-S04-C02.

168. **E10-S03-C03 : Dossier de conception du traitement – élaboration.** Les métiers impliqués dans le traitement sont parties prenantes pour l'élaboration de chaque dossier de conception des traitements.

11. Exigences relatives à la protection des données à caractère personnel par défaut[96] (E11)

11.1 Exigences relatives à la politique de protection par défaut (S01)

169. **E11-S01-C01 : Politique relative à la protection par défaut - existence.** Le demandeur a élaboré une politique qui pose la règle selon laquelle les mesures techniques et organisationnelles appropriées sont mises en œuvre pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

[96] RGPD, Art.25-1.

11.2 Exigences relatives à la procédure de protection par défaut (S02)

170. **E11-S02-C01 : Procédure relative à la protection par défaut - existence.** Le demandeur dispose d'une procédure relative à la protection par défaut. Le demandeur peut également avoir regroupé dans une seule et même procédure les exigences relatives à la protection dès la conception visée au E10-S02-C01 et à la protection par défaut visée au critère E11-S02-C01.

171. **E11-S02-C02 : Procédure relative à la protection par défaut - contenu.** La procédure relative à la protection par défaut précise :
- la démarche à suivre pour identifier les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées ;
- que cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité ;
- que les mesures qui seront retenues devront garantir que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

Cette procédure s'articule avec la justification du besoin de la collecte (E05-S01-C02, E05-S01-C05, E05-S01-C11 et E05-S01-C08) et le cloisonnement des données à caractère personnel (E14-S07-C01).

172. **E11-S02-C03 : Procédure relative à la protection par défaut - application.** Le demandeur met en œuvre la procédure relative à la protection par défaut, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que cette procédure est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

12. Exigences relatives à la redevabilité (accountability) (E12)

12.1 Exigences relatives à la documentation dédiée à la protection des données à caractère personnel (S01)

173. **E12-S01-C01 Liste de la documentation - existence.** Le demandeur a établi une liste organisée et structurée de la documentation pour démontrer la conformité aux critères.

174. **E12-S01-C02 : Liste de la documentation – mise à jour.** Les politiques, procédures internes, procédures internes, programmes, dossiers et modèles intégrés dans la liste visée au E12-S01-C01 sont revues, a minima chaque année et mises à jour autant que de besoin.

12.2 Exigences relatives au site de redevabilité (accountability) (S02)

175. **E12-S02-C01 : Site de redevabilité (accountability) - existence.** Le demandeur dispose d'un site de redevabilité (accountability) qui comprend quatre espaces :
- un espace dans lequel figure la liste organisée et structurée de la documentation visée au critère E12-S01-C01 ainsi que la documentation associée ;
- un espace de sensibilisation et formation destiné aux utilisateurs métiers comprenant les éléments visés au E16-S01-C01 ;
- un espace de conception/projet de traitement ;
- un espace plus expert/confidentiel destiné par exemple aux experts de la sécurité.

176. **E12-S02-C02 : Site de redevabilité (accountability) – disponibilité.** Le demandeur dispose d'une liste des membres du personnel habilités à accéder à ce site.

13. Exigences relatives aux analyses d'impact (E13)

13.1 Exigences relatives à la politique d'analyse d'impact (S01)

177. **E13-S01-C01 : Politique relative aux analyses d'impact - existence.** Le demandeur a élaboré une politique relative aux analyses d'impact.

178. **E13-S01-C02 : Politique relative aux analyses d'impact - contenu.** La politique relative aux analyses d'impact définie :
- les acteurs qui interviennent dans la réalisation d'une analyse d'impact ;
- la méthode à suivre, y compris pour l'analyse de risque ;
- les cas de transmission éventuelle de l'analyse d'impact à la Cnil.

13.2 Exigences relatives à la procédure d'analyses d'impact (S02)

179. **E13-S02-C01 : Procédure relative aux analyses d'impact - existence.** Le demandeur dispose d'une procédure relative aux analyses d'impact. Cette procédure s'applique préalablement à la mise en œuvre de traitements de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées ainsi qu'avant la modification substantielle de traitements de ce type existants.

180. **E13-S02-C02 : Procédure relative aux analyses d'impact[97] - contenu.** La procédure relative aux analyses d'impact précise :
- les éléments à prendre en compte pour identifier si un traitement est ou non soumis à analyse d'impact, à savoir[98] :
    - soit le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la Cnil a estimé obligatoire de réaliser une analyse d'impact relative à la protection des données à caractère personnel,
    - soit le traitement envisagé figure dans la liste des traitements pour lesquelles la Cnil a estimé qu'une analyse d'impact n'est pas requise,
    - soit le traitement remplit au moins deux des neuf critères issus des lignes directrices du CEPD :
        - évaluation/scoring (y compris le profilage) ;
        - décision automatique avec effet légal ou similaire ;
        - surveillance systématique ;
        - collecte de données à caractère personnel sensibles ou données à caractère hautement personnel ;
        - collecte de données à caractère personnel à large échelle ;
        - croisement de données à caractère personnel ;
        - personnes vulnérables[99] ;
        - usage innovant (utilisation d'une nouvelle technologie) ;
        - exclusion du bénéfice d'un droit/contrat.

[97] RGPD, Art. 35 et Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé.

[98] Cette liste est celle approuvée par la Cnil au titre de l'article 35.4 du RGPD.

[99] Patients, personnes âgées, enfants, salariés… Le CEPD précise dans ses lignes directrices concernant l'analyse d'impact (WP 248 rév. 01) : « Peuvent être comme des personnes vulnérables : les enfants, les employés, les segments les plus vulnérables de la population nécessitant une protection particulière (personnes souffrant de maladie mentale, demandeurs d'asile et personnes âgées, patients, etc.) ».

- soit le traitement ne remplit qu'un seul critère mais il est néanmoins établi qu'il est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physique.

- que les analyses d'impact doivent comprendre :
  - une description systématique des opérations de traitement envisagées et des finalités, y compris l'intérêt légitime poursuivi ;
  - une évaluation de la nécessité et de la proportionnalité des opérations de traitements au regard des finalités ;
  - une évaluation des risques pour les droits et libertés des personnes concernées selon une méthodologie reconnue d'évaluation des risques ;
  - un système de management des risques regroupant les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

La procédure du demandeur prévoit également :

- un examen régulier de la conformité du traitement au regard de l'analyse d'impact, et a minima lorsqu'il y a modification du risque présenté par l'opération de traitement. Les changements pouvant nécessiter une réévaluation du risque peuvent être une modification des sources de risque (ex : un nouveau type d'attaquant ou d'attaque redouté ou constaté à partir d'outil de détection d'incident, l'augmentation du volume d'attaque), un réajustement de la vraisemblance du risque (ex : la mise en place d'une sous-traitance ou l'usage d'un nouveau logiciel avec de nouvelles vulnérabilités), l'évolution du traitement (ex : une augmentation du volume de données ou un interconnexion avec d'autres traitements) ;
- un suivi du plan d'action établit à l'issue d'une analyse d'impact ;
- que les actions correctives adoptées en cas de manquement constaté lors de l'examen de conformité ainsi que les mesures d'atténuation des risques sont documentées et régulièrement mises à jour ;
- que le demandeur s'assure que des mesures suffisantes d'atténuation des risques sont en place pour la mise en œuvre du traitement ;
- que le responsable du traitement sollicite l'avis du délégué (DPO) ;
- que le demandeur sollicite, le cas échéant, l'avis des personnes concernées ou de leurs représentants et, dans ce cas, justifie l'avoir pris en compte ou, à défaut, justifie ne pas en l'avoir sollicité ou ne pas en disposer ;
- une consultation préalable de la Cnil concernant les risques qui n'ont pu être atténués, à la lumière des résultats de l'analyse d'impact ;
- qu'un représentant du responsable du traitement atteste avoir pris connaissance des conclusions de l'analyse d'impact (avec une date) et qu'il s'engage à mettre en œuvre le plan d'actions ;
- la rédaction d'un memorandum permettant de documenter les raisons conduisant à conclure que la réalisation d'une analyse d'impact n'est pas nécessaire ;
- l'élaboration de la liste des traitements soumis à analyse d'impact.

La procédure indique enfin qu'à défaut d'analyse d'impact, le demandeur analyse les risques selon les règles de l'art et fournit un dossier d'analyse de risque. Cette analyse de risque est proportionnée[100] aux activités de traitements en cause.

181. **E13-S02-C03 : Procédure relative aux analyses d'impact - application.** Le demandeur met en œuvre la procédure visée au E13-S02-C01, réalise un audit annuel dans le respect du critère

[100] RGPD, Art. 24-2.

E01-S03-C04 afin de s'assurer que la procédure relative aux analyses d'impact est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

13.3 Exigences relatives aux actions correctives[101] identifiées à l'issue d'une analyse d'impact (S03)

182. **E13-S03-C01 : Suivi du plan d'action.** Le demandeur tient un tableau de suivi du plan d'action élaboré à l'issue d'une analyse d'impact visé au E13-S02-C01.

13.4 Exigences relatives au contenu de l'analyse d'impact (S04)

183. **E13-S04-C01 : Consultation de la Cnil.** Si le risque résiduel reste élevé, le demandeur consultera la Cnil.

13.5 Exigences relatives aux avis et signature (S05)

184. **E13-S05-C01 : Avis du délégué (DPO)[102].** Conformément à la procédure visée au E13-S02-C02, le demandeur soumet chaque analyse d'impact à l'avis du délégué (DPO). L'avis du délégué (DPO) est également sollicité en cas d'évolution de l'analyse d'impact[103].

185. **E13-S05-C02 : Avis du Comité social et économique.** A l'instar de l'avis des personnes concernées ou de leurs représentants visé au critère E13-S02-C02, le demandeur soumet les analyses d'impacts qui concernent des traitements relevant du domaine des ressources humaines et de la sécurité à l'avis du Comité économique et social.

186. **E13-S05-C03 : Signature de la Direction Générale[104].** Le demandeur soumet chaque analyse d'impact à la signature d'un membre de la Direction Générale dont la décision, quant au plan d'action pour la mise en œuvre des actions [105] avant le déploiement du traitement et aux autres mesures d'atténuation des risques, est attendu.

14. Exigences relatives à la sécurité et la gestion des violations de données à caractère personnel (E14)

14.1 Exigences relatives à la documentation générale de sécurité[106] (S01)

187. **E14-S01-C01 : Politique de sécurité des systèmes d'information.** Le demandeur dispose d'une politique de sécurité des systèmes d'information qui précise :

---

[101] Le terme « actions correctives » ne fait pas référence aux pouvoirs dont disposent les autorités de protection des données personnelles en vertu de l'article 58-2 du RGPD, mais aux mesures d'atténuation en cas de non-conformité.

[102] Cnil, Outil PIA, version 2021.

[103] Evolution due par exemple à des nouveaux risques constatés à l'appui des incidents de sécurité, une évolution du traitement ou des moyens du traitement ou à un changement de logiciel.

[104] Cnil, Outil PIA, version 2021.

[105] Le terme « » actions correctives » ne fait pas référence aux pouvoirs dont disposent les autorités de protection des données personnelles en vertu de l'article 58-2 du RGPD, mais aux mesures d'atténuation en cas de non-conformité.

[106] Référentiel Cnil.

- les mécanismes d'authentification des personnes pouvant se connecter au système d'information ;
- la politique d'habilitation ;
- les mesures de sécurité des accès physiques aux bâtiments
- les mesures de sécurité appliquées aux serveurs ;
- les mesures de sécurités appliquées aux postes de travail ;
- les modalités de gestion des risques ;
- les modalités de gestion de la continuité d'activité ;
- les politiques de sauvegardes ;
- les modalités de gestion des incidents de sécurité ;
- la politique de gestion du matériel107 ;
- les procédures de gestion de crise ;
- les modalités de mise en œuvre de tests techniques ;
- Les analyses de risque devant être menées par le demandeur.
- la surveillance du système d'information ;
- les mesures de journalisation en application de la procédure d'exploitation des informations journalisées (logs) visée au E14-S02-C03.

188. **E14-S01-C02 : Charte informatique.** Le demandeur dispose d'une charte informatique qui précise les modalités d'utilisation des moyens informatiques et de communications électroniques mis à disposition des utilisateurs, les conditions d'administration du système d'information ainsi que les sanctions encourues en cas de non-respect de la charte.

14.2 Exigences relatives à la journalisation des accès et incidents[108] (S02)

189. **E14-S02-C01 : Système de journalisation.** Le demandeur prévoit un système de journalisation des actions réalisées par le personnel impliqué dans la mise en œuvre du traitement et également par les autres utilisateurs pouvant accéder au système d'information utilisé pour le traitement de données à caractère personnel qui porte sur les données suivantes :
- horodatage ;
- adresse IP ;
- identifiant de l'utilisateur
- actions réalisées ;
- matériel utilisé.

190. **E14-S02-C02 : Information des utilisateurs.** Le demandeur a informé les utilisateurs de la mise en place du système de journalisation centralisé ou non en distinguant les systèmes de journalisation hors application, des systèmes de journalisation figurant dans l'application ainsi que des données à caractère personnel faisant l'objet de la journalisation.

191. **E14-S02-C03 : Contrôle systématique des journaux de logs**. Le demandeur a mis en place une procédure d'exploitation des informations journalisées (logs). Les usages attendus de cette procédure sont :
- la sécurité des systèmes d'information en permettant la détection des activités suspectes ou malveillantes ;
- l'analyse de performance des systèmes d'information afin de diagnostiquer et de résoudre des problèmes et dysfonctionnements.

[107] Byod, mise au rebut, utilisation personnelle….

[108] Référentiel Cnil.

192. **E14-S02-C04 : Protection des équipements et informations.** Le demandeur met en place des mesures de sécurité visant à préserver la disponibilité des équipements de journalisation ainsi que la confidentialité et l'intégrité des informations journalisées pendant leur durée de conservation.

14.3 Exigences relatives à l'accès physique[109] (S03)

193. **E14-S03-C01 : Procédure relative à l'accès physique - existence.** Le demandeur dispose d'une procédure relative au contrôle d'accès physique.

194. **E14-S03-C02 : Procédure relative à l'accès physique - contenu.** La procédure visée au E14-S03-C01 énonce les règles et moyens de contrôle d'accès physique définis par le demandeur sur la base de son analyse de risque ou justifiées par l'état de l'art. Cette procédure prévoit notamment :
- les mesures de sécurité appliquées aux locaux de la salle blanche[110] ;
- les procédures d'habilitation d'entrée et de sortie de la salle blanche.

195. **E14-S03-C03 : Procédure relative à l'accès physique - application.** Le demandeur met en œuvre la procédure visée au critère E14-S03-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative au contrôle d'accès physique est appliquée et rédige un rapport à l'issu de l'audit.

14.4 Exigences relatives à l'anonymisation et la pseudonymisation[111] (S04)

196. **E14-S04-C01 : Procédure relative à l'anonymisation - existence.** Le demandeur dispose, dans le cas où il met en œuvre un processus d'anonymisation, d'une procédure relative à l'anonymisation.

197. **E14-S04-C02 : Procédure relative à l'anonymisation – contenu.** La procédure d'anonymisation prévoit :
- ce qui doit être anonymisé ;
- la forme de stockage des données à caractère personnel[112] ;
- les risques d'individualisation, de corrélation et d'inférence visés dans l'» Avis 05/2014 du G29 sur les Techniques d'anonymisation » ou dans tout autre recommandation ou avis du CEPD sur l'anonymisation ;
- la méthode d'anonymisation utilisée ;
- que la méthode d'anonymisation doit être irréversible ;
- une étude des risques de réidentification des personnes et/ou la réalisation de tests de résistance à la réidentification des personnes.

198. **E14-S04-C03 : Procédure relative à l'anonymisation - application.** Le demandeur met en œuvre la procédure visée au critère E14-S04-C01, réalise un audit annuel interne ou externe afin de s'assurer que la procédure relative à l'anonymisation est appliquée et rédige un rapport à l'issu de l'audit.

---

[109] Référentiel Cnil.

[110] badges, clés, biométrie, vidéosurveillance, gardiennage…

[111] Référentiel Cnil.

[112] Champs d'une base de données, extraits de textes…

199. **E14-S04-C04** : **Liste des données anonymisées.** Le demandeur conserve l'information sur les données qui ont été anonymisées.

200. **E14-S04-C05** : **Liste des outils d'anonymisation.** En application de la procédure visée au critère E14-S04-C02 le demandeur dispose de la liste des outils et des méthodes associées d'anonymisation utilisés dans le cadre de son activité. Les outils d'anonymisation intégrés dans cette liste doivent répondre aux trois critères suivants :
- individualisation ;
- corrélation ;
- inférence.

201. **E14-S04-C06 : Procédure relative à la pseudonymisation - existence.** Le demandeur dispose, dans le cas où il met en œuvre un processus de pseudonymisation, d'une procédure relative à la pseudonymisation.

202. **E14-S04-C07 : Procédure relative à la pseudonymisation – contenu.** La procédure de pseudonymisation prévoit :
- ce qui doit être pseudonymisé ;
- la forme de stockage des données[113] ;
- les risques de réidentification identifiés ;
- la méthode de pseudonymisation utilisée ;
- de déterminer ce qui peut/doit être pseudonymisé ;
- les outils de pseudonymisation à utiliser parmi la liste des outils de pseudonymisation (E14-S04-C11) ;
- si le tableau de correspondance est conservé, que celui-ci soit chiffré conformément au critère E14-S06-C01 et soit conservé de manière séparée.

203. **E14-S04-C08 : Procédure relative à la pseudonymisation - application.** Le demandeur met en œuvre la procédure visée au critère E14-C04-C08, réalise un audit annuel interne ou externe afin de s'assurer que la procédure relative à la pseudonymisation est appliquée et rédige un rapport à l'issu de l'audit.

204. **E14-S04-C09** : **Liste des données pseudonymisées.** Le demandeur conserve l'information sur les données qui ont été pseudonymisées.

205. **E14-S04-C10** : **Liste des algorithmes de pseudonymisation.** Le demandeur dispose de la liste des algorithmes de pseudonymisation utilisés dans le cadre de son activité.

206. **E14-S04-C11** : **Liste des outils de pseudonymisation**. Le demandeur dispose d'une liste décrivant les données à caractère personnel pour lesquelles la procédure de pseudonymisation visée au critère E14-S04-C07 s'applique.

14.5 Exigences relatives à l'authentification des utilisateurs[114] (S05)

207. **E14-S05-C01 : Politique relative aux mots de passe - existence.** Le demandeur dispose d'une politique relative aux mots de passe.

[113] Champs d'une base de données, extraits de textes…

[114] Référentiel Cnil.

208. **E14-S05-C02 : Politique relative aux mots de passe - contenu.** La politique relative aux mots de passe des utilisateurs prévoit les modalités de :
- l'authentification par mot de passe ;
- conservation des mots de passe ;
- l'éventuel changement du mot de passe et d'information des personnes.

La politique fait également référence à l'entropie des mots de passe, définie comme la quantité de hasard et précise que les mots de passe doivent être composés :
- d'au minimum 12 caractères avec des majuscules, des minuscules, des chiffres et des caractères spéciaux ; ou
- d'au minimum 14 caractères avec des majuscules, des minuscules, sans caractères spéciaux obligatoires ; ou
- d'une phrase contenant un minimum de 7 mots.

La politique fait également référence à la réalisation de test de devinabilité qui consiste en une vérification dynamique de chaque mot de passe par un outil dédié.

209. **E14-S05-C03 : Politique relative aux mots de passe - application.** Le demandeur met en œuvre la politique visée au critère E14-C05-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la politique relative aux mots de passe est appliquée et rédige un rapport à l'issu de l'audit.

210. **E14-S05-C04 : Politique relative aux mots de passe pour les administrateurs - existence.** Le demandeur a adapté une politique spécifique de mots de passe pour les administrateurs qui précise :
- le nombre de caractères minimum ;
- le type de caractère ;
- l'implémentation éventuelle de la double authentification ;
- la durée de validité du mot de passe ;
- le nombre de tentative maximum de connexion avant le blocage du mot de passe.

Cette politique impose également, pour les administrateurs, une entropie des mots de passe plus élevée et un renouvellement selon une périodicité pertinente et raisonnable.

211. **E14-S05-C05 : Politique relative aux mots de passe pour les administrateurs – communication.** La politique a été présentée et remise aux administrateurs.

212. **E14-S05-C06 : Stockage des mots de passe en clair**. Le demandeur impose une transformation des mots de passe lors de leur stockage au moyen d'une fonction cryptographique non réversible et sure intégrant l'utilisation d'un sel ou d'une clé.

213. **E14-S05-C07 : Coffres-forts pour les mots de passe et pour les clefs cryptographiques**. Le demandeur dispose d'un coffre-fort numérisé permettant aux utilisateurs de stocker/gérer leurs mots de passe de manière sécurisée ainsi que d'un coffre-fort pour le stockage de clefs cryptographiques utilisées pour le chiffrement.

214. **E14-S05-C08 : Tentatives d'accès à un compte**. Le demandeur limite le nombre de tentatives d'accès à un compte.

215. **E14-S05-C09 : Changement de mot de passe après réinitialisation**. Le demandeur oblige l'utilisateur à changer son mot de passe après réinitialisation.

216. **E14-S05-C10 : Politique relative aux mots de passe pour les administrateurs - application.** Le demandeur met en œuvre la politique visée au critère E14-C05-C04, réalise un audit annuel

dans le respect du critère E01-S03-C04 afin de s'assurer que la politique relative aux mots de passe pour les administrateurs est appliquée et rédige un rapport à l'issu de l'audit.

217. **E14-S05-C11 : Procédure relative à l'authentification des utilisateurs - existence.** Le demandeur dispose d'une procédure relative à l'authentification des utilisateurs.

218. **E14-S05-C12 : Procédure relative à l'authentification des utilisateurs – contenu.** La procédure relative à l'authentification des utilisateurs visée au E14-S05-C11 prévoit de :
- définir un identifiant (login) unique à chaque utilisateur ou, à défaut, les modalités d'accès partagés accompagnées de leur justification ; créer chaque compte utilisateur avec un mot de passe initial aléatoire unique, le transmettre de manière sécurisée à l'utilisateur, et le contraindre à le modifier lors de sa première connexion et lorsque qu'un nouveau mot de passe lui est fourni ;
- privilégier l'authentification multifacteur pour les comptes administrateurs ou à défaut, de justifier les raisons pour lesquelles ce process d'authentification n'est pas retenu ;
- dans le cas où des mots de passe ou des secrets différents sont utilisés, proposer la possibilité de mettre en place une solution d'authentification centralisée, de mots de passe à usage unique ou de coffres-forts sécurisés ;
- obliger l'utilisateur à changer son mot de passe après réinitialisation ;
- concernant le stockage des mots de passe, imposer une transformation au moyen d'une fonction cryptographique non réversible et sure intégrant l'utilisation d'un sel ou d'une clé
- limiter le nombre de tentatives d'accès à un compte conformément au critère E14-S05-C08.
- récupérer les données à caractère personnel, à l'exception des données à caractère personnel signalées comme étant privées, présentes sur un poste préalablement à sa réaffectation à une autre personne ;
- effacer les données présentes sur un poste préalablement à sa réaffectation à une autre personne ou pour les postes partagés en application de la procédure visée au E08-S08-C01 ;
- supprimer les données à caractère personnel temporaires à chaque reconnexion des postes partagés.

219. **E14-S05-C13 : Procédure relative à l'authentification des utilisateurs - application.** Le demandeur met en œuvre la procédure visée au critère E14-C05-C11, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative à l'authentification des utilisateurs est appliquée et rédige un rapport à l'issu de l'audit.

220. **E14-S05-C14 : Charte administrateurs.** Le demandeur dispose d'une charte administrateurs qui décrit :
- les prérogatives de l'administrateur (compte dédié à l'administration, administration du système d'information, sécurité du système d'information) ;
- la gestion des risques et des menaces (procédure d'alerte, urgence, incident de sécurité) ;
- les obligations de l'administrateur (collaboration, information, conseil et alerte, confidentialité renforcée, prise de main à distance, sécurité, obligation de continuité du service, respect des normes applicables, droit de propriété).

14.6 Exigences relatives au chiffrement des données à caractère personnel[115] (S06)

221. **E14-S06-C01 : Procédure relative au chiffrement des données à caractère personnel - existence.** Le demandeur dispose d'une procédure relative au chiffrement des données à caractère personnel.

222. **E14-S06-C02 : Procédure relative au chiffrement des données à caractère personnel – contenu.** La procédure relative au chiffrement des données à caractère personnel visée au E14-S06-C01 prévoit de :
- déterminer ce qui doit être chiffré selon la forme de stockage des données à caractère personnel, les risques identifiés et les performances exigées ;
- documenter le périmètre des données à caractère personnel qui doivent être chiffrées[116] ;
- choisir le type de chiffrement (symétrique ou asymétrique) selon le contexte et les risques identifiés et recourir à des solutions de chiffrement basées sur des algorithmes publics réputés forts et, en cas de sous traitance, selon les instructions documentées du responsable du traitement ;
- mettre en place des mesures pour garantir la disponibilité, l'intégrité et la confidentialité des éléments permettant de récupérer des secrets perdus ;
- définir les modalités de transmission des clés de chiffrement des données à caractère personnel ;
- déterminer les modalités de révocation des clés de chiffrement des données à caractère personnel en cas de compromission.

223. **E14-S06-C03 : Procédure relative au chiffrement des données à caractère personnel - application.** Le demandeur met en œuvre la procédure visée au critère E14-C06-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative au chiffrement des données à caractère personnel est appliquée et rédige un rapport à l'issu de l'audit. Ce rapport précise, pour les données à caractère personnel qui ne sont pas chiffrées, la raison de l'absence de chiffrement.

224. **E14-S06-C04 : Liste des catégories ou flux de données à caractère personnel chiffrées.** Le demandeur dispose de la liste des catégories ou flux de données à caractère personnel chiffrées.

14.7 Exigences relatives au cloisonnement des données à caractère personnel[117] (S07)

225. **E14-S07-C01 : Politique relative au cloisonnement des données à caractère personnel - existence.** Le demandeur dispose d'une politique relative au cloisonnement des serveurs contenant des données à caractère personnel.

226. **E14-S07-C02 : Politique relative au cloisonnement des données à caractère personnel – contenu.** La politique relative au cloisonnement des données à caractère personnel prévoit de :

---

[115] Référentiel Cnil.

[116] Recette, préproduction, bac à sable, archives intermédiaires ou définitives, données à caractère personnel traitées par des logiciels Saas externes, données à caractère personnel traitées par des logiciels « sur étagère », flux réseaux…

[117] Référentiel Cnil.

- identifier les seules données à caractère personnel utiles à chaque processus métier et prévoir un accès des personnes aux seules données à caractère personnel dont elles ont besoin ;
- séparer logiquement les données à caractère personnel utiles à chaque processus et gérer des droits d'accès différenciés selon les processus métiers ;
- disposer d'un environnement informatique dédié pour les systèmes traitant des données à caractère personnel les plus sensibles ;
- segmenter le réseau en sous-réseaux logiques étanches selon les services censés y être déployés conformément au critère visé au E14-S19-C02.

227. **E14-S07-C03 : Politique relative au cloisonnement des données à caractère personnel - application.** Le demandeur met en œuvre la politique visée au critère E14-C07-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative au cloisonnement des données à caractère personnel est appliquée. Cet audit porte également sur la configuration du cloisonnement de certains matériels choisis par le demandeur. Le demandeur rédige un rapport à l'issu de l'audit. Ce rapport précise, pour les données à caractère personnel qui ne sont pas chiffrées, la raison de l'absence de chiffrement [118].

228. **E14-S07-C04 : Vérification des destinataires.** Dans le cadre de la gestion des habilitations, Le demandeur vérifie de manière régulière que des profils des destinataires de données à caractère personnel ne sont pas ou plus nécessaires et supprime les permissions et les comptes obsolètes notamment en cas de départ d'un destinataire ou de changement de mission.

229. **E14-S07-C05 : Vérification des interconnexions[119].** Le demandeur vérifie régulièrement la liste des interconnexions. Il fixe une période minimale[120] pour la vérification de manière régulière de la liste des interconnexions ajoutées et détermine les conditions qui nécessitent une vérification sans délai[121].

14.8 Exigences relatives à la confidentialité des données à caractère personnel[122] (S08)

230. **E14-S08-C01 : Politique relative à l'utilisation des outils de communication - existence.** Le demandeur dispose d'une politique relative à l'utilisation des outils de communication[123].

231. **E14-S08-C02 : Politique relative à l'utilisation des outils de communication– contenu.** La politique relative à l'utilisation des outils de communication précise la nécessité de :
- communiquer des courriels groupes avec la liste des destinataires en copie cachée ;
- ne pas faire apparaître les identifiants et les mots de passe sur des courriers en masse :

[118] Impossibilité technique ou mise en œuvre de mesures de sécurité spécifiques.

[119] Les interconnexions visent la connexion entre deux systèmes ou réseaux via des flux entrant et sortant qui sont normalement isolés l'un de l'autre pour des raisons de sécurité et ne se limitent pas à celles entre le système d'information interne et internet. Les flux sortants désignent les données ou les communications qui quittent un système ou un réseau pour être envoyées à un autre via l'interconnexion. Le cloisonnement vise à minimiser les risques en limitant les flux entrants et sortants, assurant ainsi que seules les communications autorisées et sécurisées passent d'un système à un autre, réduisant ainsi les vulnérabilités potentielles.

[120] Par exemple tous les ans.

[121] Par exemple en cas de soupçon de compromission de sécurité.

[122] Référentiel Cnil.

[123] Courriers électroniques, intranet…

- faire signer aux employés un engagement de confidentialité.

232. **E14-S08-C03 : Politique relative à l'utilisation des outils de communication - application.** Le demandeur met en œuvre la politique visée au critère E14-S08-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la politique l'utilisation des outils de communication est appliquée et rédige un rapport à l'issu de l'audit.

233. **E14-S08-C04 : Procédure relative à l'envoi de courriers en masse - existence.** Le demandeur dispose d'une procédure relative à l'envoi de courriers en masse.

234. **E14-S08-C05 : Procédure relative à l'envoi de courriers en masse - contenu.** La procédure relative à l'envoi de courriers en masse visée au E14-S08-04 précise :
- les modalités de constitution de la liste des adresses électroniques concernées par l'envoi des courriers en masse ;
- les modalités de vérification du contenu des courriers en masse avant envoi, lesquelles portent sur la confidentialité des données à caractère personnel ;
- les personnes en charge de la vérification du contenu des courriers en masse avant envoi.

235. **E14-S08-C06 : Procédure relative à l'envoi de courriers en masse - application.** Le demandeur met en œuvre la procédure visée au critère E14-S08-C04, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative à l'envoi de courriers en masse est appliquée et rédige un rapport à l'issu de l'audit.

14.9 Exigences relatives aux développements informatiques[124] (S09)

236. **E14-S09-C01 : Procédure relative aux développements informatiques - existence.** Le demandeur dispose d'une procédure relative aux développements informatiques.

237. **E14-S09-C02 : Procédure relative aux développements informatiques – contenu.** La procédure relative aux développements informatiques visée au E14-S09-01 prévoit de :
- encadrer de manière stricte les zones de commentaires libres ;
- tester sur des données à caractère personnel fictives ou des données anonymisées ;
- inclure un processus de sauvegarde avant toute mise à niveau ou déploiement de logiciels.
- imposer le respect des procédures visées aux critères E10-S02-C01 et E11-S01-C01.

238. **E14-S09-C03 : Procédure relative aux développements informatiques - application.** Le demandeur met en œuvre la procédure visée au critère E14-S09-C03, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative aux développements informatiques est appliquée et rédige un rapport à l'issu de l'audit.

14.10 Exigences relatives aux accès logique et habilitation[125] (S10)

239. **E14-S10-C01 : Procédure relative aux accès logique et habilitation - existence.** Le demandeur dispose d'une procédure relative aux accès logique et habilitation.

240. **E14-S10-C02 : Procédure relative aux accès logique et habilitation – contenu.** La procédure relative aux accès logique et habilitation visée au E14-S10-C01 prévoit de :
- définir les profils d'habilitation ;

[124] Référentiel Cnil.

[125] Référentiel Cnil.

- supprimer les permissions d'accès obsolètes ;
- réaliser une revue annuelle des habilitations ;
- vérifier de manière régulière que des profils utilisateurs ne sont pas ou plus nécessaires afin d'éviter les attaques par élévation de privilèges ou encore de réduire la surface d'attaque et les impacts en cas d'incident de sécurité ;
- réaliser une revue régulière, a minima annuelle, des habilitations afin d'identifier et de supprimer les comptes (profils utilisateurs) non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur ;
- supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique[126] ainsi qu'à la fin de leur contrat.
- informer les utilisateurs de la mise en place d'un système de journalisation générale des habilitations.

241. **E14-S10-C03 : Procédure relative aux accès logique et habilitation - application.** Le demandeur met en œuvre la procédure visée au critère E14-S10-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative aux accès logique et habilitation est appliquée et rédige un rapport à l'issu de l'audit.

242. **E14-S10-C04 : Dictionnaire des profils habilitation.** Le demandeur dispose d'un dictionnaire des profils d'habilitation. Ces informations sont disponibles dans un annuaire[127]

14.11 Exigences relatives à l'informatique nomade[128] (S11)

243. **E14-S11-C01 : Procédure relative à l'informatique nomade - existence.** Le demandeur dispose d'une procédure relative à l'informatique nomade.

244. **E14-S11-C02 : Procédure relative à l'informatique nomade – contenu.** La procédure relative à l'informatique mobile prévoit :
- des moyens de chiffrement des équipements mobiles ;
- de faire des sauvegardes ou des synchronisations régulières des données à caractère personnel;
- d'exiger un secret pour le déverrouillage des ordiphones ;
- de configurer les téléphones avant de les remettre aux utilisateurs : il faut que les téléphones soient verrouillés automatiquement après une période d'inactivité (1 à 5 minutes), la carte mémoire (microSD) doit être systématiquement chiffrée le verrou distant doit être activé afin de pouvoir effacer le contenu en cas de perte ou de vol, l'installation de nouvelles applications est limitée (si possible), et l'ensemble de ces mesures doit être gérée par un système de gestion de flotte permettant de forcer l'application de ces règles ;
- l'interdiction ou l'autorisation de l'utilisation d'équipements Bring Your Own Device (BYOD) et, si une telle utilisation est autorisée, les modalités de connexion des équipements BYOD au système d'information du demandeur.

245. **E14-S11-C03 : Procédure relative à l'informatique nomade - application.** Le demandeur réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative à l'informatique mobile est appliquée et rédige un rapport à l'issu de l'audit.

---

[126] Exemple : changement de mission ou de poste.

[127] Tel que l'Active Directory.

[128] Référentiel Cnil.

14.12 Exigences relatives à l'intégrité[129] (S12)

246. **E14-S12-C01 : Procédure de contrôle d'intégrité - existence.** Le demandeur dispose d'une procédure de contrôle d''intégrité.

247. **E14-S12-C02 : Procédure de contrôle d''intégrité – contenu.** La procédure de contrôle d''intégrité visée au E14-S12-C01 prévoit de :
- définir la méthode de contrôle d'intégrité adaptée aux données à caractère personnel selon les risques identifiés (selon les besoins une fonction de hachage, un code d'authentification de messages (MAC), une fonction de signature électronique) selon les méthodes d'analyse de risques les plus communément utilisées[130]
- définir le moment auquel la fonction est appliquée et celui où le contrôle doit être effectué selon le déroulement du processus métier.

248. **E14-S12-C03 : Procédure de contrôle d'intégrité - application.** Le demandeur réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure de contrôle d'intégrité est appliquée et rédige un rapport à l'issu de l'audit.

249. **E14-S12-C04 : Table des données à caractère personnel soumises à l'intégrité.** Le demandeur établit une table des données à caractère personnel soumises à l'intégrité dans le respect de la procédure visée au E14-S12-C02.

250. **E14-S12-C05 : Outils WAF.** Le demandeur a mis en place, lorsqu'il traite des données à caractère personnel un serveur WAF pour filtrer le trafic ainsi que des mesures d'analyse permettant de prévenir, dès qu'elles surviennent, les attaques par injection SQL ou de scripts.

14.13 Exigences relatives aux locaux et bureaux physiques[131] (S13)

251. **E14-S13-C01 : Procédure relative à la sécurité des locaux et bureaux - existence.** Le demandeur dispose d'une procédure relative à la sécurité des locaux et bureaux.

252. **E14-S13-C02 : Procédure relative à la sécurité des locaux et bureaux – contenu.** La procédure relative à la sécurité des locaux et bureaux visée au E14-S13-C02 précise les modalités pour :
- restreindre les accès aux locaux au moyen de portes verrouillées ;
- installer des alarmes anti-intrusion et les vérifier périodiquement ;
- stocker les documents papiers, notamment s'ils doivent être rangés dans des armoires fermées à clé ;
- verrouiller la porte d'accès au bureau en cas d'absence prolongée ;
- tenir à jour une liste des personnes autorisées à pénétrer dans chaque zone et réexaminer régulièrement les droits d'accès aux zones de sécurité ;
- conserver une trace des accès après en avoir informé les personnes concernées ;
- tenir à jour un journal des accès des trois derniers mois au plus.

253. **E14-S13-C03 : Procédure relative à la sécurité des locaux et bureaux - application.** Le demandeur met en œuvre la procédure visée au E14-S13-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative à la sécurité des locaux et bureaux est appliquée et rédige un rapport à l'issu de l'audit.

---

[129] Référentiel Cnil.

[130] Ebios, Mehari, Octav…

[131] Référentiel Cnil.

254. **E14-S13-C04 : Plan alarme anti-intrusion.** Le demandeur dispose d'un plan d'alarme anti-intrusion ainsi qu'un état de maintenance associé.

255. **E14-S13-C05 : Liste des personnes autorisées.** Le demandeur tient à jour une liste des personnes autorisées à pénétrer dans chaque zone et réexamine régulièrement les droits d'accès aux zones de sécurité conformément à la procédure relative aux accès logique et habilitation visée au E14-S11-C01.

256. **E14-S13-C06 : Journal des accès.** Le demandeur tient à jour un journal des accès aux locaux (professionnels) et bureaux physiques des trois derniers mois au plus.

14.14 Exigences relatives à la maintenance et la destruction des données à caractère personnel[132] (S14)

257. **E14-S14-C01 : Procédure relative à la maintenance et la destruction des données à caractère personnel - existence.** Le demandeur dispose d'une procédure relative à la maintenance et la destruction des données à caractère personnel.

258. **E14-S14-C02 : Procédure relative à la maintenance et la destruction des données à caractère personnel - contenu.** La procédure relative à la maintenance et la destruction des données à caractère personnel prévoit de :
- enregistrer les interventions de maintenance dans une main courante ;
- encadrer par un responsable de l'organisme les interventions par des tiers ;
- effacer les données à caractère personnel de tout matériel avant revente, destruction ou réaffectation, conformément à la procédure de remise à zéro des matériels visée au E08-S07-C01 ;
- encadrer (sécuriser et journaliser) les opérations de télémaintenance ;
- lors des opérations de maintenance nécessitant une prise en main à distance sur un poste de travail, ne réaliser l'opération qu'après avoir obtenu l'accord de l'utilisateur, et lui indiquer à l'écran si la prise en main est effective ;
- dans le cas d'une télémaintenance par un tiers à une imprimante ou copieur multifonctions hébergé localement, prendre des mesures spécifiques pour protéger chaque accès : faire signer un engagement de confidentialité par le tiers externe, mettre en place de mots de passe robustes, spécifiques et renouvelés régulièrement, pour l'accès en télémaintenance, activer les accès entrant en télémaintenance uniquement sur demande, les accès entrant étant inactifs par défaut, journaliser les accès en télémaintenance, interdire les possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local et plus largement vers internet ;
- empêcher l'accès à des données à caractère personnel stockées sur des imprimantes ou copieurs multifonctions mis au rebut.

259. **E14-S14-C03 : Procédure relative à la maintenance et la destruction des données à caractère personnel - application.** Le demandeur met en œuvre la procédure visée au E14-S14-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative à la maintenance et la destruction des données à caractère personnel est appliquée et rédige un rapport à l'issu de l'audit.

[132] Référentiel Cnil.

14.15 Exigences relatives aux postes de travail[133] (S15)

260. **E14-S15-C01 : Procédure relative aux postes de travail - existence.** Le demandeur dispose d'une procédure relative aux postes de travail.

261. **E14-S15-C02 : Procédure relative aux postes de travail – contenu.** La procédure relative aux postes de travail visée au E14-S15-C01 prévoit de
- prévoir une procédure de verrouillage automatique de session conformément au critère visé au E14-S15-C04 ;
- utiliser des antivirus régulièrement mis à jour conformément au critère visé au E14-S15-C05 ;
- installer un « pare-feu » (firewall) logiciel conformément au critère visé au E14-S15-C06 ;
- recueillir l'accord de l'utilisateur avant toute intervention sur son poste conformément au critère visé au E14-S15-C07 ;
- protéger les écrans des regards indiscrets (filtre optique ou orientation) conformément au critère visé au E14-S15-C08 ;
- limiter les supports amovibles conformément au critère visé au E14-S15-C09 ;
- interdire le partage de répertoires ou de données à caractère personnel localement sur les postes de travail
- stocker les données à caractère personnel des utilisateurs sur un espace réseau sauvegardé et non sur les postes de travail conformément au critère visé au E14-S15-C10 ;
- sécuriser la configuration du navigateur Internet ;
- interdire l'exécution des applications téléchargées ne provenant pas de sources sûres conformément au critère visé au E14-S15-C11 ;
- s'assurer que la taille maximale des journaux d'événements est suffisante, et notamment que les événements les plus anciens ne sont pas supprimés automatiquement si la taille maximale est atteinte
- traiter l'application des mesures susvisées en cas de sous traitance.

262. **E14-S15-C03 : Procédure relative aux postes de travail - application.** Le demandeur met en œuvre la procédure visée au E14-S15-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative aux postes de travail est appliquée et rédige un rapport à l'issu de l'audit.

263. **E14-S15-C04 : Verrouillage automatique de session.** Le demandeur a prévu le verrouillage automatique de session.

264. **E14-S15-C05 : Antivírus à jour.** Le demandeur utilise des antivirus régulièrement mis à jour.

265. **E14-S15-C06 : Pare-feu.** Le demandeur installe un pare-feu tant sur les postes de travail que pour les applications web et les logiciels.

266. **E14-S15-C07 : Accord avant intervention sur poste.** Le demandeur, en application de la charte informatique visée au critère E14-S01-C02, recueille l'accord de l'utilisateur avant toute intervention sur son poste[134], à l'occasion d'un rendez-vous accepté. Le demandeur s'assure également que l'utilisateur puisse constater si la prise de main à distance est en cours et quand elle se termine[135]. Le demandeur, en application de la charte informatique visée au E14-S01-

[133] Référentiel Cnil.

[134] Par exemple en répondant à un message s'affichant à l'écran.

[135] Par exemple par l'affichage d'un message à l'écran.

C02, précise également les cas où l'accord de l'utilisateur n'est pas requis[136] et les garanties associées à cette situation[137].

267. **E14-S15-C08 : Liste collaborateurs écrans protégés.** Le demandeur dispose d'une liste des collaborateurs sont les écrans sont protégés.

268. **E14-S15-C09: Supports amovibles.** Le demandeur limite l'utilisation des supports amovibles.

269. **E14-S15-C10 : Stockage des données à caractère personnel.** Le demandeur impose dans sa charte informatique visée au critère E14-S01-C02 de stocker les données à caractère personnel sur un espace réseau sauvegardé et non sur les postes de travail. Le demandeur prévoit également les cas où le stockage des données à caractère personnel pourra temporairement être effectué sur un poste de travail[138].

270. **E14-S15-C11 : Téléchargement.** Le demandeur interdit l'exécution des applications téléchargées ne provenant pas de sources sûres.

271. **E14-S15-C12 : Taille maximale des journaux d'événements.** Le demandeur définit la taille maximale des journaux d'événements stockés sur le serveur dédié à la journalisation et prévoit une notification en cas d'insuffisance.

14.16 Exigences relatives au réseau informatique interne[139] (S16)

272. **E14-S16-C01 : VPN.** Le demandeur sécurise les accès distants des appareils informatiques nomades par VPN et s'assure que les mesures de sécurité configurées sur le VPN correspondent à celles définies pour le traitement dans le dossier de conception visé au E06-S04-C02[140].

273. **E14-S16-C02 : Wi-Fi.** Le demandeur met en œuvre le protocole WPA2 ou WPA2-PSK, ou supérieur, pour les réseaux Wi-Fi.

274. **E14-S16-C03 : Procédure appareil non professionnel[141].** Le demandeur dispose d'une procédure limitant les connexions d'appareil non professionnel sur le réseau et interdit l'accès de ces appareils non professionnels au système d'information sans passer par un réseau adapté à cet usage.[142]

---

[136] Par exemples, en situation d'urgence, en cas de panne critique du système, absence prolongée de l'utilisateur ou enquête interne…

[137] Par exemples : formalisation de comptes rendus d'intervention, principe d'intervention minimale des techniciens, journalisation des accès.

[138] Par exemple en cas de difficulté d'accès au réseau du demandeur.

[139] Référentiel Cnil.

[140] Chiffrement des flux, authentification obligatoire, double authentification, mise à jour…

[141] Le terme « appareil non professionnel » désigne des appareils qui ne sont pas gérés par le demandeur mais dont l'usage est autorisé dans le cadre professionnel.

[142] VPN…

14.17 Exigences relatives à la sauvegarde et continuité d'activité[143] (S17)

275. **E14-S17-C01 : Sauvegardes régulières.** Le demandeur définit une fréquence de sauvegarde régulière et effectue des sauvegardes à cette fréquence. Il précise également quand une sauvegarde supplémentaire est nécessaire, en particulier avant :
- la mise à niveau d'un logiciel qui a été développé et/ou testé conformément à E14-S09-C02 ;
- l'application de mises à jour de sécurité critiques conformément à E14-S21-C02 ;
- la migration vers un nouveau matériel de l'inventaire informatique conformément à E14-S20-C01.

276. **E14-S17-C02 : Stockage des sauvegardes.** Le demandeur stocke les supports de sauvegarde dans des locaux et bureaux répondant aux critères de la procédure E14-S13-C01 et avec des moyens de sécurité pour le convoyage des sauvegardes. Les sauvegardes seront chiffrées conformément à la procédure relative au chiffrement des données à caractère personnel visée au E14-S06-C01 et à la procédure relative à la confidentialité des données à caractère personnel visée au E14-S08-C01.

277. **E14-S17-C03 : Localisation des sauvegardes.** Le demandeur dispose d'une politique relative à la localisation géographique des sauvegardes. Cette politique indique le lieu de localisation des serveurs de sauvegarde.

278. **E14-S17-C04 : Procédure de disponibilité des sauvegardes.** Le demandeur dispose d'une procédure relative à la disponibilité des sauvegardes afin de s'assurer que l'organisation, les personnels, systèmes et locaux nécessaires au traitement sont disponibles dans un délai correspondant aux besoins des métiers.

279. **E14-S17-C05 : Procédure de continuité d'activité.** Le demandeur dispose d'une procédure de continuité d'activité prévoyant la réalisation de tests de continuité d'activité tous les deux ans.

14.18 Exigences relatives à la sécurité de l'exploitation[144] (S18)

280. **E14-S18-C01 : Procédure d'exploitation.** Le demandeur documente les procédures d'exploitation, les tient à jour et les communique à tous les utilisateurs concernés.

281. **E14-S18-C02 : Inventaire logiciels et matériels.** Le demandeur tient à jour l'inventaire des logiciels visé au E04-S02-C03 et des matériels visés au E14-S20-C06 utilisés en exploitation.

282. **E14-S18-C03 : Redondance matérielle.** Le demandeur utilise des unités de stockage de données à caractère personnel utilisant des mécanismes de redondance matérielle ou bien des mécanismes de duplication des données à caractère personnel entre plusieurs serveurs et/ou sites.

283. **E14-S18-C04 : Conditions physiques d'hébergement.** Le demandeur s'assure que les conditions physiques d'hébergement sont appropriées à l'usage prévu des matériels, et incluent des mécanismes de secours (onduleur et/ou alimentation de secours et/ou groupe électrogène).

[143] Référentiel Cnil.

[144] Référentiel Cnil

284. **E14-S18-C05 : Continuité d'activité et reprise d'activité.** Le demandeur prévoit les conditions de continuité et de reprise d'activité en cas d'incident dans un Plan de Reprise d'Activité (PRA) et un Plan de Continuité d'Activité (PCA)[145] ainsi que les modalités de leur activation notamment en cas de mode dégradé.

285. **E14-S18-C06 : Procédure de gestion des incidents de sécurité.** Le demandeur met en place une procédure de gestion des incidents de sécurité permettant de les enregistrer, les qualifier et les traiter. Cette procédure prévoit :
- les procédures d'escalade ;
- l'activation du Plan de Continuité d'Activité ;
- la constitution des cellules de gestion de crise ;
- les modalités de dépôt de plainte le cas échéant ;
- la sensibilisation des métiers aux signalements des incidents de sécurité ;
- des exigences relatives à la journalisation des accès et incidents visées au E14-S02 ;
- un renvoi à la procédure relative aux violations de données à caractère personnel visée au E14-S23-C01 ;
- une analyse des événements de sécurité détectés par les outils de surveillance de l'activité réseau visée au critère E14-S19-C05.

14.19 Exigences relatives à la sécurité des canaux informatiques[146] (S19)

286. **E14-S19-C01 : Cartographie du réseau.** Le demandeur maintien à jour une cartographie détaillée du réseau.

287. **E14-S19-C02 : Segmentation du réseau.** Le demandeur segmente le réseau en sous-réseaux logiques étanches selon les services censés y être déployés.

288. **E14-S19-C03 : Communication directe.** Le demandeur interdit toute communication directe entre des postes internes et l'extérieur. Différencier un réseau interne pour lequel aucune connexion venant d'Internet n'est autorisée, et un réseau dit DMZ accessible depuis Internet.

289. **E14-S19-C04 : Flux autorisés à l'aide d'un pare-feu.** Le demandeur a paramétré son pare feu pour n'autoriser que certains flux.

290. **E14-S19-C05 : Surveillance de l'activité réseau.** Le demandeur dispose 'd'une procédure de surveillance de l'activité réseau lui permettant de faire une analyse de l'activité sur son réseau à partir d'un logiciel '''Il informe les personnes concernées de cette surveillance par le biais de la politique interne de protection des données à caractère personnel visée au E01-S02-C05.

291. **E14-S19-C06 : Plan de réponse en cas d'intrusion.** Le demandeur prévoit un plan de réponse en cas d'intrusion majeure pour délimiter et circonscrire la compromission.

---

[145] Le PCA est un ensemble de procédures et de mesures mises en place pour garantir la continuité des activités essentielles d'une organisation en cas de perturbation majeure (catastrophe naturelle, cyberattaque, etc.). Il vise à minimiser l'impact sur les opérations et à assurer la reprise rapide des activités critiques.

Le PRA est un composant du PCA qui se concentre spécifiquement sur la restauration des systèmes informatiques et des données après une interruption. Il détaille les actions à entreprendre pour rétablir les services IT dans un délai acceptable.

[146] Référentiel Cnil.

292. **E14-S19-C07 : Flux d'administration.** Le demandeur sécurise les flux d'administration et restreint voire interdit l'accès physique et logique aux ports de diagnostic et de configuration à distance.

293. **E14-S19-C08 : Procédure relative au raccordement d'équipements informatiques.** Le demandeur a établi une procédure interdisant le raccordement aux réseaux d'équipements informatiques non maîtrisés.

294. **E14-S19-C09 : Procédure relative aux outils de prise de main à distance.** Le demandeur a établi une procédure relative aux outils de prise de main à distance. Cette procédure précise :
- la liste des outils de prise en main à distance autorisés par le demandeur ;
- les bonnes pratiques de sécurité à appliquer pour chacun des outils ;
- les méthodes de surveillance et de journalisation de ces outils.

295. **E14-S19-C10 : Procédure relative aux interfaces sans fil.** Le demandeur a établi une procédure relative aux interfaces sans fil (réseaux tels que Wifi, Bluetooth, infrarouge, 4G). Cette procédure précise :
- la configuration des outils d'interface sans fil ;
- leur modalité d'accès[147] ;
- les bonnes pratiques de sécurité à appliquer pour chacun des outils ;
- les méthodes de surveillance et de journalisation de ces outils.

14.20 Exigences relatives à la sécurité des matériels[148] (S20)

296. **E14-S20-C01 : Inventaire des ressources informatiques.** Le demandeur tient à jour un inventaire des ressources informatiques utilisées.

297. **E14-S20-C02 : Cloisonnement des ressources en cas de partage des locaux.** Le demandeur cloisonne les ressources de l'organisme en cas de partage de locaux.

298. **E14-S20-C03 : Procédure relative au dimensionnement.** Le demandeur dispose d'une procédure prévoyant la nécessité de vérifier que le dimensionnement des capacités de stockage et de traitement, ainsi que les conditions d'utilisation, sont appropriés à l'usage prévu des matériels, notamment en termes de place, d'humidité et de température.

299. **E14-S20-C04 : Procédure de sécurisation des matériels les plus critiques.** Le demandeur dispose d'une procédure prévoyant la nécessité de vérifier que l'alimentation des matériels les plus critiques visés au E14-S20-C05 est protégée contre les variations de tension et qu'elle est secourue, ou qu'elle permet au moins de les arrêter normalement.

300. **E14-S20-C05 : Liste des matériels les plus critiques.** Le demandeur dispose d'une liste des matériels les plus critiques et d'une cartographie du système d'information permettant de s'assurer de la cohérence de la liste des matériels critiques.

301. **E14-S20-C06 : Chiffrement des postes nomades.** Le demandeur chiffre les données à caractère personnel stockées sur les postes nomades.

[147] Gestion des identifiants …

[148] Référentiel Cnil.

302. **E14-S20-C07 : Filtre de confidentialité sur les écrans.** Le demandeur prévoit dans la charte informatique visée au critère E14-S01-C02 ou dans la PSSI visée au critère E14-S01-C01, la faculté de positionner un filtre de confidentialité sur certains postes de travail et décrit les métiers, situations et postes concernés. Le personnel du demandeur est informé de cette faculté dans la charte informatique visée au critère E14-S01-C02 ou dans tout autre document porté à sa connaissance.

303. **E14-S20-C08 : Procédure relative aux supports amovibles.** Le demandeur dispose d'une procédure pour sécuriser l'usage des supports amovibles qui prévoit de :
- limiter l'usage des supports amovibles à ceux fournis par le service en charge de l'informatique ;
- interdire la connexion de clés USB sur des matériels non sécurisés ;
- limiter l'utilisation des clés USB aux activités professionnelles ;
- désactiver la fonctionnalité d'exécution automatique sur tous les postes ;
- chiffrer les données à caractère personnel stockées sur un support amovible ;
- restituer les supports amovibles défectueux ou plus utiles au service en charge de l'informatique. Détruire de manière sécurisée les supports de données à caractère personnel qui sont inutiles ;

304. **E14-S20-C09 : Procédure de sécurisation des imprimantes.** Le demandeur dispose d'une procédure pour sécuriser l'usage des imprimantes et copieurs multifonctions prévoit de :
- changer les mots de passe "constructeur" par défaut ;
- désactiver les interfaces réseau inutiles. Désactiver ou supprimer les services inutiles ;
- chiffrer les données à caractère personnel sur le disque dur lorsque cette fonction est disponible ;
- limiter l'envoi de documents numérisés aux adresses de messagerie internes et dans certains cas limiter l'envoi de documents numérisés à une seule adresse de messagerie ;
- dans le cas d'une maintenance par un tiers, prévoir les mesures destinées à empêcher l'accès aux données à caractère personnel ;
- dans le cas d'une télémaintenance par un tiers à une imprimante ou copieur multifonctions hébergé localement, prendre des mesures spécifiques pour protéger chaque accès ;
- empêcher l'accès à des données à caractère personnel stockées sur des imprimantes ou copieurs multifonctions mis au rebut.

14.21 Exigences relatives aux serveurs[149] (S21)

305. **E14-S21-C01 : Procédure d'accès aux outils et interfaces d'administration.** Le demandeur dispose d'une procédure destinée à limiter l'accès aux outils et interfaces d'administration aux personnes habilitées.

306. **E14-S21-C02 : Procédure d'installation des mises à jour critiques.** Le demandeur dispose d'une procédure prévoyant l'installation sans délai les mises à jour critiques[150].

[149] Référentiel Cnil.

[150] Une mise à jour critique est une mise à jour logicielle ou système qui corrige des vulnérabilités de sécurité majeures ou des erreurs graves pouvant compromettre la sécurité, la stabilité ou les performances d'un logiciel, d'un système d'exploitation ou d'une application et ayant une note élevée en termes d'indice CVE.

307. **E14-S21-C03 : Protocole d'administration.** Le demandeur utilise un protocole sécurisé pour l'administration des serveurs. Il est possible de justifier des dérogations à l'utilisation de protocoles obsolètes (explicitement identifiés et documentés), par exemple par la mise en place de mesures strictes de cloisonnement des flux concernés.

14.22 Exigences relatives aux sites web[151] (S22)

308. **E14-S22-C01 : Protocole TLS.** Le demandeur utilise pour ses sites web le protocole TLS 1.3 ou la version du protocole TLS conforme à l'état de l'art et vérifier sa mise en œuvre.

309. **E14-S22-C02 : Mot de passe encapsule dans les URL.** Le demandeur vérifier qu'aucun mot de passe ou identifiant n'est encapsule dans les URL.

310. **E14-S22-C03 : Chiffrement des flux.** Le demandeur prévoit que le chiffrement des flux est garanti par TLS.

311. **E14-S22-C04 : Audits de sécurité.** Le demandeur effectue, conformément au critère 4E20-S01-C02, un audit annuel dans le respect du critère E01-S03-C04 de sécurité sur le site. Le résultat de cet audit alimente le plan d'action visé au E20-S03-C01.

14.23 Exigences relatives aux violations de données à caractère personnel[152] (S23)

312. **E14-S23-C01 : Procédure relative aux violations de données à caractère personnel - existence.** Le demandeur dispose d'une procédure relative aux violations de données à caractère personnel.

313. **E14-S23-C02 : Procédure relative aux violations de données à caractère personnel – contenu.** La procédure relative aux violations de données à caractère personnel prévoit :
- l'analyse de signalements d'événements relatifs à la sécurité ;
- l'analyse des incidents relatifs à la sécurité ;
- l'identification du personnel du demandeur impliqué dans la gestion des incidents relatifs à la sécurité ;
- l'identification des parties prenantes externes ;
- la qualification des évènements de sécurité[153] en incident de sécurité ;
- les cas de violation de données à caractère personnel ;
- les obligations en cas de violations de données à caractère personnel ;
- les dérogations à l'information des personnes ;
- le contenu de la notification à la Cnil ;
- le délai pour notifier à la Cnil ;
- que faire si le délai de 72h pour notifier est dépassé ;
- le rôle du sous-traitant en cas de violation de données à caractère personnel ;
- comment apprécier l'absence de risque, le risque et le risque élevé ;

L'indice CVE (Common Vulnerabilities and Exposures) est un système de référence international utilisé pour l'identification et la référencement des vulnérabilités informatiques. Il fournit une liste normalisée de noms et de numéros d'identification uniques pour les vulnérabilités de sécurité.

[151] Référentiel Cnil.

[152] Référentiel Cnil.

[153] Anomalies détectées, violation de données avérée …

- les pouvoirs de la CNIL[154] et, le cas échéant, des autres autorités de contrôle compétentes en matière de violation de données à caractère personnel ;
- la nécessité d'élaborer un plan de retour d'expérience.

314. **E14-S23-C03 : Procédure relative aux violations de données à caractère personnel - application.** Le demandeur met en œuvre la procédure visée au E14-S23-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative aux violations de données à caractère personnel est appliquée par les métiers impliqués dans le traitement et rédige un rapport à l'issu de l'audit.

315. **E14-S23-C04 : Registre des violations de données à caractère personnel.** Le demandeur a constitué le registre des violations de données à caractère personnel dont le contenu est défini au E07-S03-C01.

316. **E14-S23-C05 : Plan de retour d'expérience.** Le demandeur établit, à la suite de chaque violation de données à caractère personnel, le plan de retour d'expérience visé dans la procédure relative aux violations de données à caractère personnel et en assure le suivi.

15. Exigences relatives aux droits des personnes (E15)

15.1 Exigences relatives à la politique de gestion des droits des personnes (S1)

317. **E15-S01-C01 : Politique de gestion des droits des personnes - existence.** Le demandeur a élaboré une politique de gestion des droits des personnes.

318. **E15-S01-C02 : Politique de gestion des droits des personnes - contenu.** La politique de gestion des droits des personnes identifie :
- la(les) personne(s) ou le service chargé de centraliser les demandes d'exercice de droits émanant des personnes concernées ;
- la(les) personne(s) ou le service chargé de traiter ces demandes ;
- les modalités permettant aux personnes concernées d'exercer leurs droits.

15.2 Exigences relatives à la procédure de gestion des droits des personnes (S2)

319. **E15-S02-C01 : Procédure de gestion des droits des personnes - existence.** Le demandeur dispose d'une procédure de gestion des droits des personnes qui s'applique au traitement de toutes les demandes d'exercice de droit (recevable ou non) et permet de répondre aux demandes d'exercice de droit dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de la demande.

320. **E15-S02-C02 : Procédure de gestion des droits des personnes - contenu.** La procédure relative à la gestion des droits des personnes comprend :
- la description des étapes communes d'une demande d'exercice de droits par la personne concernée (recueil de la demande, vérification de l'identité de la personne auteur de la demande d'exercice de droits, accuser de réception de la demande et demandes

[154] La Cnil dispose de pouvoirs en cas de violation de données personnelle : pouvoir de contrôle, d'enquête et de sanction.

facultatives d'informations complémentaires, réponse à une demande d'exercice des droits, délai de réponse, le processus de traitement d'une demande « complexe », les vérifications à effectuer concernant le droit des tiers et qui peuvent conduire à masquer certains éléments, les cas de refus, les cas de demande de paiement, le cas de la sous-traitance, le cas des défunts) ;
- les étapes à suivre pour traiter une demande d'exercice du droit d'accès, incluant le cas visé au E09-S01-C01 où le sous-traitant aide le demandeur à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits ;
- les étapes à suivre pour traiter une demande d'exercice du droit de rectification ;
- les étapes à suivre pour traiter une demande d'exercice du droit d'opposition ;
- les étapes à suivre pour traiter une demande d'exercice du droit d'effacement ;
- les étapes à suivre pour traiter une demande d'exercice du droit à la limitation du traitement ;
- les étapes à suivre pour traiter une demande d'exercice du droit à la portabilité ;
- les étapes permettant à la personne concernée de transmettre des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès ;
- les étapes à suivre pour traiter une demande émanant des héritiers sur les données à caractère personnel des défunts ;
- des modèles de réponse à ces demandes ;
- le suivi des demandes d'exercice des droits.

321. **E15-S02-C03 : Délai de réponse.** Le demandeur, conformément à la procédure visée au E15-S02-C02, répond aux demandes d'exercice de droits dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de cette demande[155].

322. **E15-S02-C04 : Demande complexe**. Le demandeur peut, conformément à la procédure E15-S02-C02, prolonger de 2 mois le délai visé au E15-S02-C03 compte tenu de la complexité et du nombre de demandes. Le demandeur, conformément à la procédure E15-S02-C02, informe la personne concernée de la prolongation du délai de réponse à sa demande et des motifs de ce report dans un délai d'un mois à compter de la réception de la demande.

323. **E15-S02-C05 : Vérifications concernant les droits des tiers.** Le demandeur répond, conformément à la procédure visée au E15-S02-C02, à une demande de droit d'accès dans le respect des droits des tiers (vie privée, secret des correspondances). En pratique, cela peut conduire à masquer, dans ce qui est communiqué à la personne concernée, les informations qui ne la concernent pas.

324. **E15-S02-C06 : Cas de refus.** Le demandeur doit, conformément à la procédure visée au E15-S02-C02, rédiger un mémorandum permettant de documenter le caractère manifestement infondé ou excessif[156] de la demande à laquelle il refuse de donner suite.

---

[155] RGPD, Art. 12-3.

[156] Par exemple :
- les demandes (d'accès ou autres) présentées par une personne autre que la personne à laquelle se rapportent les données sans justification d'un mandat de représentation ;
- les demandes (d'accès ou autres) qui ne permettent pas d'identifier la personne concernée, en dépit d'une relance du responsable du traitement incitant la personne concernée à compléter sa demande ;

325. **E15-S02-C07 : Gratuité de l'exercice des droits.** Le demandeur prévoit un principe de gratuité de l'exercice des droits. Il se réserve la possibilité de demander le paiement de « frais raisonnables basés sur les coûts administratifs » :
- pour toute copie supplémentaire demandée par la personne concernée[157];
- si la demande est manifestement infondée ou excessive.

326. **E15-S02-C08 : Procédure de gestion des droits des personnes - application.** Le demandeur met en œuvre la procédure visée au critère E15-S02-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure de gestion des droits des personnes est appliquée par les métiers et rédige un rapport à l'issu de l'audit.

15.3 Exigences relatives au suivi des demandes d'exercice de droits (S3)

327. **E15-S03-C01 : Suivi des demandes - existence.** Le demandeur établit, conformément à la procédure visée au E15-S02-C02, un suivi des demandes d'exercice des droits.

328. **E15-S03-C02 : Suivi des demandes - statistiques.** Le demandeur établit des statistiques annuelles afin d'identifier si le nombre de demande émanant des personnes concernées est en augmentation, si les demandes sont traitées dans les délais ainsi que la durée moyenne de traitement d'une demande. Les statistiques annuelles identifient également la proportion des demandes traitées dans le délai d'un mois, sans prolongation du délai, afin que des actions soient identifiées et mises en œuvre si le report du délai s'avère être une pratique quasi-systématique ou risque de le devenir en l'absence d'actions préventives. Ces statistiques font partie des indicateurs visés au E20-S02-C01 et E20-S02-C02.

329. **E15-S03-C03 : Suivi des demandes – retour d'expérience.** Le demandeur présente, à l'aide du suivi des demandes et des statistiques annuelles, deux fois par an dans le cadre du comité de gouvernance de la donnée personnelle visé au E03-S02-C04 un retour d'expérience au sujet de la gestion des demandes d'exercice de droits aboutissant, le cas échéant, à la mise en place d'un plan d'amélioration.

16. Exigences relatives à la formation et la sensibilisation (E16)

16.1 Exigences relatives au programme de formation et de sensibilisation (S1)

330. **E16-S01-C01 : Programme de formation et sensibilisation- existence.** Le demandeur établit et met en œuvre un programme de formation et de sensibilisation des métiers aux procédures du présent référentiel ainsi qu'à la réglementation sur la protection des données à caractère personnel afin de poursuivre la diffusion de la culture Informatique et libertés dans son

- les demandes répétées de rectification, de suppression et de limitation si la personne concernée ne fait que répéter une demande initiale à laquelle le responsable du traitement a déjà répondu, ou formule une autre demande mais qui ne contient aucun nouveau motif ;
- les demandes de rectification, de suppression, de limitation du traitement et de portabilité si la personne concernée a déjà obtenu du responsable du traitement la confirmation que des données à caractère personnel la concernant ne font pas l'objet d'un traitement.

[157] Par exemple si une personne exerce son droit chaque semaine.

organisme. Le délégué (DPO) intervient, conformément au E02-S02-C02, dans le cadre de ce programme à travers sa mission d'information des employés qui procèdent au traitement.

331. **E16-S01-C02 : Programme de formation et sensibilisation - application.** Le demandeur réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que le programme de formation et sensibilisation est suivi et rédige un rapport à l'issu de l'audit.

16.2 Exigences relatives aux autres actions d'information et de sensibilisation (S2)

332. **E16-S02-C01 : Réponses RGPD.** Le demandeur met à la disposition de ses collaborateurs des outils[158] qui leur permettent de trouver, et à tout moment, des réponses aux questions les plus courantes dans le domaine du droit de la protection des données à caractère personnel.

333. **E16-S02-C02 : Veille documentaire.** Le demandeur établit une veille documentaire en droit de la protection des données à caractère personnel, a minima chaque trimestre.

334. **E16-S02-C03 : Lettre d'information.** Le demandeur diffuse, à minima chaque trimestre, une lettre d'information qui propose une vue d'ensemble de l'actualité en matière de protection des données à caractère personnel.

335. **E16-S02-C04 : Questionnaire à Choix Multiples (QCM).** Le demandeur s'assure, chaque année, par le biais d'un Questionnaire à Choix Multiples (QCM), de la compréhension par son personnel de la réglementation sur la protection des données à caractère personnel ainsi que des politiques et procédures établies à ce sujet.

17. Exigences relatives aux transferts internationaux de données à caractère personnel (E17)

17.1 Exigences relatives à la politique de transferts internationaux de données à caractère personnel (S01)

336. **E17-S01-C01 : Politique relative aux transferts internationaux de données à caractère personnel - existence.** Le demandeur a élaboré une politique qui énonce sa position au sujet des transferts de données à caractère personnel hors de l'Union européenne.

337. **E17-S01-C02 : Politique relative aux transferts internationaux de données à caractère personnel - contenu.** La politique relative aux transferts internationaux de données à caractère personnel identifie les pays vers lesquels le demandeur autorise ces transferts et ceux vers lesquels il les interdit et en justifie les raisons. Cette politique est portée à la connaissance des métiers impliqués dans le traitement.

17.2 Exigences relatives à la procédure relative aux transferts internationaux de données à caractère personnel (S02)

338. **E17-S02-C01 : Procédure relative aux transferts internationaux de données à caractère personnel - existence.** Le demandeur dispose d'une procédure à respecter pour la mise en place de transferts de données à caractère personnel hors UE.

[158] ChatBot, FAQ, forum de discussion…

339. **E17-S02-C02 : Procédure relative aux transferts internationaux de données à caractère personnel - contenu**. La procédure relative aux transferts de données à caractère personnel hors UE prévoit :
- la réalisation d'une cartographie des transferts de données à caractère personnel hors UE visée au critère E17-S03-C01 ;
- qu'il doit être préalablement vérifié si le transfert est envisagé vers un pays bénéficiant d'une décision d'adéquation adoptée par la Commission européenne et, dans l'affirmative, si les conditions prévues pour l'adéquation sont remplies par l'importateur des données ;
- que le demandeur ne puisse transférer des données à caractère personnel hors UE vers un pays ne bénéficiant pas d'une décision d'adéquation adoptée par la Commission européenne que s'il a prévu des garanties appropriées résultant de l'élaboration d'un arbre de décision[159] permettant la sélection des outils d'encadrement des transferts visés au critère E17-S04-C01. La réalisation de l'arbre de décision revient à suivre les étapes suivantes :
    - Etape 1 : vérification si le transfert est envisagé vers un pays bénéficiant d'une décision d'adéquation[160] ;
    - Etape 2 : en l'absence d'une telle décision d'adéquation, recours à des garanties appropriées[161] ,
      Ou, en l'absence de garanties appropriées, transfert par dérogation[162] ;
    - Etape 3 : pas de transfert s'il n'est pas possible de l'encadrer selon les articles 45, 46 ou 49 du RGPD.
- que l'arbre de décision devra être réévalué en cas d'évolution des traitements de données à caractère personnel concernés par les transferts et/ou d'évolution du contexte de ces traitements de données à caractère personnel ;
- pour les transferts de données à caractère personnel vers des pays situés hors de l'Union européenne ne bénéficiant pas d'un niveau de protection adéquate, une évaluation de la législation du pays tiers vers lequel le transfert de données à caractère personnel est envisagé. L'évaluation du niveau de protection dont bénéficieront les données à caractère personnel transférées doit porter sur la ou les législations spécifiques applicables aux transferts en cause, c'est-à-dire les législations applicables dans le pays des destinataires de ces transferts ainsi que sur les pratiques de l'autorité du pays tiers. Elle a pour objet de déterminer si les garanties contenues dans l'outil d'encadrement du transfert envisagé peuvent être respectées dans la pratique ou si le cadre juridique de destination du transfert a pour effet de diminuer ou d'écarter l'application de ces garanties. Dans le cas où la législation du pays tiers aboutit à écarter entièrement ou partiellement les garanties qui figurent dans l'outil de transfert, des mesures supplémentaires doivent être mises en place ;
- les cas où une autorisation de la Cnil est nécessaire et l'obtention de l'autorisation par la Cnil.

La procédure fait également état de l'impossibilité pour le demandeur de transférer les données à caractère personnel dans le cas où les flux ne peuvent pas être encadrés ou en l'absence de mesures supplémentaires efficaces.
La procédure fixe également les conditions à remplir pour la sélection de chaque outil de transfert en précisant notamment que :

---

[159] L'arbre de décision permettra par exemple d'identifier, en fonction des situations de transferts, quelles sont les clauses contractuelles types de la Commission européenne qui doivent être utilisées.

[160] Décision d'adéquation prévue à l'article 45 du RGPD.

[161] Outils de transfert visés à l'article 46 du RGPD.

[162]Dérogations prévues par l'article 49 du RGPD.

- les dérogations au principe d'encadrement général des transferts vers un Etat non membre de l'Union ne peuvent être mobilisées que dans des situations particulières : le demandeur doit s'efforcer de mettre en place des garanties appropriées et ne doit recourir à ces exceptions qu'en l'absence de telles garanties.

La procédure précise en synthèse le résultat à obtenir à l'issue de son application, à savoir :

- une cartographie des transferts (l'identification des traitements de données à caractère personnel qui répondent à la définition d'un transfert) ;
- l'identification des transferts vers les pays ayant fait l'objet d'une décision d'adéquation ainsi que la trace d'une vérification que les modalités à respecter s'appliquent ;
- en l'absence d'une telle décision d'adéquation, l'identification de l'outil retenu pour encadrer les transferts, la preuve de sa mise en place[163] et la trace d'une vérification que l'outil retenu est pertinent pour la cible d'évaluation[164] ;
- si le transfert est réalisé par dérogation à ces outils globaux d'encadrement, la justification des conditions pour envisager la dérogation et la mise en place des garanties prévues par l'article 49 du RGPD.

340. **E17-S02-C03 : Procédure relative aux transferts internationaux de données à caractère personnel - application.** Le demandeur met en œuvre la procédure visée au E17-S02-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure relative aux transferts internationaux de données à caractère personnel est appliquée par les métiers impliqués dans le traitement et rédige un rapport à l'issu de l'audit.

17.3 Exigences relatives à la cartographie des transferts internationaux de données à caractère personnel (S03)

341. **E17-S03-C01** : **Cartographie des transferts internationaux de données à caractère personnel.** Le demandeur établit et tient à jour une cartographie transferts de données à caractère personnel hors UE qui décrit, pour chaque traitement concerné :

- la finalité du transfert ;
- l'identité du destinataire ;
- le pays d'établissement du destinataire ;
- la nature des traitements opérés chez l'importateur ;
- les catégories de personnes concernées par le transfert ;
- les catégories de données à caractère personnel transférées répondant à la classification visée au E05-C01-S01 ;
- la durée de conservation des données à caractère personnel chez l'importateur ;
- la nature des garanties mises en œuvre par l'importateur des données à caractère personnel pour assurer un niveau de protection suffisant au regard de la protection des données à caractère personnel transférées ;
- la nature et modalités d'information des personnes concernées.

Elle précise également la fréquence à laquelle une revue de la cartographie des transferts internationaux de données à caractère personnel est effectuée.

[163] CCT signées, approbation des BCR…

[164] Objet des CCT, périmètre des BCR, description du transfert sur le certificat…

17.4 Exigences relatives à l'encadrement des transferts internationaux de données à caractère personnel (S04)

342. **E17-S04-C01** : **Encadrement des transferts internationaux de données à caractère personnel**. Le demandeur a encadré les transferts de données à caractère personnel vers des sociétés tierces situées hors de l'Union européenne et/ou les transferts de données à caractère personnel hors UE intra groupe en se fondant sur :
- une décision d'adéquation de la Commission européenne concernant certains pays assurant un niveau de protection adéquat ;
- les clauses contractuelles types (CCT) de la Commission européenne ;
- des clauses contractuelles types adoptées par la Cnil et approuvées par la Commission européenne ;
- des clauses contractuelles spécifiques (considérées comme conformes aux modèles de clauses de la Commission européenne) autorisées par la Cnil ;
- des règles internes d'entreprises (BCR) ;
- un mécanisme de certification ou code de conduite[165] approuvés en tant qu'outil de transfert ;
- un arrangement administratif ou un texte juridiquement contraignant et exécutoire pris pour permettre la coopération entre autorités publiques[166].

A défaut, le demandeur justifie de l'impossibilité de mettre en place l'un des sept outils susvisés.

343. **E17-S04-C02 : Dérogations au principe d'encadrement des transferts internationaux de données à caractère personnel.** Les dérogations suivantes au principe d'encadrement général des transferts de données à caractère personnel hors UE peuvent être mobilisées par le demandeur :
- la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le demandeur ou à la mise en œuvre de mesures précontractuelles prises à sa demande ;
- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le demandeur et une autre personne physique ou morale le transfert est nécessaire pour des motifs importants d'intérêt public ;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- le transfert a lieu au départ d'un registre qui est légalement destiné à fournir des informations au public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime ;
- le transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées et pour une durée limitée et non reconductible, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de

[165] Comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées.

[166] RGPD, Art. 38-1

données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel.

Le demandeur s'efforce de mettre en place des garanties appropriées encadrant le transfert envisagé et ne recourt à ces dérogations qu'en l'absence de telles garanties.

17.5 Exigences relatives à la vérification du respect des outils d'encadrement des transferts internationaux de données à caractère personnel (S05)

344. **E17-S05-C01** : **Vérification du respect des outils d'encadrement des transferts par les importateurs**. Le demandeur a établi et met en œuvre un plan d'audit destiné à vérifier le respect par les importateurs de données à caractère personnel concernés des outils d'encadrement des transferts visés au E17-S04-C01. Cette vérification n'est toutefois pas nécessaire dans le cas d'un transfert vers un pays ayant fait l'objet d'une décision d'adéquation.

18. Exigences relatives aux sous-traitants (E18)

18.1 Exigences relatives à la procédure sous-traitants (S01)

345. **E18-S01-C01 : Procédure sous-traitants - existence.** Le demandeur a établi une procédure qui encadre le recours à des sous-traitants. Cette procédure prévoit que le demandeur :
- s'assure, conformément au critère E18-S02-C01, que le sous-traitant présente des garanties suffisantes concernant la mise en œuvre de mesures techniques et organisationnelles adaptées afin que le traitement réponde aux exigences de la réglementation sur la protection des données à caractère personnel et garantisse la protection des droits des personnes ;
- donne son autorisation au sous-traitant, conformément au critère E09-S01-C01, avant que celui-ci ne confie un traitement de données à caractère personnel à un sous-traitant ultérieur.
- fournit des instructions qui doivent reprendre l'ensemble des exigences comme si elles étaient mises en œuvre par le responsable du traitement en tant que tel.

346. **E18-S01-C02 : Procédure sous-traitants - contenu.** La procédure du demandeur encadrant le recours aux sous-traitants prévoit notamment :
- qu'un questionnaire est communiqué aux sous-traitant en phase précontractuelle permettant une première évaluation de leur conformité à la réglementation sur la protection des données à caractère personnel ;
- les modalités de traitement des réponses reçues à la suite de l'envoi du questionnaire ;
- de faire signer aux sous-traitants une déclaration indiquant que les membres de son personnel qui traitent les données à caractère personnel du demandeur sont soumis à une obligation de confidentialité ;
- les actions à mettre en place dans l'hypothèse où un changement de sous-traitant ultérieur serait envisagé en cours de prestation ;
- les modalités d'obtention par le sous-traitant d'une autorisation préalable du demandeur pour la mise en place d'un transfert hors UE ;
    - le cas de changements significatifs dans les moyens de sécurité du traitement ;
- la signature du contrat, conformément aux critères E09-S01-C01 et E09-S01-C02, avant que le demandeur donne instruction au sous-traitant de démarrer les opérations de traitement qu'il effectue pour son compte.

347. **E18-S01-C03 : Procédure sous-traitants - application.** Le demandeur met en œuvre la procédure visée au E18-S01-C01, réalise un audit annuel dans le respect du critère E01-S03-C04 afin de s'assurer que la procédure sous-traitant est appliquée par les métiers impliqués dans le traitement et rédige un rapport à l'issu de l'audit.

18.2 Exigences relatives au choix des sous-traitants (S02)

348. **E18-S02-C01 : Evaluation du caractère suffisant des garanties.** Le demandeur évalue, au cas par cas et en tenant compte de la nature, de la portée, du contexte, des finalités du traitement ainsi que des risques pour les droits et libertés des personnes concernées, le caractère suffisant des garanties fournies par le sous-traitant en prenant en considération les éléments suivants :
- les connaissances spécialisées du sous-traitant[167];
- la fiabilité du sous-traitant et ses ressources ;
- les documents pertinents transmis par le sous-traitant[168] ;
- la réputation du sous-traitant sur le marché ;
- l'adhésion du sous-traitant à un code de conduite ou à un mécanisme de certification approuvé ;
- la prise en compte par le sous-traitant des mesures d'atténuation des risques en cas d'analyse d'impact qui le concerne.

349. **E18-S02-C02 : Vérification des garanties.** Le demandeur vérifie, à une fréquence adéquate, les garanties du sous-traitant, y compris au moyen d'audits et d'inspections, le cas échéant.

18.3 Exigences relatives à l'audit des sous-traitants (S03)

350. **E18-S03-C01 : Plan d'audit des sous-traitants - existence.** Le demandeur a établi un plan d'audit annuel dans le respect du critère E01-S03-C04 de ses sous-traitants afin de vérifier les garanties apportées par ces derniers conformément au critère E18-S02-C02 Ce plan d'audit détermine :
- les sous-traitants à auditer et les critères pour déterminer ceux à auditer en priorité ;
- le type d'audit (à distance, sur site ou par voie de questionnaire pour recueillir les informations nécessaires) qui serait nécessaire et approprié pour chaque cas.

Ces audits seront réalisés par le demandeur ou un tiers mandaté par lui.

351. **E18-S03-C02 : Plan d'audit des sous-traitants – suivi.** Le demandeur suit la réalisation du plan d'audit annuel dans le respect du critère E01-S03-C04 de ses sous-traitants. Les résultats des audits lui permettront, le cas échéant, de demander sous-traitant de prendre des mesures ultérieures, par exemple remédier aux lacunes et aux défaillances constatées.

[167] Par exemple, l'expertise technique en ce qui concerne les mesures de sécurité et les violations de données.

[168] Par exemple, la politique en matière de respect de la vie privée, les conditions de service, l'enregistrement des activités de traitement, la politique en matière de gestion des documents, la politique de sécurité de l'information, les rapports des audits externes en matière de protection des données, les certifications internationales reconnues comme la série ISO 27000.

18.4 Exigences relatives à la formation et la sensibilisation du personnel sur les relations avec les sous-traitants (S04)

352. **E18-S04-C01 : Formation et sensibilisation.** Le demandeur a prévu, dans le programme annuel de formation et sensibilisation du personnel visé au E16-S01-C01, une intervention sur la thématique des relations avec les sous-traitants.

353. **E18-S04-C02 : Questionnaire à Choix Multiples (QCM).** Le demandeur a prévu de soumettre les participants aux actions de formation et de sensibilisation visées au E18 à un QCM.

19. Exigences relatives au secteur d'activité (E19)

19.1 Exigences relatives au référentiel (S01)

354. **E19-S01-C01 : Référentiel.** Le demandeur dispose d'un référentiel identifiant les réglementations sectorielles, visées au critère E06-S04-C02, applicables à la cible d'évaluation qu'il est tenu de suivre ainsi que les codes de conduite approuvés par la Cnil et les référentiels publiés par la Commission applicables à son secteur d'activité visés au E04-S01-C01Les éléments de ce référentiel sont précisés dans la politique générale de protection des données à caractère personnel visée au E01-S02-C04.

19.2 Exigences relatives à la conciliation des exigences sectorielles et du droit des données à caractère personnel (S02)

355. **E19-S02-C01 : Procédure conciliation exigences sectorielles et droit des données à caractère personnel - existence.** Le demandeur a établi une procédure décrivant le process afin de concilier les exigences issues de la réglementation sur la protection des données à caractère personnel avec celles découlant de sa réglementation sectorielle.

20. Exigences relatives à la conformité (E20)

20.1 Exigences relatives à la politique de contrôle interne (S01)

356. **E20-S01-C01 : Politique de contrôle interne - existence.** Le demandeur a élaboré une politique de contrôle interne en matière de protection des données à caractère personnel.

357. **E20-S01-C02 : Politique de contrôle interne - contenu.** La politique de contrôle interne prévoit :
- la mise en place d'un contrôle périodique (audit) dans le domaine de la protection des données à caractère personnel ;
- l'élaboration d'un plan d'audit annuel ;
- l'élaboration des rapports d'audits référencés dans les critères dont les conclusions font l'objet du plan d'action prévu au critère E20-S03-C01.

20.2 Exigences relatives aux indicateurs (S02)

358. **E20-S02-C01 : Indicateurs de conformité.** Le demandeur a établi des indicateurs de conformité destinés à évaluer, après application des mesures et avant audits annuels visés au E01-S03-C04 susceptibles d'aboutir à des corrections, l'efficacité des règles mises en place en matière de protection des données à caractère personnel.

359. **E20-S02-C02 : Indicateurs de maturité[169].** Le demandeur a établi des indicateurs de maturité en matière de protection des données à caractère personnel (la maturité représentant le formalisme avec laquelle les activités liées à la protection des données sont gérées).

20.3 Exigences relatives aux retours d'expérience (S03)

360. **E20-S03-C01 : Plan de retour d'expérience - existence.** Le demandeur élabore, à la suite des opérations de contrôle interne en matière de protection des données à caractère personnel, un plan de retour d'expérience aboutissant à un plan d'action. Le demandeur interprète et tire les conséquences des indicateurs visés au E20-S02 dans le plan de retour d'expérience conduisant au plan d'action.

361. **E20-S03-C02 : Plan de retour d'expérience - suivi.** Le demandeur réalise un suivi du plan d'action élaboré à la suite du plan de retour d'expérience.

21. Exigences relatives à la définition de la cible de l'évaluation (E21)

362. **E21-C01 : Liste des traitements soumis au processus de certification.** Le demandeur définit, à partir de la liste des traitements visée au critère E04-S02-C02, la liste des traitements de données à caractère personnel qu'il souhaite soumettre au processus de certification[170] et pour lesquels il est responsable du traitement. Le demandeur précise, pour chaque traitement de données à caractère personnel inscrit dans cette liste :
- sa finalité (notamment avec l'objectif d'identifier les réglementations sectorielles applicables visées au E19-S02-C01) ;
- les sous finalité ;
- les données à caractère personnel traitées ;
- les catégories de personnes concernées ;
- les destinataires ou catégories de destinataires des données à caractère personnel ;
- les sous-traitants ;
- les modalités d'exercice des droits des personnes ;
- les transferts vers des pays tiers.

363. **E21-C02 : Liste des logiciels[171].** Le demandeur établi et tient à jour la liste des logiciels liés aux traitements de données à caractère personnel qui se trouvent dans la cible d'évaluation utilisés dans le cadre de son activité.

---

[169] Par exemples le niveau de maturité 0 pourrait correspondre à « une pratique inexistante ou incomplète », le niveau 1 « Pratique informelle », le 2 « Pratique répétable et suivie », le 3 « Processus défini », le 4 « Processus contrôlé » et le 5 « Processus continuellement optimisé ». L'évaluation du niveau de maturité pourrait porter sur différents types d'activités gérées par le demandeur telles que la gouvernance des données personnelles, le recensement des traitements et leur inscription au registre, la gestion des violations de données, la gestion des risques de sécurité...

[170] Le demandeur peut décider de soumettre au processus de certification l'ensemble des traitements mis en œuvre dans le cadre de son activité. Sur le plan méthodologique, ces traitements peuvent être regroupés en 23 principaux systèmes d'information visés en annexe 1 figurant dans le document « Lexing Certification RGPD – Guide d'évaluation ».

[171] La liste des logiciels a pour objet de croiser la liste des applications avec la liste des traitements de données à caractère personnel. Dans plus de 90% des cas, lors du diagnostic on constate qu'il existe des

364. **E21-C03 : Liste des technologies[172].** Le demandeur établi et tient à jour la liste des technologies utilisées dans le cadre de son activité auxquelles peuvent s'appliquer des obligations réglementaires spécifiques. Le demandeur documente ces obligations pour les traitements dans la cible d'évaluation.

logiciels gérés par la DSI qu'on ne retrouve ni dans le registre des traitements, ni dans la liste des responsables du traitement. C'est ainsi un moyen de détecter les angles morts.

[172] La liste des technologies a un impact majeur sur les données à caractère personnel. Il en est ainsi par exemple de la biométrie ou de la vidéosurveillance.