Grille d'analyse

AU-053 – Contrôle d'accès biométrique avec base centrale

Table des matières

Introduction

Dans le cadre d'une demande concernant la mise en œuvre d'un dispositif biométrique, la CNIL s'appuie sur les justifications apportées par le responsable de traitement. La grille d'analyse a pour but de **démontrer que les risques sont maîtrisés, à l'aide d'une réflexion sur trois axes** :

1. **le choix du dispositif et de ses modalités de mise en œuvre**, qui permet d'évaluer que celui-ci constitue une solution proportionnée au regard du contexte spécifique dans lequel il sera mis en œuvre et de la finalité poursuivie ;
2. **le respect des exigences**, qui permet d'évaluer que les conditions de mise en œuvre respectent notamment les obligations juridiques de la loi Informatique et Libertés ainsi que les recommandations de la CNIL ;
3. **l'appréciation des risques résiduels**, qui permet d'évaluer que les risques sur la vie privée des personnes concernées, subsistant après application des mesures organisationnelles et techniques choisies, sont maîtrisés.

Ces trois axes sont destinés à aider à prendre conscience des possibles impacts du traitement intégrant un dispositif biométrique et à mieux cibler les solutions répondant aux besoins. Ils sont également nécessaires pour fournir des lignes directrices lors de l'instruction des dossiers et anticiper les interrogations de la Commission.

Note : le concours du fournisseur du dispositif peut être utile, notamment s'il a lui-même mené une étude d'impact sur la vie privée (EIVP, plus connue sous son nom en anglais de *Privacy Impact Assessment* – PIA), dans laquelle les descriptions techniques, mesures et conditions de mise en œuvre pourraient déjà être formalisées.

Les éléments de cette étude serviront uniquement à éclairer de manière efficace la Commission dans le cadre de l'instruction du dossier présenté. En effet, la présentation d'une telle analyse ne signifie pas que le dispositif soumis à la CNIL sera autorisé.

Le premier axe : étude du dispositif prévu au regard de ses caractéristiques techniques et ses modalités de mise en œuvre

Le responsable de traitement doit justifier de la pertinence de son système par rapport à son besoin, notamment :

- de l'usage de la biométrie par rapport à un dispositif non biométrique, afin de démontrer qu'il n'existe pas un moyen moins intrusif répondant à l'objectif de la mise en place du dispositif ;
- du choix du dispositif biométrique retenu plutôt que l'un des autres dispositifs biométriques disponibles, afin d'expliquer en quoi le dispositif biométrique envisagé répond au besoin présenté par le responsable de traitement.

Pour ce faire, le tableau ci-dessous doit être renseigné :

Caractéristiques	Description	Justification[1]
Usage du dispositif biométrique (plutôt que sans biométrie)	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Type de technologie employée2	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Données traitées3	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Stockage des données biométriques4	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Nombre de dispositifs concernés et lieu(x) d'implantation	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Nombre de personnes concernées par lieu	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Typologie de la population5	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Dispositions complémentaires tenant compte des contraintes d'utilisation (si besoin)6	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.

[1] *Justifier les choix décidés en expliquant leur nécessité. Ces justifications peuvent être issues du contexte d'utilisation du dispositif et des risques de sécurité qu'il est censé contribuer à traiter.*

[2] *Contour de la main, reconnaissance vocale, réseau veineux du doigt ou de la paume, reconnaissance de l'empreinte digitale, reconnaissance de l'iris de l'œil, reconnaissance faciale, ADN notamment.*

3 Données biométriques initiales, gabarits biométriques, gabarits révocables par exemple, et historique d'accès.

4 Supports individuels (cartes, clés USB) ou base de données interne au dispositif ou base de données distante. Une base centralisée contient les données biométriques de plusieurs usagers sur un même support, local au dispositif, ou distant à travers un réseau.

5 La typologie de la population permet d'apprécier le choix du dispositif biométrique en fonction des catégories d'usagers en termes de morphologie, de contrainte professionnelle, de prise en compte d'un handicap.

6 Les contraintes d'utilisation sont liées aux difficultés de captation de la donnée biométrique (déformation de la voix, visage couvert, port de gants ou lunettes, etc.). Des dispositions accompagnant le dispositif biométrique doivent alors être mises en œuvre (sas d'isolement, support visuel pour guider la position du visage, etc.).

Caractéristiques	Description	Justification[1]
Modalités d'enrôlement7	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Taux de fausses acceptations	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Taux de faux rejets	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Capacité de paramétrage8	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Autres caractéristiques (si besoin)	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.

La CNIL vérifiera que les réponses ont bien été fournies, qu'elles sont justifiées et pertinentes.

7 L'enrôlement de l'usager doit être encadré par une personne habilitée à l'administration du dispositif biométrique. Cet enrôlement pourra s'effectuer directement sur le dispositif ou à distance sur un poste spécifique dédié à cette tâche.

8 *Le dispositif biométrique possède-t-il des possibilités de réglages de sa fiabilité ? Si oui, quelles sont les personnes habilitées à manipuler ces paramètres ?*

Le deuxième axe : étude du respect des exigences de la CNIL

Le responsable de traitement est tenu de décrire, de manière détaillée, les mesures mises en œuvre afin de satisfaire les exigences de la CNIL.

Ces exigences, identifiées comme étant nécessaires pour réduire les risques à un niveau acceptable et apporter une confiance suffisante envers le dispositif choisi, visent à :

- respecter les obligations juridiques de la loi Informatique et Libertés ;
- respecter les recommandations de la CNIL encadrant l'usage de la biométrie ;
- réduire la gravité et la vraisemblance des risques que la mise en œuvre d'un dispositif biométrique fait peser sur la vie privée des personnes concernées.

Pour ce faire, le tableau suivant doit être renseigné[9] :

Exigences permettant d'atteindre les objectifs de la CNIL	Description des mesures prévues OU justification
Exigences portant sur les données	
Collecter et utiliser les seules données biométriques nécessaires10 sous la forme d'un gabarit ne permettant pas de recalculer la donnée biométrique d'origine	Cliquez ici pour taper du texte.
Chiffrer les données biométriques à l'aide d'un algorithme cryptographique et d'une gestion des clés conformes à l'état de l'art11	Cliquez ici pour taper du texte.
Associer un code d'intégrité aux données (par exemple, signature par hachage)	Cliquez ici pour taper du texte.
Interdire tout accès externe à la donnée biométrique (« match-on-card » ou module de sécurité physique/logique type HSM)	Cliquez ici pour taper du texte.
Effectuer le contrôle d'accès par une comparaison entre l'échantillon calculé et le gabarit d'enrôlement enregistré sans copie du gabarit	Cliquez ici pour taper du texte.
Minimiser la durée de conservation des données et veiller à l'effectivité de leur effacement à l'issue de leur durée de conservation, dès la fin de l'habilitation de la personne concernée	Cliquez ici pour taper du texte.
Supprimer la donnée biométrique en cas d'accès non autorisé au terminal de lecture-comparaison ou au serveur distant	Cliquez ici pour taper du texte.
Exigences portant sur l'organisation	

9 Le responsable de traitement doit soit décrire les mesures prévues pour la respecter, soit justifier dûment pourquoi elle ne l'est pas.

10 En particulier, imposer des contraintes à l'enrôlement (distance du capteur, luminosité, angle, arrière-plan, temps de pose, etc.) qui permettront de garantir que seules les données utiles des personnes collaborant activement seront traitées.

11 Une politique de chiffrement et de gestion des clés doit être clairement définie (changement des clés par défaut, algorithmes et tailles des clés conformes à l'état de l'art, renouvellement prévu, etc.).

Exigences permettant d'atteindre les objectifs de la CNIL	Description des mesures prévues OU justification
Informer les personnes concernées, de manière complète, spécifique et intelligible, via des supports clairs et synthétiques. Consulter les Instances représentatives du personnel si nécessaire	Cliquez ici pour taper du texte.
Responsabiliser les personnes concernées sur les bonnes conditions d'utilisation des matériels	Cliquez ici pour taper du texte.
Mettre à disposition un dispositif alternatif « de secours » ou utilisé à titre exceptionnel 12, sans contrainte, ni surcoût pour les personnes n'utilisant pas la solution biométrique	Cliquez ici pour taper du texte.
Tester le système selon une procédure formalisée, avant sa mise en place et après toute modification, dans un environnement dédié et sans recourir à des données réelles	Cliquez ici pour taper du texte.
Déterminer les actions à entreprendre en cas d'échec de l'authentification13	Cliquez ici pour taper du texte.
Gérer de manière stricte l'accès physique et logique au dispositif et bases de données par les personnes habilitées14	Cliquez ici pour taper du texte.
Former spécifiquement les administrateurs et personnes habilitées à gérer les données15	Cliquez ici pour taper du texte.
Intégrer une mesure technique ou organisationnelle de détection anti-fraude	Cliquez ici pour taper du texte.
Prévenir les personnes concernées en cas d'accès non autorisé à leurs données	Cliquez ici pour taper du texte.
Formaliser, appliquer et faire connaître une procédure de secours en cas d'incident (prévoyant notamment le ré-enrôlement)	Cliquez ici pour taper du texte.
Exigences portant sur les matériels	

[12] *Pour les personnes ne répondant pas aux contraintes du dispositif biométrique (enrôlement ou lecture de la donnée biométrique impossible), une « solution de secours » doit être mise en œuvre pour assurer une continuité du service proposé, limitée toutefois à un usage exceptionnel.*

13 Présenter les mesures prises dans le cas du rejet d'une personne par le dispositif biométrique (rejet suite à l'échec de N tentatives, alerte auprès des administrateurs, etc.).

14 Une politique de gestion des droits et des accès doit être clairement définie. Il s'agit de formaliser les différentes catégories de personnes habilitées (utilisateurs, administrateurs et gestionnaires de bases de données, personnes en charge de la gestion des données, personnes techniques de maintenance…), leurs droits sur les données, la manière dont les habilitations sont gérées, la manière dont leur accès est contrôlé, la manière dont les secrets sont gérés, les traces journalisées, la manière dont les traces sont gérées, etc.

15 Enrôlement, traitements, effacement…

Exigences permettant d'atteindre les objectifs de la CNIL	Description des mesures prévues OU justification
Mettre en œuvre des mesures permettant d'être alerté en cas de tentative d'effraction sur le lecteur ou le dispositif de stockage16	Cliquez ici pour taper du texte.
Réserver un matériel spécifique au stockage des données	Cliquez ici pour taper du texte.
Utiliser des matériels certifiés aux conditions d'usage et/ou en termes de sécurité	Cliquez ici pour taper du texte.
Garantir la traçabilité du cycle de vie du matériel	Cliquez ici pour taper du texte.
Obtenir un engagement de responsabilité de la part des administrateurs	Cliquez ici pour taper du texte.
Journaliser les opérations effectuées sur les supports	Cliquez ici pour taper du texte.
Mettre en place des mesures de sauvegarde	Cliquez ici pour taper du texte.
Formaliser et tester une procédure de récupération du système	Cliquez ici pour taper du texte.
Exigences portant sur les logiciels	
Réserver un logiciel spécifique à l'usage des données	Cliquez ici pour taper du texte.
Signer le logiciel et vérifier sa signature	Cliquez ici pour taper du texte.
Tenir les logiciels à jour selon une procédure formalisée	Cliquez ici pour taper du texte.
Vérifier que les modifications apportées par les éditeurs de logiciels ne favorisent pas la fuite de données	Cliquez ici pour taper du texte.
Recourir à des mécanismes de détection et de protection contre les logiciels malveillants et logiciels espions, éprouvés et tenus à jour	Cliquez ici pour taper du texte.
Limiter les actions des usagers sur les logiciels	Cliquez ici pour taper du texte.
Garantir la traçabilité du cycle de vie des logiciels	Cliquez ici pour taper du texte.
Vérifier régulièrement les licences des logiciels utilisés	Cliquez ici pour taper du texte.
Exigences portant sur les canaux informatiques	
Sécuriser les canaux informatiques (canaux réservés et chiffrés)	Cliquez ici pour taper du texte.
Mettre en place des mesures empêchant la transmission des gabarits stockés	Cliquez ici pour taper du texte.

La CNIL vérifiera que ses objectifs sont atteints. Dans le cas où les exigences de la CNIL sont appliquées, les objectifs seront considérés comme atteints. Dans les autres cas, elle évaluera la

[16] *En cas de stockage de la donnée sur une base locale intégrée au dispositif biométrique, toute tentative d'ouverture ou d'arrachement du terminal de lecture/comparaison doit être détectée, suivie d'un signalement à l'administrateur du dispositif.*

pertinence et la suffisance des mesures choisies par le responsable de traitement au regard des objectifs.

Le troisième axe : appréciation des risques résiduels sur la vie privée des personnes concernées

Le responsable de traitement doit apprécier les risques que le traitement de données biométriques qu'il souhaite mettre en œuvre va générer sur la vie privée des personnes concernées :

- d'une part, il doit identifier les **impacts potentiels sur la vie privée**[17] des personnes concernées en cas d'atteinte à la disponibilité, à l'intégrité et à la confidentialité de leurs données biométriques, et en estimer la **gravité**[18] en tenant compte des mesures existantes ou prévues ;
- d'autre part, il doit identifier les **principales menaces**[19] qui pourraient permettre que ces impacts surviennent, et en estimer la **vraisemblance**[20] en tenant compte des mesures existantes ou prévues.

Notes :

- cette partie a pour objet de sensibiliser dès à présent les responsables du traitement à l'exercice de l'étude d'impact sur la vie privée (EIVP, plus connue sous son nom en anglais de *Privacy Impact Assessment* – PIA) ;
- le responsable de traitement peut autant recourir à une méthode éprouvée (ex : guides PIA de la CNIL[21]) que mener cette réflexion de manière empirique ;
- les risques sur les données biométriques et données associées des personnes concernées doivent être pris en compte autant durant la collecte, la conservation et la transmission de ces données.

Pour ce faire, le tableau ci-dessous doit être renseigné :

---

17 Les dommages sur les personnes concernées peuvent être corporels, matériels ou moraux.

18 L'échelle suivante peut être utilisée pour estimer la gravité des risques :

1. *Négligeable : les personnes concernées ne seraient pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteraient sans difficulté.*
2. *Limitée : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés.*
3. *Importante : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés.*
4. *Maximale : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.*

19 Voir notamment l'annexe « Menaces génériques » du guide de la CNIL

20 L'échelle suivante peut être utilisée pour estimer la vraisemblance des risques :

1. *Négligeable : le risque ne devrait pas se (re)produire.*
2. *Limitée : le risque pourrait se (re)produire.*
3. *Importante : le risque devrait se (re)produire un jour ou l'autre.*
4. *Maximale : le risque devrait certainement se (re)produire prochainement.*

21 Guides « étude d'impact sur la vie privée » (http://www.cnil.fr/linstitution/actualite/article/article/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil/).

Risques	Impacts potentiels résiduels	Gravité résiduelle	Principales menaces résiduelles	Vraisemblance résiduelle
Accès non autorisé aux données biométriques	Cliquez ici pour taper du texte.	Choisissez un élément.	Cliquez ici pour taper du texte.	Choisissez un élément.
Modification non désirée des données biométriques	Cliquez ici pour taper du texte.	Choisissez un élément.	Cliquez ici pour taper du texte.	Choisissez un élément.
Disparition des données biométriques	Cliquez ici pour taper du texte.	Choisissez un élément.	Cliquez ici pour taper du texte.	Choisissez un élément.

La CNIL vérifiera les réponses apportées par le responsable de traitement, et notamment que les impacts envisagés sont bien des impacts sur la vie privée des personnes concernées, et non des impacts sur l'organisme, et que la gravité et la vraisemblance ne sont pas sous-estimées.

L'exemple fictif suivant illustre l'utilisation du tableau précédent :

Dans le contexte d'élévation du niveau de sécurité pour un accès à une zone sensible au sein d'un organisme bancaire, la mise en place d'un dispositif biométrique de contrôle d'accès physique est présentée comme une réponse adéquate. Cet accès est limité à un nombre connu d'employés habilités. Le dispositif proposé doit répondre à plusieurs contraintes notamment un haut degré de fiabilité écartant le risque de fausse acceptation et une grande rapidité d'exécution n'entravant pas la fluidité des passages.

De nombreux agents habilités se déplacent entre différents sites. Dans le cas de l'usage d'un support individuel, les problèmes de perte ou de vol restent similaires à ceux rencontrés avec le dispositif classique par badge concernant la disponibilité de l'accès. Pour cette raison et afin d'assurer l'accès aux locaux aux personnes habilitées mêmes en l'absence de leur badge, une solution de conservation des données biométriques en base centrale est préférée.

Risques	Impacts potentiels résiduels	Gravité résiduelle	Principales menaces résiduelles	Vraisemblance résiduelle
Accès non autorisé aux données biométriques	Utilisation des données pour incriminer une personne (attaque ciblée contre elle ou pour détourner les soupçons des forces de l'ordre). Ré-identification d'une personne pour un délit ou un crime (par des services de renseignement, la police, etc.). Perte de la confiance de l'authentification / identification du fait que des données biométriques ont été compromises.	3. Importante	Observation de données interprétables sur un écran, vol d'un terminal (ex : ordinateur portable) permettant d'accéder aux données, utilisation de fonctionnalités d'administration avancées, contagion par un code malveillant lors d'une configuration par les développeurs ou les mainteneurs, interception de flux sur le réseau interne ou externe permettant d'observer des données interprétables.	2. Limitée
Modification non désirée des données biométriques	Usurpation d'identité sans qu'elle puisse facilement le démontrer et ses conséquences (ex : licenciement pour faute grave, poursuites pour avoir compromis des secrets de l'entreprise, vol, etc.). Dans le cas d'une base centralisée, mauvaise identification de la personne pouvant entrainer des conséquences diverses liées à la nature de la base (limitée pour un lieu de travail où une pièce d'identité pourra facilement démontrer l'erreur).	2. Limitée	Modifications inopportunes dans une base de données, utilisation de fonctionnalités d'administration avancées.	2. Limitée
Disparition des données biométriques	Service ou lieu inaccessible. Obligation de la personne à procéder à un nouvel enrôlement. La gravité est limitée car la disparition sera détectée rapidement.	2. Limitée	Surexploitation des capacités de traitement, panne de courant, dysfonctionnement d'un dispositif de stockage entraînant un effacement, erreur de manipulation menant à la suppression de données, effacement d'un exécutable en production ou de code sources, arrêt des mises à jour de maintenance de sécurité par l'éditeur.	2. Limitée