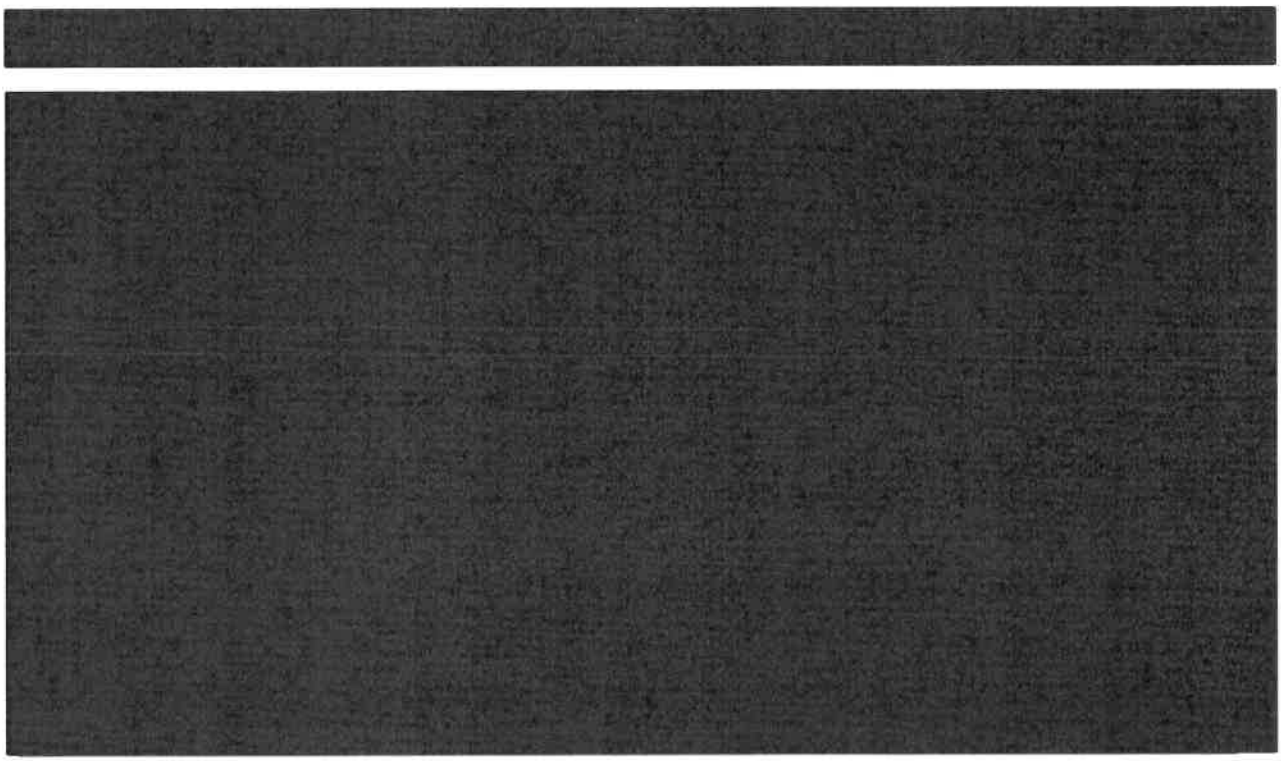
Appli carte Vitale V7 : Analyse d'Impact sur la Protection des Données

Version : 0.3 / Date 10/10/2025
Rédigé par : **GIE SESAM-Vitale** / Approuvé par : **Cnam / CCMSA**
Sécurité : **DIFFUSION RESTREINTE**

GIE SESAM-Vitale
5, boulevard Marie et Alexandre Oyon – 72019 LE MANS Cedex 2
www.sesam-vitale.fr

NB : ne pas effacer cette page. Cette page est masquée, elle ne sera pas imprimée.

[redacted]



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Historique des versions

Date	Version	Évolution du document	Rédacteur
04/09/2025	0.1	Version initiale de l'AIPD relative à la version V7 de l'ApCV	GIE SESAM-Vitale
18/09/2025	0.2	Prise en compte des remarques suite à relecture interne équipe sécurité et DPO GIE SV	GIE SESAM-Vitale
10/10/2025	0.3	Prise en compte des remarques de la Cnam et du GIE SV	GIE SESAM-Vitale

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Tables des matières

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

1 INTRODUCTION

1.1 Concept d'application Carte Vitale

Depuis 2016, l'Assurance Maladie et le GIE SESAM Vitale travaillent sur le concept de l'application carte Vitale, la déclinaison smartphone de la carte Vitale que près de 60 millions d'assurés utilisent depuis 1998 pour s'identifier et faire valoir leurs droits chez un professionnel de santé.

Cette application mobile, ou ApCV, a pour vocation d'offrir les mêmes services que son ainée plastique (facturation SESAM Vitale, accès par les professionnels de santé aux téléservices des régimes obligatoires et complémentaires, au DMP ou au dossier pharmaceutique...).

Elle va aussi proposer des nouveaux services, orientés assurés, comme une clé d'accès aux portails de santé (ex : Mon Espace Santé) ou la possibilité d'en déléguer son usage auprès d'un tiers.

Après une phase d'expérimentation terrain commencée en octobre 2019 et limitée aux caisses Régime Général et MSA du Rhône et des Alpes maritimes, un pilote a été lancé en juin 2023 associant les assurés de ces régimes ainsi que de la MGEN dans 8 premiers départements.

L'application carte Vitale est maintenant déployée avec un parcours d'activation CNIe-France Identité sur tout le territoire Français et la généralisation parcours d'activation PVID (Prestataire de Vérification d'Identité à Distance) devrait être finalisée en fin d'année 2025.

Le parcours d'activation dérivé de la CNIe et de France Identité est le parcours préférentiel d'activation de l'appli carte Vitale pour la population éligible (cf. décret de généralisation de l'appli carte vitale).

Ce parcours favorise le déploiement et l'activation des deux applications France Identité et appli carte Vitale en cohérence avec la stratégie de l'état sur les identités numériques. Pour les détenteurs d'une CNIe, il s'agit d'inciter les assurés à s'enrôler avec l'application FIN (France Identité Numérique) au début du parcours d'enrôlement appli carte Vitale (avec détection automatique de l'application FIN ou redirection pour le téléchargement et l'activation de l'application FIN).

Plan de déploiement 2025 appli carte Vitale :

- La généralisation France entière du parcours d'activation de l'appli carte vitale avec FIN / CNIe a été réalisée au 1er trimestre 2025.
- Le parcours avec PVID est étendu progressivement par régions sur l'année 2025 et réservé aux cas non couverts par FIN (mineurs 16 / 18 ans, assurés ayant une autre pièce d'identité). La généralisation est prévue en 3 vagues :
    - Mai 2025 : +4 régions +7 millions d'utilisateurs éligibles ;
    - Juillet 2025 : +2 régions +3,9 millions d'utilisateurs éligibles ;
    - Nov. 2025 : +6 régions (dont Île-de-France) +21,8 millions d'utilisateurs éligibles.

A fin 2025, la volumétrie cible d'utilisateurs équipés d'une ApCV est de 2,3 millions.

A la suite, le programme permettra d'améliorer certains services déployés au premier rang desquels l'usage dans les établissements.

L'Assurance Maladie et le Ministère chargé de la Santé souhaitent aussi dès ces premières étapes que l'ApCV puisse être utilisée par l'assuré pour accéder à son Espace de Santé soit via un bouton spécifique soit via FranceConnect.

Le présent document porte sur le système ApCV dans son ensemble (infrastructure, application mobile et services) tel qu'il a été mis en œuvre sur le terrain entre fin 2025 et début 2026 (version V7).

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

1.2 Objet du document

Ce document constitue l'Analyse d'Impact relative à la Protection des Données (AIPD) de la version V7 de l'appli carte Vitale (ApCV).

Il sera mis à jour à chaque évolution importante de l'appli carte Vitale, afin notamment de prendre en compte les nouveaux usages et l'évolution du nombre d'utilisateurs éligibles.

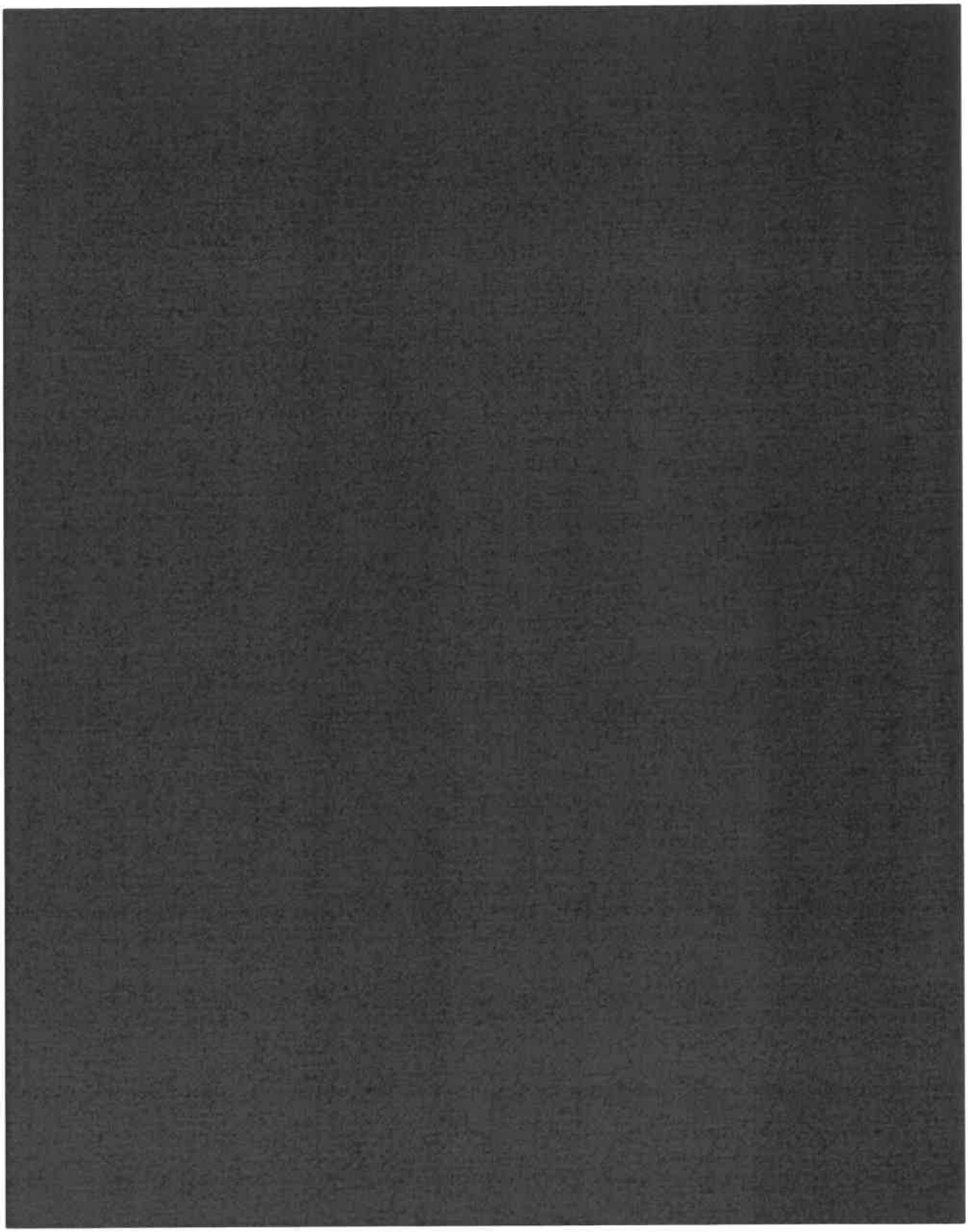
Il est organisé de la manière suivante :

- En introduction, la démarche ainsi que les principales différences avec l'AIPD V5 du 10/03/2025 ;
- Le contexte : concept d'appli carte Vitale, cycle de vie de l'utilisation de l'application mobile, les acteurs, les systèmes, les traitements et la synthèse des données traitées ;
- La démarche de l'analyse de risques ;
- L'étude des principes fondamentaux communs aux différents processus ;
- Les mesures de sécurité appliquées à l'application mobile (appli carte Vitale ou ApCV), au SI ApCV et au SI Sécurité, et les risques associés (risques pour les personnes mais également pour l'Assurance Maladie) ;
- Les processus liés au cycle de vie du dispositif ApCV, les processus services aux Professionnels de Santé et aux Etablissements de Santé, les processus services aux Assurés et les processus transverses. Pour chaque processus, l'AIPD décrit :
  - Le processus,
  - Le circuit de la donnée,
  - Les mesures permettant de garantir le respect des principes fondamentaux de minimisation, exactitude et durée de conservation des données traitées,
  - Les mesures de sécurité,
  - Les risques (risques initiaux, plan d'action et risques résiduels) ;
- La vision consolidée des risques permettant d'identifier les scénarios de risques sur la vie privée transverses aux différents processus ;
- Le plan d'action ;
- La validation de l'AIPD via l'évaluation par les responsables de traitements des mesures liées au respect des principes fondamentaux et des risques d'atteinte à la vie privée.

1.3 [redacted]

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

1.4 Terminologie

Définitions

Terme	Définition
Ouvrant droit (ou assuré)	Personne dont la situation ouvre des droits à l'Assurance Maladie (condition de travail ou condition de résidence).
Ayant droit	Personne rattachée à l'Ouvrant droit et bénéficiant du fait de ce rattachement des services de l'Assurance Maladie.
Bénéficiaires	Ensemble des ayants droit et de l'ouvrant droit
Actif primaire (ou bien essentiel)	Un actif primaire (ou bien essentiel) est décrit comme un élément du système cible ayant besoin d'être protégé (information ou fonction). Il doit être valorisé de telle sorte que les impacts occasionnés et les dommages effectifs sur la réalisation des objectifs puissent être identifiés.
Actif en support (ou bien support)	Actif (ou bien) sur lequel reposent les actifs primordiaux (matériel, logiciel, réseau, personnel, site géographique ou organisation).
Caisse	Equivalent à un organisme d'Assurance Maladie obligatoire ayant en gestion les bénéficiaires.
Organisme gestionnaire	Cf. Caisse.
Utilisateur	Bénéficiaire de l'Assurance Maladie en possession d'un smartphone sur lequel est installée une ApCV.

Tableau 1 : Définitions

Acronymes et sigles

Terme	Désignation
AD	Ayant Droit
AIPD	Analyse d'Impact relative à la Protection des Données
AM	Assurance Maladie (AMO et AMC)
AMO / AMC	Assurance Maladie Obligatoire / Complémentaire
ApCV	Appli carte Vitale
CAN	Card Access Number (code à 6 chiffres en bas à droite de la face avant de la CNIe)
CCMSA	Caisse Centrale de la MSA

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Terme	Désignation
[redacted]	
Cnam	Caisse Nationale d'Assurance Maladie
CNDA	Centre National de Dépôt et d'Agrément
CNI	Carte nationale d'identité
CNIe	Carte nationale d'identité électronique
CNIL	Commission Nationale Informatique et Liberté
CPS	Carte du Professionnel de Santé
CTI	Centre de Traitement Informatique des régimes d'Assurance Maladie
DCP	Données à Caractère Personnel
[redacted]	
DMT	Datamart
DP	Dossier Pharmaceutique
DPD	Délégué à la Protection des Données
DPO	Data Protection Officer
DRE	Demande de Remboursement Électronique
DWH	Datawarehouse
ENS	Espace numérique de santé
ETL	Extraction, Transformation, Loading
ES	Etablissement de Santé
FI	Fournisseur d'Identités
FS	Fournisseur de Services
FS-PS	Fournisseur de Service PS
FSE	Feuille de Soin Electronique
FSV	Fournitures SESAM-Vitale
GIE SV	Groupement d'Intérêt Economique SESAM-Vitale
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
[redacted]	
IAS	Identification, Authentication and Signature
IHM	Interface Homme-Machine
IR	Inter-Régimes

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Terme	Désignation
IVI	Industriel de Vérification d'Identité
[redacted]	
LPS	Logiciel du Professionnel de santé (logiciels spécifiques destinés à aider la pratique médicale)
MES	Mon Espace Santé
MIE	Moyen d'Identification Electronique
MSA	Mutualité Sociale Agricole
NFC	Near Field Communication
NIR	Numéro d'inscription au Répertoire national d'identification des personnes physiques (communément appelé numéro de sécurité sociale)
OD	Ouvrant droit
OIDC	OpenId Connect
[redacted]	
PCA	Plan de Continuité d'Activité
PS	Professionnel de Santé
PSSI	Politique de Sécurité des Systèmes d'Information
PPS	Poste de travail du Professionnel de Santé
[redacted]	
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RPCA	Responsable du Plan de Continuité d'Activité
SDK	Software Development Kit (kit de développement logiciel)
SGBD	Système de Gestion de Bases de Données
SI	Système d'Information
SID	Système d'Information Décisionnel
SOC	Security Operations Center
[redacted]	
SV	SESAM-Vitale
TLS	Transport Layer Security

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Terme	Désignation
[redacted]	
TEE	Trusted Execution Environnement

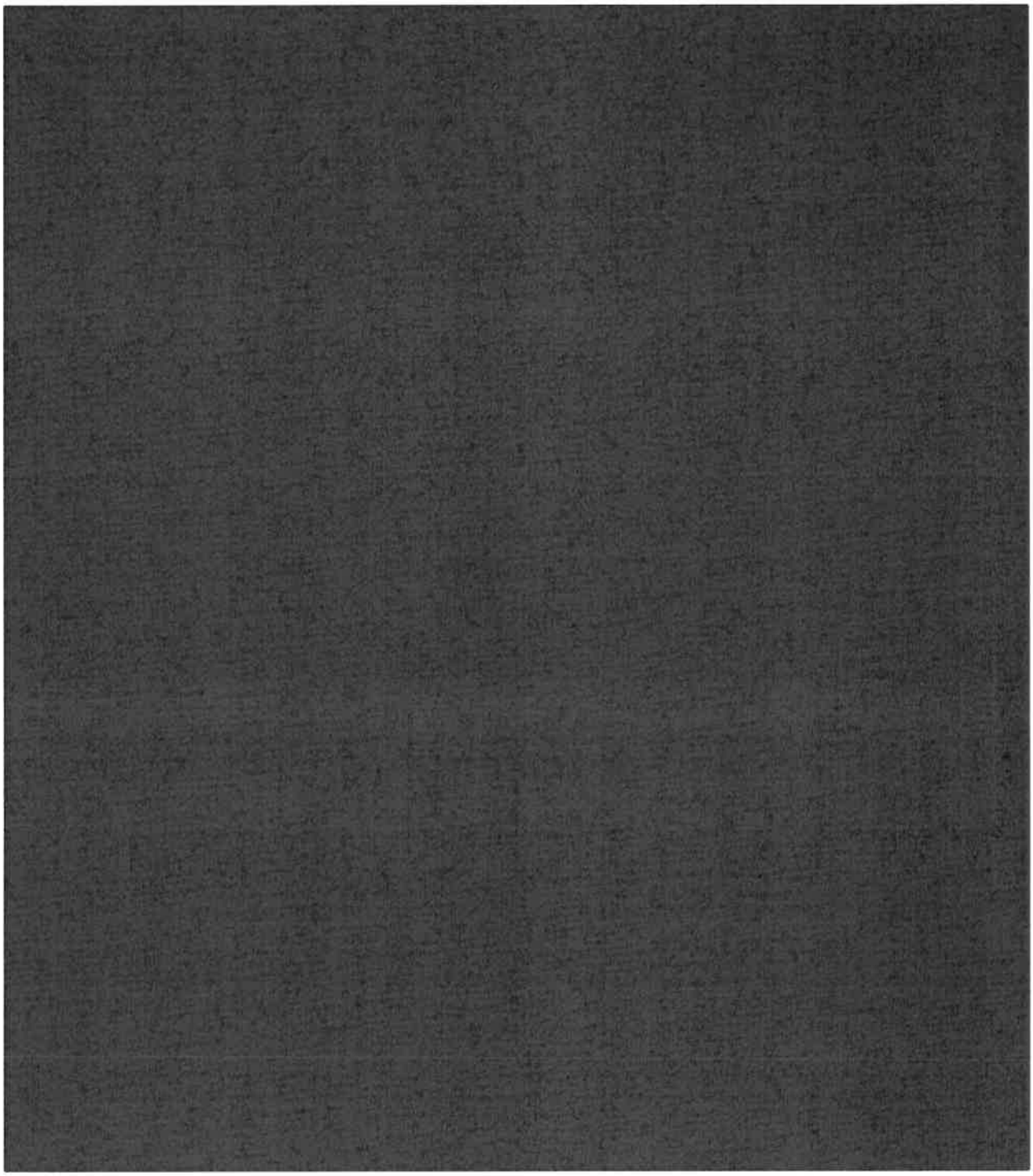
Tableau 2 : Acronymes et sigles

1.5 [redacted]

1.5.1 [redacted]

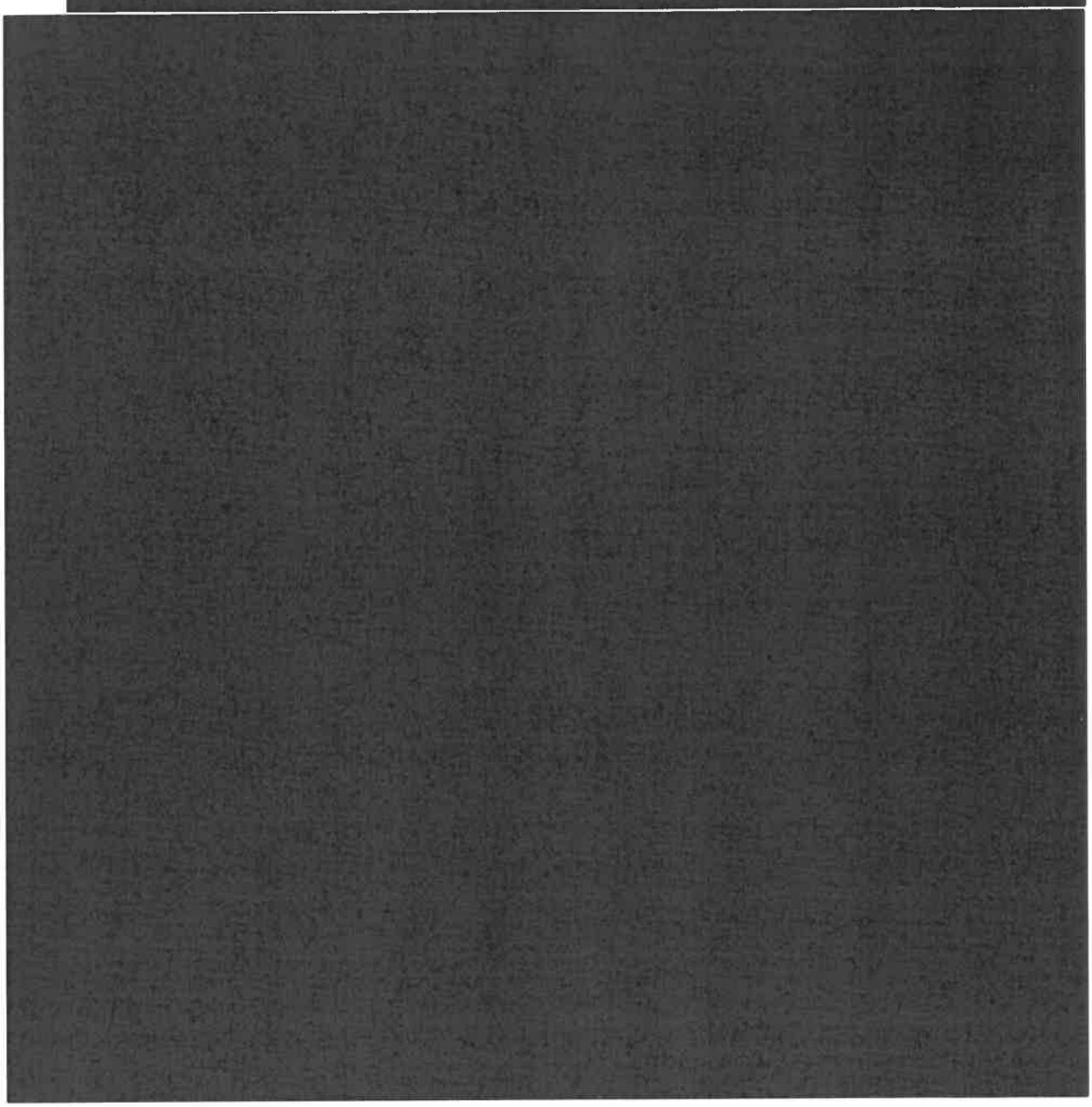
1.5.2 [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

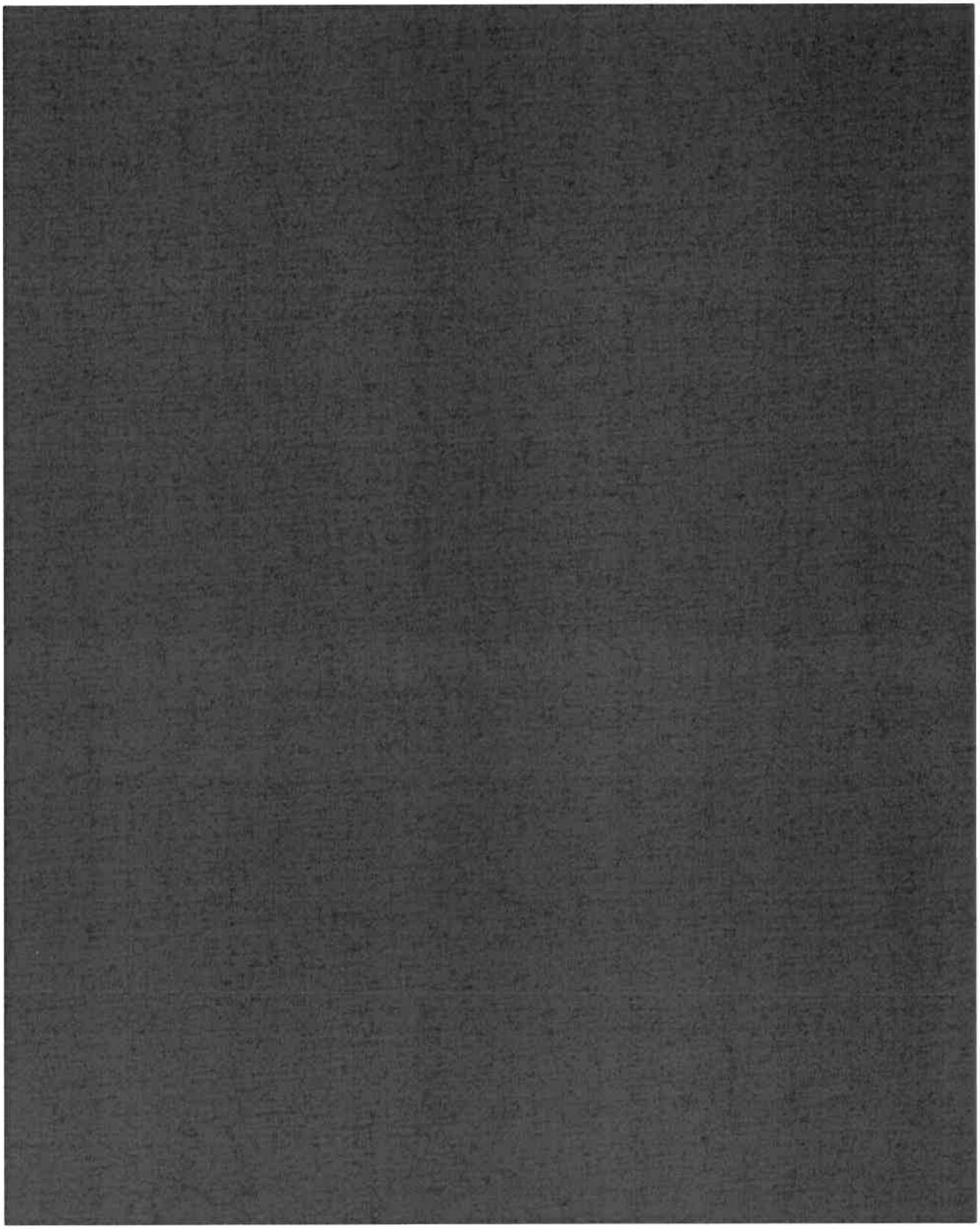


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

1.5.3



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

2 PRESENTATION DU CONTEXTE

2.1 Cycle de vie de l'utilisation de l'appli carte Vitale

Les assurés téléchargent l'appli carte Vitale sur leur smartphone iOS ou Android depuis les stores officiels App Store et Google Play.

Une activation est ensuite nécessaire pour :

[redacted]

- Fournir les données nécessaires au fonctionnement de l'ApCV ;
  - Les différentes identités (civiles, AMO, patient) de l'assuré et des ayants droit ;
  - Organisme gestionnaire de l'assuré et des ayants droit ;
  - Données techniques et cryptographiques.

Une fois l'ApCV activée, l'assuré peut l'utiliser :

- En proximité, dans le cadre d'une consultation chez un PS :

[redacted]

  - L'ApCV intervient ensuite pour sécuriser l'accès aux téléservices intégrés (TLSi), la facturation SESAM-Vitale (FSE/DRE) et l'accès aux services Web DMP PS et amelipro.
- A distance (dans des versions ultérieures, hors périmètre du présent document) :
  - Pour accéder aux services de l'Assurance Maladie comme Mon Espace Santé (MES) ;
  - Pour accéder aux services autorisés conformément à la procédure figurant à l'article Art. R 161-33-15 du code de la sécurité sociale modifié par le Décret n°2022-1719 du 28 décembre 2022 ;
  - Comme fournisseur d'identité sur FranceConnect, de niveau eIDAS faible dans un premier temps et de niveau eIDAS substantiel en cible.

2.2 Présentation des acteurs

Utilisateur

Il s'agit de l'utilisateur de l'appli carte Vitale.

Professionnel de Santé (PS)

Le Professionnel de Santé facture, accède aux téléservices (TLSi) et aux services (amelipro, WebDMP PS) de l'Assurance Maladie grâce aux données d'identification portées par l'ApCV.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

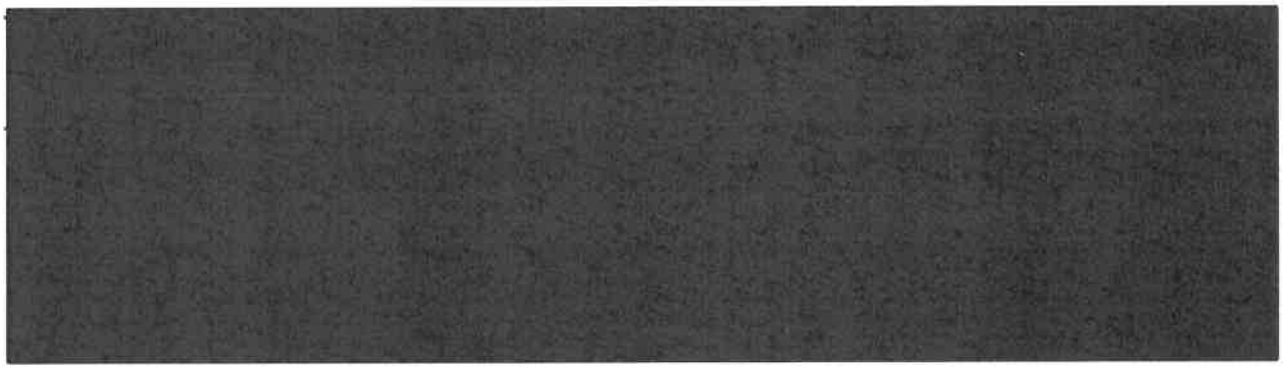
Organismes d'Assurance Maladie obligatoires

Les AMO (Cnam, CCMSA et régimes ayant une délégation de gestion du régime obligatoire) mettent à disposition de leurs assurés l'application mobile carte Vitale. Elles prennent en charge la gestion de la relation avec les assurés (support niveaux 1 et 2) :

- Exercice des droits des assurés : réception des demandes, traitement et retours vers les assurés ;
- Support : grâce au portail de gestion du support mis à disposition par le GIE SV, elles peuvent suivre la délivrance de l'ApCV aux assurés, bloquer un utilisateur dans le cadre de la lutte contre la fraude et procéder à la révocation d'une ApCV en cas de perte ou de vol de smartphone déclaré par l'assuré ;
- Information des personnes via les mentions d'information sur les sites institutionnels ;
- Gestion des violations de données et notification à la CNIL ;
- Organisation de l'Homologation RGS de leurs services.

Inter-régime

Le système Inter-régime (opéré par la Cnam) met à disposition des services métier inter-régimes permettant de vérifier l'éligibilité de l'utilisateur à la possession de l'ApCV et fournir les services permettant à l'ApCV d'acquérir les données d'identification.



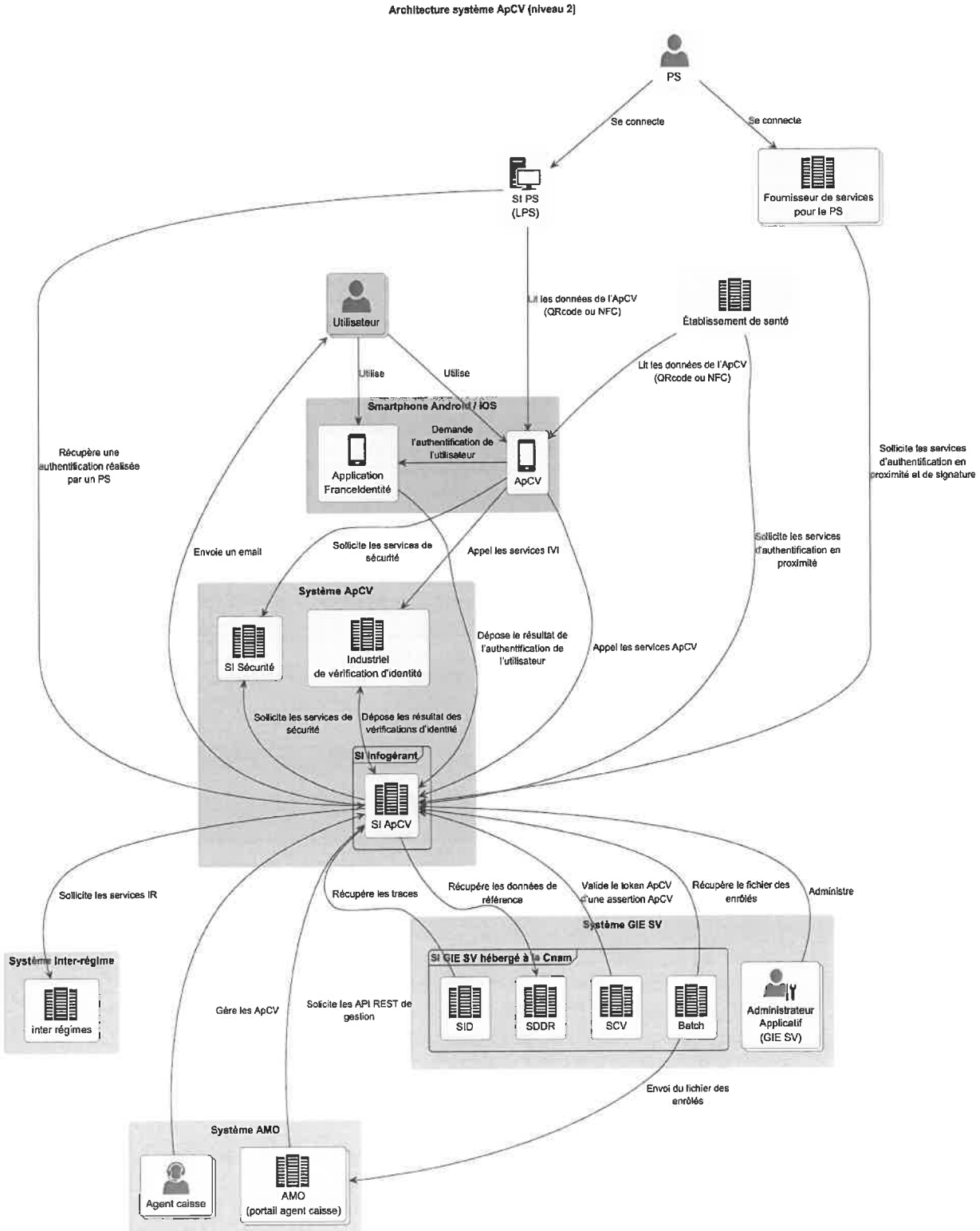
GIE SESAM-Vitale

Le GIE SV :

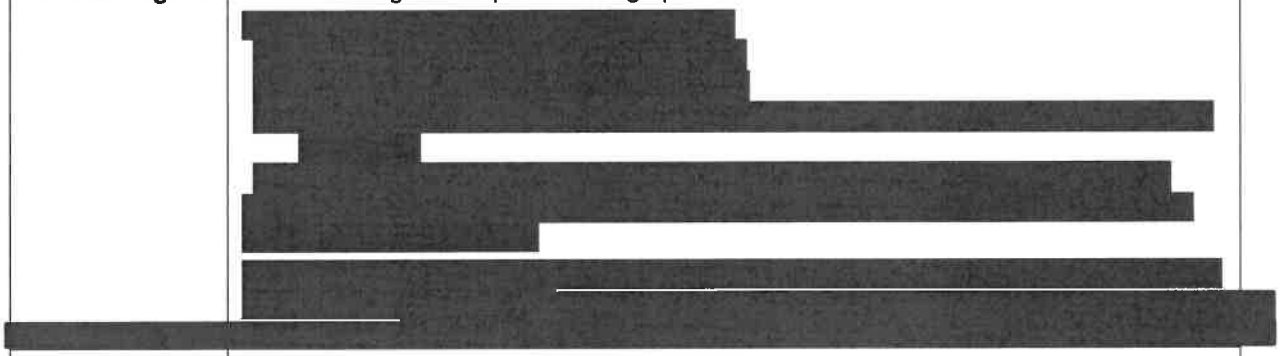
- Développe et publie pour le compte des AMO l'appli carte Vitale sur les stores Apple et Google ;
- Développe et met à disposition le portail de gestion du support aux AMO ;
- Conçoit, met en œuvre et exploite le SI ApCV au niveau applicatif ;
- Fournit le support de niveaux 2 et 3 ;
- Organise l'Homologation RGS sur le périmètre ApCV dont il a la charge ;
- Contribue par son expertise à la qualification de la violation de données, de son descriptif et des mesures associées.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

2.3 Présentation des systèmes



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Système	Description
SI AMO	Il s'agit du SI de chaque AMO. Chaque SI fournit trois services sollicités par les services Inter-régime : le service d'éligibilité, le service de rapprochement d'identités et le service de Famille de droits. Toutes les semaines, le SI ApCV envoie la liste des ApCV enrôlées à chaque SI AMO. L'agent Caisse accède au portail de gestion du support des ApCV offert par le SI ApCV. À terme, il pourra également se connecter à son portail Agent local qui sollicitera des web-services de gestion du support offerts par le SI ApCV (équivalent au portail de gestion du support).
SI ApCV	Il s'agit du système d'information de gestion des ApCV. Ce SI offre l'ensemble des services techniques nécessaires à l'ApCV, les services de gestion de support ApCV ainsi que les services d'administration et de supervision du SI. On y trouve la base technique des ApCV ainsi que la base des utilisateurs pseudonymisés. De manière temporaire, on y trouve également les données d'identification et d'authentification des bénéficiaires obtenues soit pour le SI PS soit pour un fournisseur de services (PS ou utilisateurs)
SID ApCV	Quotidiennement, le SID ApCV (Système d'Information Décisionnel) reçoit les données du SI ApCV et les stocke dans le datawarehouse avant de calculer les indicateurs statistiques dans les datamarts (DMT) décisionnels. En complément, un ELK à usage décisionnel est également mis en œuvre avec la V7 de l'ApCV pour permettre la réalisation de tableaux de bord supplémentaires.
SI du GIE SV	C'est à partir de ce SI que les postes de travail des administrateurs et des superviseurs applicatifs se connectent au SI ApCV. L'application DORIS (système de gestion des données des industriels) récupère la liste des produits agréés par le CNDA et les convertit en données de référence avant d'être envoyées au SI ApCV.
SI Inter-régime	Le SI Inter-régime est pris en charge par la Cnam. 
SI IVI	Le SI IVI est le système d'information de l'Industriel de Vérification d'Identité sollicité lors du processus d'activation d'un utilisateur. Cet industriel fournit un SDK inclus dans l'ApCV. Ce SDK offre des services locaux et appelle des services distants de l'industriel permettant ▪ d'authentifier une pièce d'identité, ▪ d'acquérir les données inscrites sur la pièce d'identité et ▪ de contrôler la cohérence entre la photo de la pièce d'identité et un selfie incluant une « preuve du vivant ». Ces services sont hébergés et opérés par l'industriel. L'industriel émet des traces de preuves à destination du SI ApCV.
SI PS	C'est le système d'information équipant le PS ou la structure de santé. Il s'interface avec le SI ApCV pour authentifier et identifier l'utilisateur d'une ApCV.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Système	Description
SI Sécurité	Le SI Sécurité est le système d'information fourni par [redacted]. Il porte les fonctions de sécurité en lien avec le SDK Sécurité intégré dans l'application mobile.
Smartphone	Il s'agit du smartphone de l'utilisateur. Dans le périmètre du SI ApCV, le smartphone contient l'ApCV, active la caméra pour l'activation et communique avec le SI IVI (activation uniquement dans le cadre du parcours d'activation IVI) et le SI ApCV et le SI Sécurité (pendant toute la durée de vie de l'app).

2.4 Présentation des processus

Le présent dossier **porte sur la version V7** de l'appli carte Vitale. Les processus suivants sont dans le périmètre :

- **Processus liés au dispositif ApCV :**
  - Activation de l'ApCV avec deux parcours disponibles (parcours IVI et parcours France Identité) ;
  - Gestion de l'appli carte Vitale par les AMO : suivi de la délivrance, blocage/déblocage d'un utilisateur dans le cadre de la gestion de la fraude et révocation de l'appli carte Vitale en cas de perte / vol.
- **Processus services aux PS :**
  - Authentification de proximité ;
  - Accès aux téléservices (TLSi) ;
  - Facturation SESAM-Vitale.
- **Processus services aux Assurés :**
  - Consultation des résumés de facture ;
  - Changement d'adresse mail.
- **Processus services aux ES :**
  - Authentification ApCV avec et sans CPx.
- **Processus transverses :**
  - Décisionnel et informationnel.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

2.5 Synthèse des données à caractère personnel traitées dans les différents processus

2.5.1 Définitions

Nom	Description
Système mobile	Représente le support physique sur lequel est installé l'ApCV : un smartphone ou une tablette.
[redacted]	
Identifiant ApCV	Identifie de manière unique une application installée sur un smartphone. Il est généré à la 1ère activation et ne change pas jusqu'à ce que l'utilisateur désinstalle l'application.
Identifiant profil ApCV	Identifie de manière unique un profil. Il est généré à chaque début d'enrôlement d'un utilisateur.
N° de série	C'est l'équivalent du n° de série de la carte Vitale pour permettre une traçabilité au niveau des factures émises. Il est attribué pour chaque profil au sein de la plage des numéros de série carte Vitale réservée pour l'ApCV, une fois l'activation validée.
UserID	Il s'agit de l'identifiant de l'utilisateur dans le SI [redacted]. Le UserID est généré par le SI [redacted] et fourni au SI ApCV lors de l'activation d'une ApCV dans le SI Sécurité.

2.5.2 Données dans l'appli carte Vitale

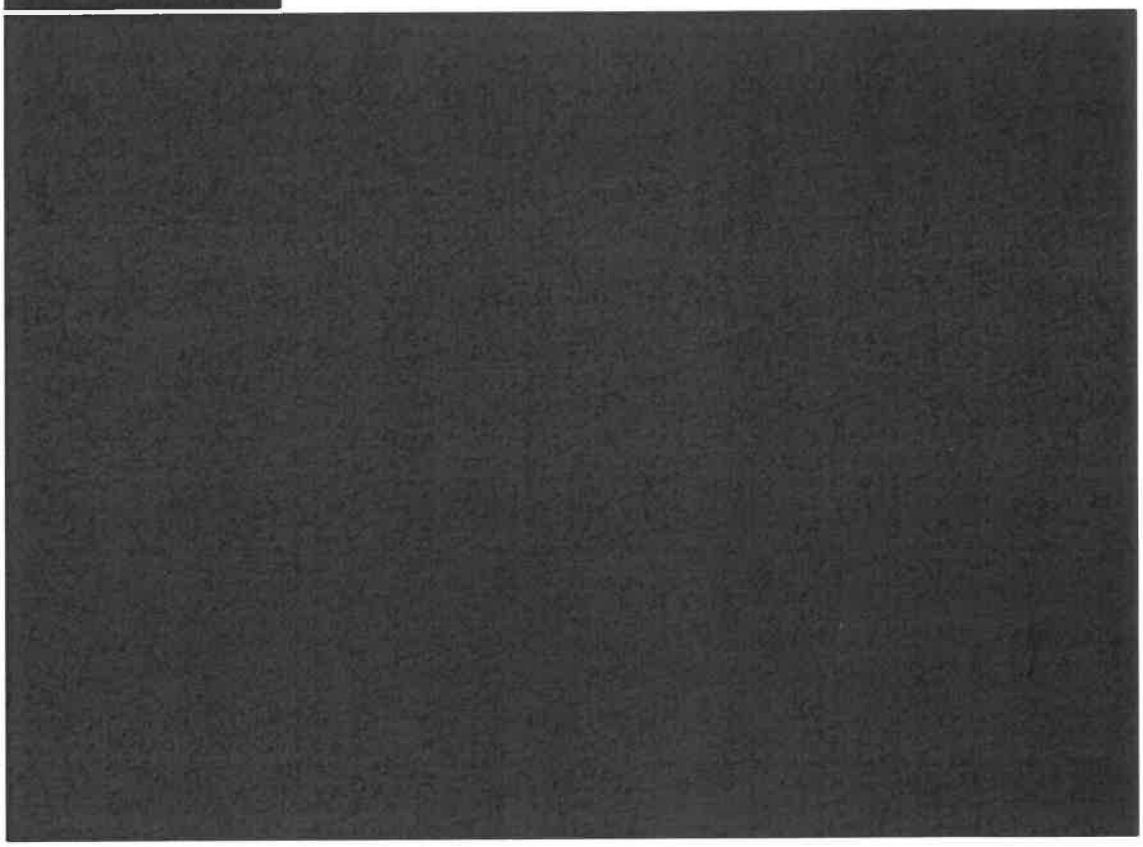
Dans l'ApCV, les données et fonctionnalités sont réparties en deux catégories :

- Les données et fonctionnalités de **catégorie 1** sont protégées par un mot de passe vérifié localement à l'ouverture de l'application. Elles sont disponibles avec ou sans connexion réseau.

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Le schéma ci-dessous présente la structure d'une appli carte Vitale stockée sur le smartphone.
Le SDK Sécurité fourni par [redacted] dispose de deux stockages sécurisés [redacted]



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

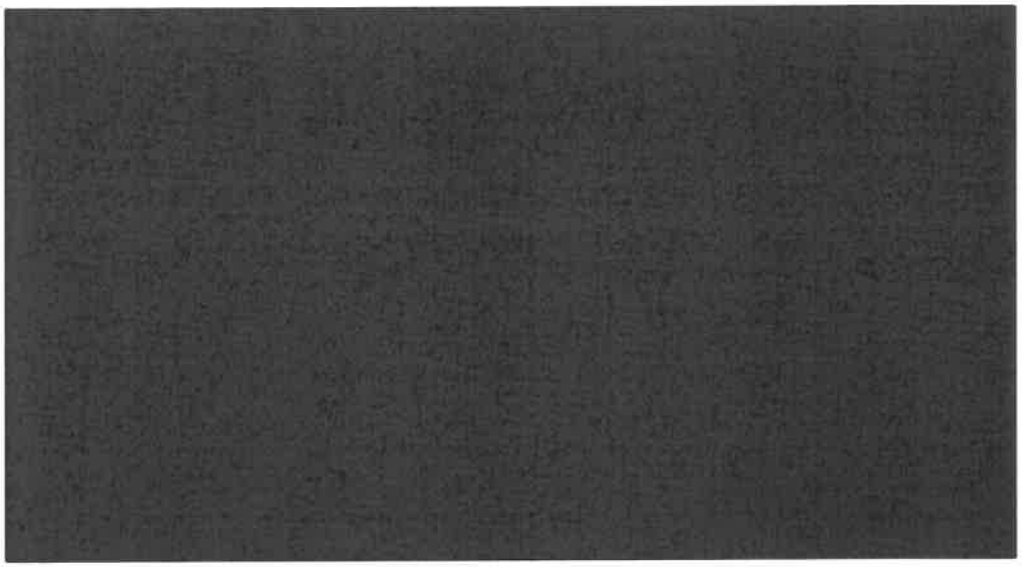
Le tableau ci-dessous recense les documents stockés [redacted]

Document	Détail des données
Document EC (Etat Civil)	**Identité Etat civil de l'utilisateur de l'appli carte Vitale :** Prénoms Nom de famille Nom d'usage Date de naissance Genre Code INSEE de la ville de naissance (si né en France) Code INSEE du pays de naissance (si né hors de France)
Document AMO-INS	**Identité AMO de chaque bénéficiaire :** NIR Nom de famille Nom d'usage Prénom Date de naissance Rang de naissance Qualité du bénéficiaire **Contrat AMO de chaque bénéficiaire :** NIR Nom de l'assuré Prénom de l'assuré Code Régime Code Caisse Code Centre *Note : l'ApCV ne contient pas de données relatives aux droits des bénéficiaires,* [redacted] **Identité Patient de chaque bénéficiaire :** Matricule INS Date de naissance Lieu de naissance Nom de naissance Prénoms de naissance Sexe
Document PHOTO	Photo de l'utilisateur restituée par l'Industriel de Vérification d'Identité ou France Identité selon le parcours d'activation
Document COORD	Adresse e-mail de l'utilisateur de l'ApCV (connue du Régime ou fournie par France Identité selon le processus d'activation)
Messages de type Résumés de facture	Identifiant national, prénom et nom PS Identifiant facturation PS Identité du bénéficiaire (NIR, prénom et nom) Date et montant de la facture (montant total et montant payé par l'assuré) Organisme(s) d'Assurance Maladie destinataires de la (ou des) facture(s) : AMO (code régime, code caisse, code centre) et AMC

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

2.5.3 Données dans le SI ApCV

Le schéma ci-dessous présente la structure d'une l'appli carte Vitale stockée dans le SI ApCV :



Le tableau ci-dessous décrit les données stockées dans le SI ApCV :

Données	Détail des données
Données métier ApCV	Identifiant ApCV Identifiant profil ApCV N° de série NIR pseudonymisé
Résumés de facture (stockage temporaire, cf. processus facturation)	Identifiant national, prénom et nom PS Identifiant facturation PS Identité du bénéficiaire (NIR, prénom et nom) Date et montant de la facture (montant total et montant payé par l'assuré) Organisme(s) d'Assurance Maladie destinataires de la (ou des) facture(s) : AMO (code régime, code caisse, code centre) et AMC Code acte des prestations (lettre clé) – Note : cette donnée est reçue dans la facture transmise au SI ApCV mais n'est pas conservée par le SI ApCV ni présente dans le résumé de facture descendu sur l'appli carte Vitale (mesure de minimisation).
Fichier des enrôlés (stockage temporaire, cf. processus activation)	NIR Identifiant profil ApCV Code Régime Code Caisse Code Centre Date de l'activation

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Données temporaires d'activation (stockage temporaire, détruites une fois l'activation finalisée)	NIR Adresse e-mail (connue du Régime ou fournie par France Identité selon le processus d'activation) Identité Etat civil (traits d'identité restitués par l'IVI ou identité fournie par France Identité selon le processus d'activation) Photo de l'utilisateur (selfie ou photo fournie par France identité selon le processus d'activation)
Traces de fonctionnement (cf. §5.2.1.4)	[redacted] Identifiant ApCV Identifiant profil ApCV NIR pseudonymisé Identifiant national PS Identifiant facturation PS (numéro Assurance Maladie) Adresse IP du smartphone
Traces fonctionnelles de sécurité du portail de gestion du support (cf. §5.2.1.4)	Identifiant profil ApCV Identifiant pseudonymisé agent Caisse
Traces fonctionnelles de sécurité des IHM d'administration fonctionnelle (cf. §5.2.1.4)	Identifiant administrateur fonctionnel
Traces contractuelles INTEROPS (cf. §5.2.1.4)	Identifiant pseudonymisé agent Caisse Identifiant profil ApCV

2.5.4 Données dans le SI Sécurité

Le tableau ci-dessous décrit les données stockées dans le SI Sécurité :

Données	Détail des données
Données métier	Documents et messages (cf. contenu décrit au §2.5.2) : - Document EC - Document AMO-INS - Document PHOTO - Document COORD - Messages de type Résumé de facture Les documents et messages sont stockés temporairement dans le SI Sécurité le temps que le SDK récupère les données : les données non récupérées par le SDK dans un délai de 7 jours sont automatiquement supprimées.
Données techniques	[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Caractéristiques techniques du smartphone de l'utilisateur	Marque et modèle Plateforme (Android/iOS) et version de l'OS Langue et Timezone Caractéristiques techniques : - NFC (true/false) - BLE (true/false) [redacted] - Type de biométrie disponible (visage, iris, empreinte digitale) - Force du dispositive biométrique (strong/weak)

2.5.5 Données dans le SI IVI (phase d'activation)

Le tableau ci-dessous décrit les données stockées dans le SI IVI :

Données	Détail des données
Flux vidéo	Données capturées à l'aide de la caméra du smartphone : - Vidéo du titre d'identité - Vidéo du visage de l'utilisateur
Données biométriques	Données utilisées lors du traitement biométrique de la photographie issue du titre d'identité de l'utilisateur et de la vue de son visage - Vidéo du titre d'identité - Vidéo du visage de l'utilisateur - Gabarits biométriques
Dossier de preuve	Données conservées dans le dossier de preuve : - Vidéo du titre d'identité - Vidéo du visage de l'utilisateur - Noms et prénoms de l'utilisateur - Date et lieu de naissance - Numéro du titre d'identité - Date de délivrance du titre d'identité - Date d'expiration du titre d'identité

2.5.6 Données dans le SID ApCV (SI Décisionnel)

Le tableau ci-dessous décrit les données stockées dans le SID ApCV :

Données	Détail des données
Données issues des traces de fonctionnement et importées dans le SID	**SID lot 1 (données présentes pour la V7 de l'appli carte Vitale) :** Identifiant ApCV Identifiant profil ApCV Contrat AMO (code régime, caisse, centre) [redacted] **SID lot 2 (données présentes pour la V7 de l'appli carte Vitale) : données du lot 1 +** Smartphone (fabricant, modèle, OS et version) Année de naissance

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

3 PRESENTATION DE LA DEMARCHE D'ANALYSE DE RISQUES

3.1 Démarche d'analyse de risques

La méthodologie respecte la démarche proposée par la norme ISO 27005 décrite ci-dessous :

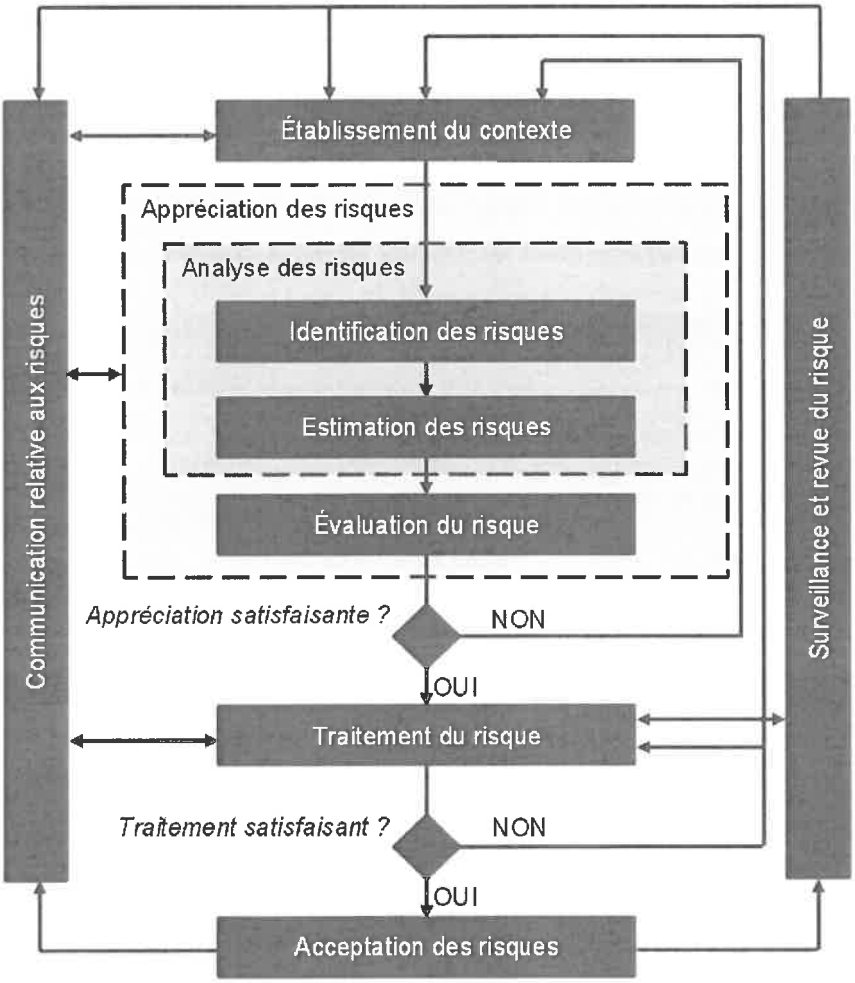


Figure 1 : Processus de gestion des risques

L'analyse de risque sera agrémentée par les référentiels identifiés ci-après dont la base des menaces de la méthodologie EBIOS 2010. Ainsi, les principaux objectifs visés sont les suivants :

- **Établissement du contexte**
- **L'appréciation des risques**
- **Le traitement des risques**
- **Le suivi et la réévaluation des risques**

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

3.2 Démarche d'analyse d'impact relative à la protection des données

Conformément à l'esprit du RGPD, l'ensemble des risques sur la vie privée résiduels (ceux non couverts par les mesures de sécurité retenues) est présenté, étant entendu que les responsables de traitements s'engagent à appliquer les mesures prévues et détaillées dans le présent document.

Pour les cas les plus courants d'impacts sur la vie privée, la méthode d'évaluation du niveau d'impact sur la vie privée est décrite ci-dessous.

Niveau d'impact sur la vie privée en cas d'indisponibilité du service et donc des données à caractère personnel

En cas d'indisponibilité de l'appli carte Vitale, les utilisateurs pourront toujours :

- Pour les opérations en proximité PS, utiliser leur carte Vitale ;
- Pour l'authentification à distance FranceConnect, se connecter via un autre fournisseur d'identité ;
- Pour l'authentification aux services en ligne des acteurs de la sphère santé sociale (ex : Mon Espace Santé), se connecter en utilisant les modes d'authentification existants.

Le niveau d'impact est évalué à **négligeable (1)** : les personnes concernées pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté, comme par exemple une perte de temps.

Niveau d'impact sur la vie privée en cas de violation de l'intégrité ou de la confidentialité des données à caractère personnel

Le niveau d'impact dépend de la catégorie des DCP concernées :

- Pour les **DCP courantes** (données d'identité), le niveau d'impact est évalué à **négligeable (1)** : les personnes concernées pourraient connaître quelques désagréments qu'elles surmonteront sans difficulté, par exemple la réception de courriers non sollicités ou publicités ciblées ;
- Pour les **données sensibles** (données de santé, données biométriques) ou **perçues comme sensibles** (NIR, INS) lorsqu'elles sont associées à des données permettant d'identifier des personnes ou des usages, le niveau d'impact est évalué à **important (3)** : la divulgation de données de santé pourrait à l'extrême entrainer une perte d'emploi ;
- Pour les **données perçues comme sensibles** (NIR, INS) lorsqu'elles ne sont pas associées à des données permettant d'identifier les personnes, le niveau d'impact est évalué à **négligeable (1)**.

A noter que les vols de données considérés dans le cadre de la présente AIPD peuvent concerner à la fois :

- **Les données traitées directement par l'appli carte Vitale**: il s'agit des données stockées dans l'appli carte Vitale sur le smartphone de l'assuré (ex : données d'identité), dans le SI AMO (ex : droits de l'assuré), dans le SI IVI (ex : données biométriques d'activation) ou le SI ApCV (ex : résumés de factures) ;
- **Les données auxquelles l'assuré accède grâce à l'appli carte Vitale**: il s'agit des données hébergées par les services auxquels l'appli carte Vitale permet d'accéder via une authentification à distance (ex : consultation de Mon Espace Santé ou accès à tout service hors du périmètre de l'Assurance Maladie). A noter que ces services ne sont pas disponibles dans la V7 de l'appli carte Vitale objet de la présente version de l'AIPD.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Est considérée comme donnée de santé toute donnée qui permet de reconstituer le parcours de soin d'un assuré, par exemple : résumés de factures (note : même si les résumés de facture ne contiennent ni le code acte, ni la spécialité du PS, l'identifiant et le nom du PS permettent d'identifier sa spécialité, ce qui constitue une donnée susceptible de donner une indication sur la santé de la personne), réalisation d'une authentification de proximité chez un PS (même remarque que pour les résumés de factures), historiques de remboursement, données de Mon Espace Santé...

3.3 Principe général d'évaluation des risques

L'estimation des risques porte sur les menaces et vulnérabilités pondérées par les mesures mises en œuvre dans cette version.

L'échelle de probabilité des menaces est présentée en annexe 13.3.1.

L'impact est évalué selon deux axes :

1. Impact VP (pour Vie Privée), sur une l'échelle définie en annexe 13.3.2 ;
2. Impact AM (pour Assurance Maladie), sur l'échelle définie en annexe 13.3.3.

Chaque risque est ainsi évalué avec deux niveaux distincts sur l'échelle définie dans l'annexe 13.3.4 :

1. Risque VP : niveau de risque sur la Vie Privée ;
2. Risque AM : niveau de risque sur l'Assurance Maladie.

Le **niveau de risque retenu** est le **niveau le plus élevé** entre les deux évaluations (risque sur la vie privée et sur l'Assurance Maladie).

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

4 ETUDE DES PRINCIPES FONDAMENTAUX

Ce paragraphe présente le dispositif de conformité aux principes de protection de la vie privée.

Les données traitées, leur minimisation, leur exactitude et leur durée de conservation ainsi que les circuits de la donnée seront détaillés pour chaque processus.

4.1 Détermination des rôles et des acteurs

Les rôles et responsabilités des acteurs sont repris pour chaque processus :

- Les organismes AMO (Cnam et CCMSA) sont les responsables conjoints de traitement. Ils décident des finalités des traitements et valident les moyens des traitements.

- Le GIE SESAM-Vitale est sous-traitant. Il propose et développe les moyens du traitement pour le compte de ses membres dans le cadre des missions qui lui sont confiées.

4.2 Finalité du traitement

Ce traitement a pour finalité principale de mettre en œuvre et de gérer une application, de manière sécurisée, permettant aux bénéficiaires comme aux Professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte Vitale physique et particulièrement dans les buts suivants :

- Initialiser et activer une Application soit en utilisant l'identité numérique régalienne via l'application France Identité, soit en réalisant un traitement biométrique (rapprochement automatisé entre le selfie et le titre d'identité).
- Renforcer la lutte contre la fraude Professionnels de Santé et assurés dans le cadre de la prise en charge des soins par l'Assurance Maladie.
- Utiliser l'appli carte Vitale comme moyen d'identification électronique dématérialisé pour les services Assurance Maladie et la sphère santé.
- Piloter et évaluer quantitativement et qualitativement le déploiement de l'appli carte Vitale et le fonctionnement des services associés.

4.3 Base légale du traitement

La base légale retenue pour le traitement est la mission d'intérêt public au sens de l'article 6.1 e du RGPD. En effet :

- La finalité principale du traitement de données est la gestion et la mise en œuvre d'une application permettant aux assurés comme aux professionnels de santé de bénéficier des services équivalents à ceux disponibles avec une carte Vitale physique.
- Cette finalité fait partie intégrante des missions de service public dévolues à l'Assurance Maladie au même titre que la gestion et la mise en œuvre de la carte sur support physique (article L. 161-31 du CSS). L'application permet principalement la facturation (article L. 211-1 du CSS), l'identification et la consultation des droits de manière indirecte, traitements existants déjà mis en œuvre par l'Assurance Maladie sans nécessité de recueillir le consentement des personnes concernées.
- Le traitement de données est mis en œuvre avant tout pour répondre aux missions de service public de l'Assurance Maladie (art. 6.1.e RGPD) et ce, même si la personne réalise un acte positif de téléchargement et d'usage des services.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Justification de l'exception aux traitements de données particulières :

Données biométriques :

Lors de la procédure d'activation, un traitement biométrique sur les données de l'utilisateur ApCV est réalisé.

Le traitement qui sera mis en œuvre avec l'appli carte Vitale consiste en un rapprochement automatisé entre le selfie de l'assuré et la photo d'un titre d'identité. Ce rapprochement associé à un contrôle de preuve du vivant, permettra de vérifier l'identité du futur utilisateur de l'appli carte Vitale. Il s'agit de vérifier d'une part, que la personne souhaitant disposer d'une appli carte Vitale qui manipule le dispositif mobile correspond bien à celle du titre d'identité qu'elle produit (passeport, CNI ou titre de séjour) et que d'autre part ce titre correspond bien à un assuré connu et identifié dans les bases assurés des régimes. Le contrôle de preuve du vivant permet de s'assurer que celui qui manipule le dispositif mobile n'usurpe pas l'identité d'un tiers, par exemple en utilisant sa photo imprimée sur un support physique ou encore en utilisant des mécanismes de type *deep fake*.

La vérification de l'identité du futur utilisateur de l'application est d'autant plus indispensable qu'au-delà de la facturation possible (ou de l'accès à des télé-services médico-administratifs), l'application a vocation à servir de moyen d'identification pouvant être utilisé par l'assuré pour s'identifier et s'authentifier auprès de services en ligne (ex : Mon Espace Santé).

Il convient de préciser que l'objectif de ce traitement biométrique n'est pas la conservation d'empreintes ou de toute autre donnée biométrique dans la durée mais uniquement un traitement unique et ponctuel avec une conservation limitée au temps de réalisation des contrôles nécessaires. Les données ne sont conservées que le temps du rapprochement automatisé suivi du délai de traitement manuel si nécessaire. De plus, le SI IVI (chargé de vérifier cette identité à l'initialisation) est étanche et sans liens avec les autres SI de l'Assurance Maladie.

Le traitement de données biométrique ainsi mis en œuvre est donc réalisé pour sécuriser l'identité de la personne bénéficiaire des services de l'Assurance Maladie et dans le cadre de sa lutte contre la fraude pour assurer la finalité d'exécution de ses obligations en matière de la sécurité sociale et de la protection sociale.

L'enjeu de vérification de l'identité du porteur est au cœur de l'exercice des droits des personnes, et également de la lutte contre la fraude. Aussi, dans ce contexte, le traitement biométrique envisagé, limité et encadré dans son contenu, s'inscrit dans la même préoccupation de bonne gestion des assurés et de leur prise en charge.

La lutte contre la fraude fait partie de la mission d'intérêt public de l'Assurance Maladie en application des dispositions du chapitre IV ter du titre Ier et du livre Ier et de la première partie du code de la sécurité sociale relatives au contrôle et à la lutte contre la fraude ainsi que des articles L. 224-14 et L. 315-1 du code de la sécurité sociale et des articles L. 723-2 et L. 723-11 du code rural et de la pêche maritime.

La Loi Informatique et Libertés (LIL) ne ferme pas cette possibilité. En revanche, l'obligation d'avis motivé et publié de la CNIL est requise pour les traitements de l'Etat ou pour le compte de l'Etat conformément à l'article 32 de la LIL modifiée par l'ordonnance n°2018-1125 du 12 décembre 2018.

Ainsi, il apparaît que le traitement biométrique entre dans le champ de l'exception prévue à l'article 9-2 b) du RGPD, car il est nécessaire aux fins de l'exécution des obligations et de l'exercice de droits propres à l'Assurance Maladie en matière de droit de la sécurité sociale et de la protection sociale.

Données de santé :

L'exception mobilisée pour le traitement des données de santé est également celle du 9-2 b) du RGPD car il est nécessaire aux fins de l'exécution des obligations et de l'exercice de droits propres à l'Assurance Maladie en matière de droit de la sécurité sociale et de la protection sociale.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

4.4 Droits des personnes concernées

4.4.1 Mesures d'information des personnes

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Présentation des conditions d'utilisation / confidentialité	1) [MES06] Information individualisée par l'existence des Conditions Générales d'Utilisation (CGU) et de la Politique de protection des données personnelles au moment de l'activation (case à cocher attestant de la prise de connaissance des CGU pour pouvoir activer l'appli), les informations suivantes sont portées à la connaissance de l'utilisateur : o Identité et coordonnées du RT o Finalités du traitement o Catégories de données concernées o Durée de conservation des données o Modalités d'exercice des droits 2) [MES137] A chaque mise à jour des CGU et de la Politique de protection des données personnelles, une fenêtre pop-up dans l'applications précise les modifications substantielles apportées avec un lien vers les CGU et la Politique de protection des données personnelles. L'utilisateur doit attester, par une case à cocher, avoir pris connaissance des nouvelles CGU et de la Politique de protection des données personnelles pour accéder à l'application. 3) [EX31] Concernant le traitement biométrique : o Information spécifique avant le démarrage du traitement biométrique pour rappeler qu'il y a un traitement de données biométriques ; o Information sur le fait que les personnes ne souhaitant pas voir leurs données biométriques traitées pourront toujours bénéficier d'une prise en charge au moyen d'une carte vitale physique. Info dans CGU et la Politique de protection des données personnelles + site InfocarteVitale + FAQ. 4) [EX23] Conseil aux porteurs d'ApCV d'avoir leur carte Vitale sur eux lors de leur visite chez un PS afin de pallier une éventuelle indisponibilité de l'application. Info dans CGU et la Politique de protection des données personnelles + site InfocarteVitale + FAQ. 5) Information adaptée aux mineurs via le site InfocarteVitale.	
Possibilité d'accéder aux conditions d'utilisation/confidentialité	À tout moment, les utilisateurs peuvent consulter une page d'information rappelant ces informations dans l'appli carte Vitale.	
Conditions lisibles et compréhensibles	Une boucle d'amélioration continue de la lisibilité des CGU et de la Politique de protection des données personnelles est mise en place sur la base des retours des utilisateurs issus des enquêtes menées par la Cnam et d'entretiens avec les utilisateurs.	

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Existence de clauses spécifiques au dispositif	Indication et présentation du traitement biométrique effectué au moment de l'activation et du démarrage du traitement biométrique. Gestion effective du caractère facultatif de l'usage de l'application carte Vitale.	
Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.)	Oui, avec les CGU et la Politique de protection des données personnelles affichées à l'activation puis à tout moment et la mention d'information sur le traitement publiée par les responsables de traitement NB : la mention d'information concerne également les données PS traitées.	
Présentation détaillée des données personnelles collectées	Oui dans les CGU et la Politique de protection des données personnelles, ainsi que dans la mention d'information sur le traitement publiée par les responsables de traitement.	
Présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers	L'application n'accède à aucun identifiant de l'appareil : l'identification de l'ApCV se fait par des identifiants générés par le SI ApCV (Identifiant ApCV et Identifiant Profil ApCV).	
Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.)	Oui dans les CGU et la Politique de protection des données personnelles, ainsi que dans la mention d'information sur le traitement publiée par les responsables de traitement.	
Informations des personnes sur leurs droits : Mise à jour d'un registre des traitements par chaque DPO	Oui fait par chaque responsable de traitement et par les sous-traitants	
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation	Indication de l'hébergement sécurisé dans les CGU et la Politique de protection des données personnelles.	
Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité	Oui, l'utilisateur de l'ApCV est invité à prendre contact avec son organisme d'Assurance Maladie	

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité	Publication d'une nouvelle version de l'application mobile intégrant la modification des CGU et affichage des nouvelles CGU et Politique de protection des données personnelles au lancement suivant de l'application et fenêtre pop-up d'information sur les modifications. Publication d'une mention d'information par les responsables de traitement.	
Concernant la transmission de données à des tiers :	Les autorités publiques sont destinataires des données statistiques agrégées et anonymisées	
- **Présentation détaillée des finalités de transmission à des tiers**	Sans objet	
- **Présentation détaillée des données personnelles transmises**	Sans objet	
- **Indication de l'identité des entreprises tierces**	Les sociétés en charge de l'infogérance du Système d'Information appli carte Vitale, de la vérification d'identité et de la sécurisation des données contenues dans l'application (sous-traitants ultérieurs) sont citées dans les CGU et la Politique de protection des données personnelles.	

4.4.2 Exercice du droit d'accès

Les traitements ne bénéficient pas d'une exemption au droit d'accès, prévue par l'article 49 de la loi Informatique et libertés et l'article 15 du RGPD.

Lorsqu'un assuré exerce son droit d'accès, l'ensemble des caractéristiques du traitement lui sont fournies conformément au paragraphe 1 de l'article 15, ainsi qu'une copie de ses données personnelles faisant l'objet du traitement.

Mesures pour le droit d'accès	Données contenues dans l'application ApCV	Données externes à l'application (ex : SI ApCV)
Possibilité d'accéder à l'ensemble des données personnelles de l'utilisateur, via les interfaces courantes	Oui directement depuis l'application carte Vitale pour les utilisateurs	Oui via une demande complémentaire à l'organisme de rattachement (pour les assurés et les PS)
Possibilité de consulter, de manière sécurisée, les traces d'utilisation liées à la personne concernée	Non. Les traces ne sont pas consultables dans l'application, mais elles sont remontées au SI lorsque la connexion réseau est présente. Elles sont donc accessibles dans les mêmes conditions que les données externes à l'application ci-contre.	Pas de consultation directe de l'utilisateur. Les traces d'usages sont accessibles sur demande explicite à l'organisme gestionnaire (assurés) ou à la caisse de rattachement (PS)

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Mesures pour le droit d'accès	Données contenues dans l'application ApCV	Données externes à l'application (ex : SI ApCV)
Possibilité de télécharger une archive de l'ensemble des données à caractère personnel liées à la personne concernée	Non. Les données sont disponibles en consultation dans l'application.	Non.

4.4.3 Exercice du droit à la portabilité

Le droit à la portabilité prévu par l'article 55 de la loi Informatique et libertés et par l'article 20 du RGPD n'est pas applicable aux présents traitements qui ne sont fondés ni sur le consentement, ni sur l'exécution d'un contrat.

4.4.4 Exercice du droit de rectification

Le traitement ne bénéficie pas d'une exemption au droit de rectification prévu par l'article 50 de la loi Informatique et libertés et l'article 16 du RGPD.

Les professionnels de santé concernés par le traitement peuvent exercer leurs droits de rectification des données les concernant auprès du délégué à la protection des données personnelles de leur organisme de rattachement ou du directeur de leur organisme de rattachement.

Les assurés concernés par le traitement peuvent exercer leurs droits de rectification des données les concernant auprès de leur organisme de rattachement (auprès du délégué à la protection des données ou du directeur de l'organisme), les données stockées dans l'ApCV n'étant pas modifiables directement par l'assuré (à l'exception de l'adresse mail de contact pour FranceConnect) :

- Les données liées aux AMO sont mises à jour automatiquement à la prochaine utilisation de l'ApCV, à partir d'un service de l'Inter-Régimes ;
- Le NIR et les informations d'état civil issues de la pièce d'identité ne peuvent pas être mis à jour : l'utilisateur doit effectuer une nouvelle activation de l'ApCV sur son smartphone pour constater la mise à jour des données.

4.4.5 Exercice des droits d'opposition et d'effacement

L'exercice des droits des personnes concernées sur la gestion des éventuelles oppositions et demande d'effacement qui peuvent s'en suivre, devra être analysé à la lumière des articles 17 et 21 du RGPD et 51 et 53 de la loi Informatique et libertés.

En revanche, l'exercice du droit d'opposition et donc d'effacement doit être écarté pour le traitement des données issues de l'usage de l'application (données permettant la liquidation et son contrôle) – Article R 161-33-20-I du code de la sécurité sociale modifié par le décret n°2022-1719 du 28 décembre 2022.

Le droit d'opposition n'est par ailleurs pas applicable non plus au traitement de données automatisé nécessaire à la délivrance de l'appli carte Vitale - Article R 161-33-18- IV du code de la sécurité sociale modifié par le décret n°2022-1719 du 28 décembre 2022.

La recevabilité des demandes d'opposition/effacement faites par les utilisateurs et les PS seront analysées au cas par cas avec mise en balance de leurs intérêts particuliers et des intérêts des responsables de traitement (motifs légitimes et impérieux pour ces derniers).

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

S'agissant des utilisateurs enrôlés lors de la première phase de l'expérimentation (avec traitement de données basé sur le consentement), ils peuvent, après avoir été informés du démarrage d'une nouvelle phase de l'expérimentation (avec changement de base légale du traitement notamment) décider de ne pas poursuivre et retirer leur consentement. Ce retrait de consentement est géré comme dans la première phase de l'expérimentation et entraîne l'effacement de leurs données au niveau du SI ApCV.

Concernant les données contenues dans l'application directement, l'utilisateur peut effacer les données (fonction réinitialiser l'ApCV) ou désinstaller l'application.

Mesures pour le droit à l'effacement	Données contenues dans l'application ApCV	Données externes à l'application (ex : SI ApCV)
Possibilité de supprimer les données personnelles	Oui	Voir précision ci-dessus
Indication des données personnelles qui seront conservées malgré tout (contraintes techniques, obligations légales, etc.)	Sans objet	Oui dans les CGU et la Politique de protection des données personnelles
Indications claires et étapes simples pour effacer les données avant de mettre l'appareil au rebut	Fonction de réinitialisation des données disponible dans l'application mobile Vitale et décrite dans les CGU et la Politique de protection des données personnelles	Sans objet
Conseils fournis pour remise à zéro en cas de vente de l'appareil	Fonction de réinitialisation des données disponible dans l'application mobile Vitale Mise à disposition d'une FAQ accessible depuis l'application mobile et dans les CGU et la Politique de protection des données personnelles	Sans objet
Possibilité d'effacer les données en cas de vol de l'appareil	Suite à la déclaration de perte/vol du smartphone, l'ApCV est mise en opposition dans le SI ApCV et un ordre d'effacement des données locales de l'ApCV est envoyé par le SI ApCV à la prochaine connexion de l'ApCV à celui-ci.	Sans objet

4.4.6 Exercice du droit à la limitation du traitement

L'exercice des droits des personnes concernées sur la gestion des éventuelles oppositions et demande d'effacement qui peuvent s'en suivre, devra être analysé à la lumière des articles 18 et 21 du RGPD et 53 de la loi Informatique et libertés.

Concernant les utilisateurs et pour :

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

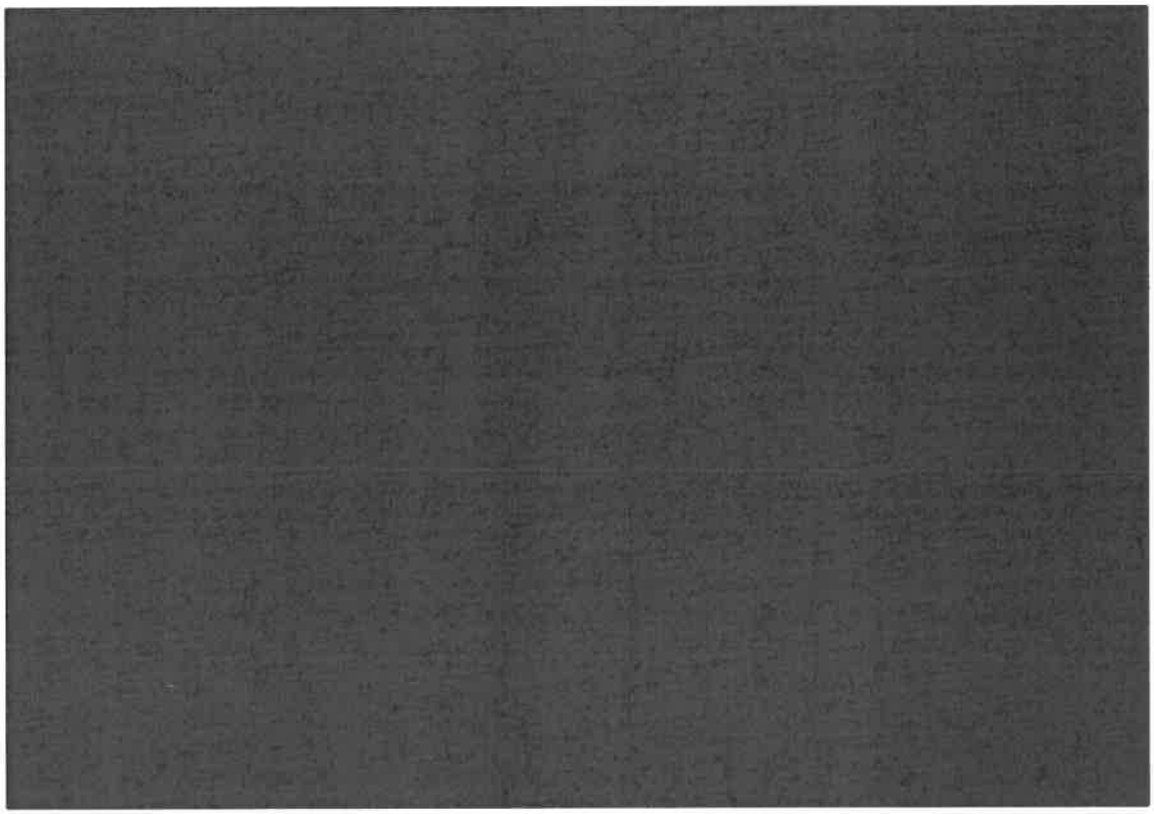
- l'exercice du droit à la limitation en lien avec une demande d'opposition : sans objet pour la finalité principale du traitement (facturation/remboursement des soins) pour lesquelles les données des assurés sont traitées. Sans objet pour la partie activation (désinstallation de l'application) ;
- l'exercice du droit à la limitation en lien avec une demande de rectification : Il convient de déterminer la réponse à apporter au cas par cas et en tenant compte des impacts sur la vie privée pour l'utilisateur concerné ;
- l'exercice du droit à la limitation avec demande de conservation des données qui devaient être effacées : pour l'activation, il convient de s'assurer auprès du titulaire du marché Vérification d'identité qu'il peut conserver plus longtemps le dossier de preuves d'un utilisateur. Les autres process relèvent des régimes qui appliqueront les procédures habituelles.

Concernant les PS et pour :

- l'exercice du droit à la limitation en lien avec le droit de rectification et le droit d'opposition : pour la partie informationnelle du décisionnel (listings PS) : possibilité au cas par cas (traitement manuel) de ne pas intégrer pendant une période donnée ou définitivement un PS dans les listings ;
- l'exercice du droit à la limitation avec demande de conservation des données qui devaient être effacées : données conservées 5 ans, il est peu probable que ce droit s'applique dans ce cas de figure.

4.5 Gestion et notification des violations de données

Détection des violations de données :



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

En fonction du degré de risque sur la vie privée des personnes, les responsables de traitement notifient cette violation à la CNIL et le cas échéant, les Régimes la notifient aux personnes concernées.

Les modalités d'organisation de la notification des violations de données entre les différents acteurs du traitement sont définies dans les différents contrats conclus : le contrat entre les responsables conjoints, le contrat de sous-traitance entre les responsables conjoints et le GIE SESAM-Vitale ainsi que le marché public passé par le GIE SESAM-Vitale avec l'Industriel de Vérification d'Identité.

[redacted]

4.6 Détermination et description des mesures pour la sous-traitance

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28
GIE SESAM-Vitale	Développement et publication de l'application carte Vitale sur les stores Apple et Google ; Développement et mise à disposition d'un portail de gestion du support aux AMO ; Conception, mise en œuvre et exploitation le SI ApCV au niveau applicatif ; Support de niveau 3.	Appli mobile SI ApCV Portail de gestion du support	Contrat de sous-traitance RT/GIE SV [redacted]	Reprise des éléments de l'article 28 du RGPD Conclusion du contrat nécessaire à la conformité RGPD du traitement
Sous-traitant ultérieur (sous-traitant du GIE SV) - Industriel Vérification Identité	Mise à disposition des produits et services nécessaires à la vérification d'identité lors de la procédure d'activation	Activation SI IVI	Marché PCN-19-04 « Appli carte Vitale – Vérification d'identité ». Titulaire [redacted] Sous-traitant du titulaire : [redacted]	Le contrat de sous-traitance à travers une clause conforme à l'article 28 du RGPD insérée dans les documents contractuels du marché et travaux avec le Titulaire du marché pour établir les procédures d'exercice des droits des personnes et la gestion des violations de données

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28
Sous-traitant ultérieur (sous-traitant du GIE SESAM-Vitale) - Infogérance ApCV	Hébergement et infogérance des systèmes informatiques du SI ApCV (hors SI décisionnel)	SI ApCV (hors SI décisionnel)	Marché PAN-21-08 « Infogérance ApCV » Titulaire : [redacted] (qualifié SecNumCloud sur le périmètre hébergement de production)	Le contrat de sous-traitance à travers une clause conforme à l'article 28 du RGPD insérée dans les documents contractuels du marché et travaux avec le Titulaire du marché pour établir les procédures d'exercice des droits des personnes et la gestion des violations de données
Sous-traitant ultérieur (sous-traitant du GIE SESAM-Vitale) – Sécurisation de l'application carte Vitale	Mise en place d'un socle de sécurité destiné à renforcer le niveau de sécurité des données stockées dans l'application carte Vitale.	SDK et SI Sécurité	Marché PI-19-06 « Sécurisation de l'application carte Vitale » Titulaire : [redacted]	Le contrat de sous-traitance à travers une clause et une annexe conformes à l'article 28 du RGPD insérées dans les documents contractuels du marché
[redacted]				
Sous-traitant ultérieur (sous-traitant du GIE SV) – Assistance technique	Intervention pour de l'assistance technique réalisée par des prestataires dans le domaine décisionnel et réalisation logicielle	SID ApCV	Sociétés titulaires des marchés d'AT décisionnel et Réalisation logicielle	Les documents contractuels des marchés intègrent le contrat de sous-traitance à travers une clause conforme à l'article 28 du RGPD

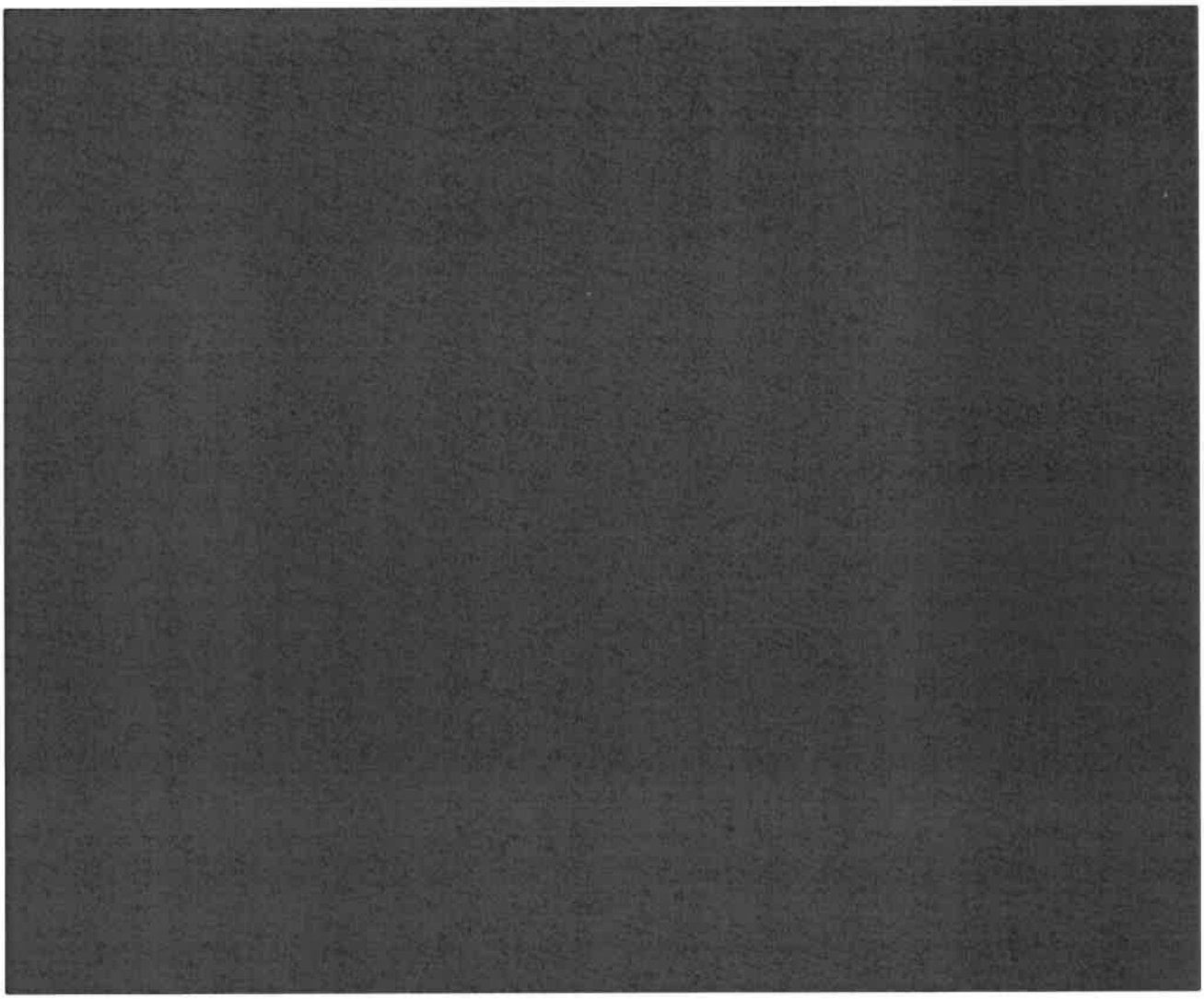
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28
Amazon Polly	Synthèse vocale pour donner les consignes à l'utilisateur lors de l'inscription	Appli mobile	AWS shared responsibility model	Pas de traitement de DCP, les seules données envoyées à AWS sont les phrases à lire à l'utilisateur. Celles-ci sont génériques (ex : « Veuillez présenter votre document à la caméra ») et ne contiennent aucune information en lien avec l'utilisateur. Par ailleurs, l'IVI n'a pas donné son consentement pour que Amazon Polly utilise les données envoyées.

4.7

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5 SECURITE DE L'APPLICATION MOBILE ET DES SI

5.1 Appli carte Vitale (ApCV)

5.1.1 Présentation de l'application mobile

Conception de l'application

L'ApCV est développée par le GIE SV, avec les langages natifs des OS mobiles iOS et Android pour être mise à disposition sur les stores publics officiels Apple (App Store) et Google (Google Play).

Elle intègre un SDK sécurité développé par la société [redacted]

Publication dans les stores

[MES125] L'application est publiée sur les stores Apple et Google, qui imposent un processus de publication dont les principales étapes sont les suivantes :

1. Création d'un compte développeur (ou compte principal) et optionnellement de comptes secondaires pour cloisonner les droits entre les différents acteurs du cycle de vie de l'application ;
2. Génération d'un bi-clés et d'un certificat de signature de code associés au compte développeur ;
3. Signature et dépôt de l'application dans le store ;
4. Validation de l'application par Apple et Google ;
5. Publication de l'application (mise à disposition des utilisateurs).

Le GIE SV a souscrit un compte développeur en tant qu'organisation GIE SESAM-Vitale auprès d'Apple et Google et a mis en place des mesures de sécurité fortes pour protéger l'accès à ces comptes. L'ensemble des mesures relatives au processus de publication sont décrites au §5.1.2.10.

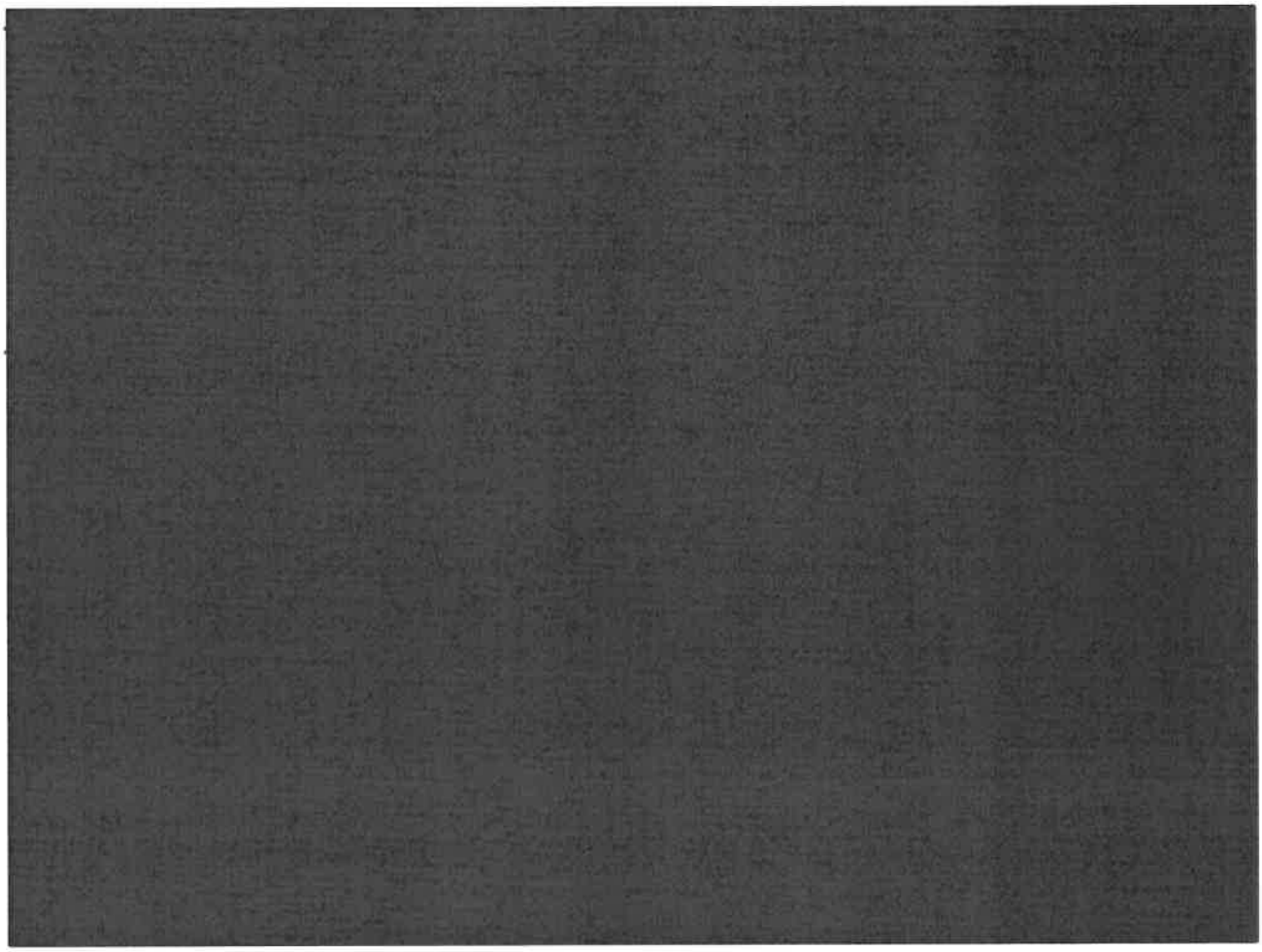
5.1.2 Mesures de sécurité

5.1.2.1 Sécurité du développement

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

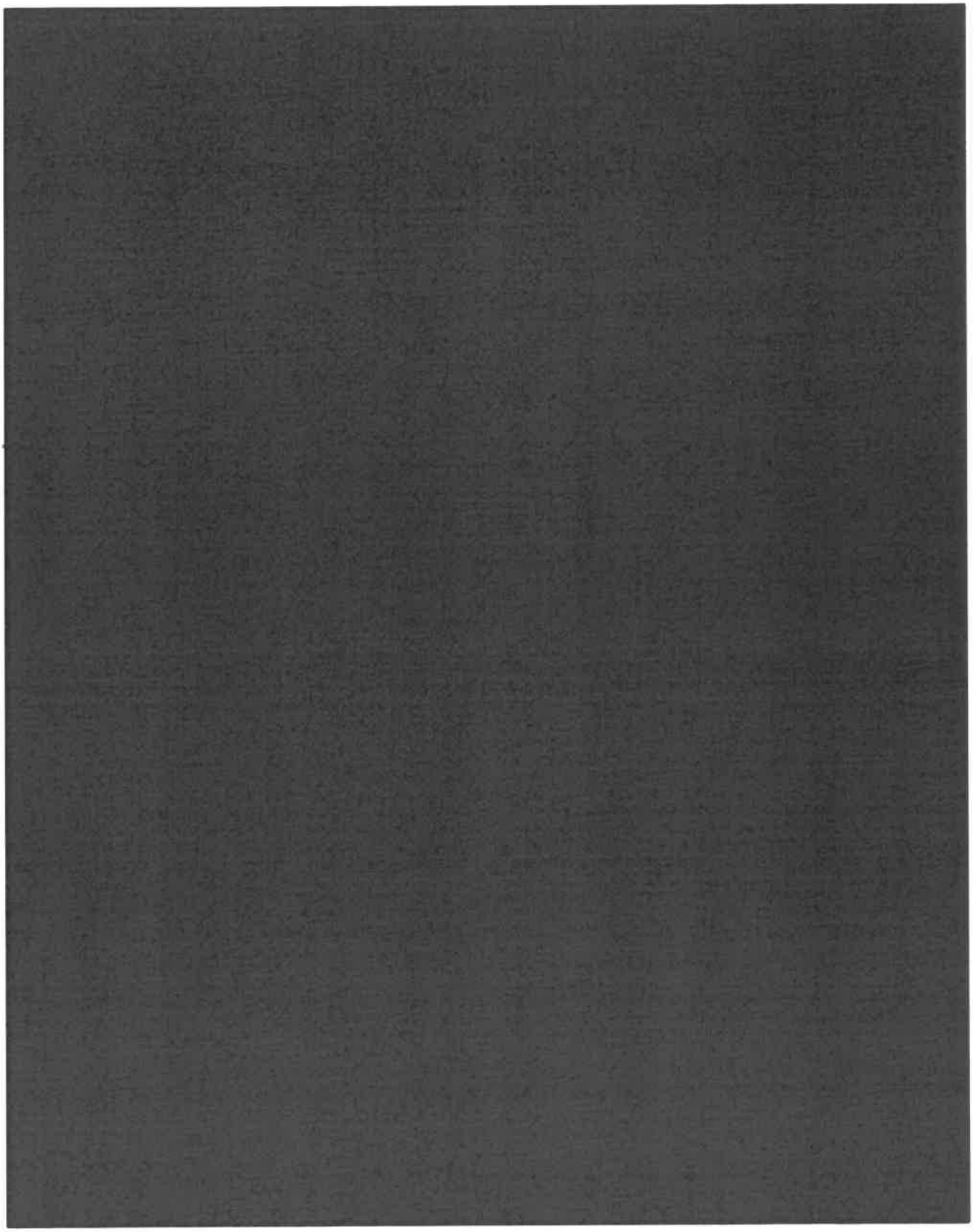
5.1.2.2 Obfuscation et RASP



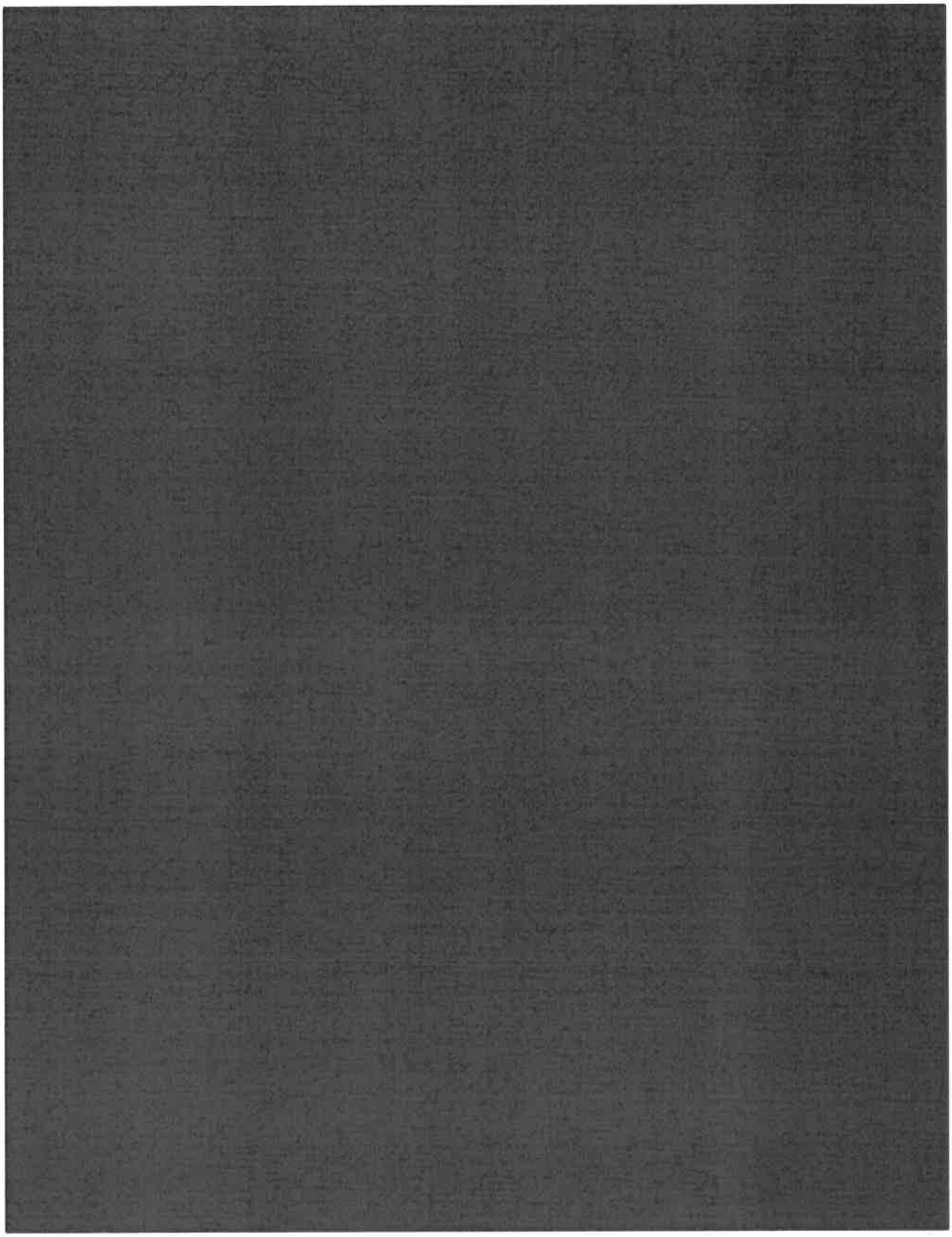
5.1.2.3 Stockage sécurisé

5.1.2.4 Clés cryptographiques utilisées par l'ApCV

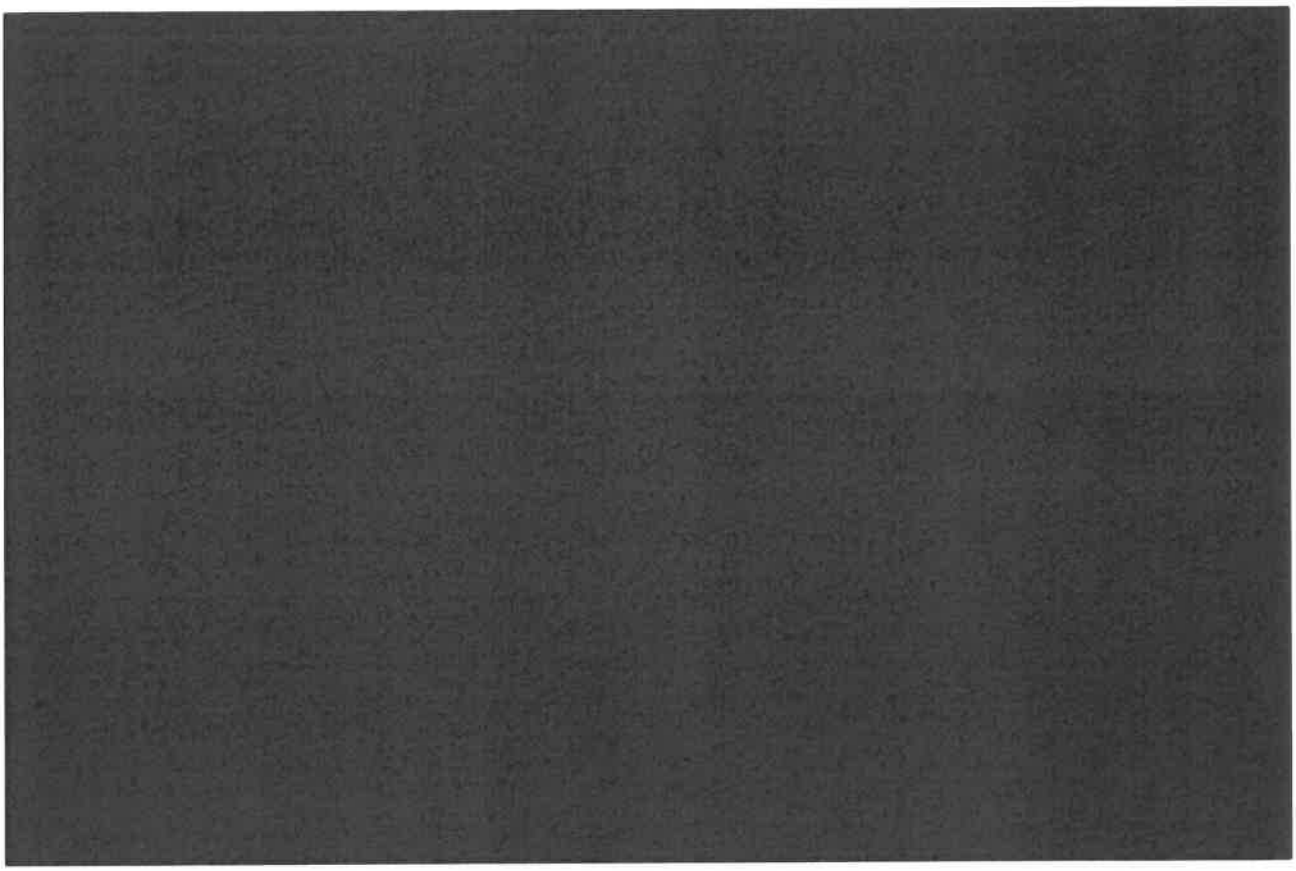
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



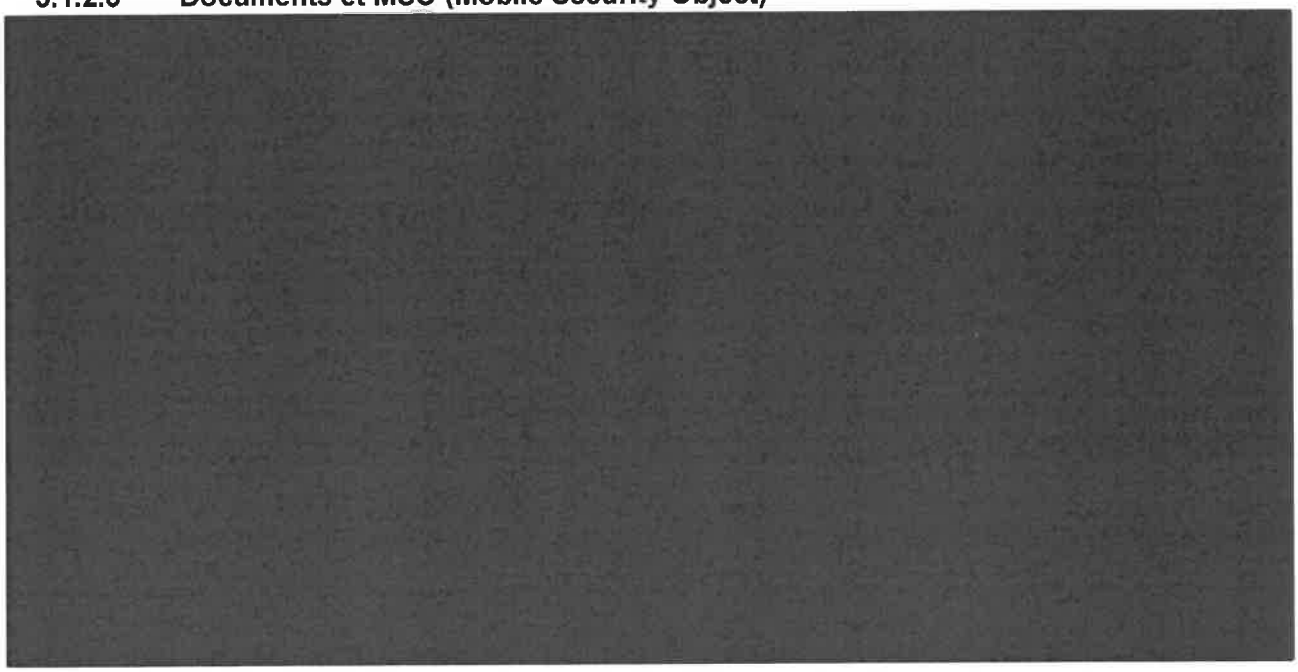
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



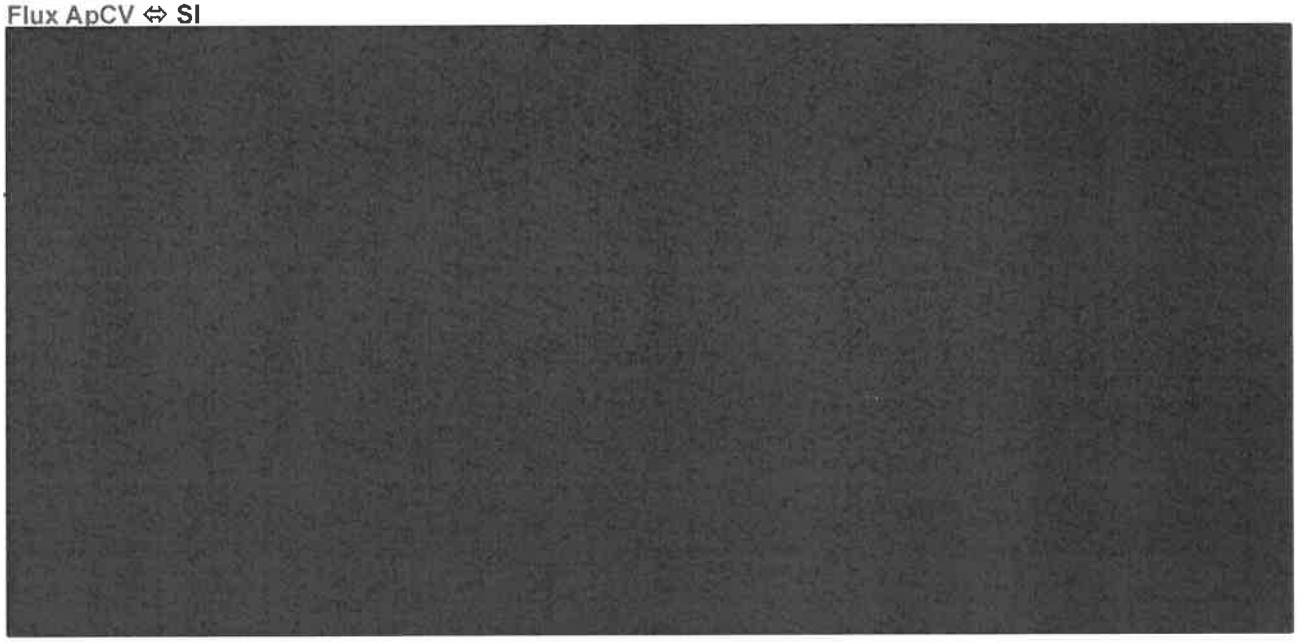
5.1.2.5 Documents et MSO (Mobile Security Object)



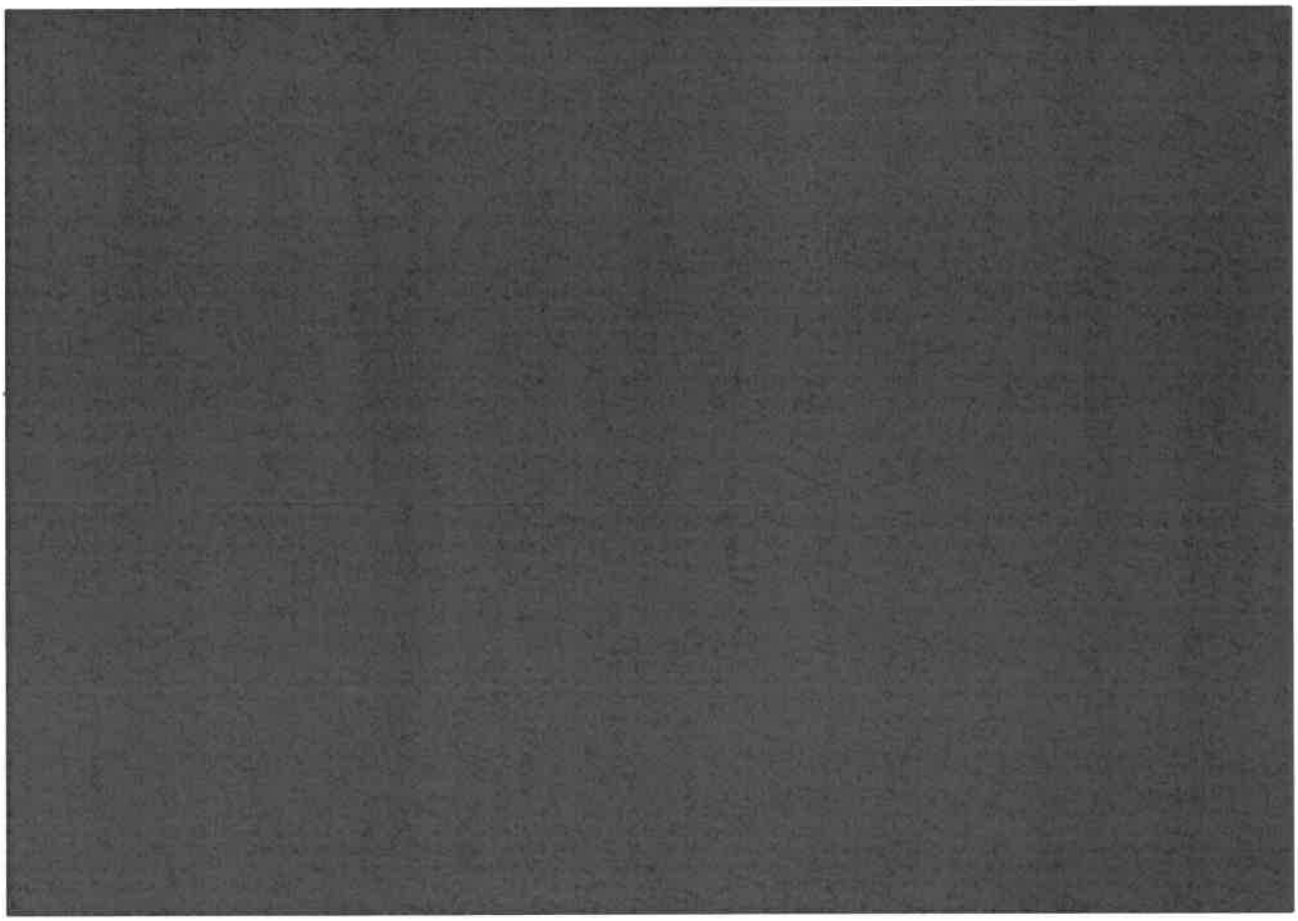
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.1.2.6 Sécurité des flux

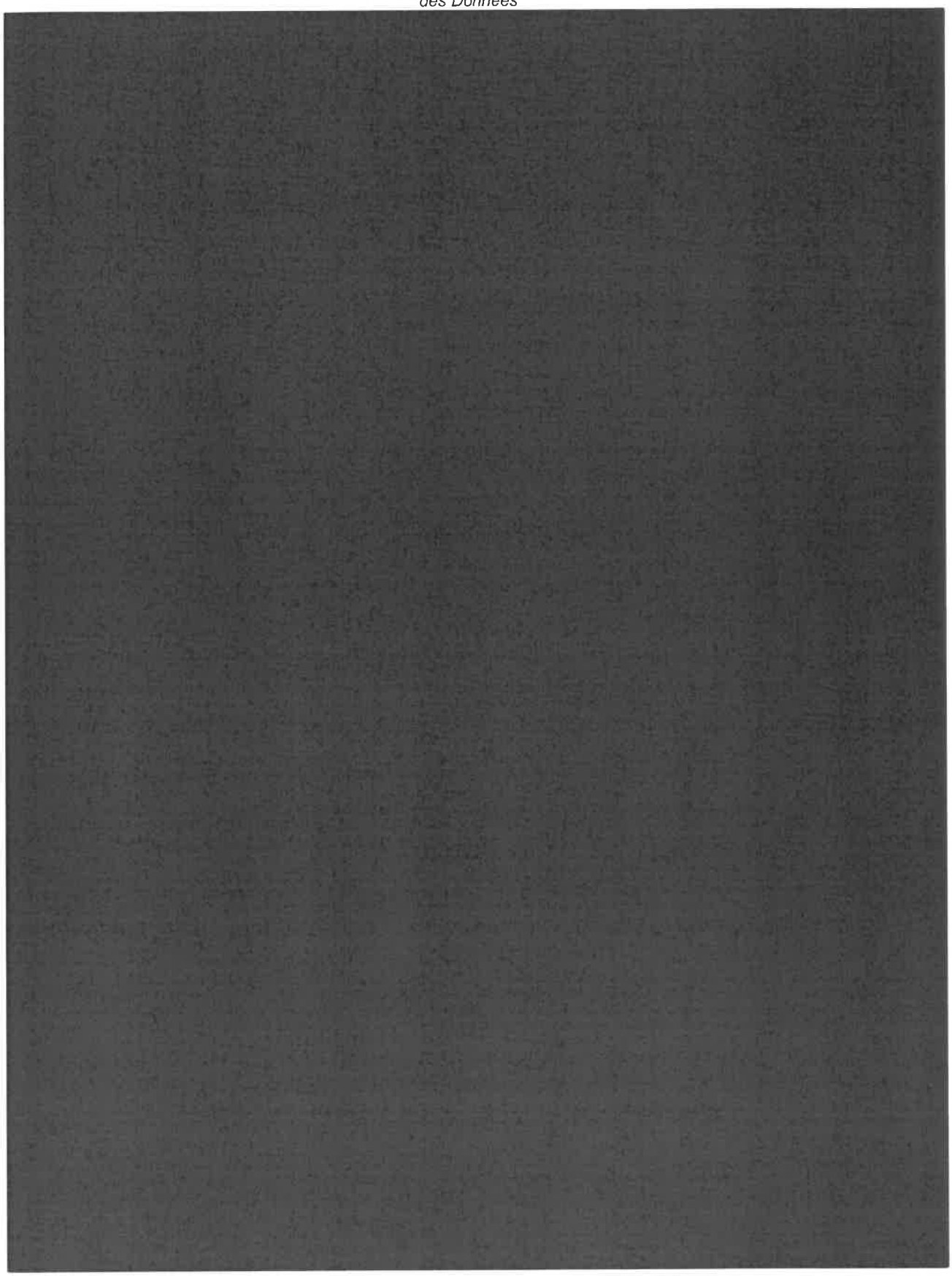
Flux ApCV ⇔ SI



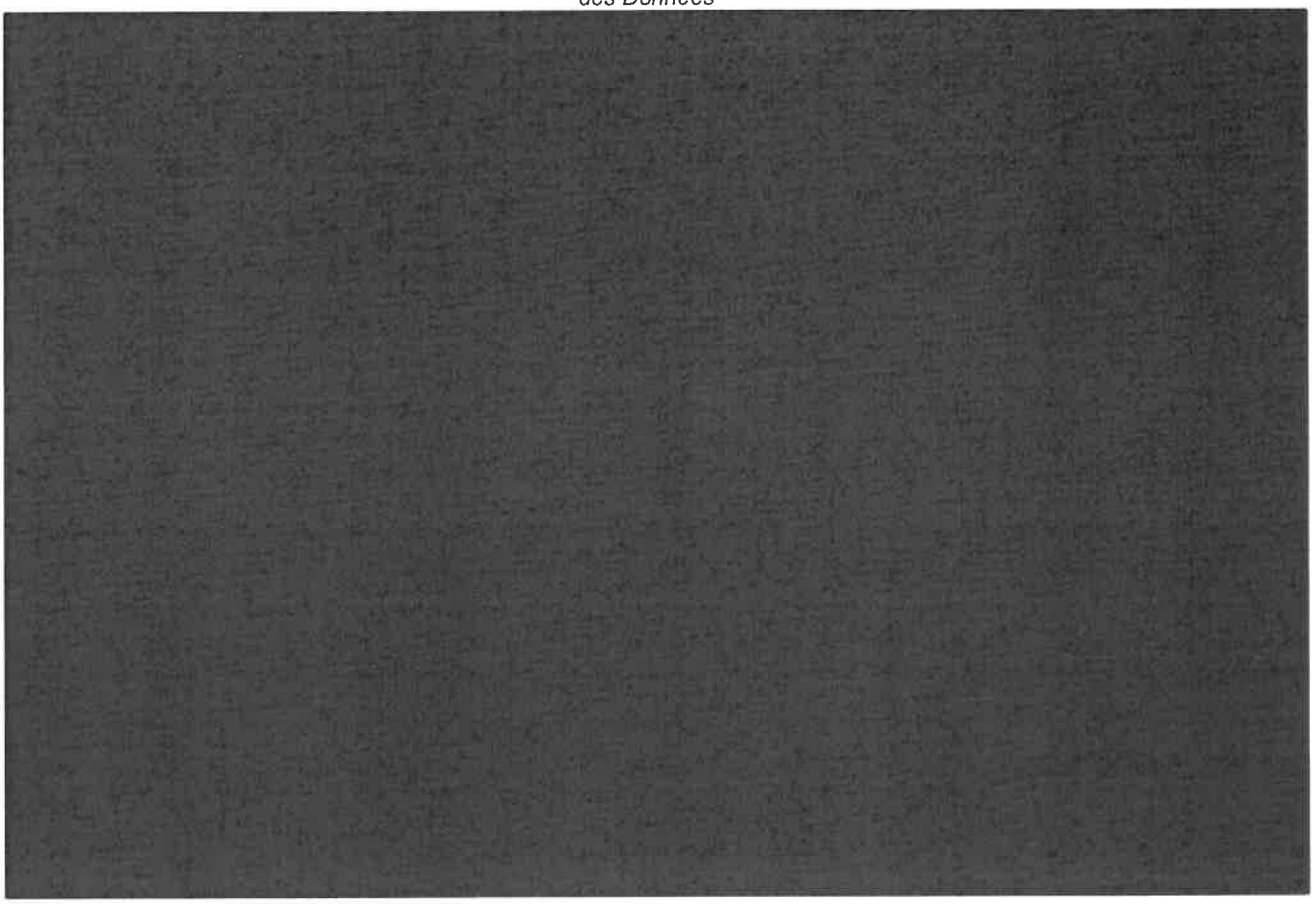
5.1.2.7 Déverrouillage de l'ApCV (mot de passe)



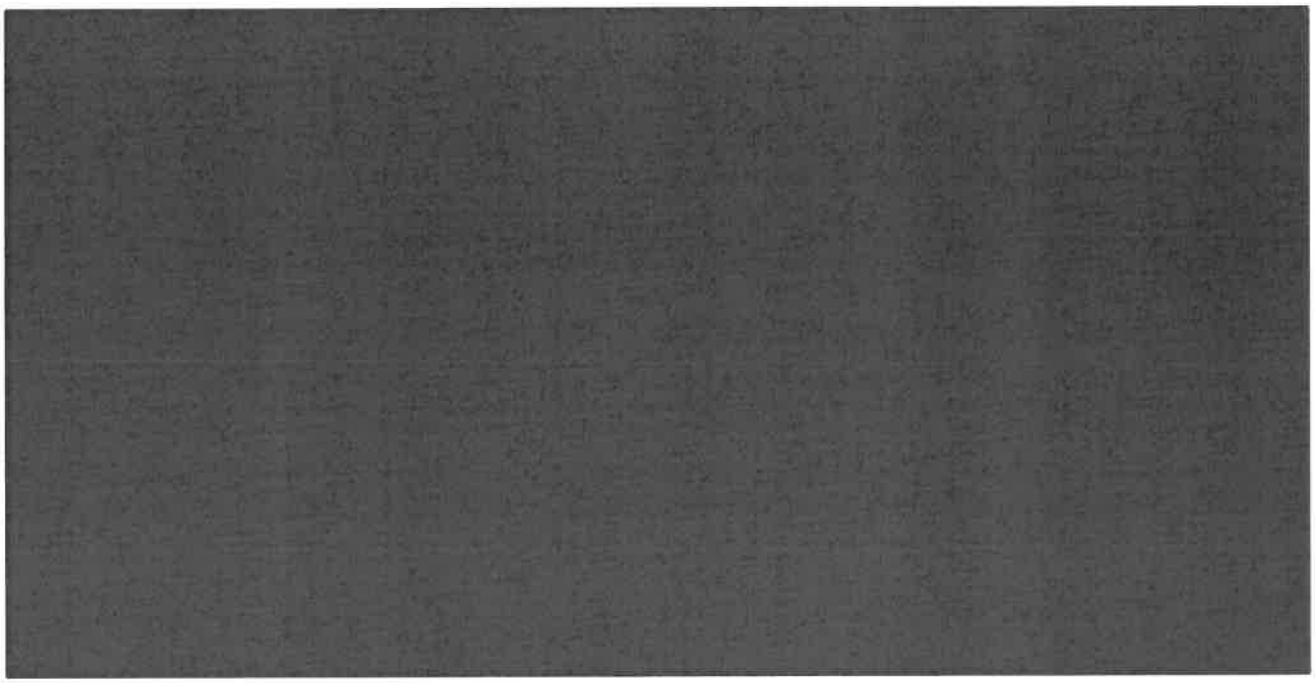
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



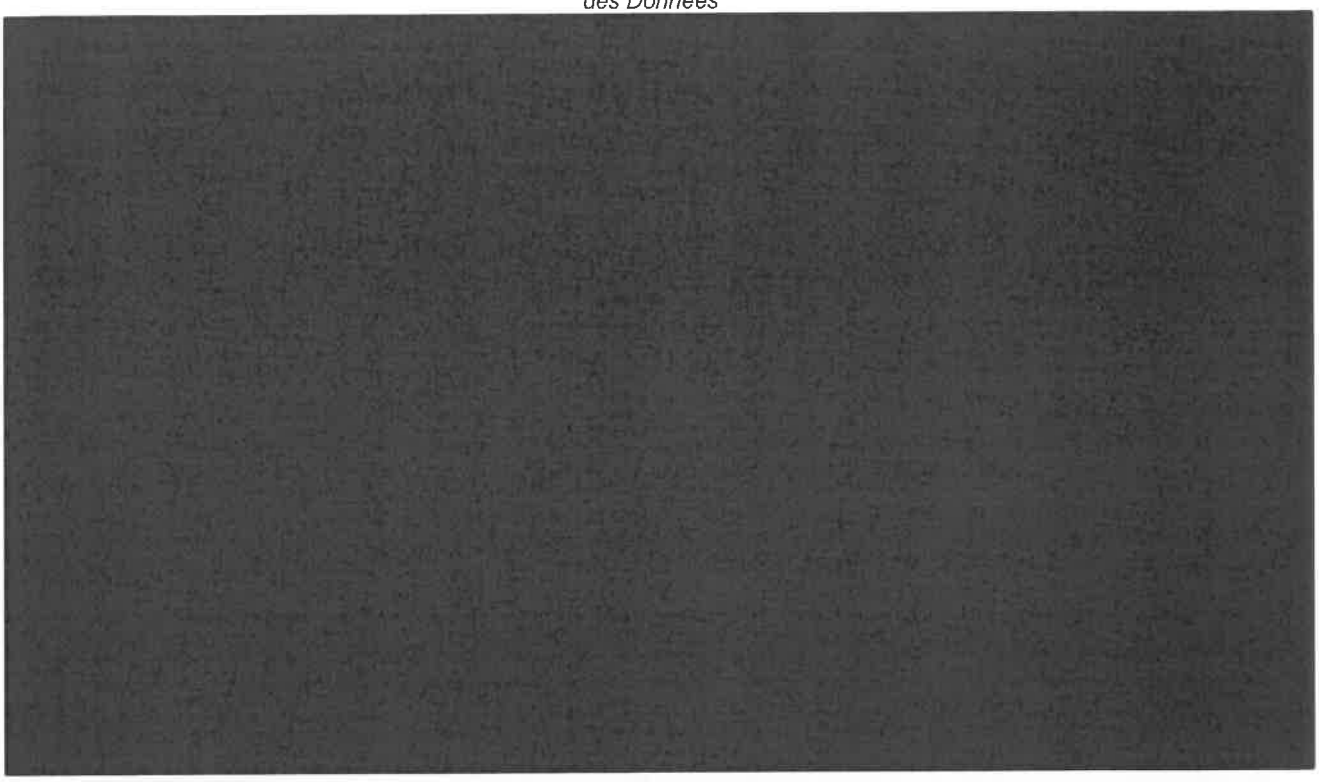
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



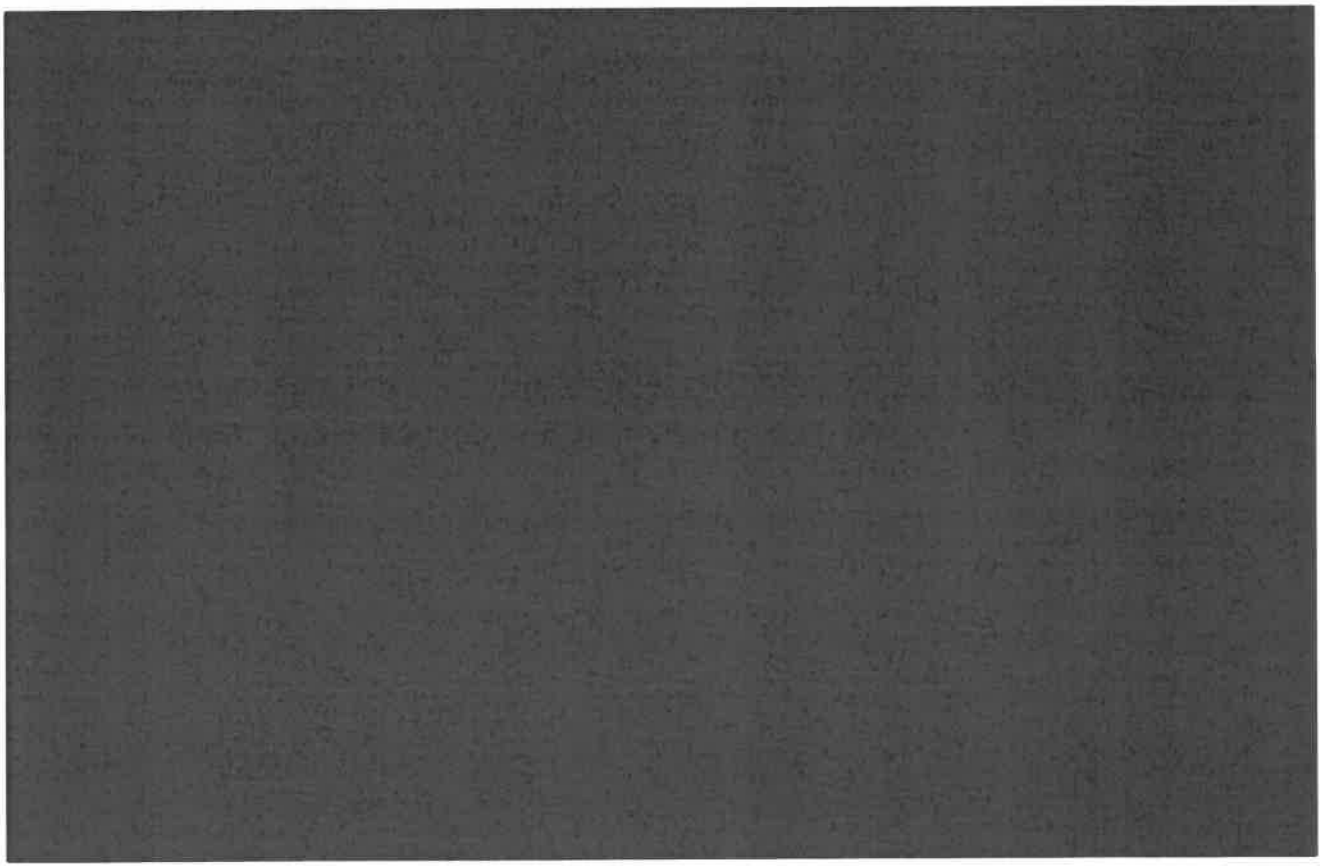
5.1.2.8 Déverrouillage de l'ApCV (biométrie)



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



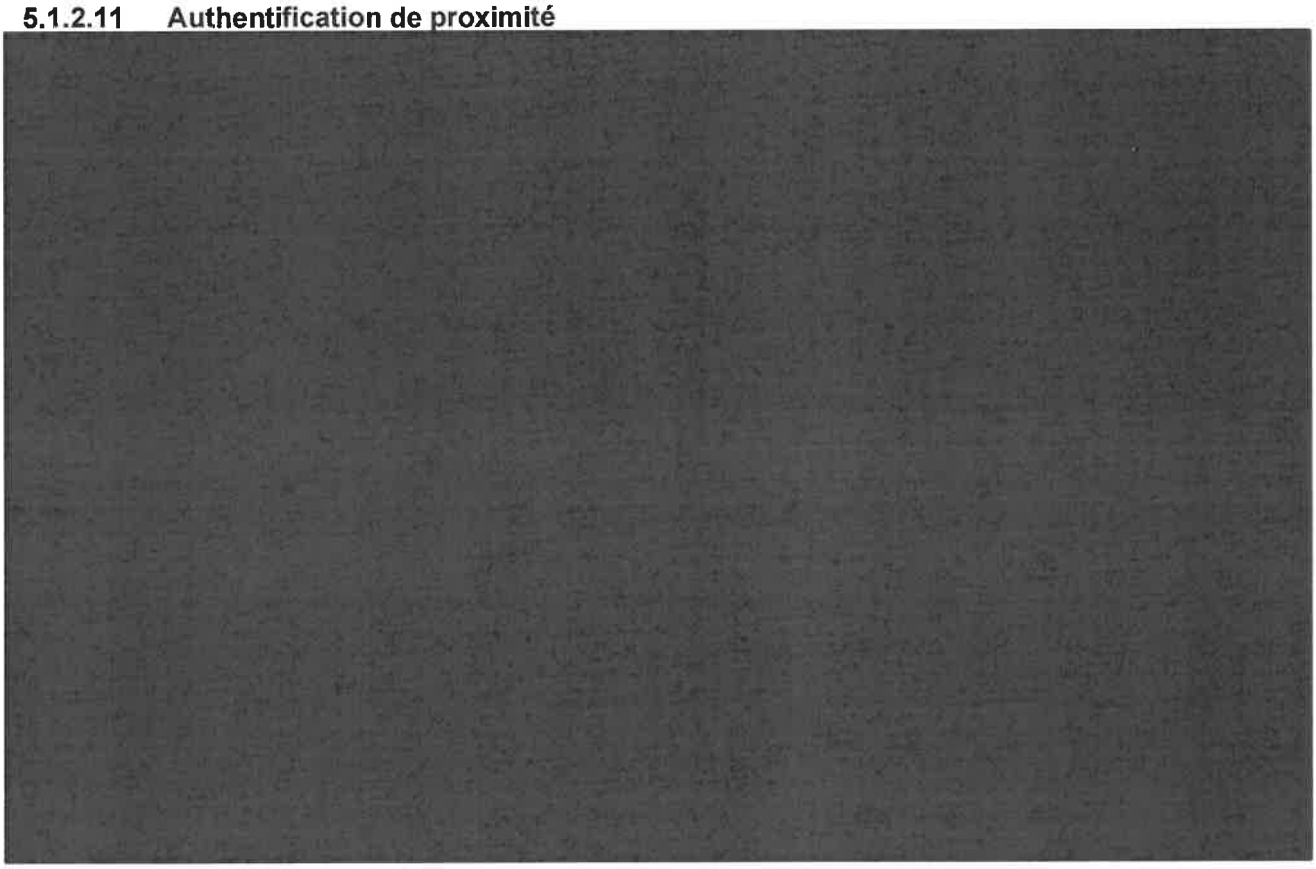
5.1.2.9 Authentification de l'ApCV vis-à-vis du SI ApCV



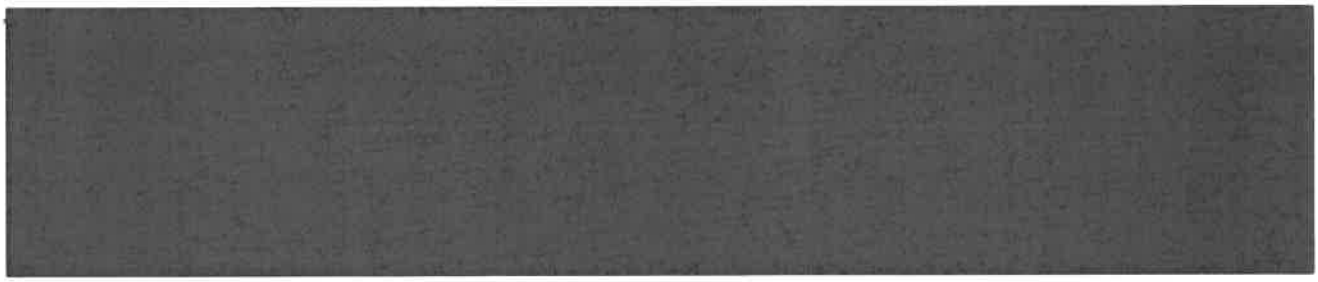
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.1.2.10 Authentification du SDK vis-à-vis du SI Sécurité

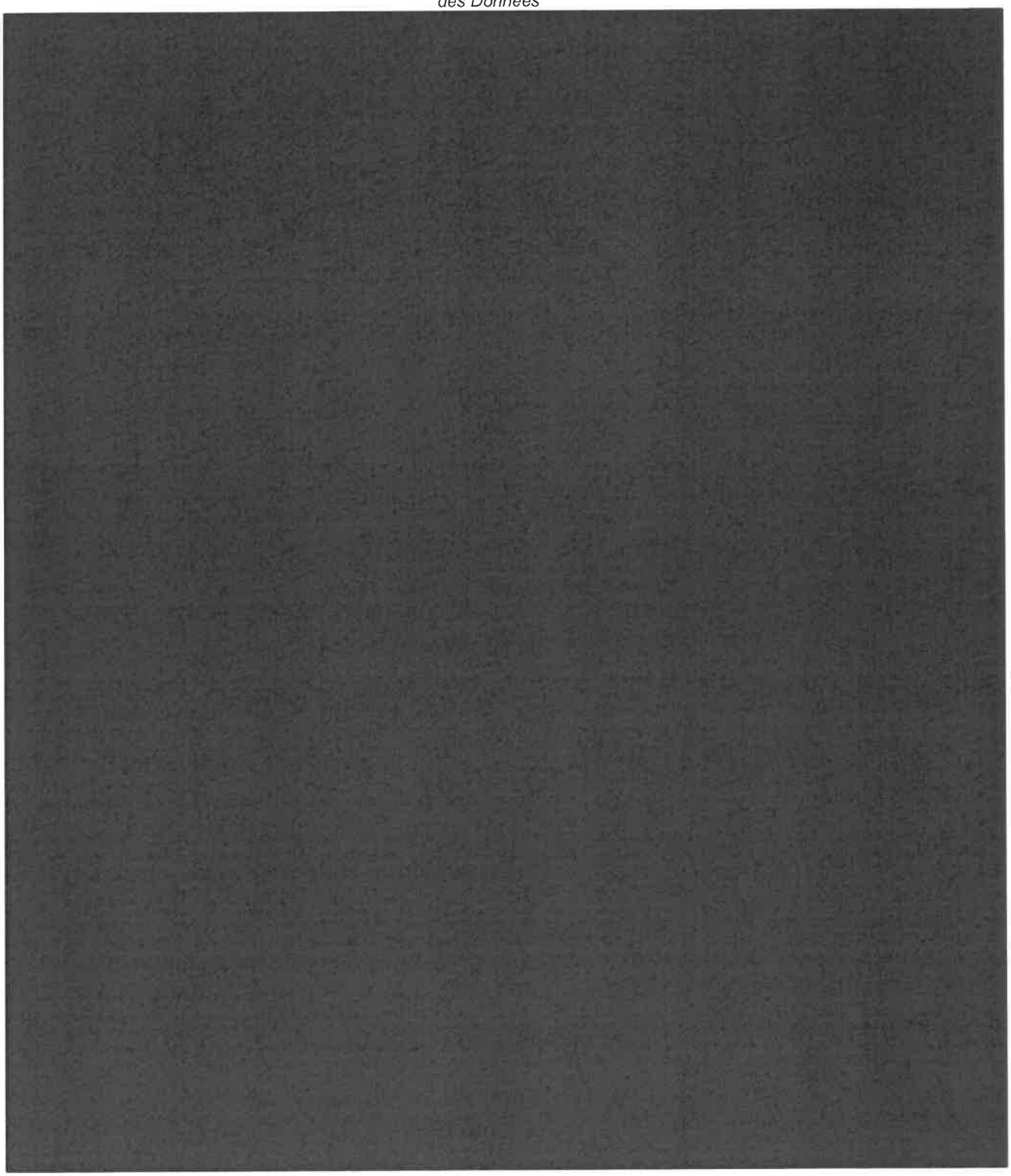
5.1.2.11 Authentification de proximité



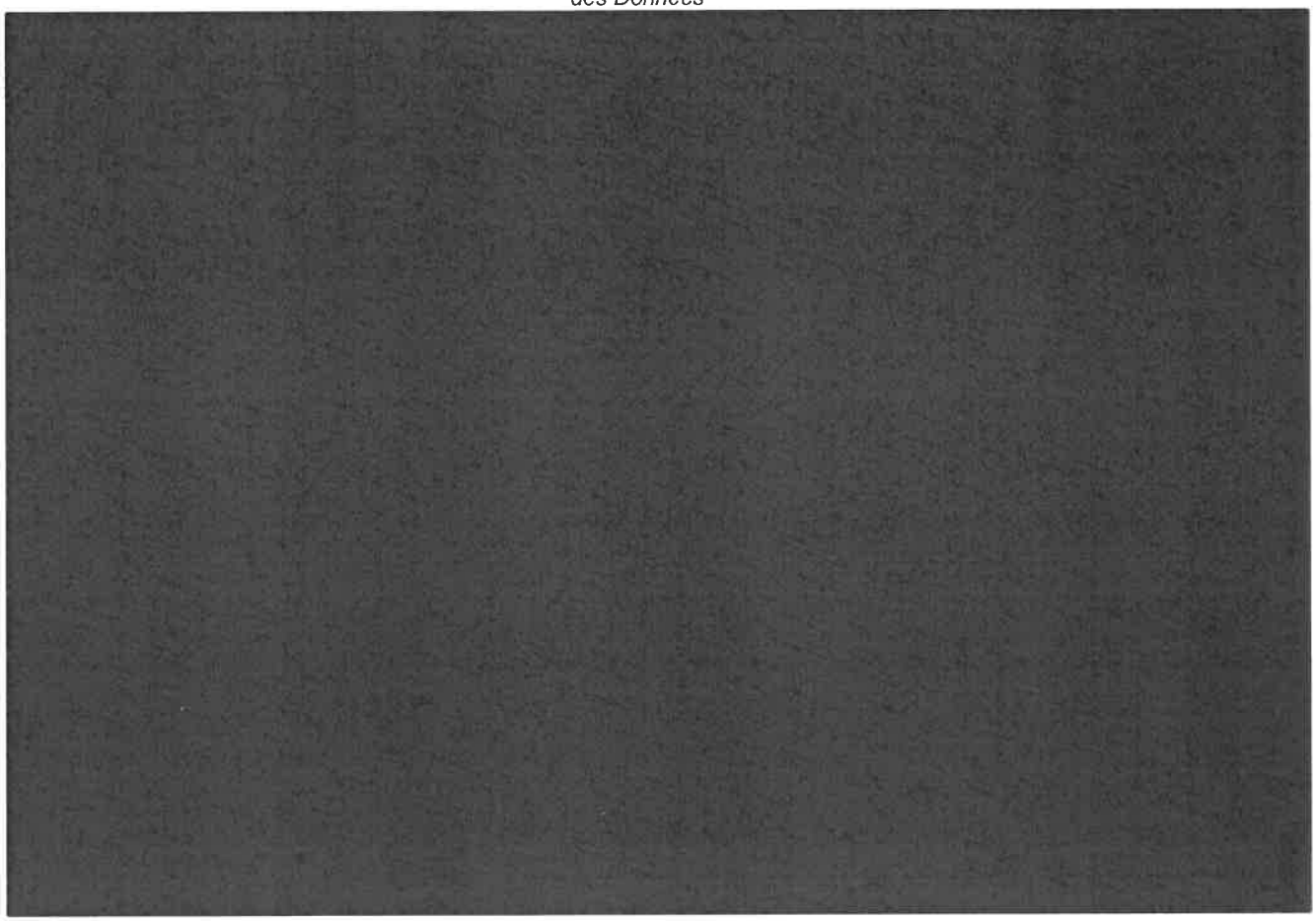
5.1.2.12 Publication de l'application mobile ApCV sur les stores Apple et Google



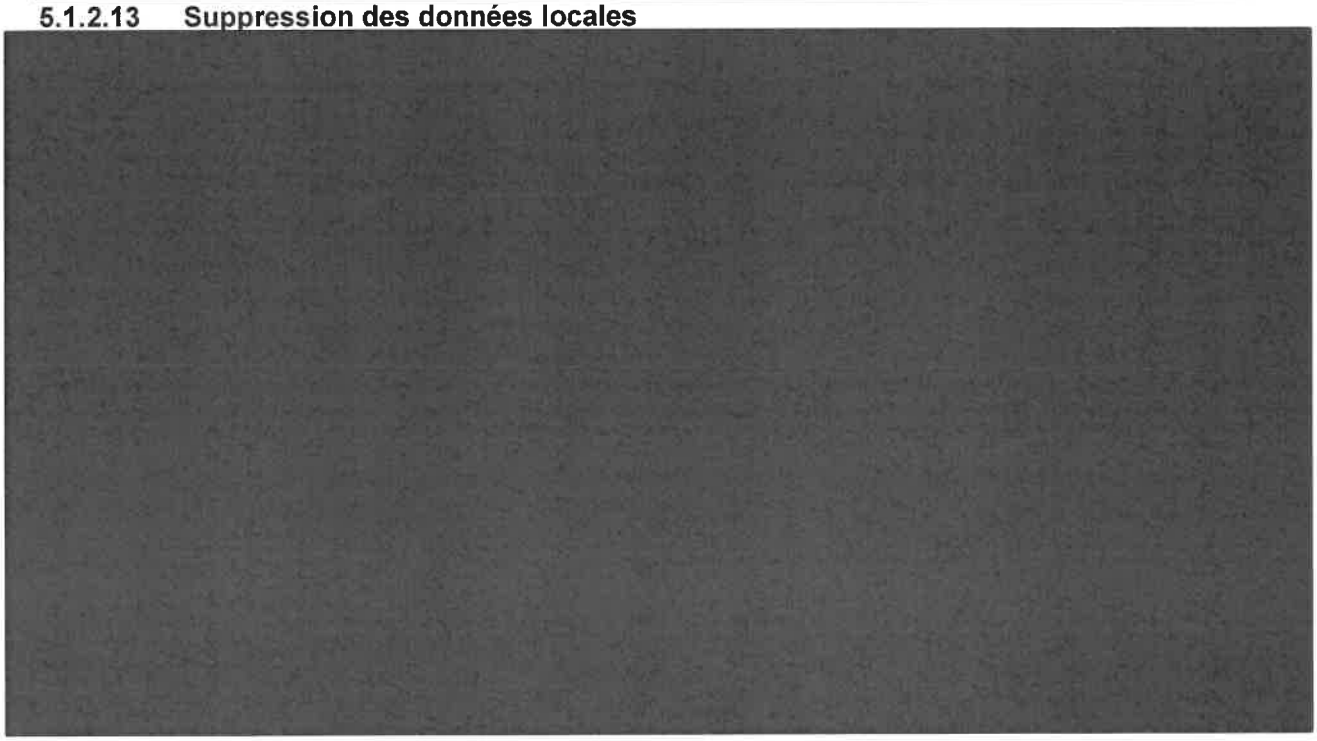
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

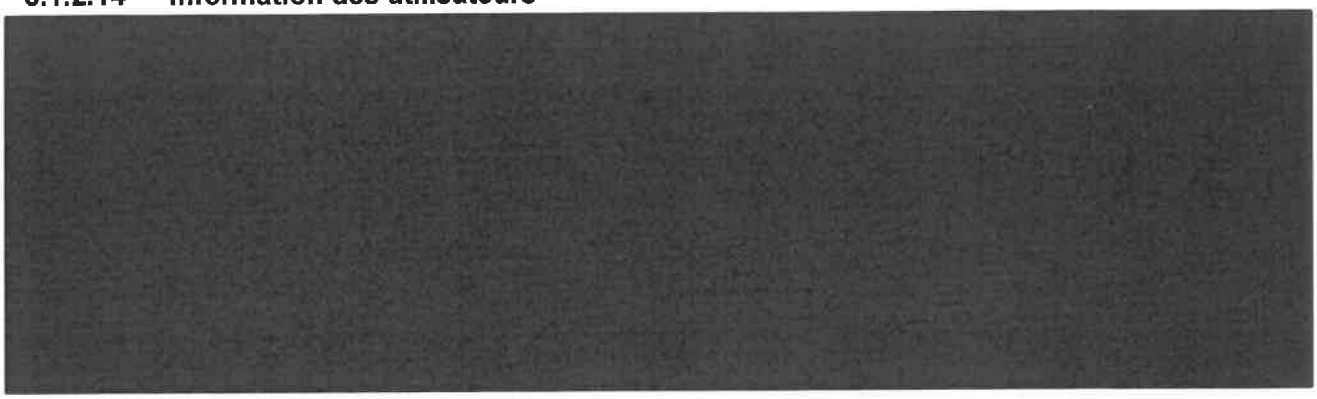


5.1.2.13 Suppression des données locales

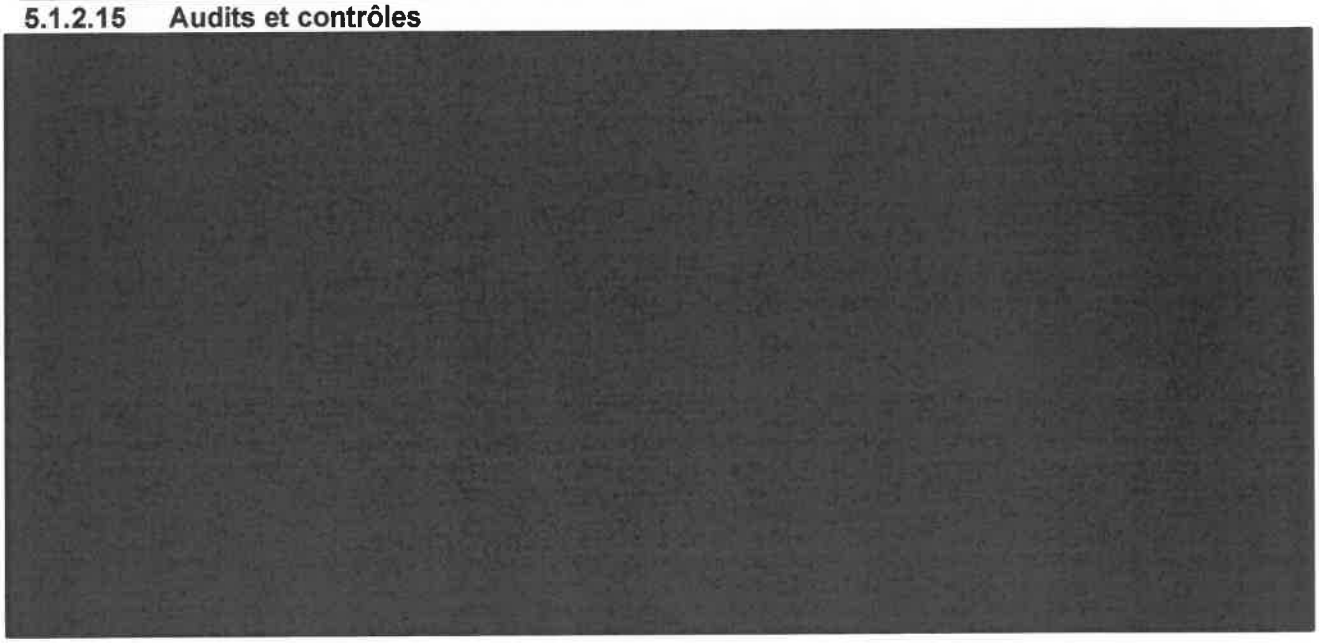


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.1.2.14 Information des utilisateurs



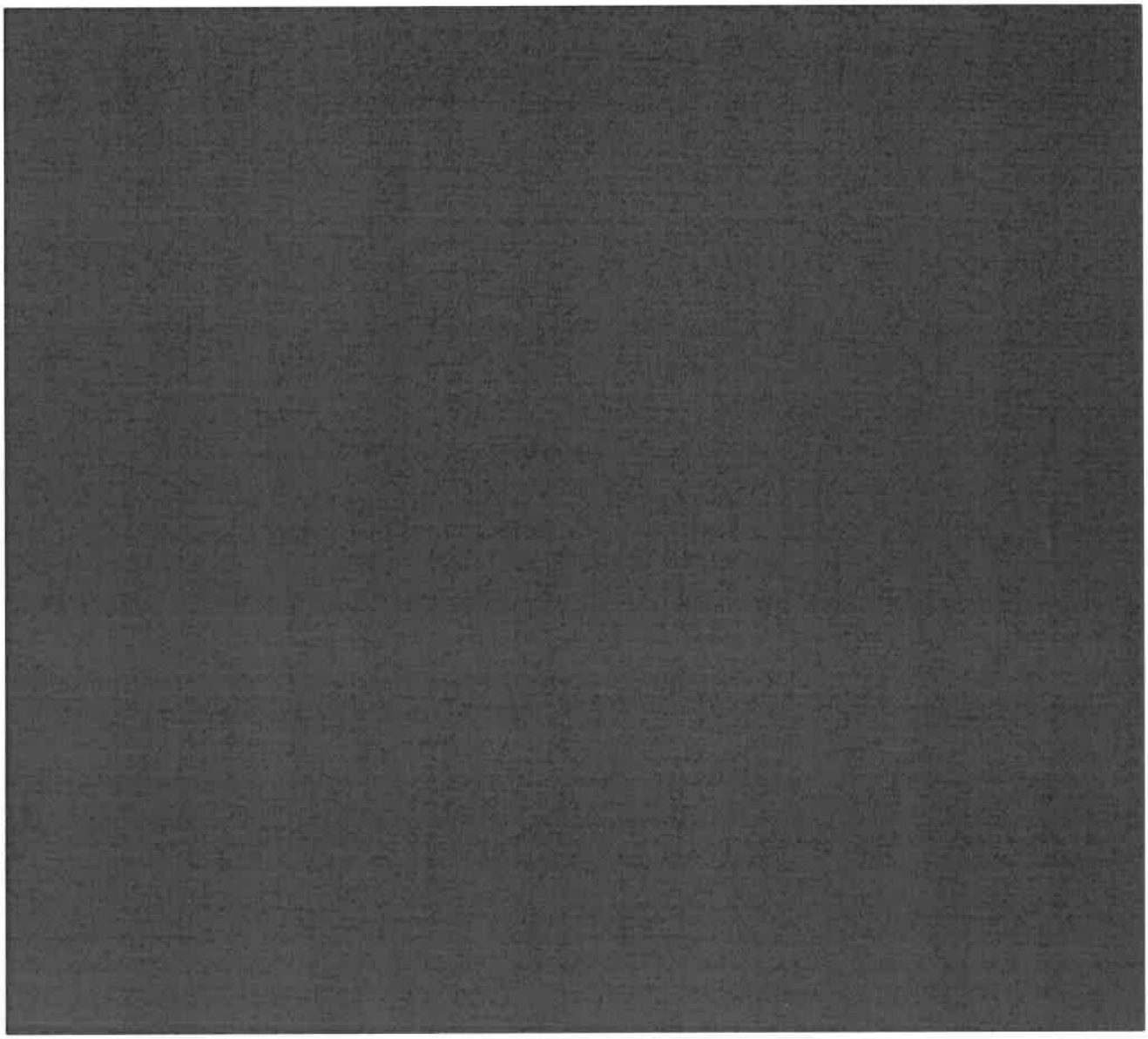
5.1.2.15 Audits et contrôles



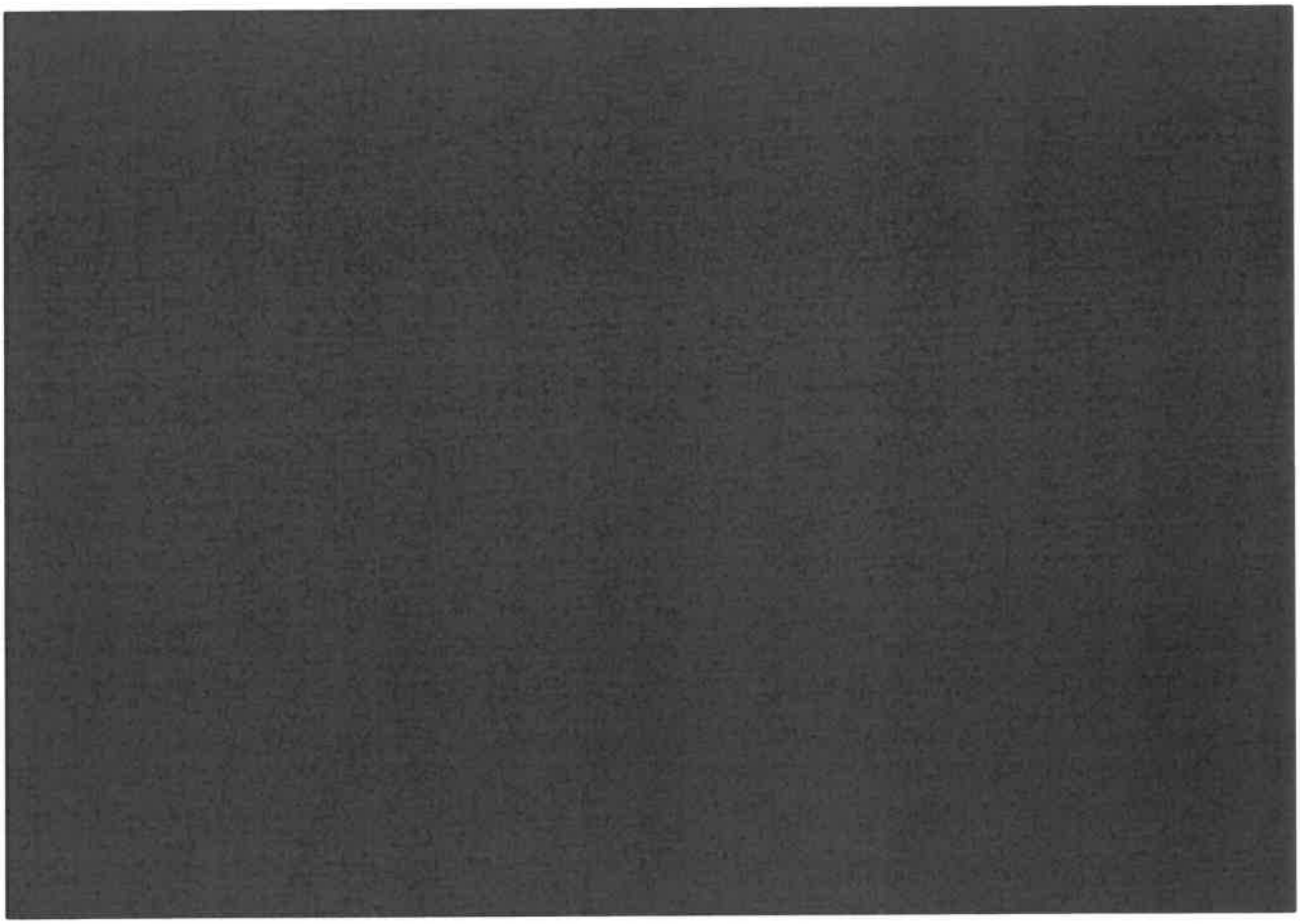
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.1.3 Risques

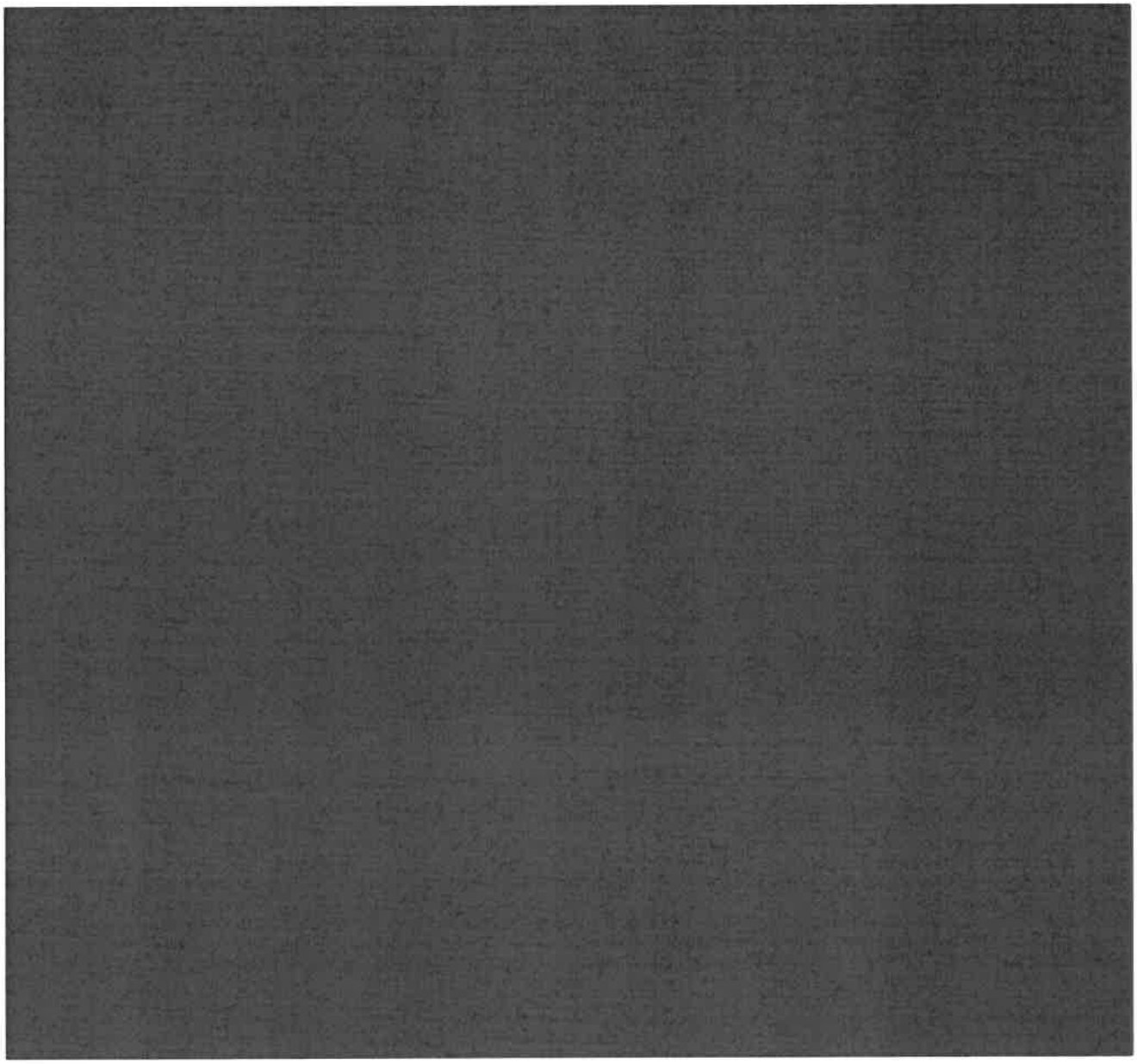
5.1.3.1 Présentation des risques



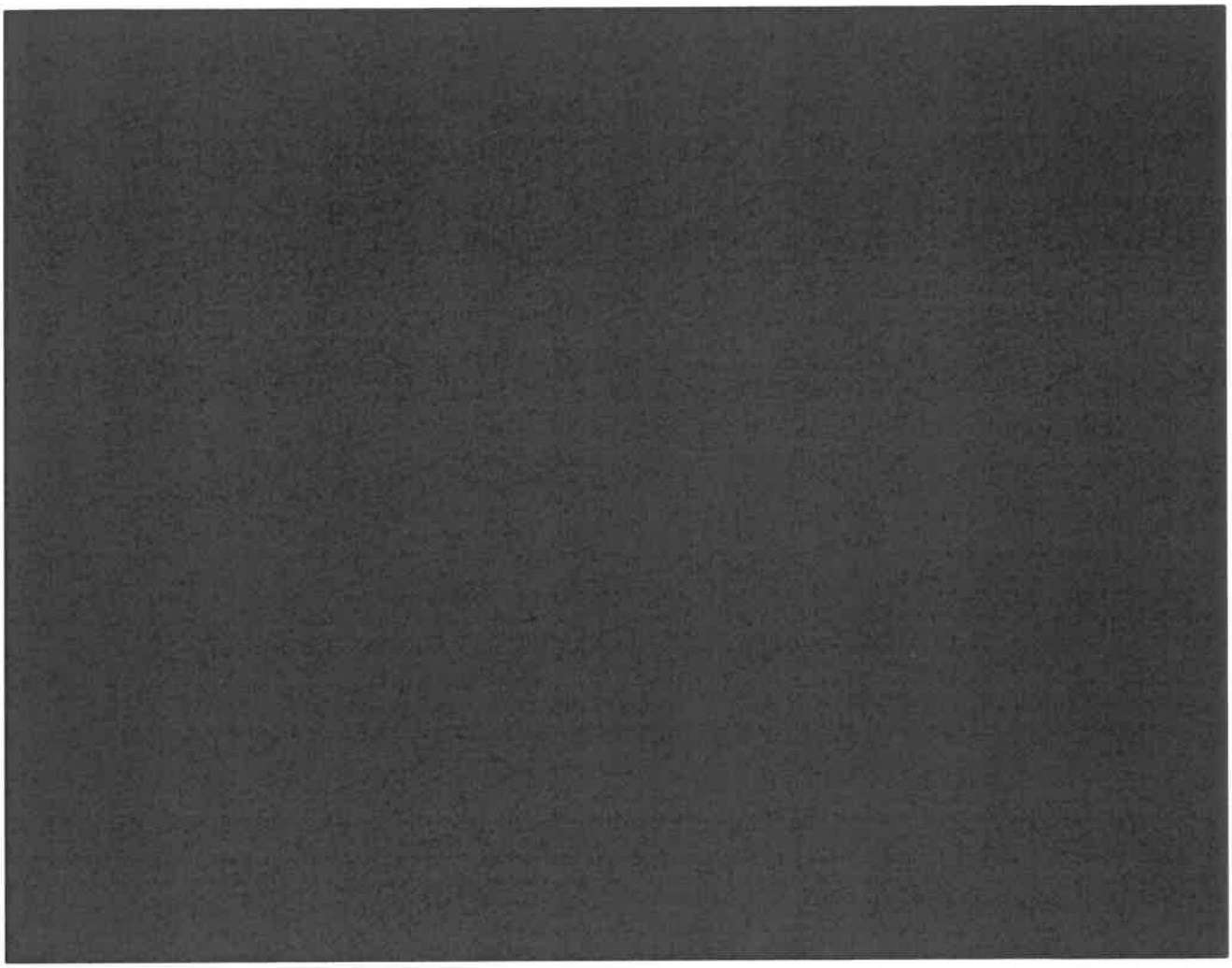
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



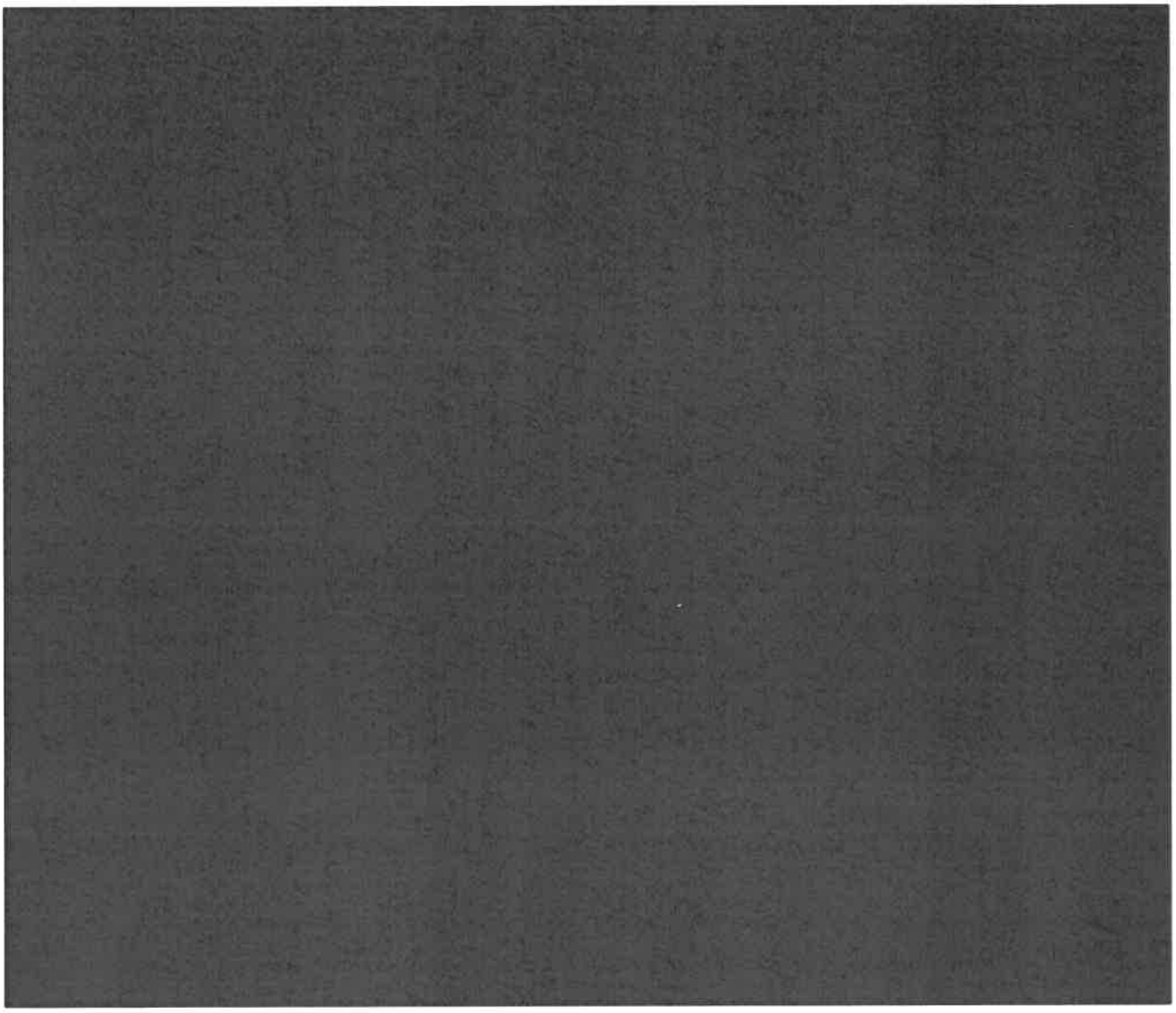
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



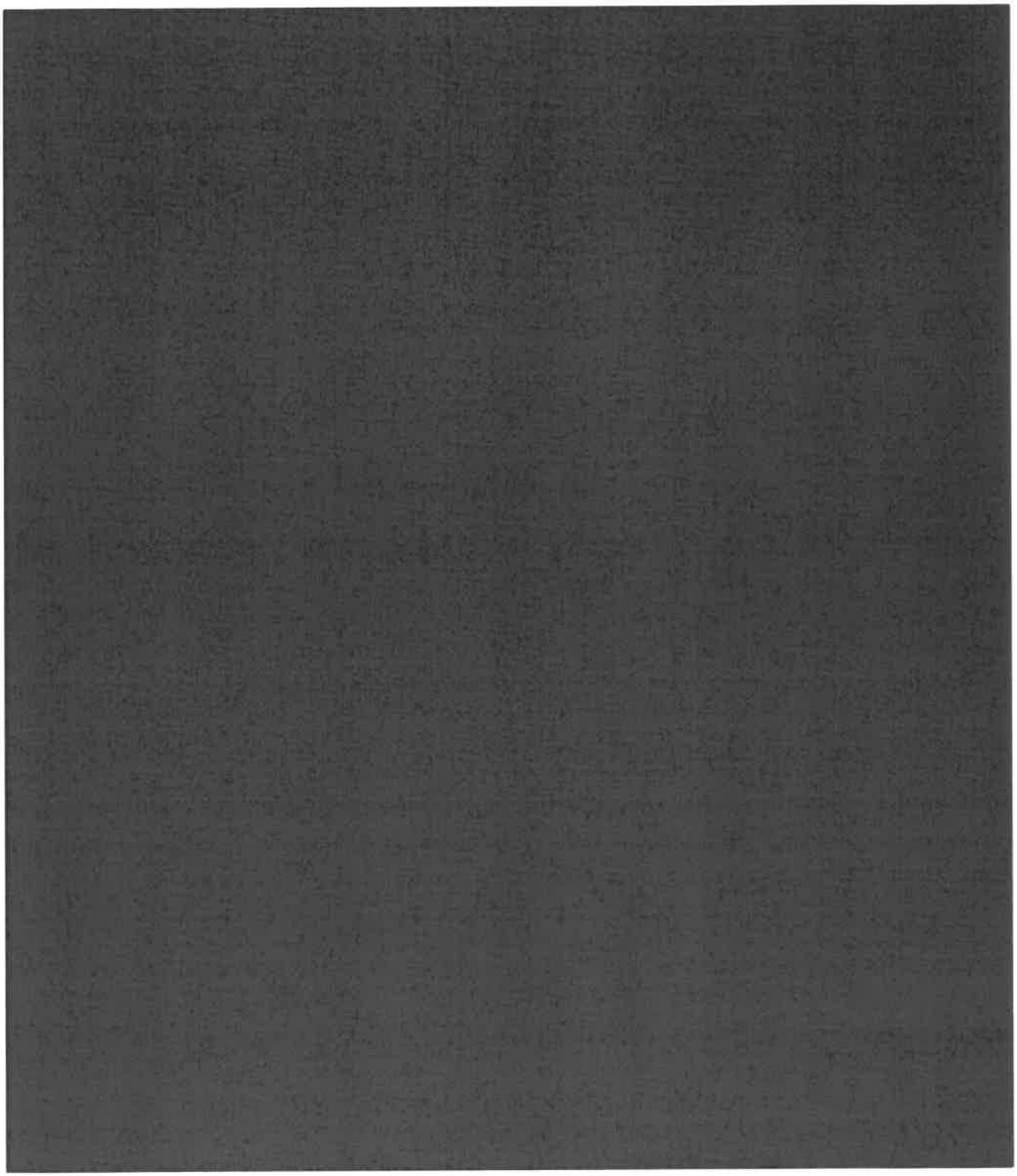
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



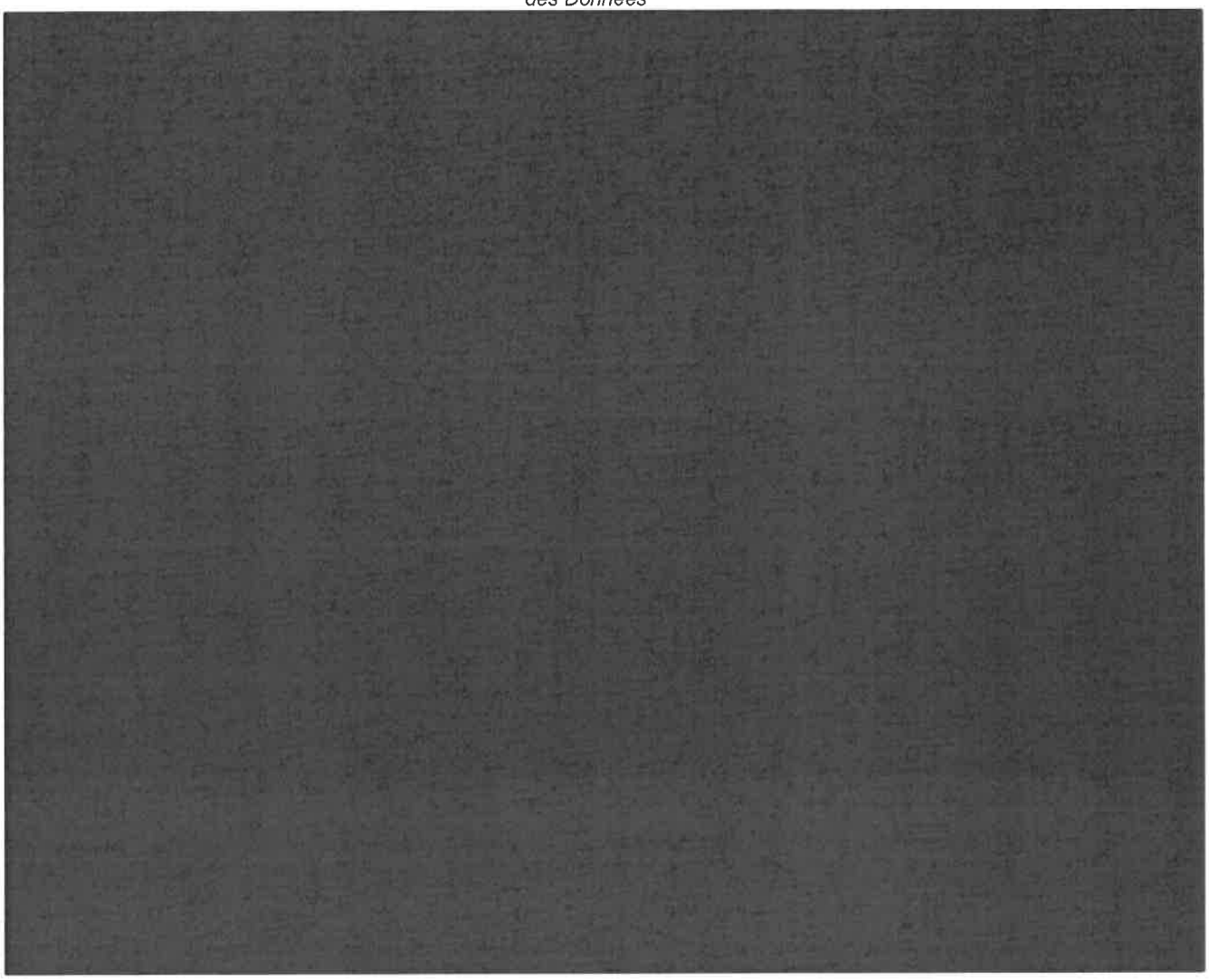
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



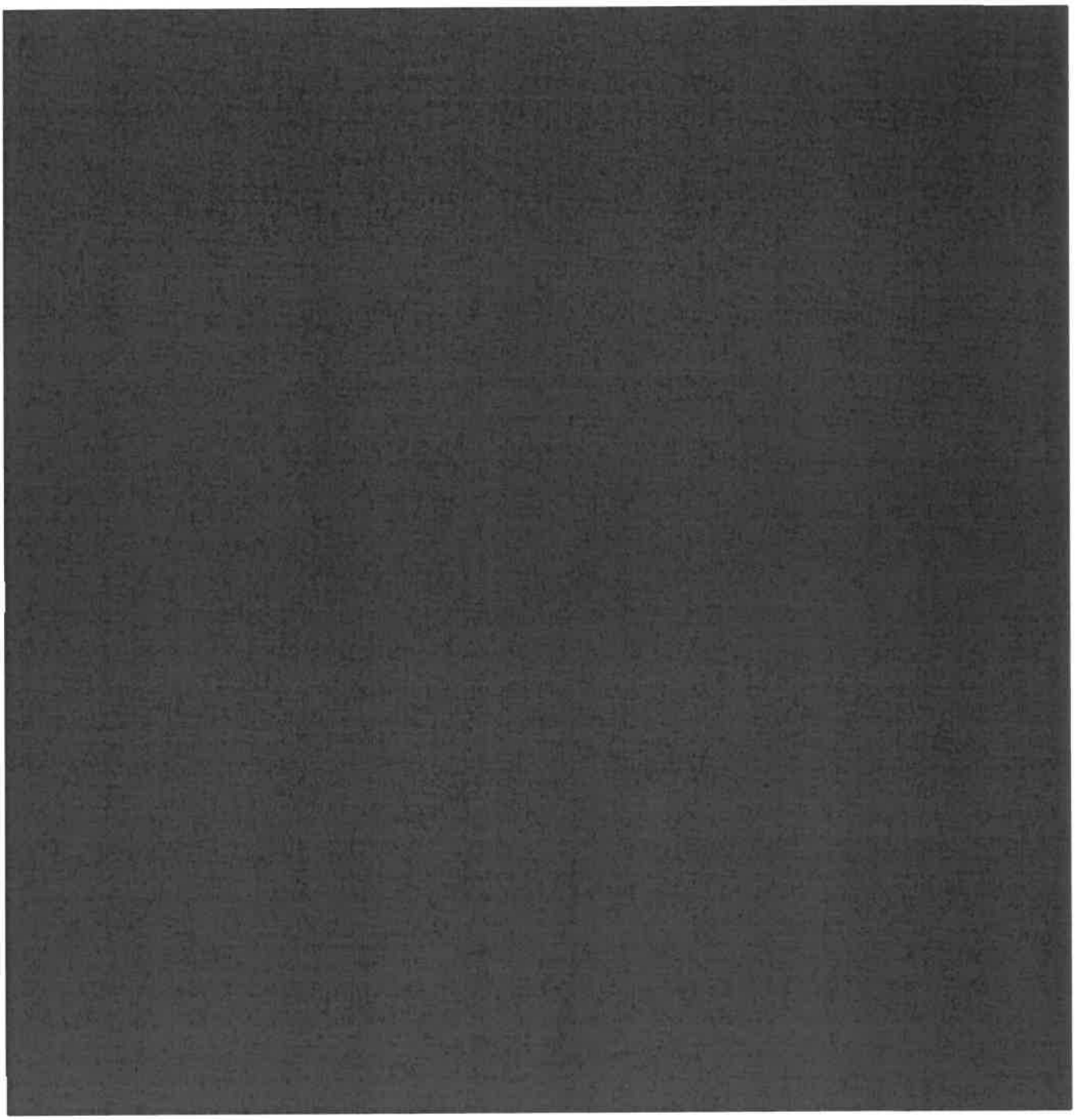
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



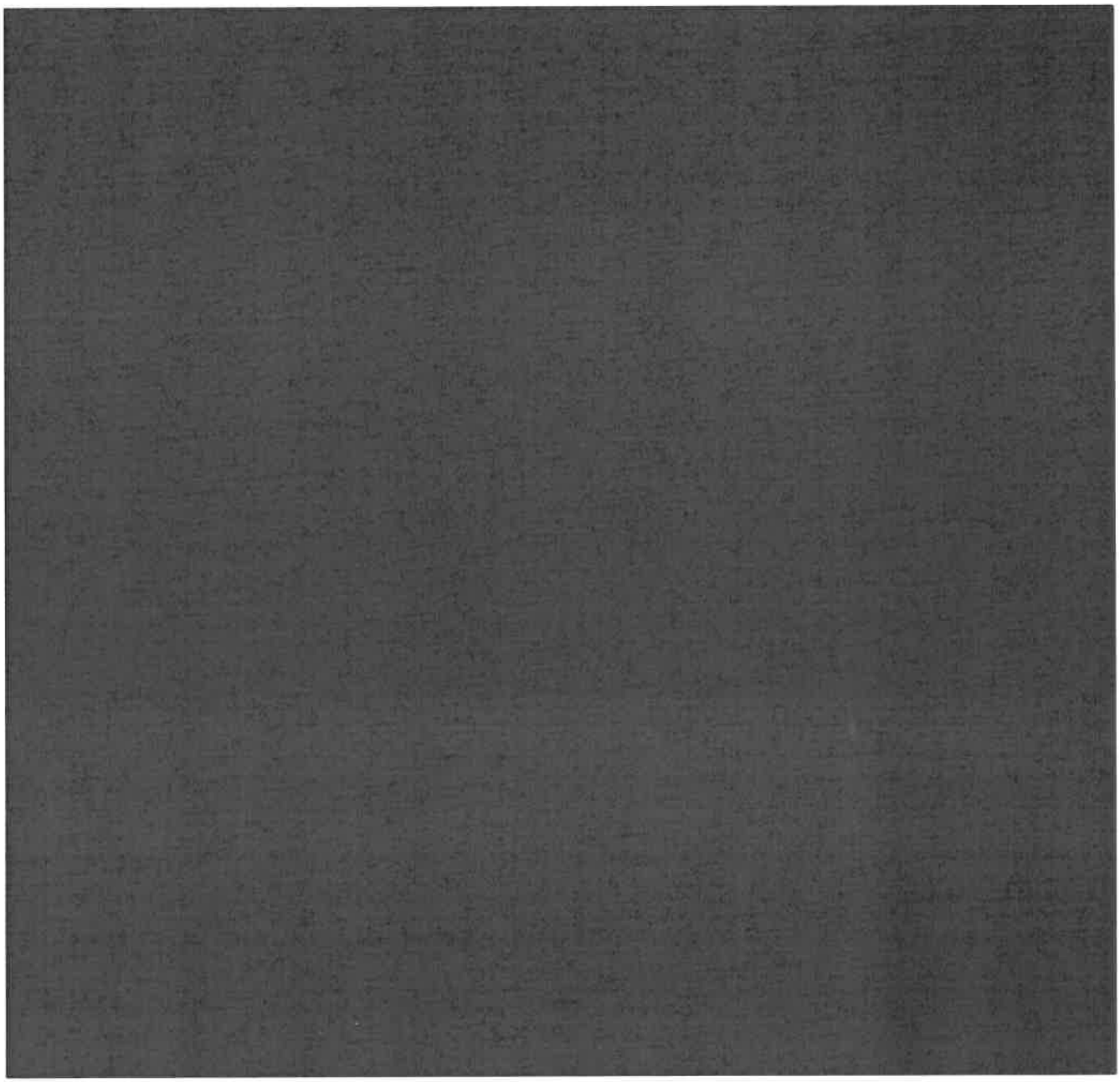
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



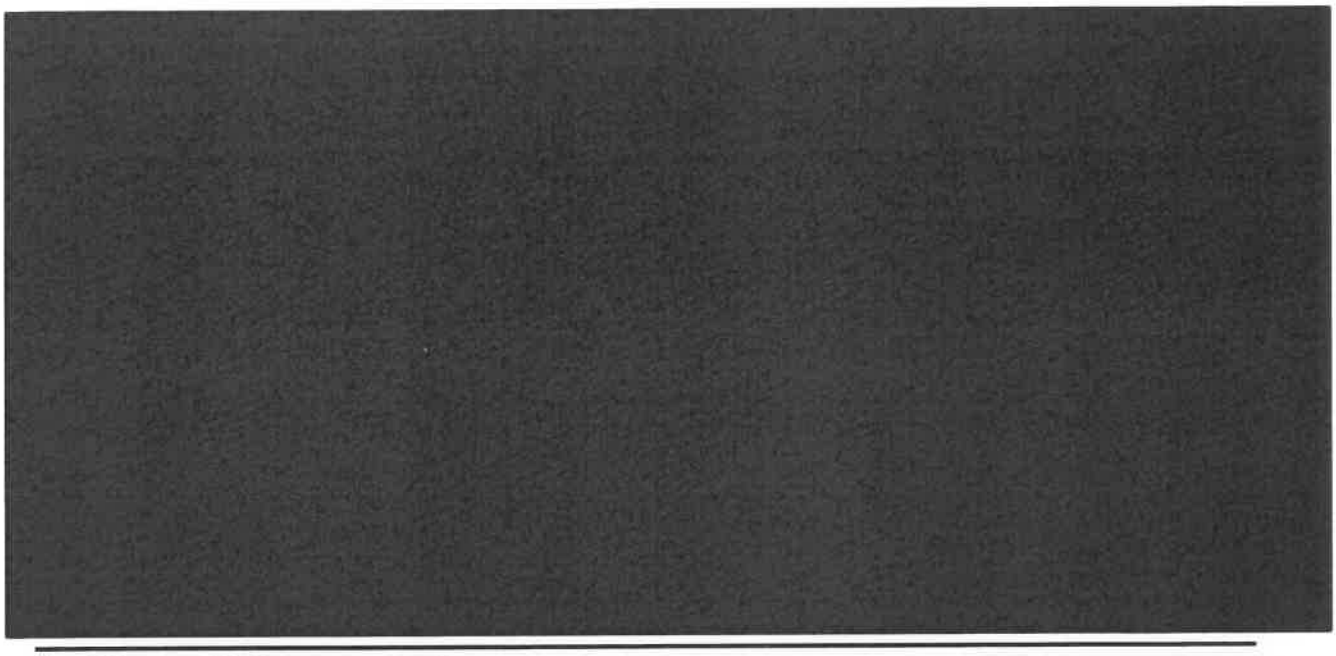
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



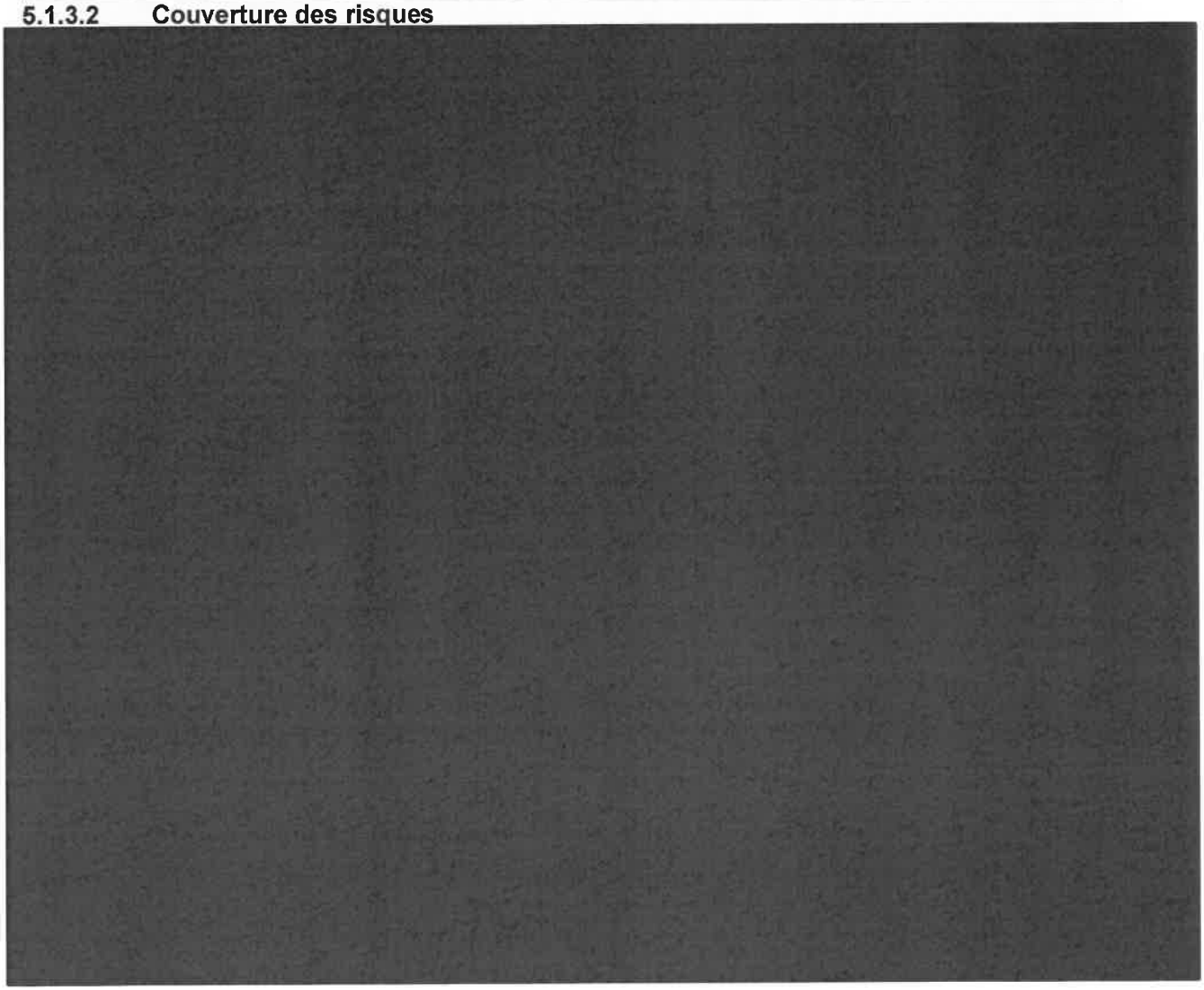
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

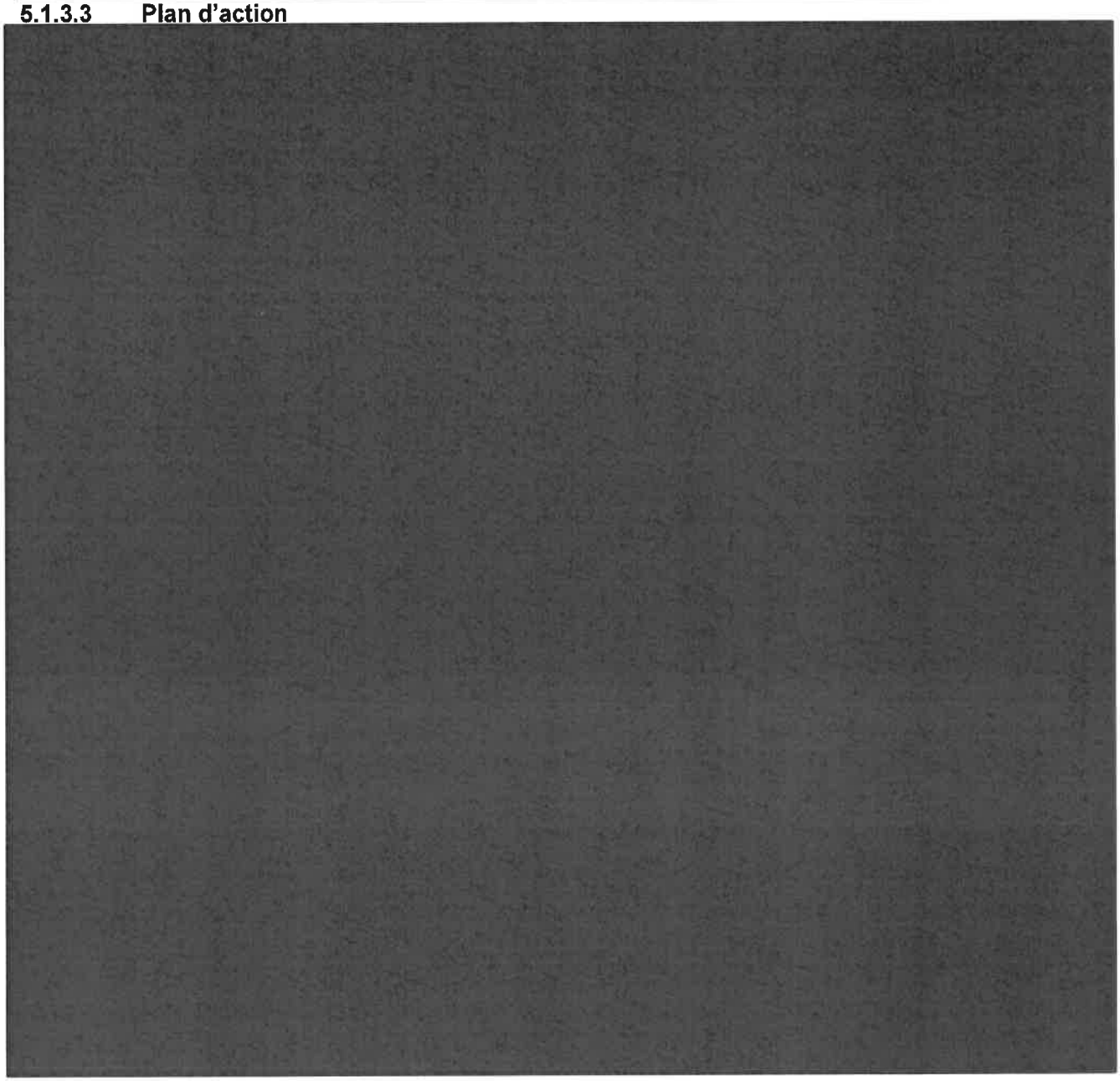


5.1.3.2 Couverture des risques

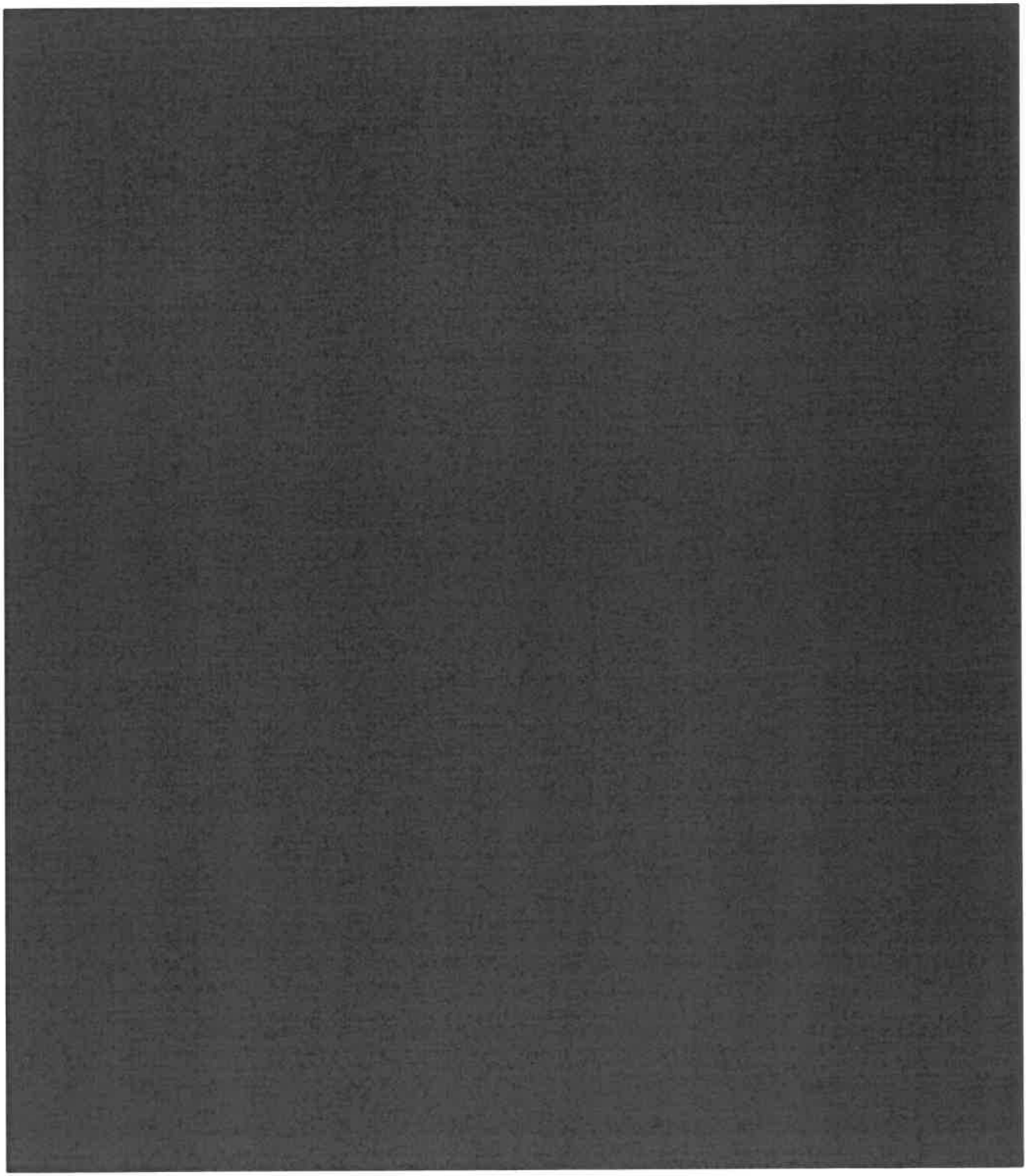


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

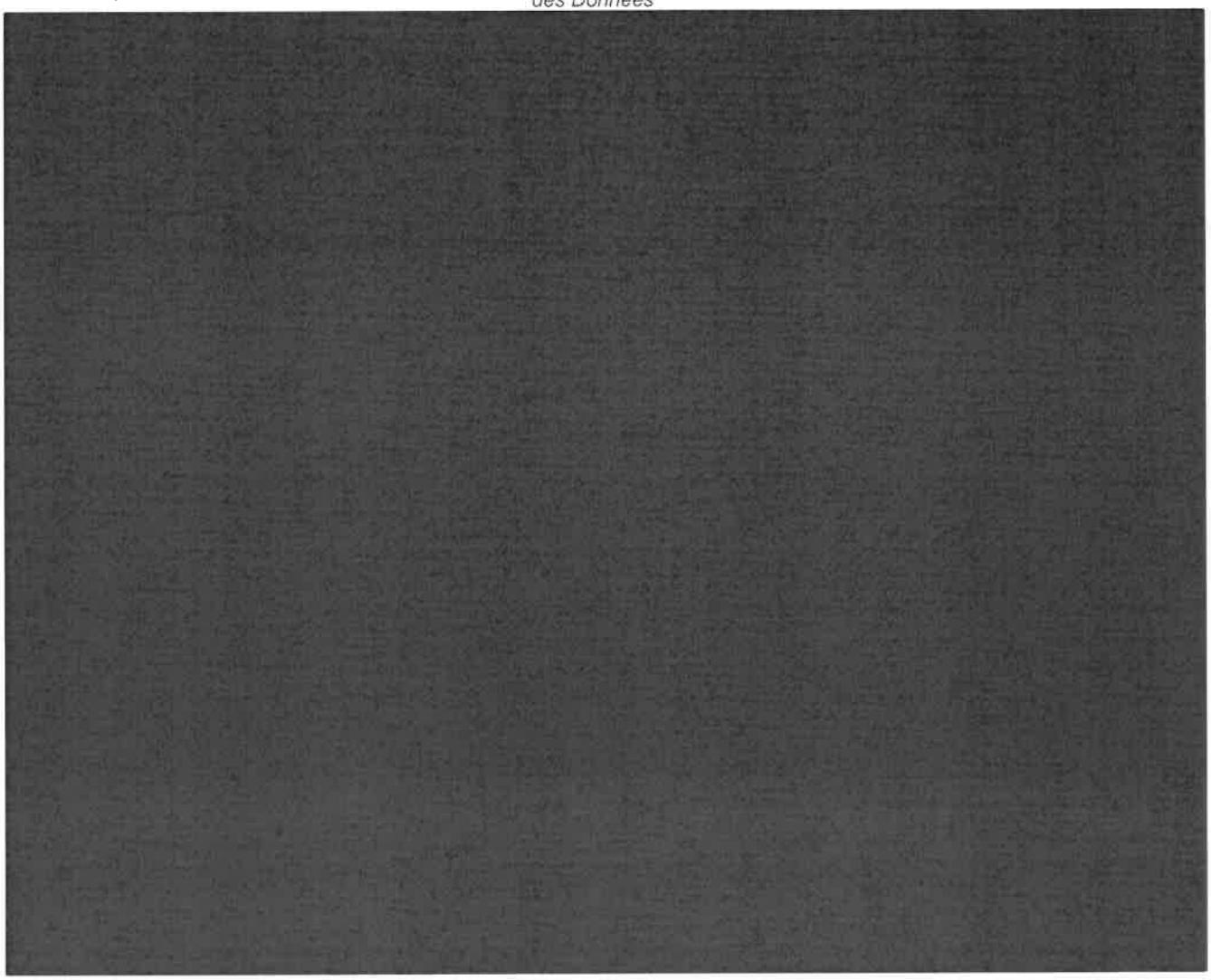
5.1.3.3 Plan d'action



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.2 SI ApCV

5.2.1 Présentation du SI ApCV

5.2.1.1 Hébergement

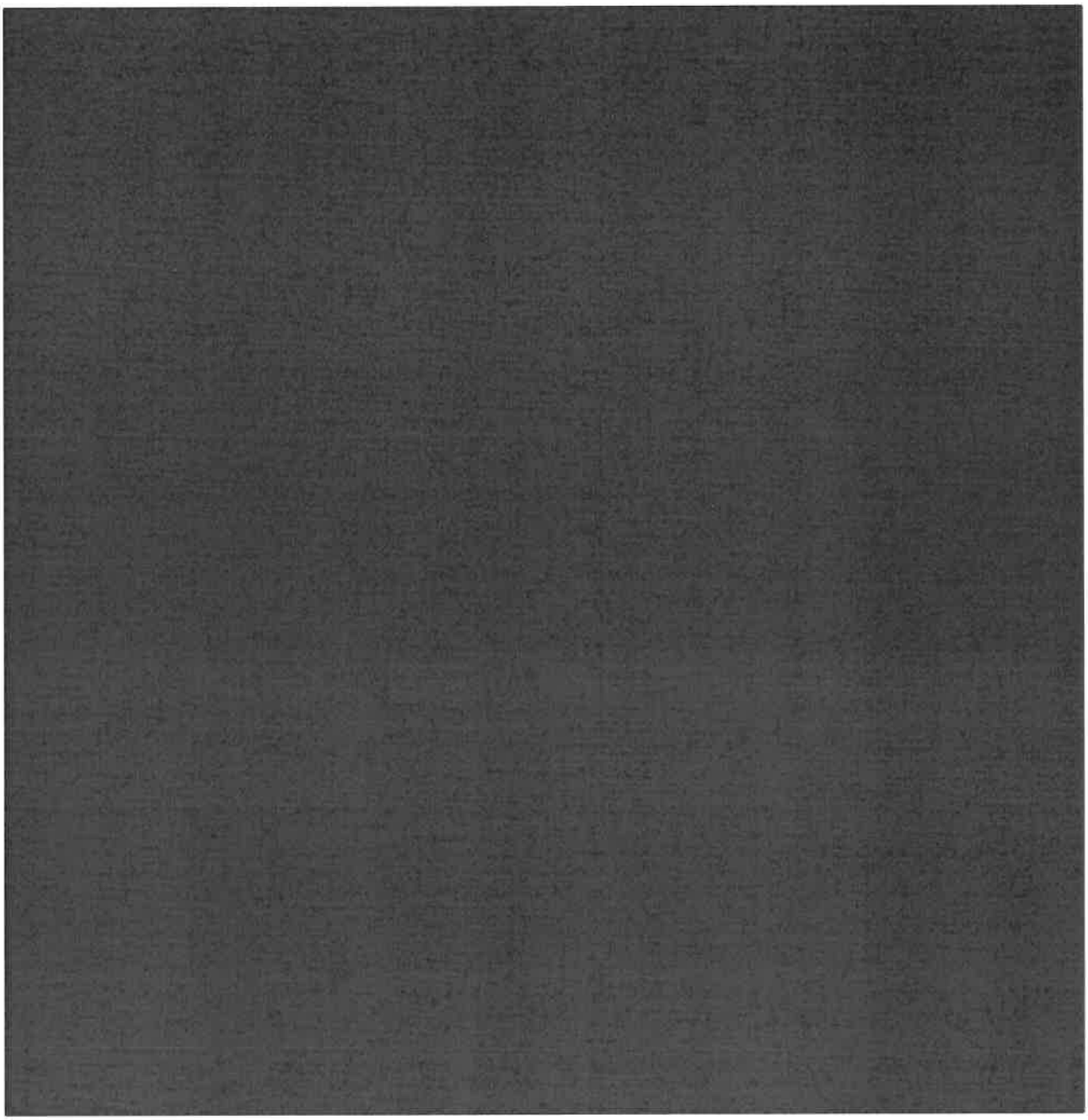
Le SI ApCV est hébergé et infogéré par [redacted]

[redacted] fournit un PAS précisant ses engagements sécurité sur le périmètre ApCV. L'application effective du PAS et son efficacité font l'objet de vérifications et d'un suivi durant les phases de transition et d'exploitation. La dernière version du PAS est revue et mise à jour a minima annuellement et chaque fois qu'il apparaît, après concertation entre [redacted] et le GIE SV, que la version applicable ne permet plus de répondre aux besoins du projet (évolutions du contexte).

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.2.1.2 Architecture globale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.2.1.3 Environnements

[redacted]

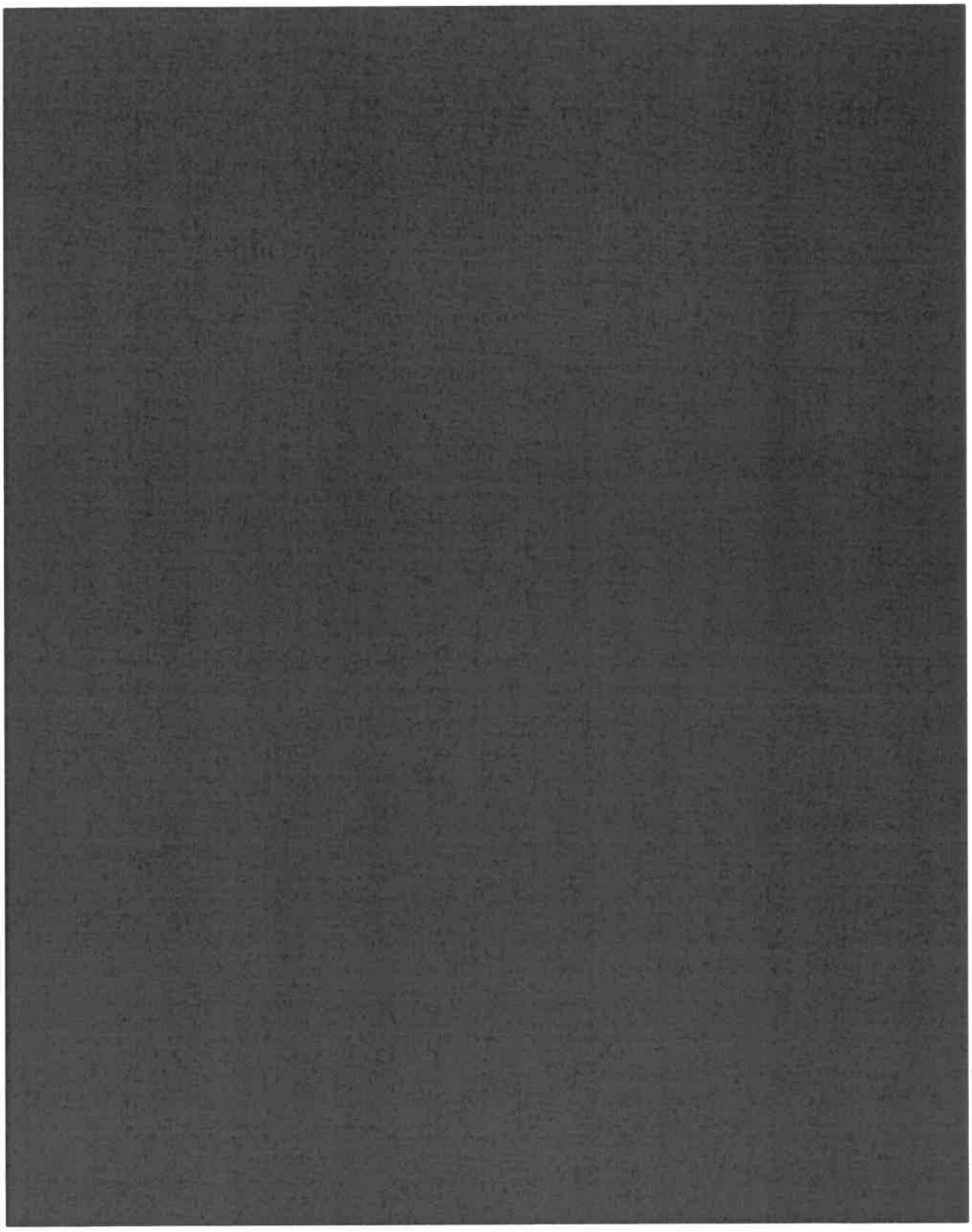
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.2.1.4 Gestion des traces

[redacted]

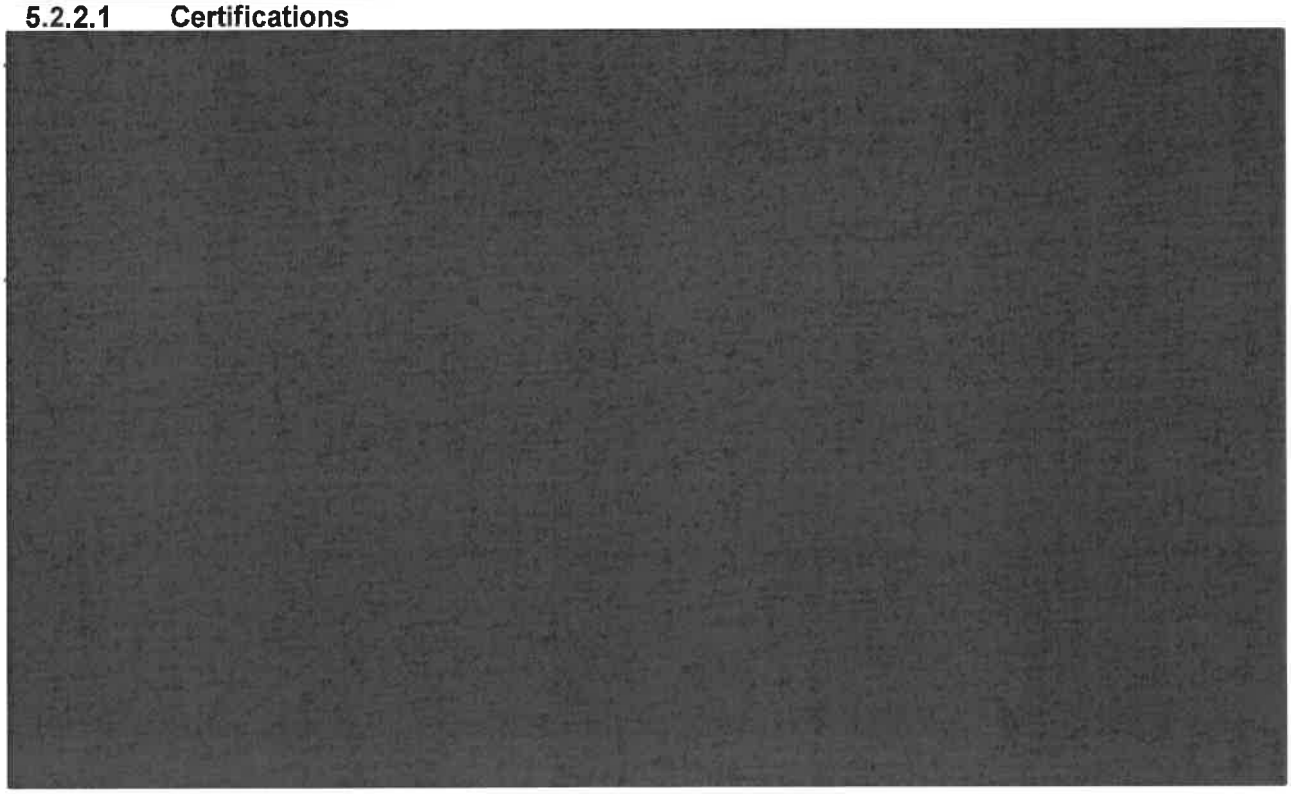
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



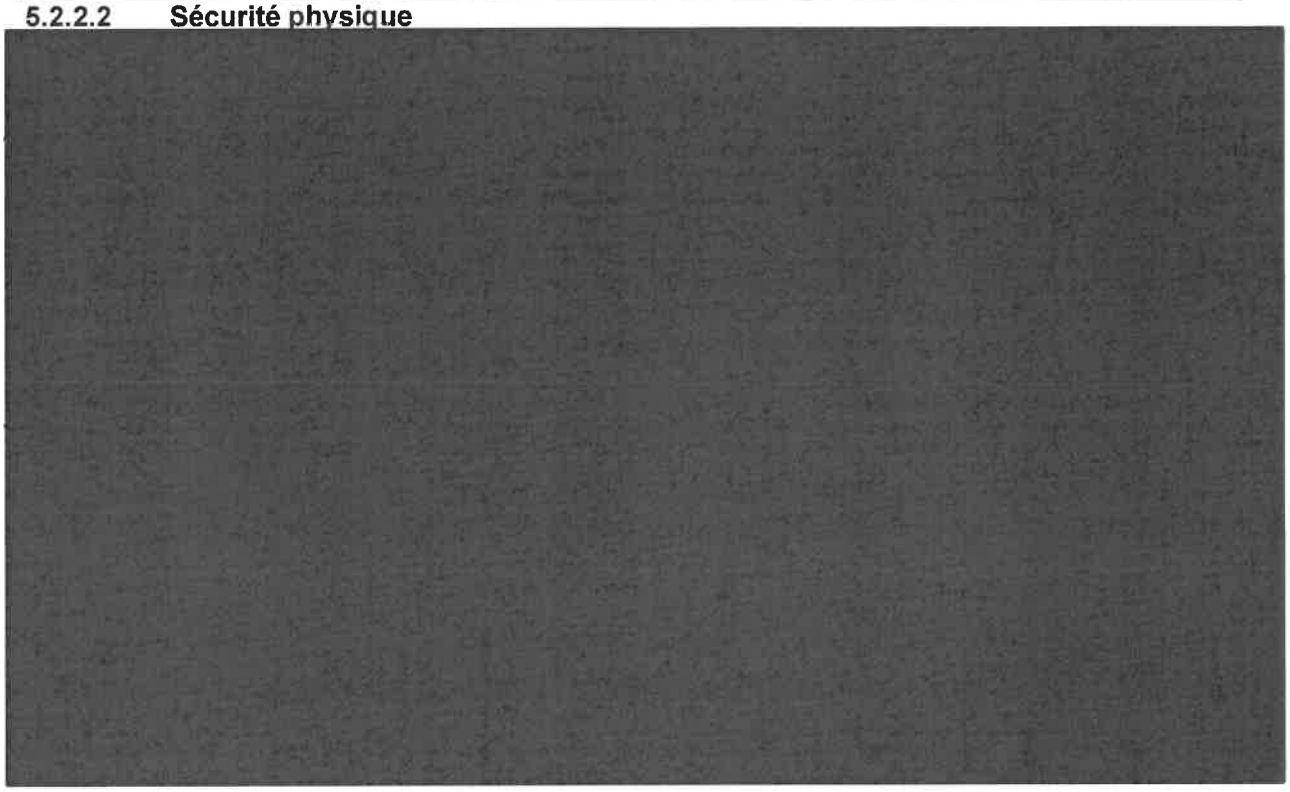
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.2.2 Mesures de sécurité

5.2.2.1 Certifications

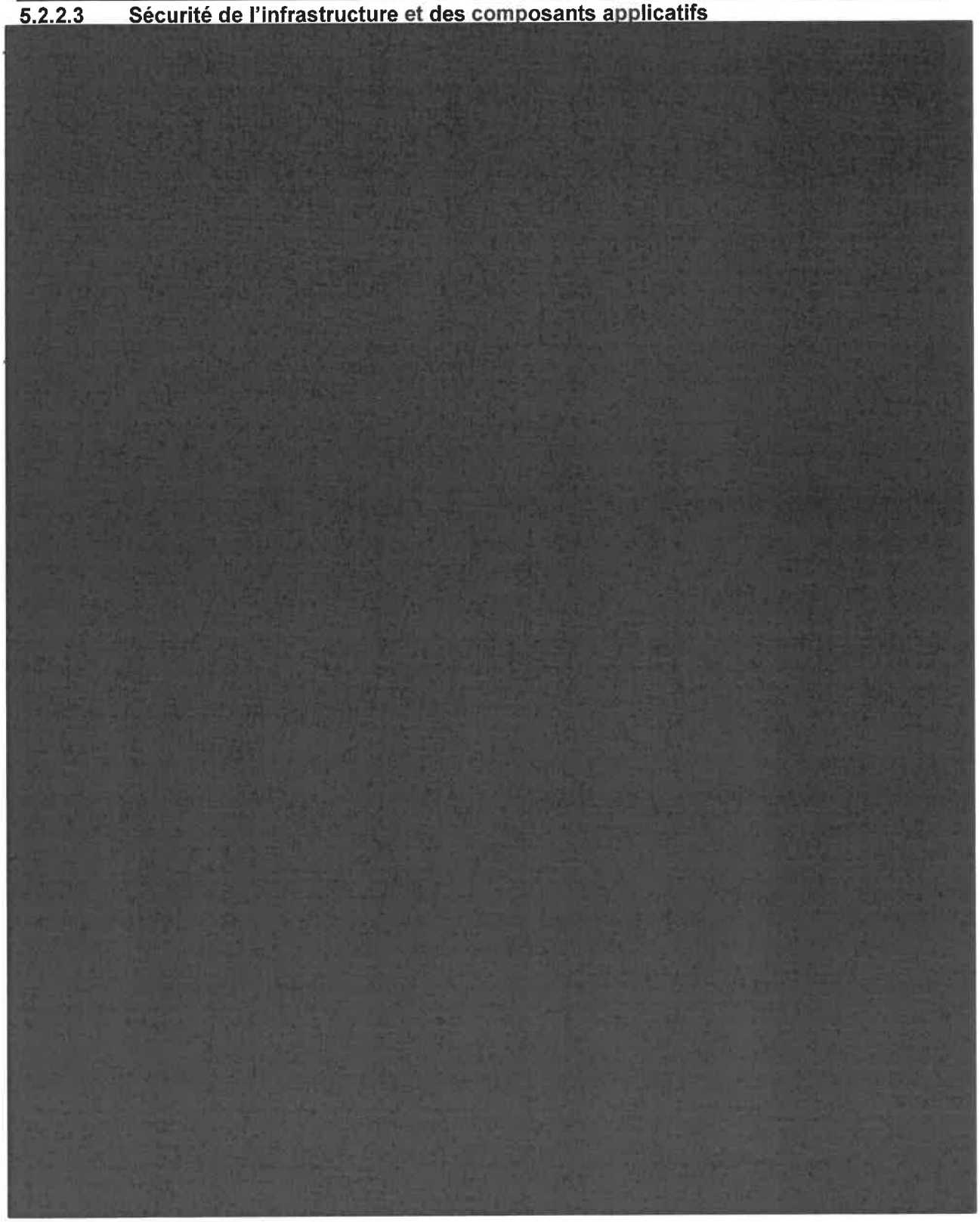


5.2.2.2 Sécurité physique



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.2.2.3 Sécurité de l'infrastructure et des composants applicatifs



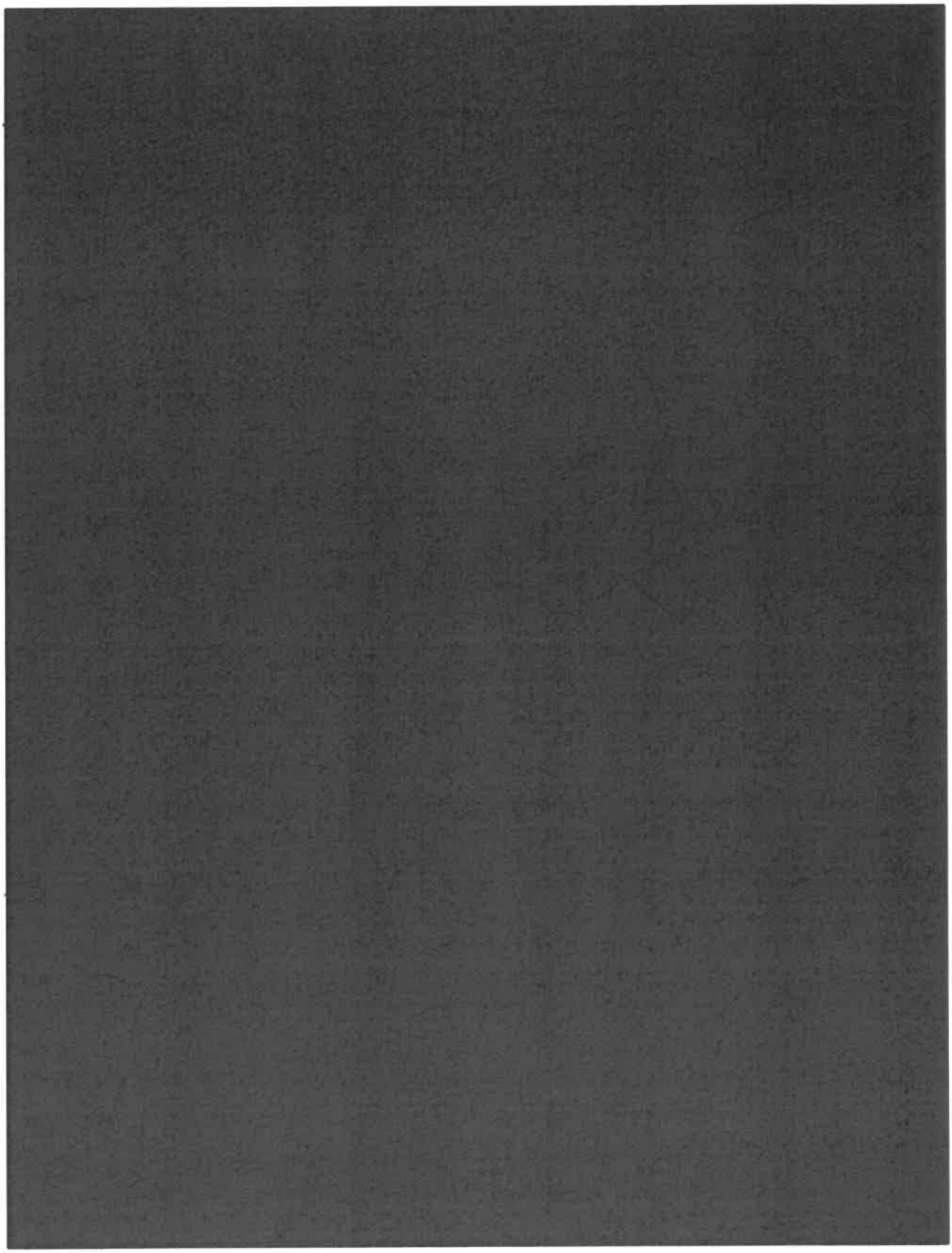
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.2.2.4 Sécurité des données métier

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.2.2.5 Sécurité du développement

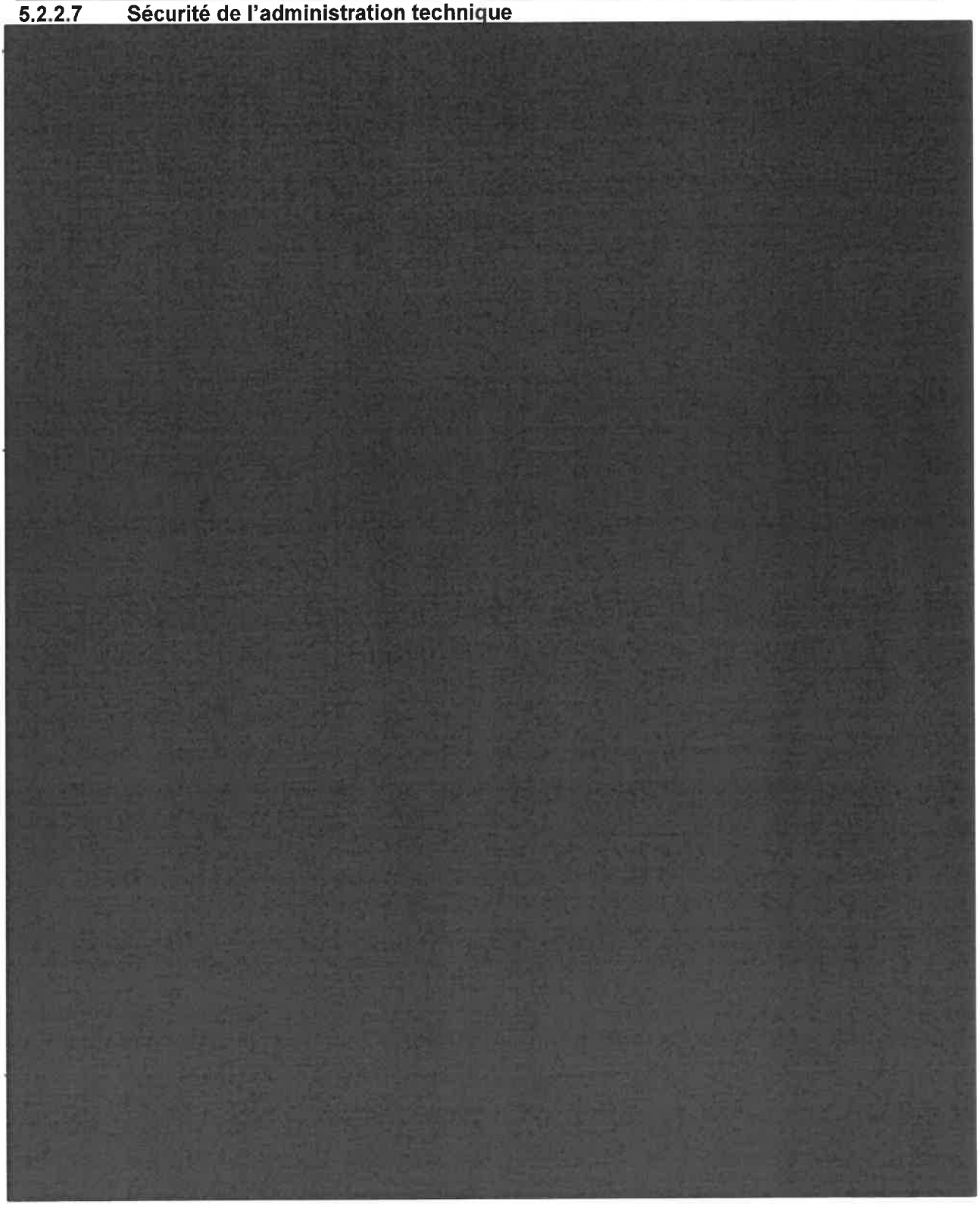
[redacted]

5.2.2.6 Sécurité des clés cryptographiques

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.2.2.7 Sécurité de l'administration technique



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.2.2.8 Sécurité de l'administration fonctionnelle

[redacted]

5.2.2.9 Supervision sécurité de l'infrastructure

[redacted]

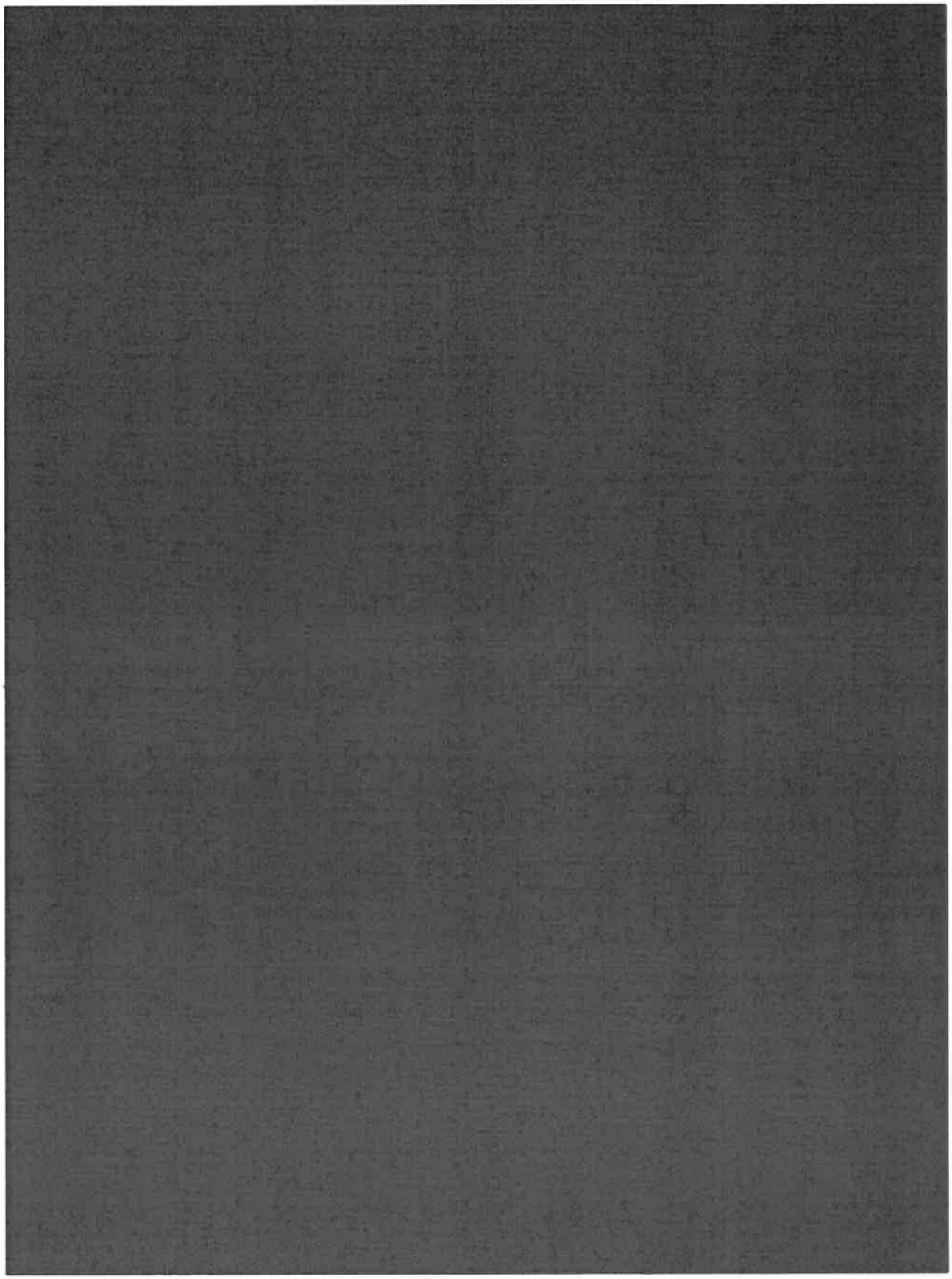
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.2.2.10 Gestion des incidents de sécurité

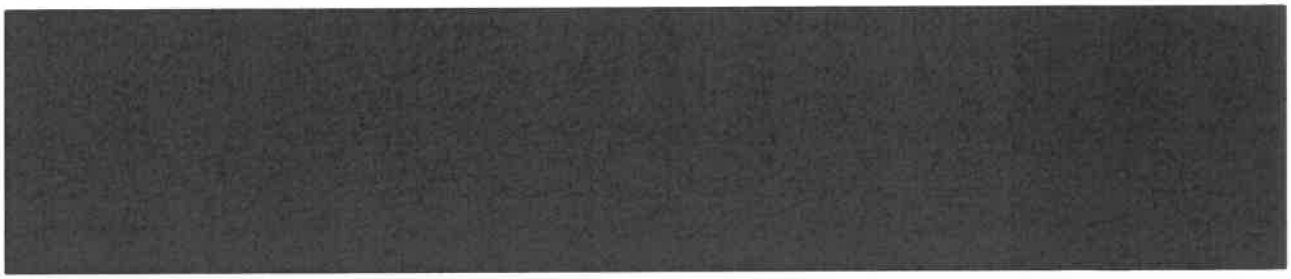
[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

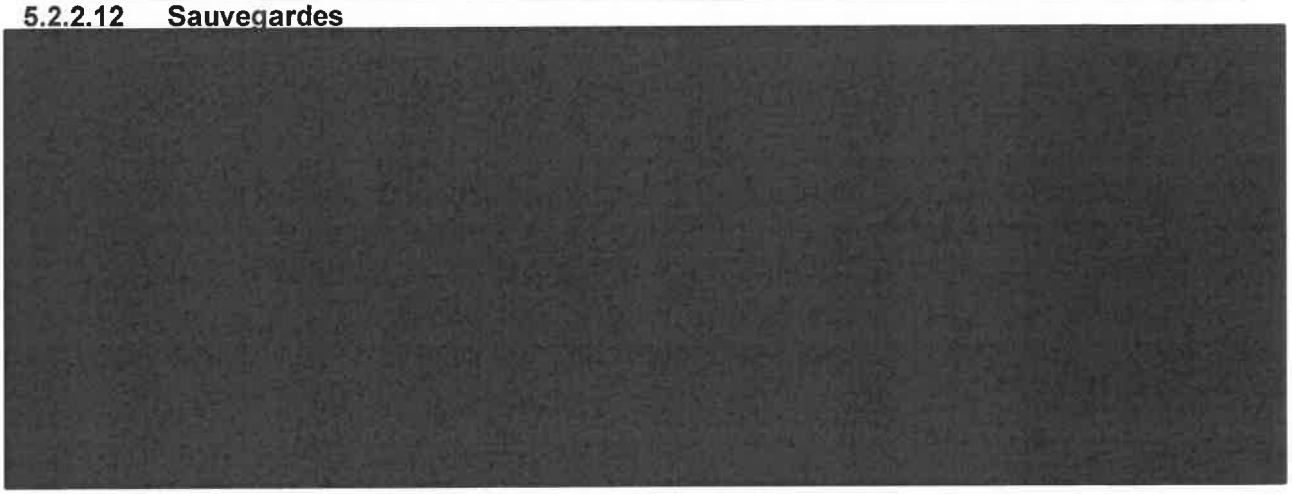


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

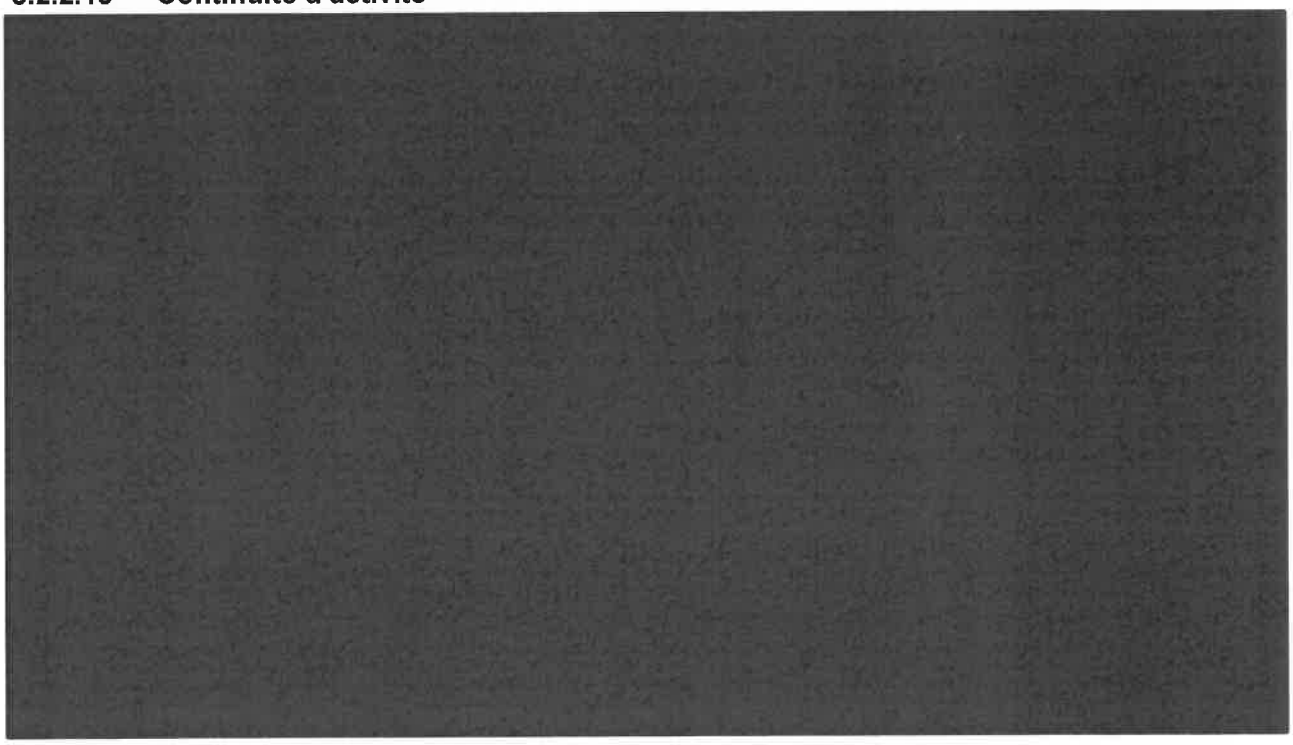
5.2.2.11 Surveillance des transactions



5.2.2.12 Sauvegardes



5.2.2.13 Continuité d'activité



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

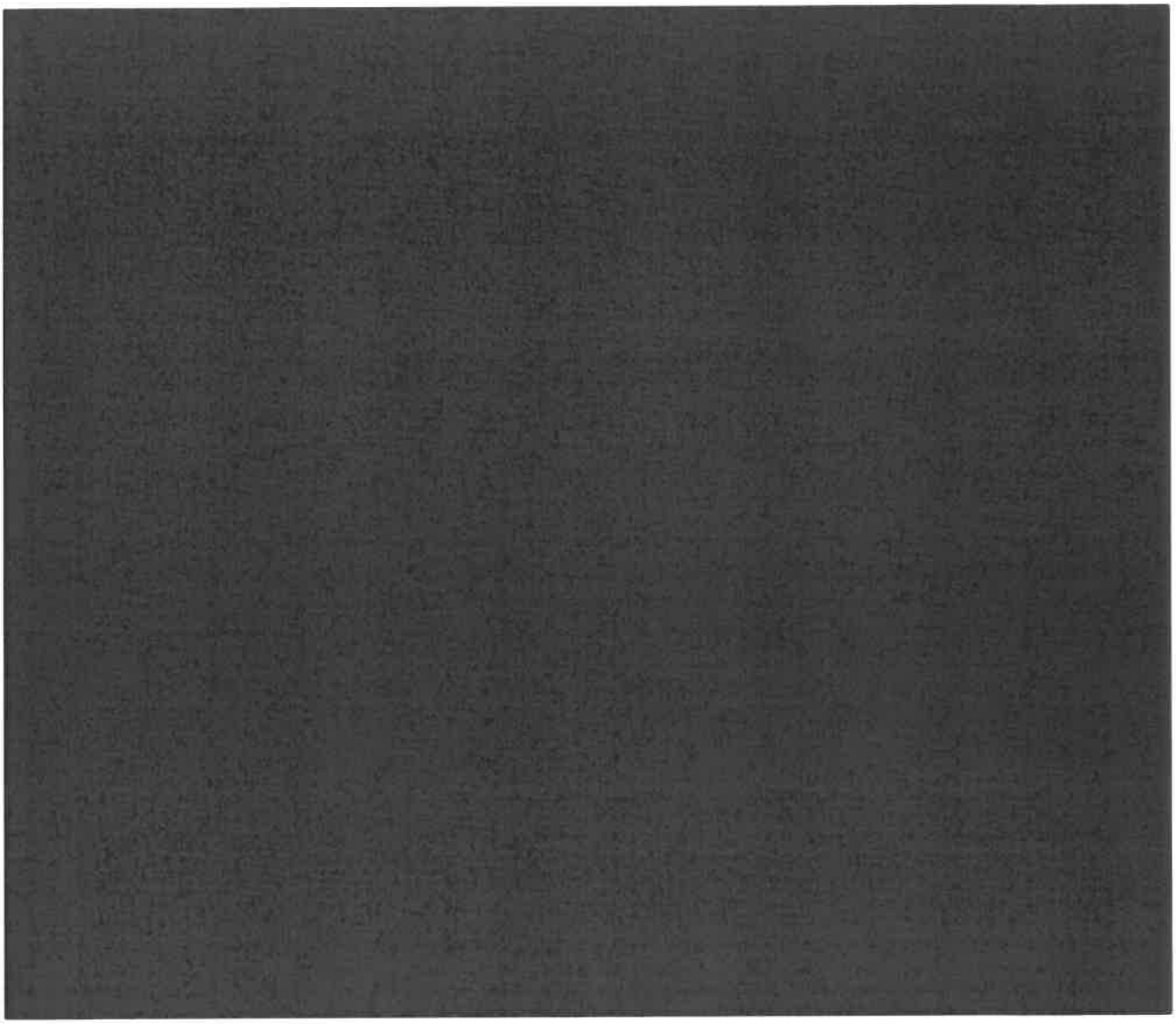
5.2.2.14 Audits et contrôles

[redacted]

5.2.2.15 Synthèse des mesures de sécurité

[redacted]

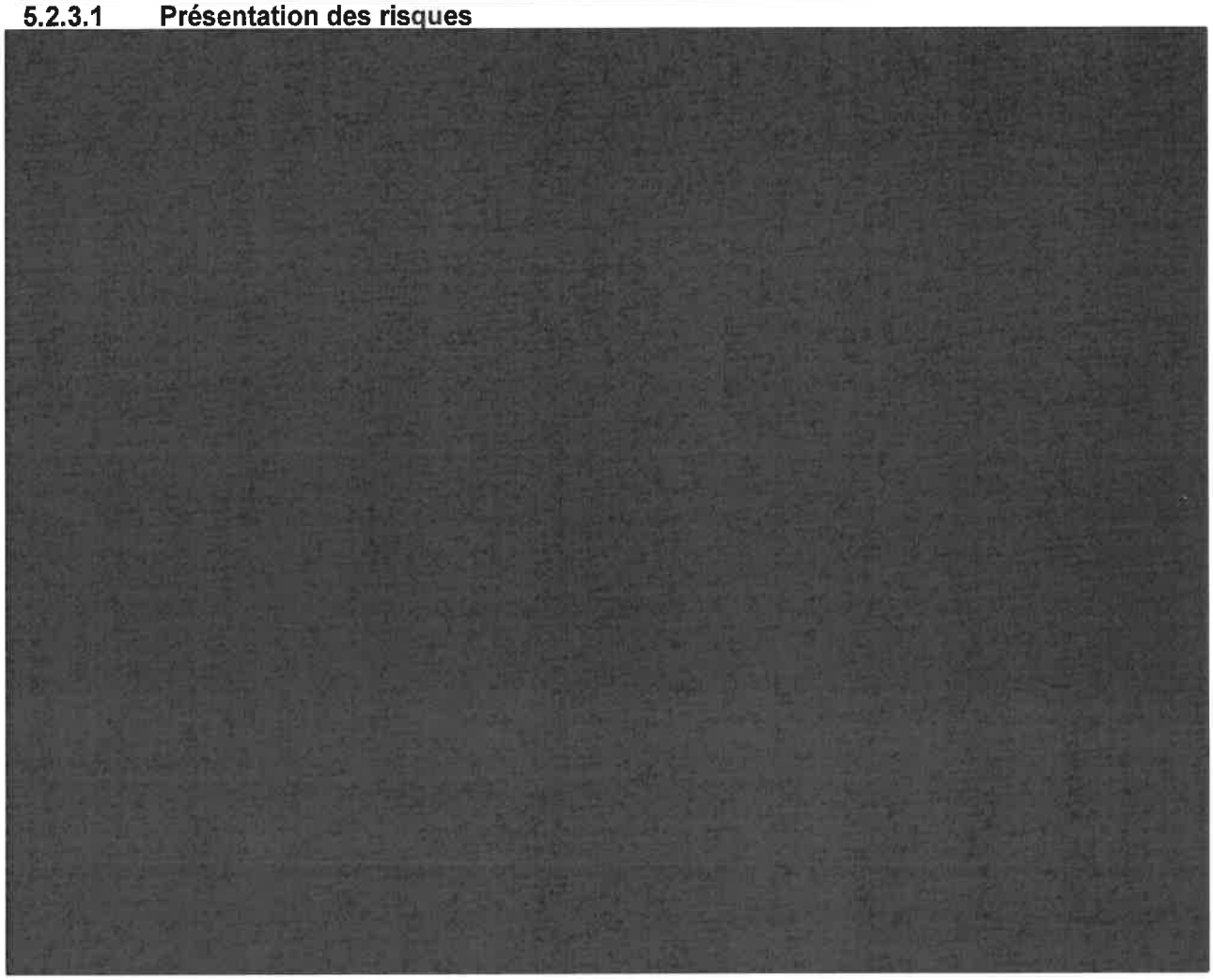
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



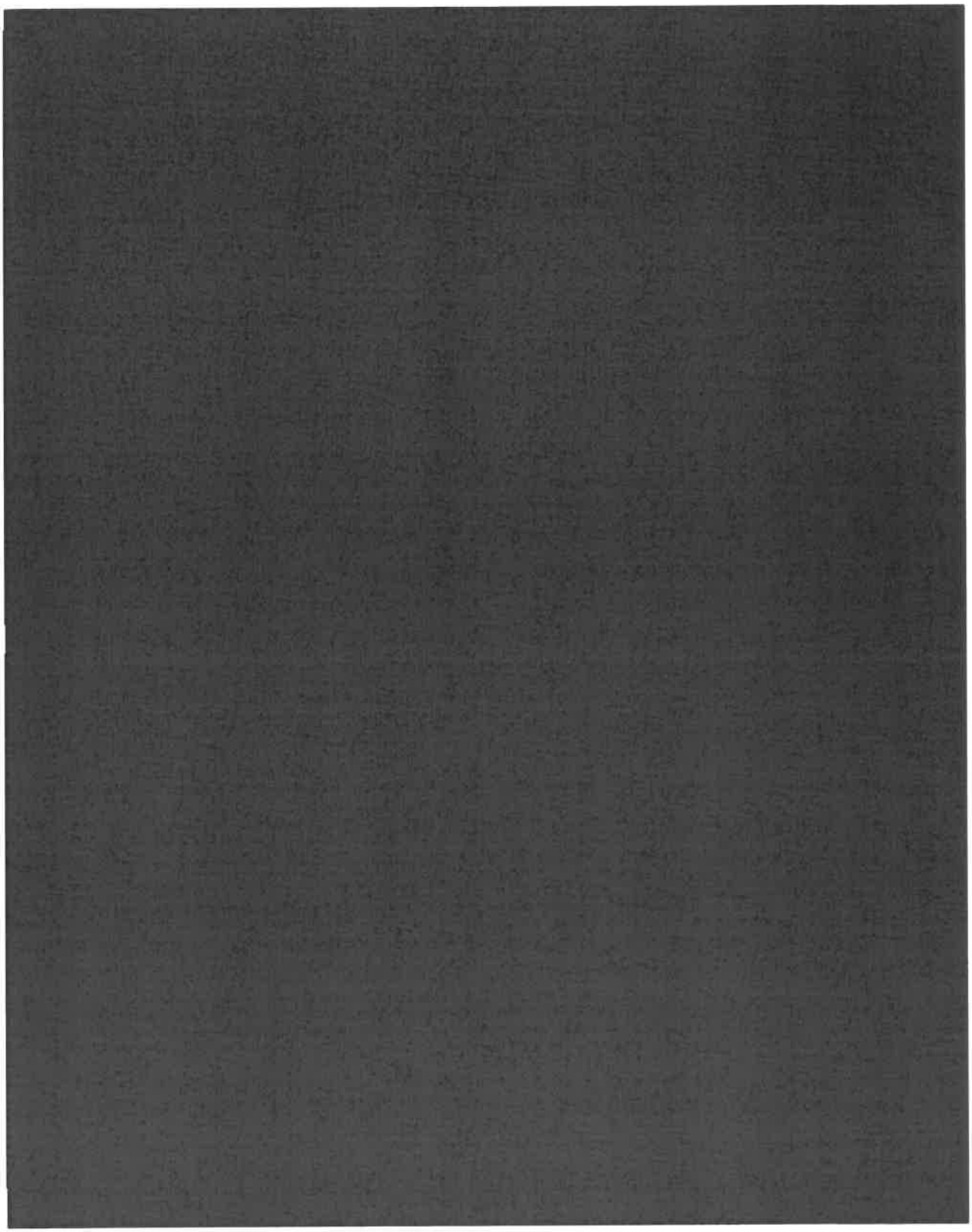
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.2.3 Risques

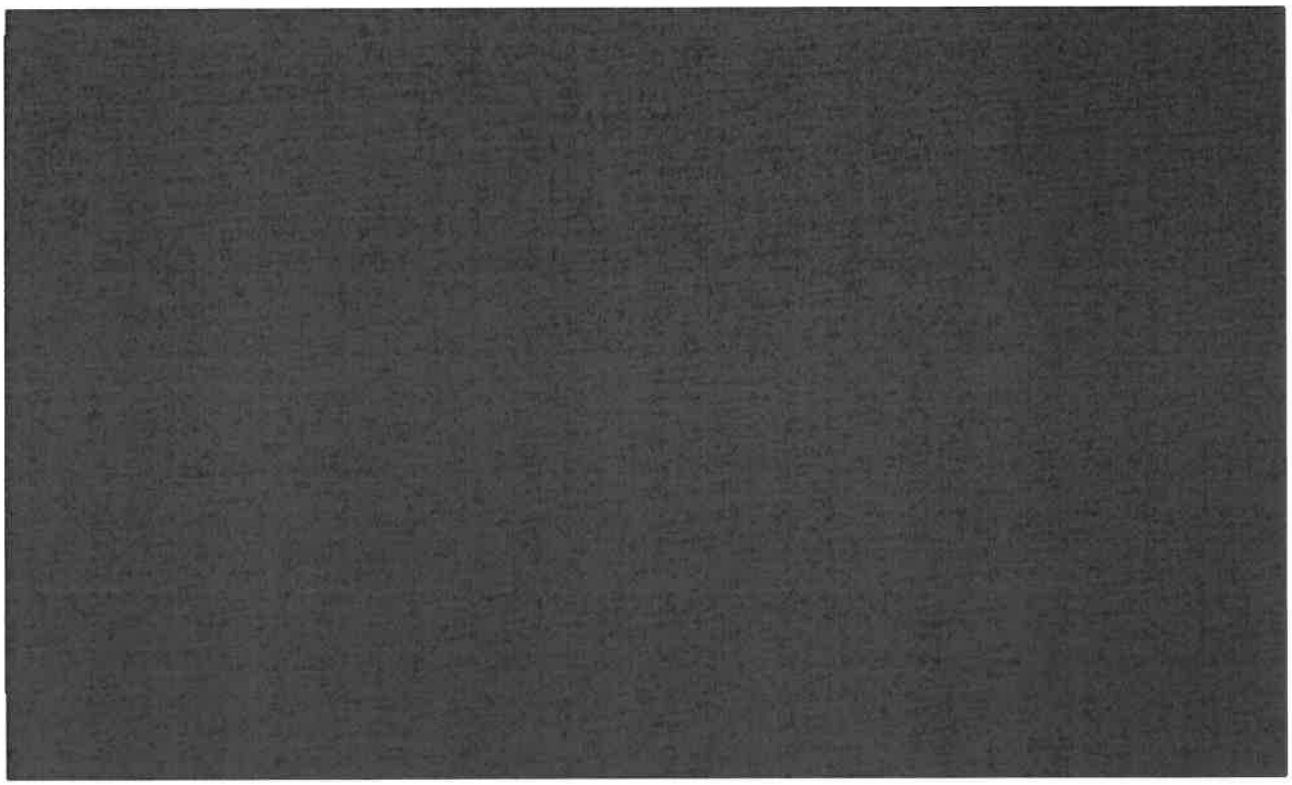
5.2.3.1 Présentation des risques



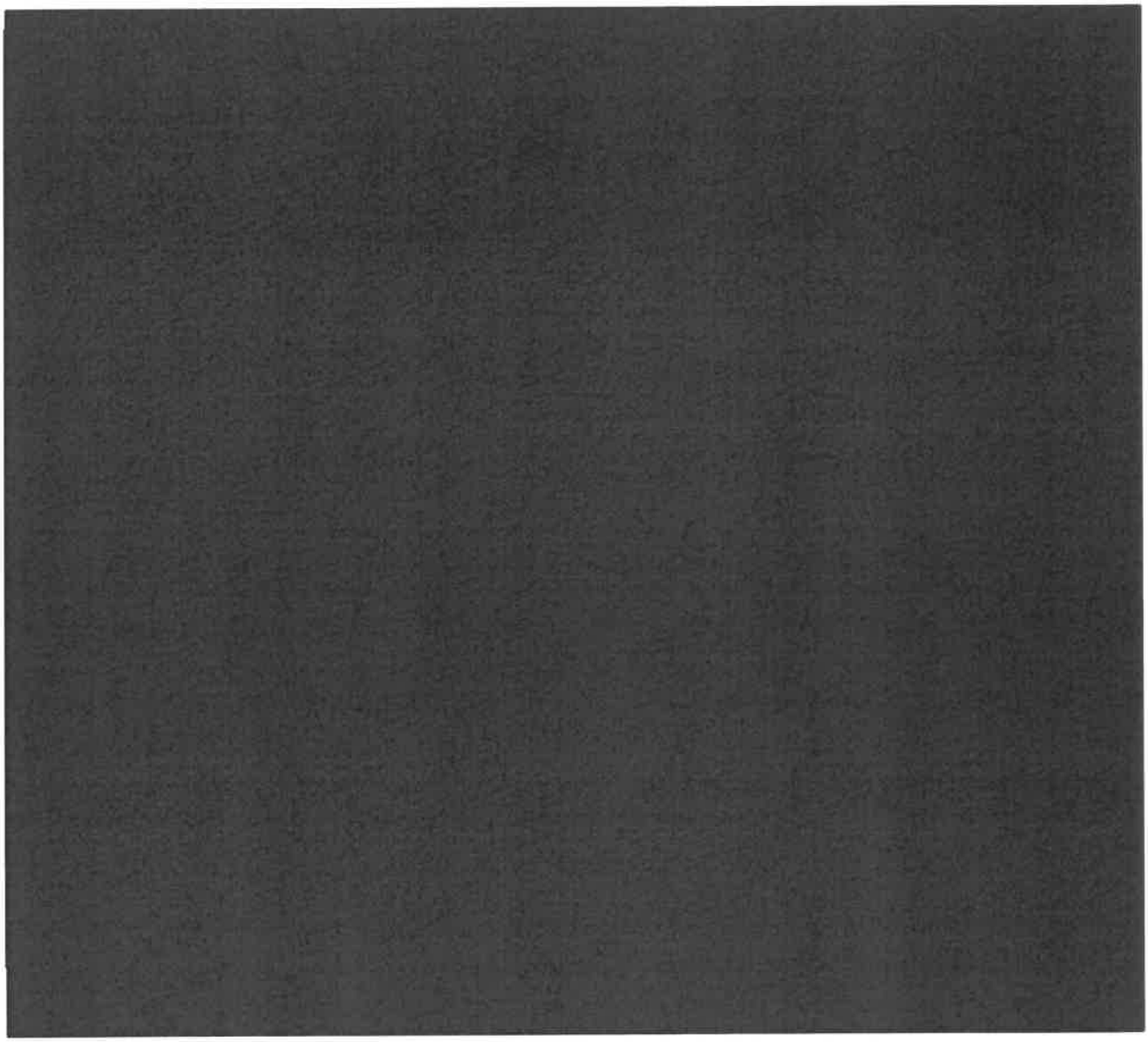
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



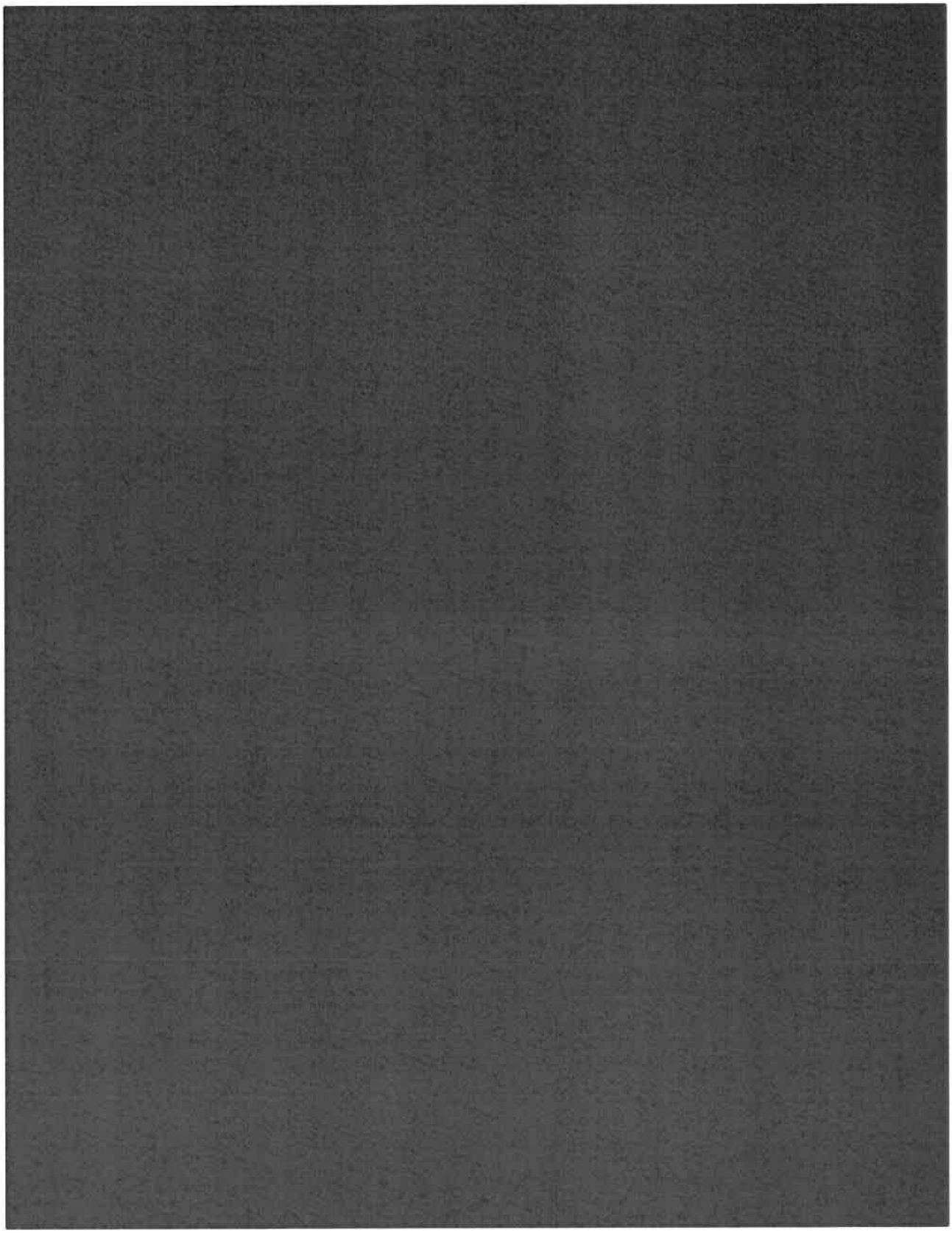
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



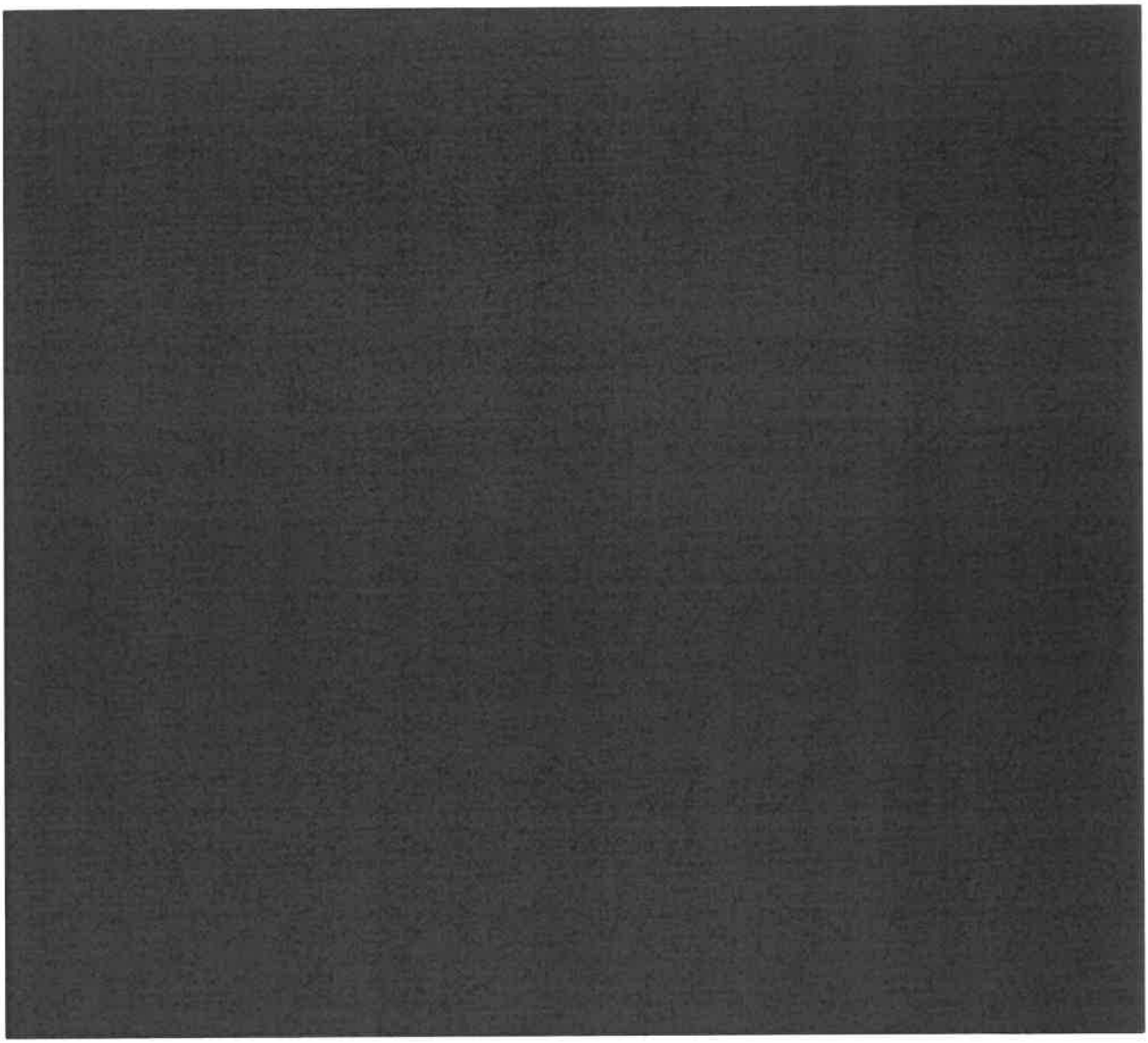
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



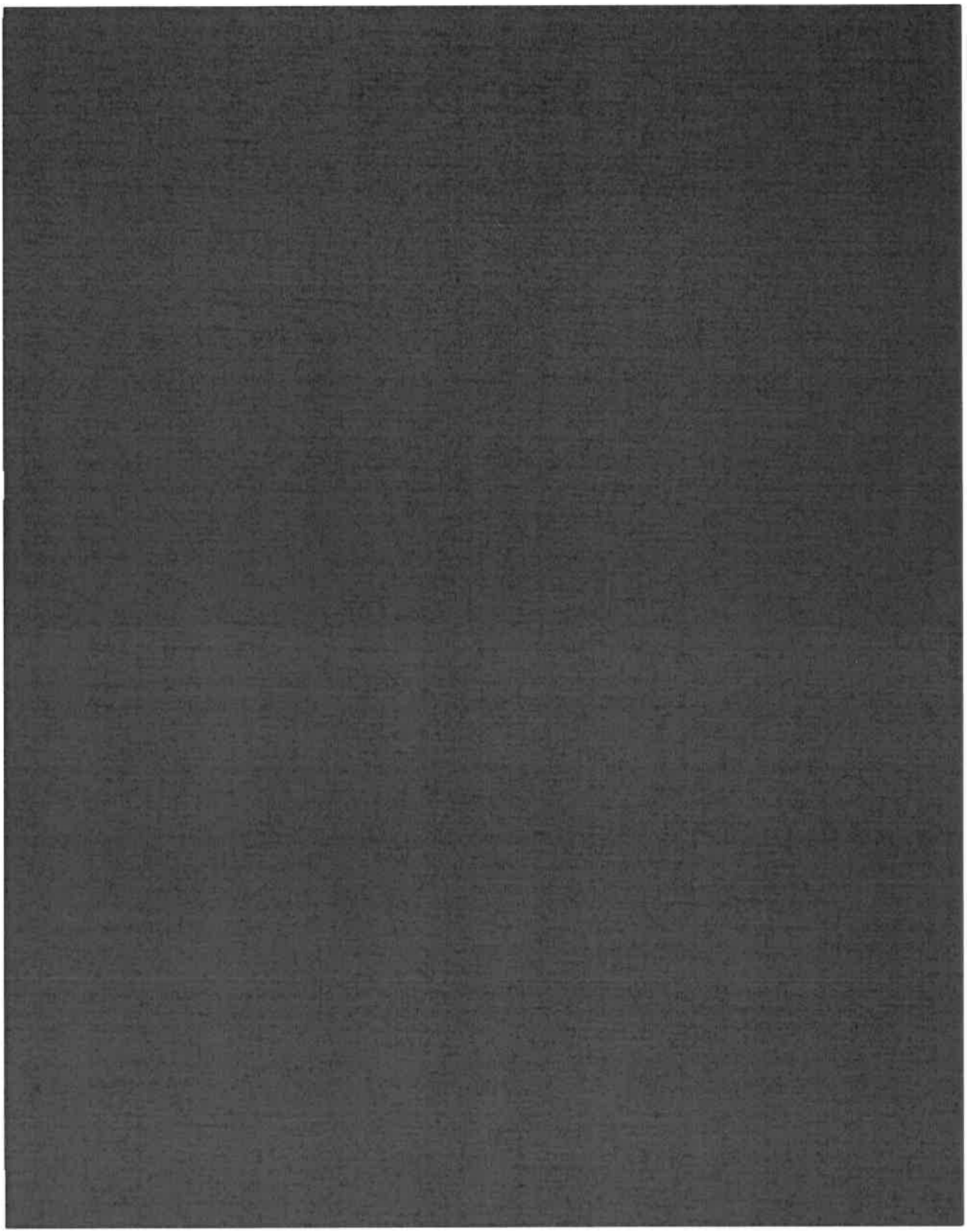
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



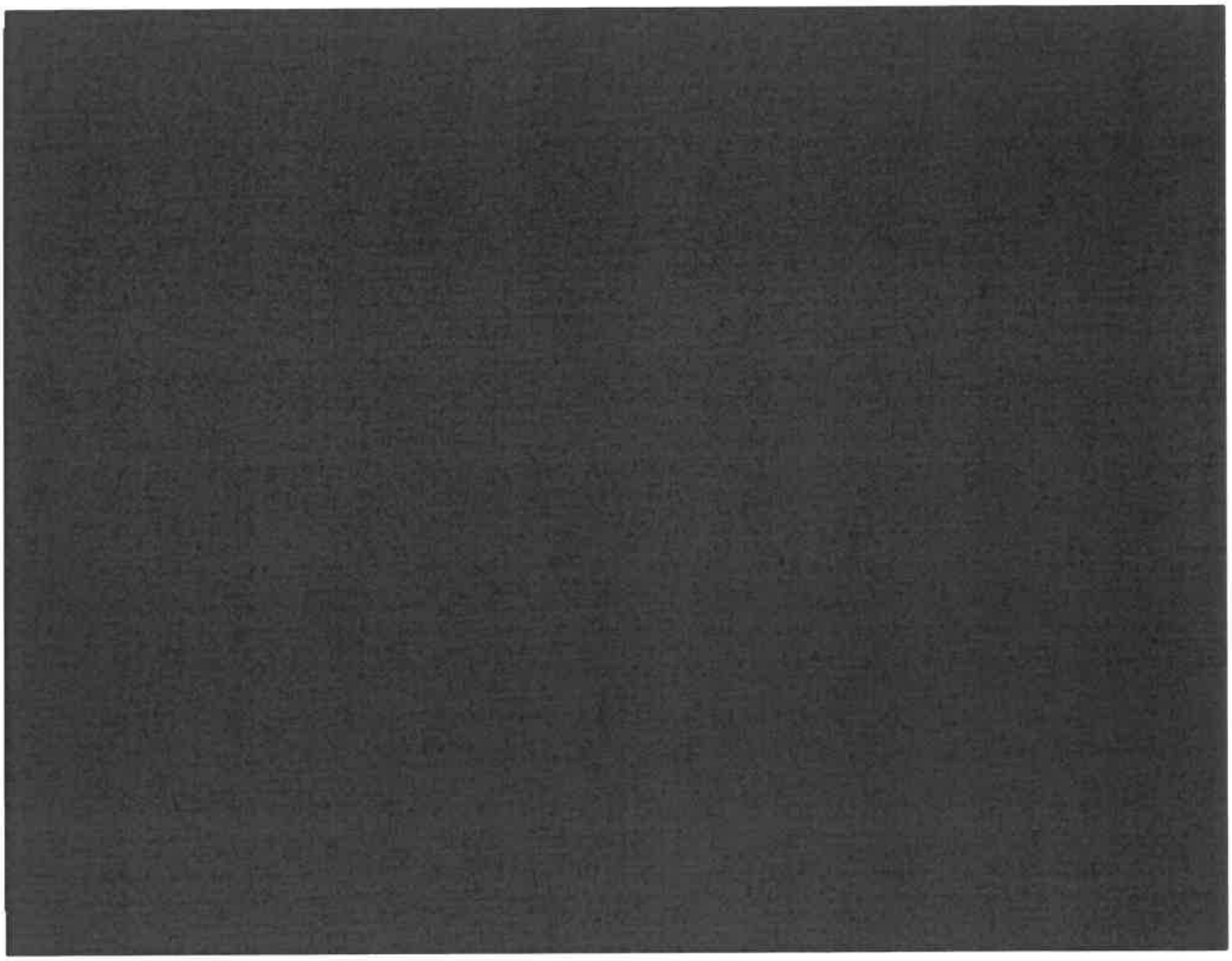
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



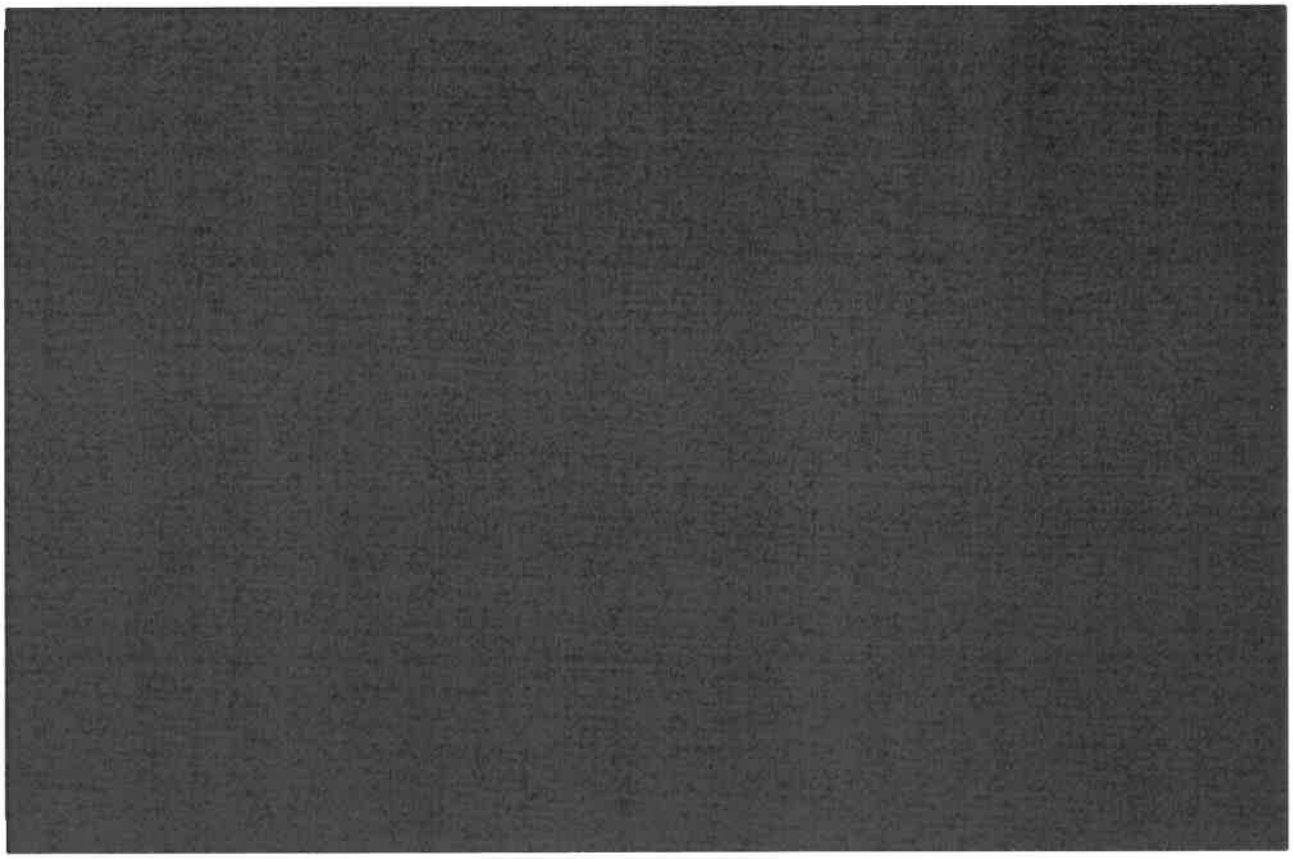
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



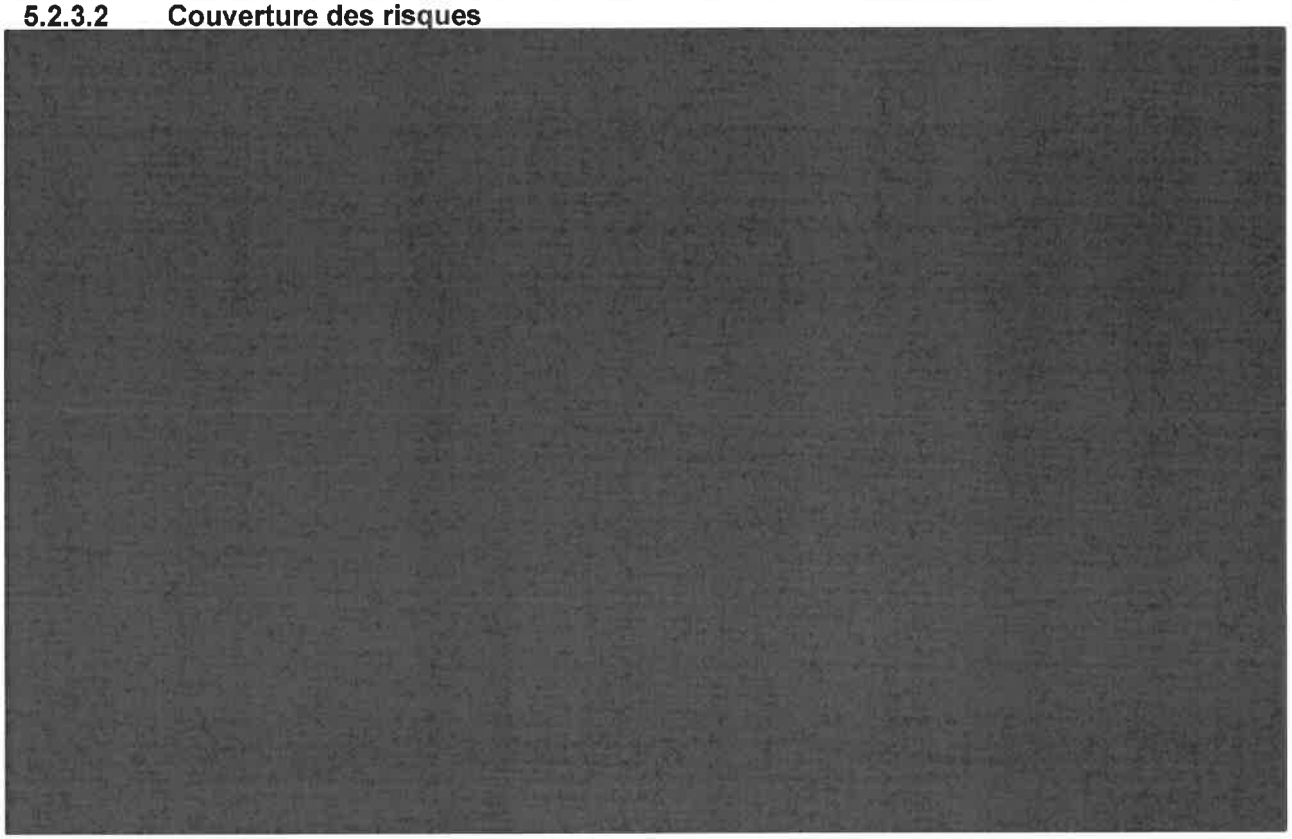
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



5.2.3.2 Couverture des risques



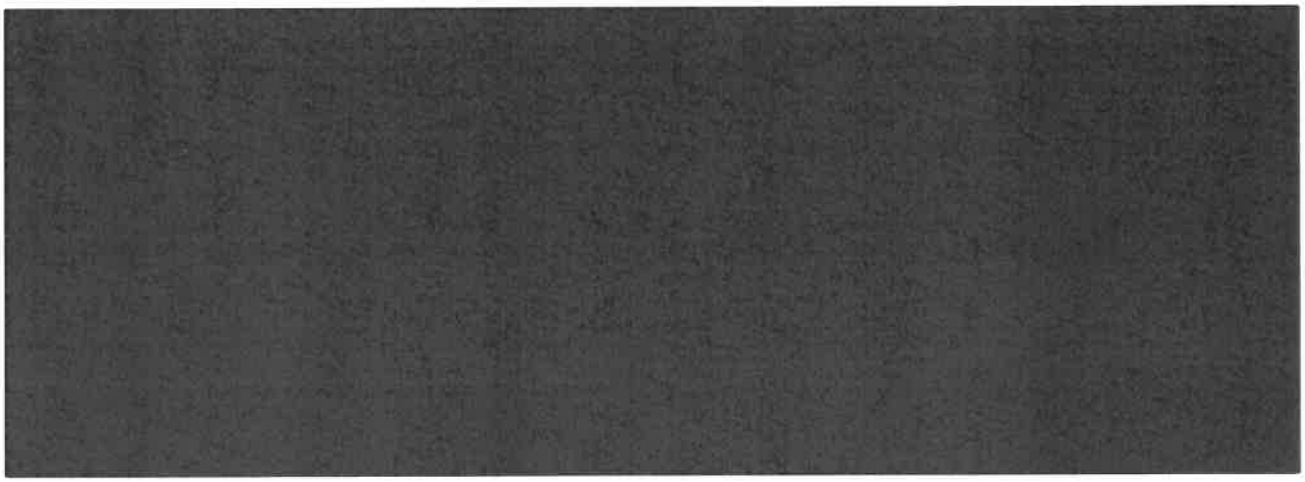
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.2.3.3 Plan d'action

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

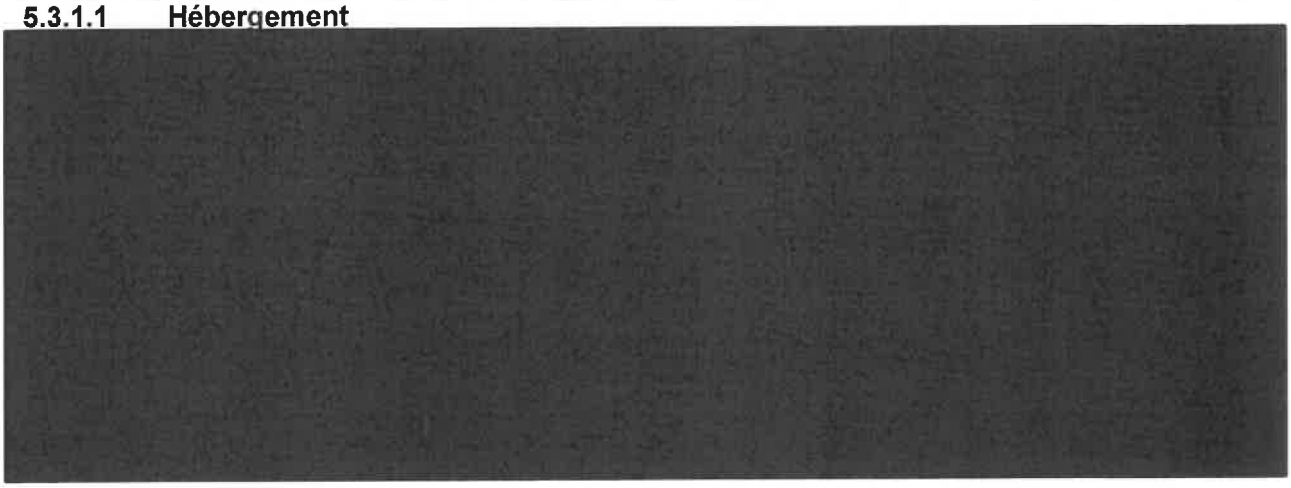


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.3 SI Sécurité

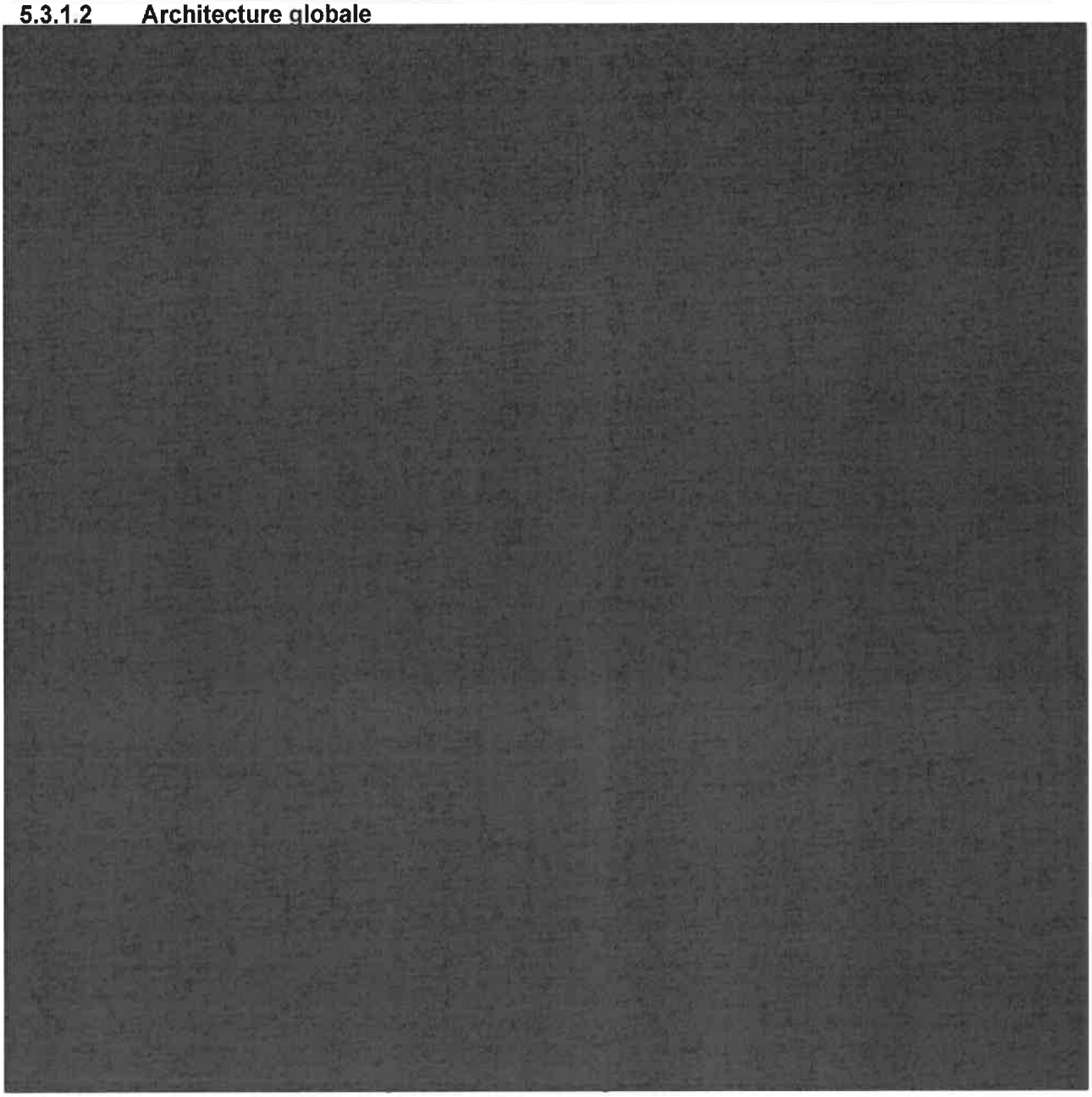
5.3.1 Présentation du SI Sécurité

5.3.1.1 Hébergement



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

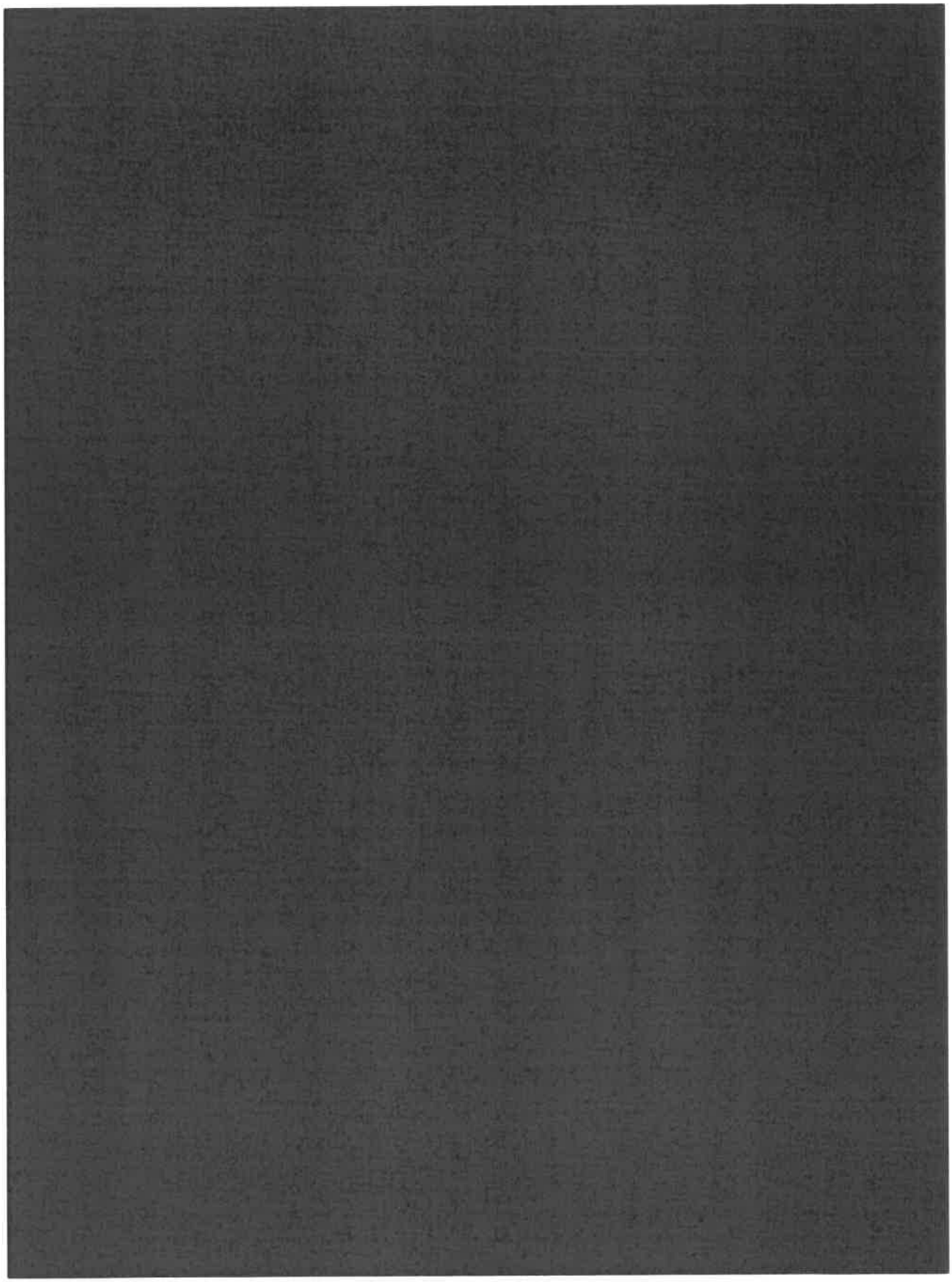
5.3.1.2 Architecture globale



5.3.1.2.1 Architecture physique

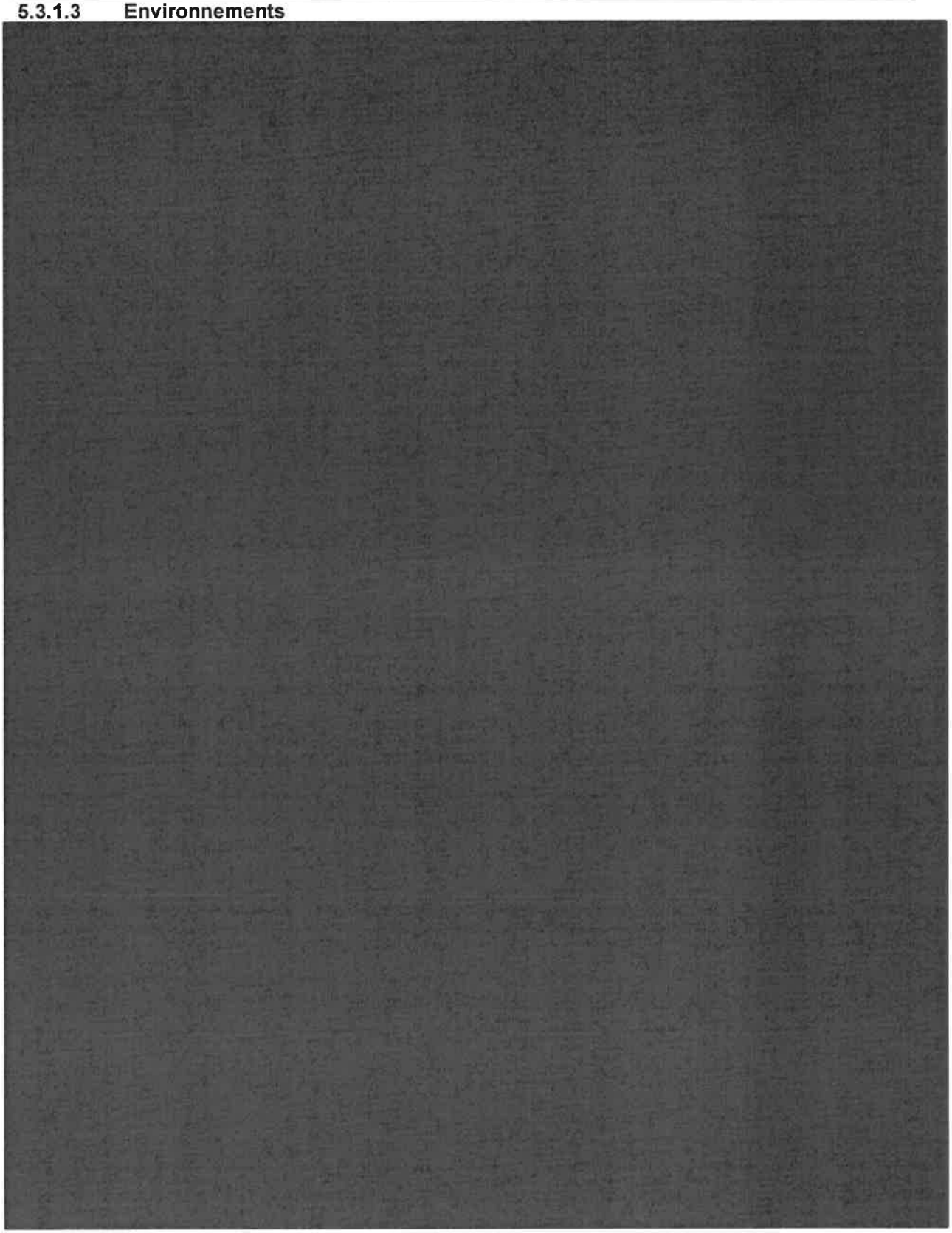
5.3.1.2.2 Virtualisation du réseau

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.3.1.3 Environnements



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.3.1.4 Gestion des traces

[redacted]

5.3.2 Mesures de sécurité

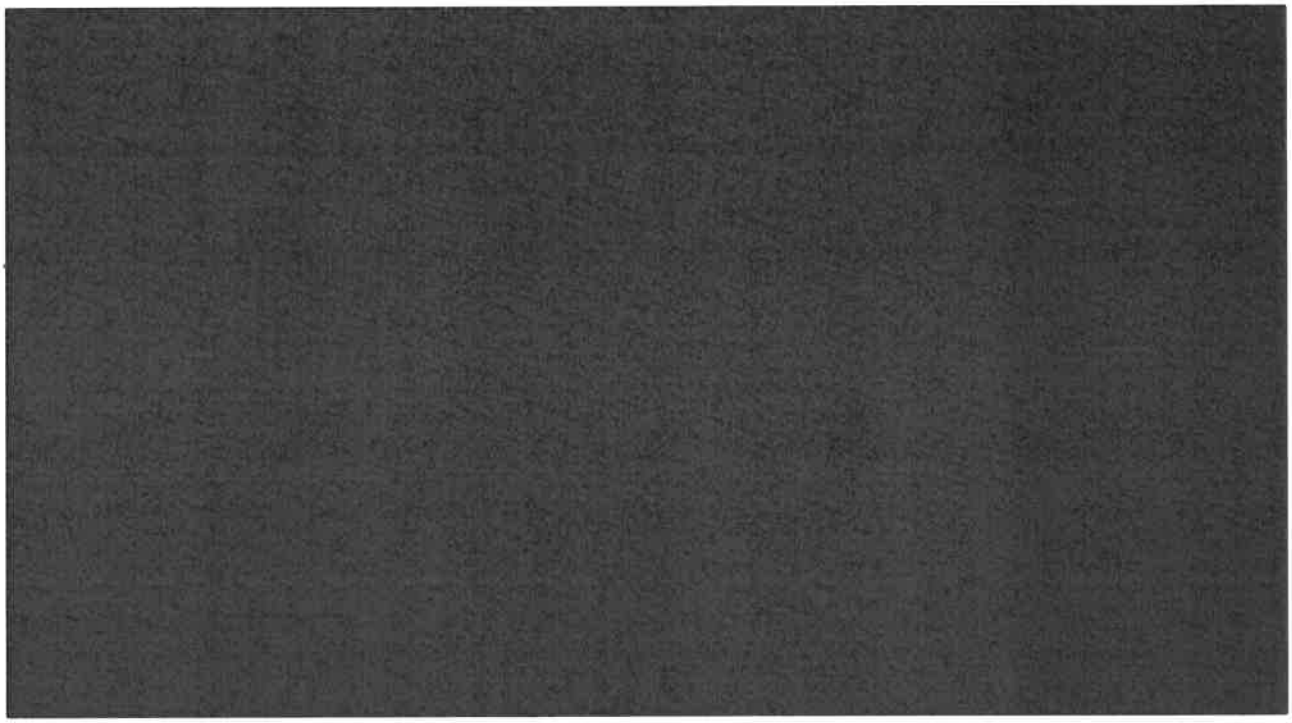
5.3.2.1 Certifications des sites d'hébergement

[redacted]

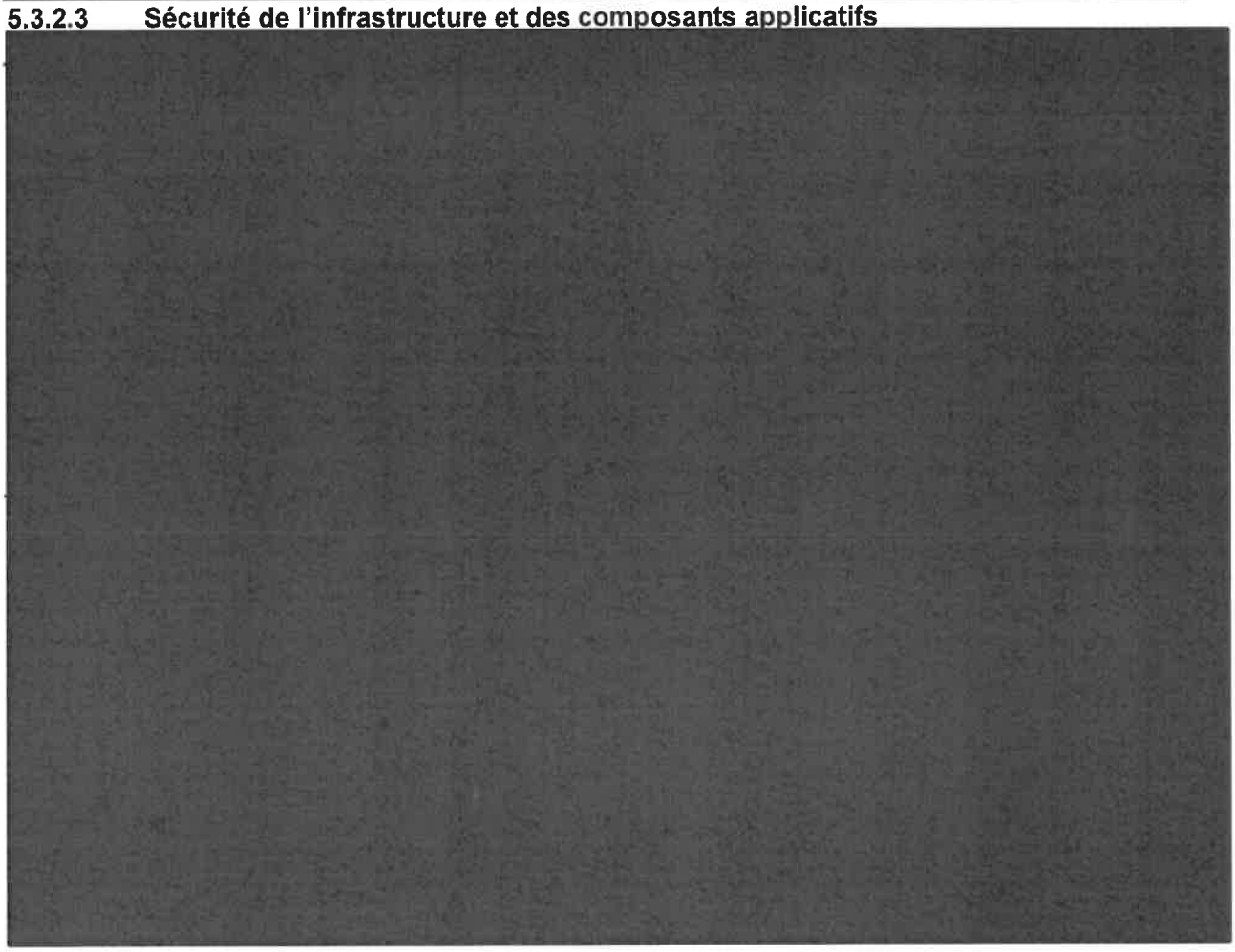
5.3.2.2 Sécurité physique

[redacted]

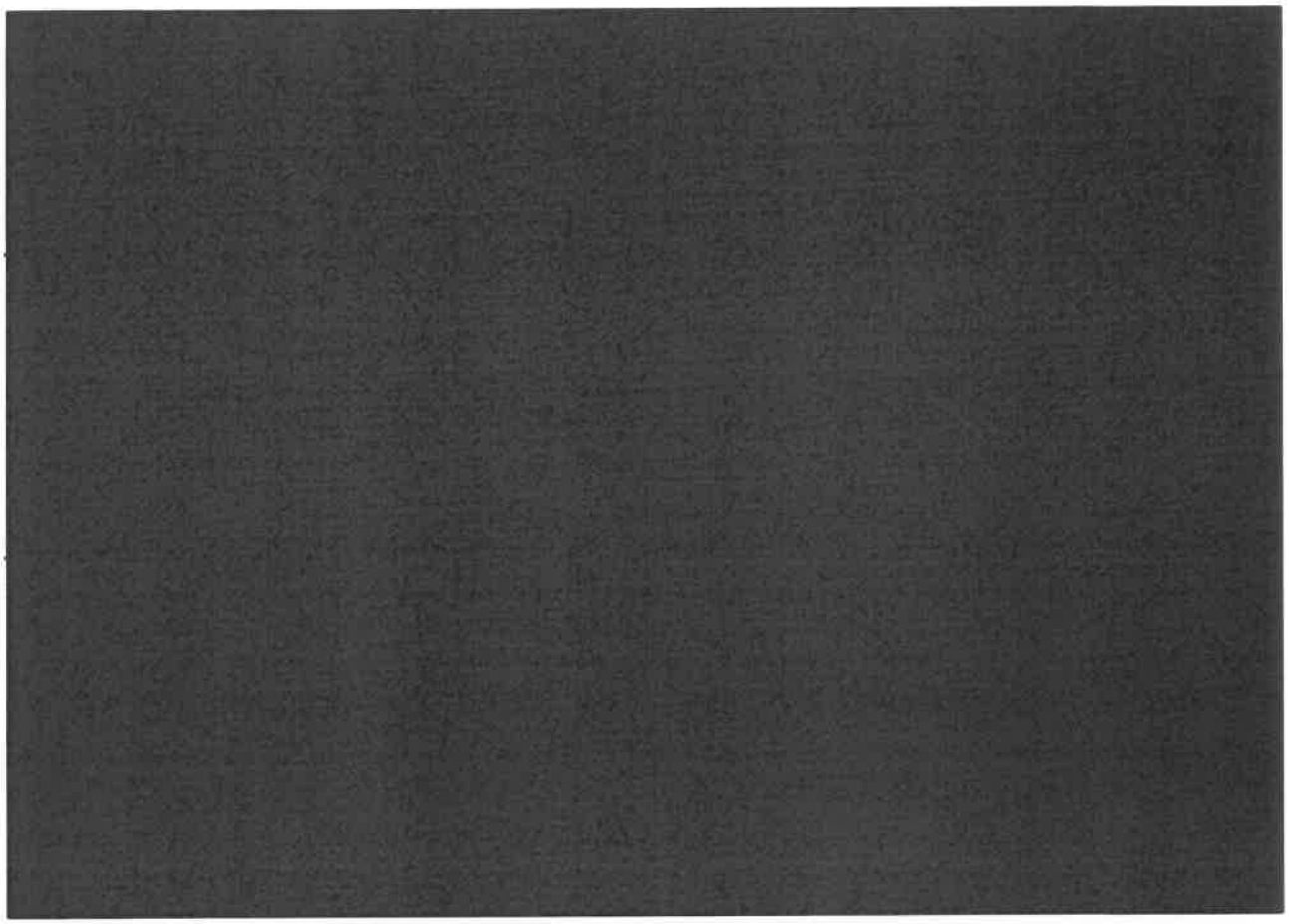
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



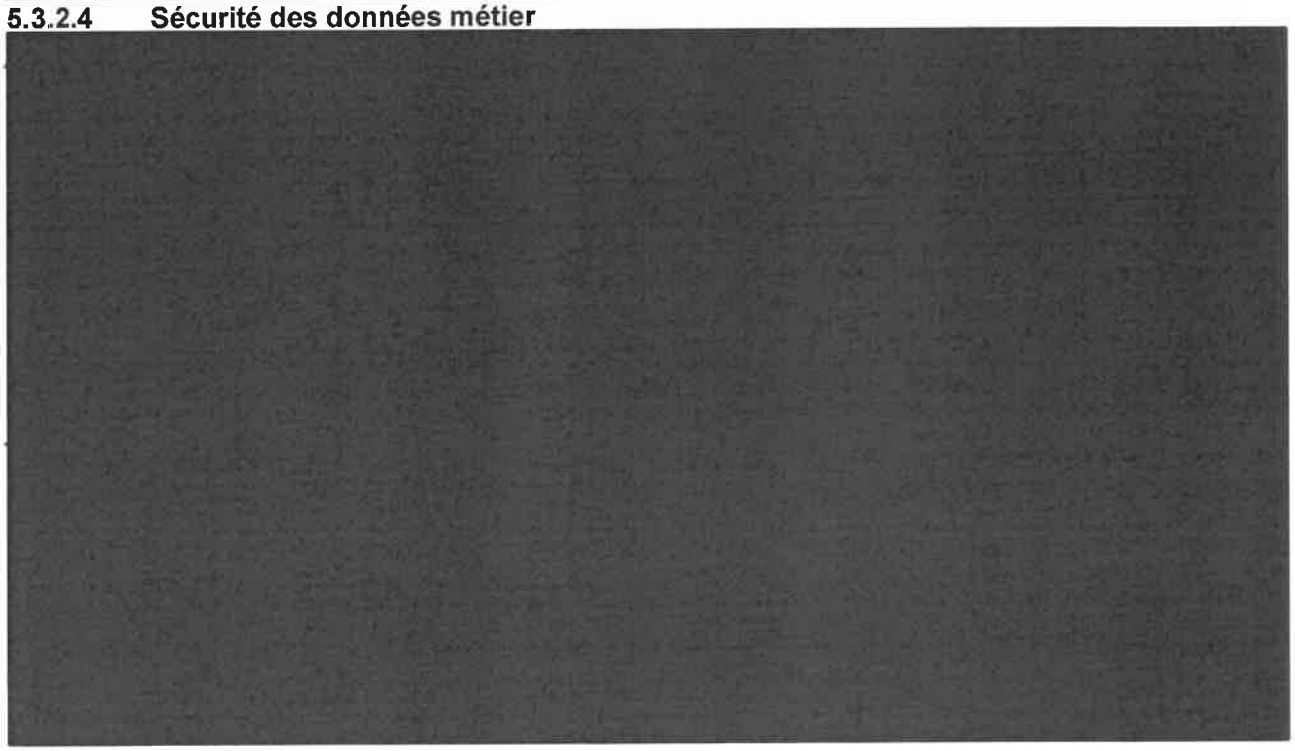
5.3.2.3 Sécurité de l'infrastructure et des composants applicatifs



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

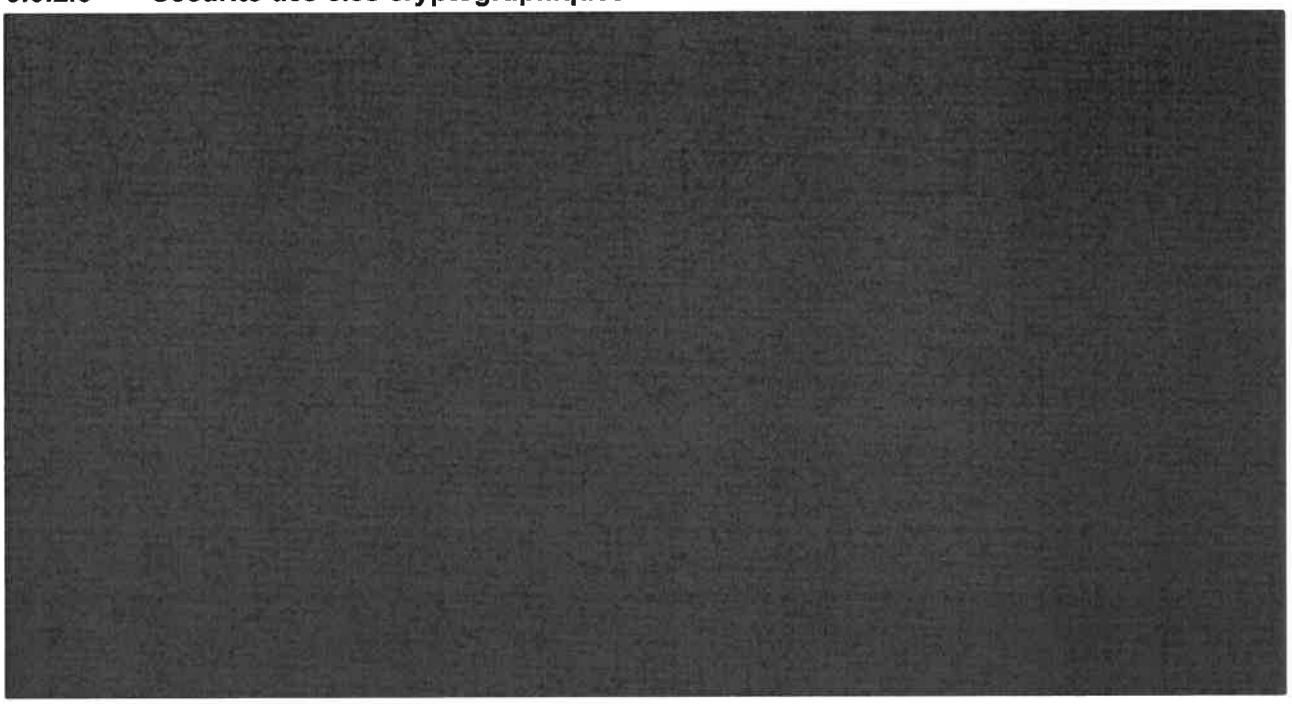


5.3.2.4 Sécurité des données métier

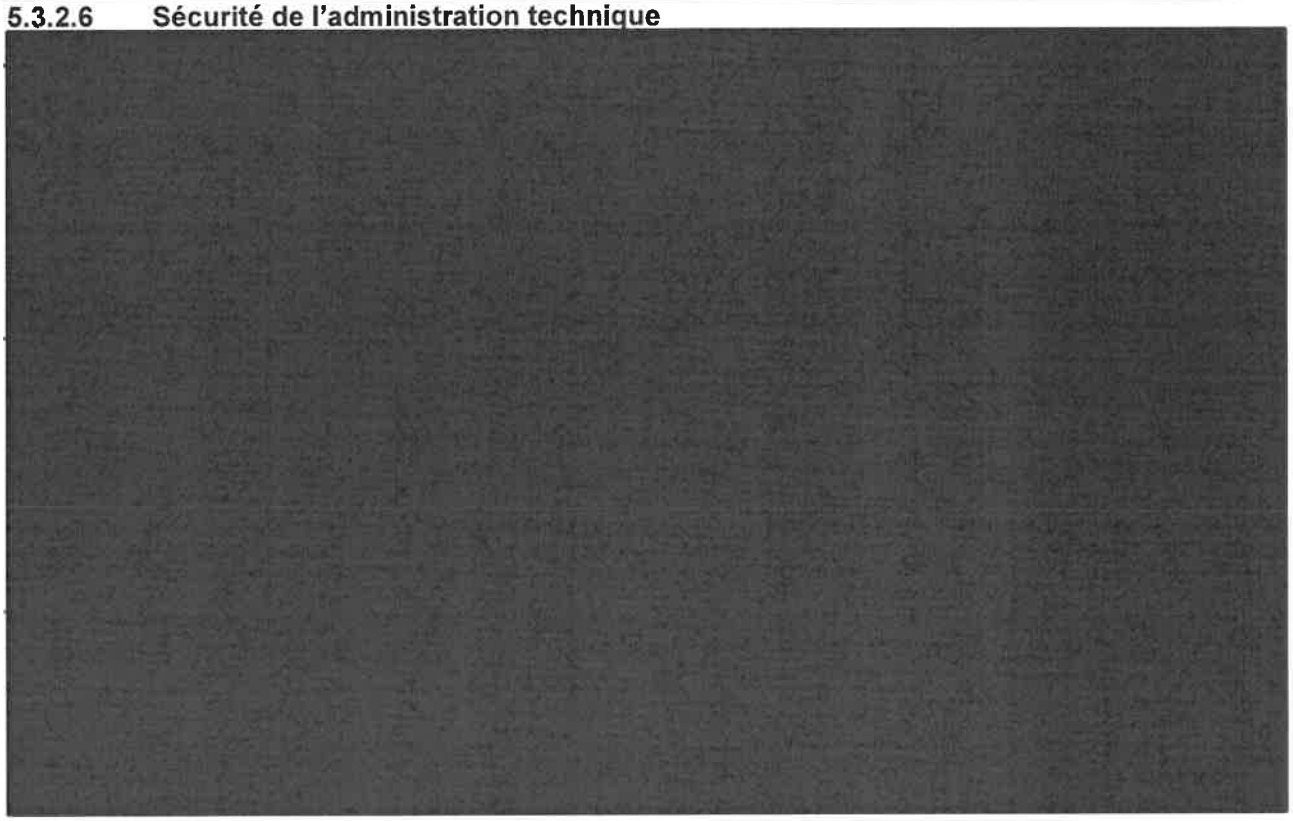


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.3.2.5 Sécurité des clés cryptographiques



5.3.2.6 Sécurité de l'administration technique



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

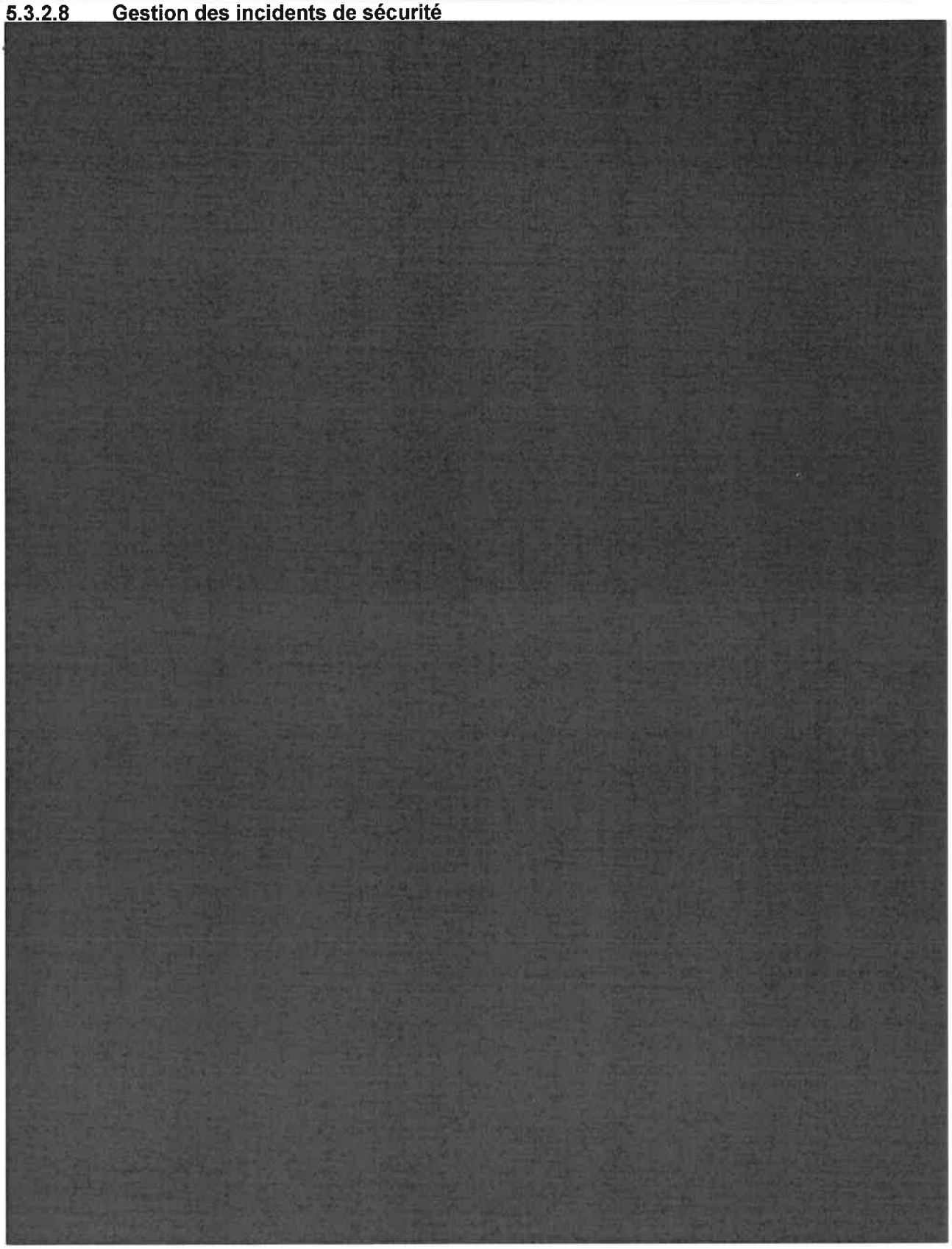
[redacted]

5.3.2.7 Supervision sécurité de l'infrastructure

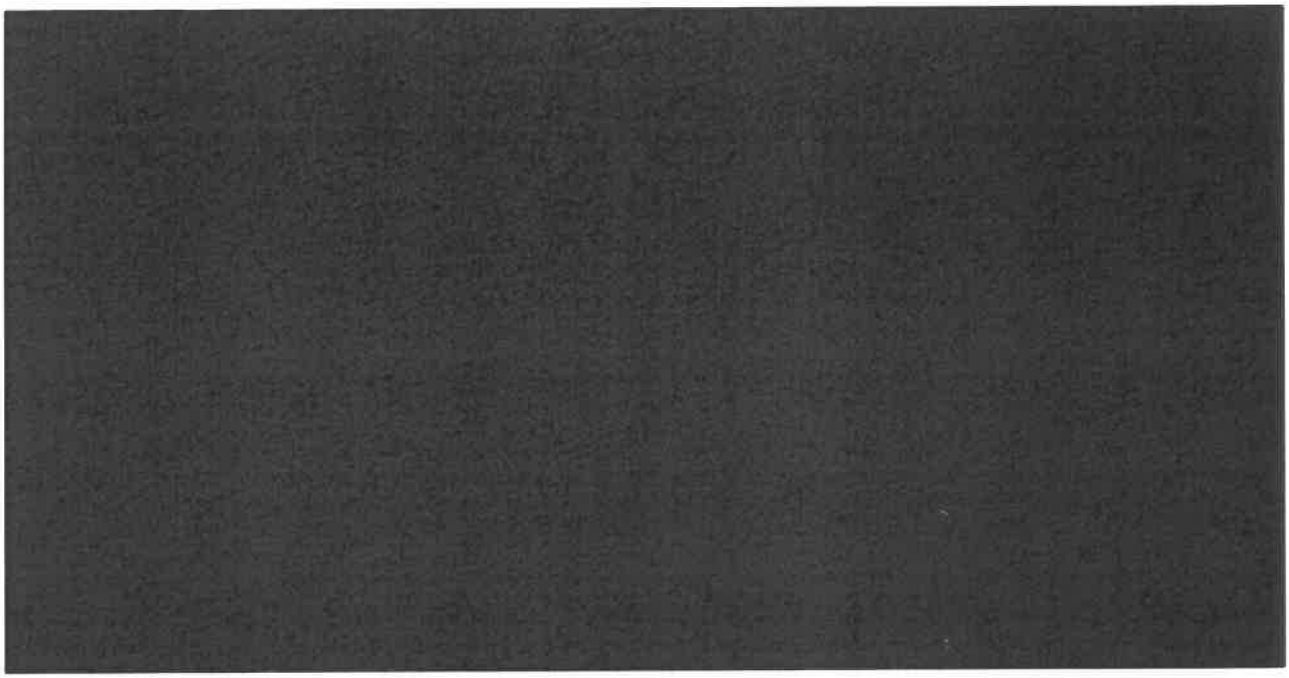
[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

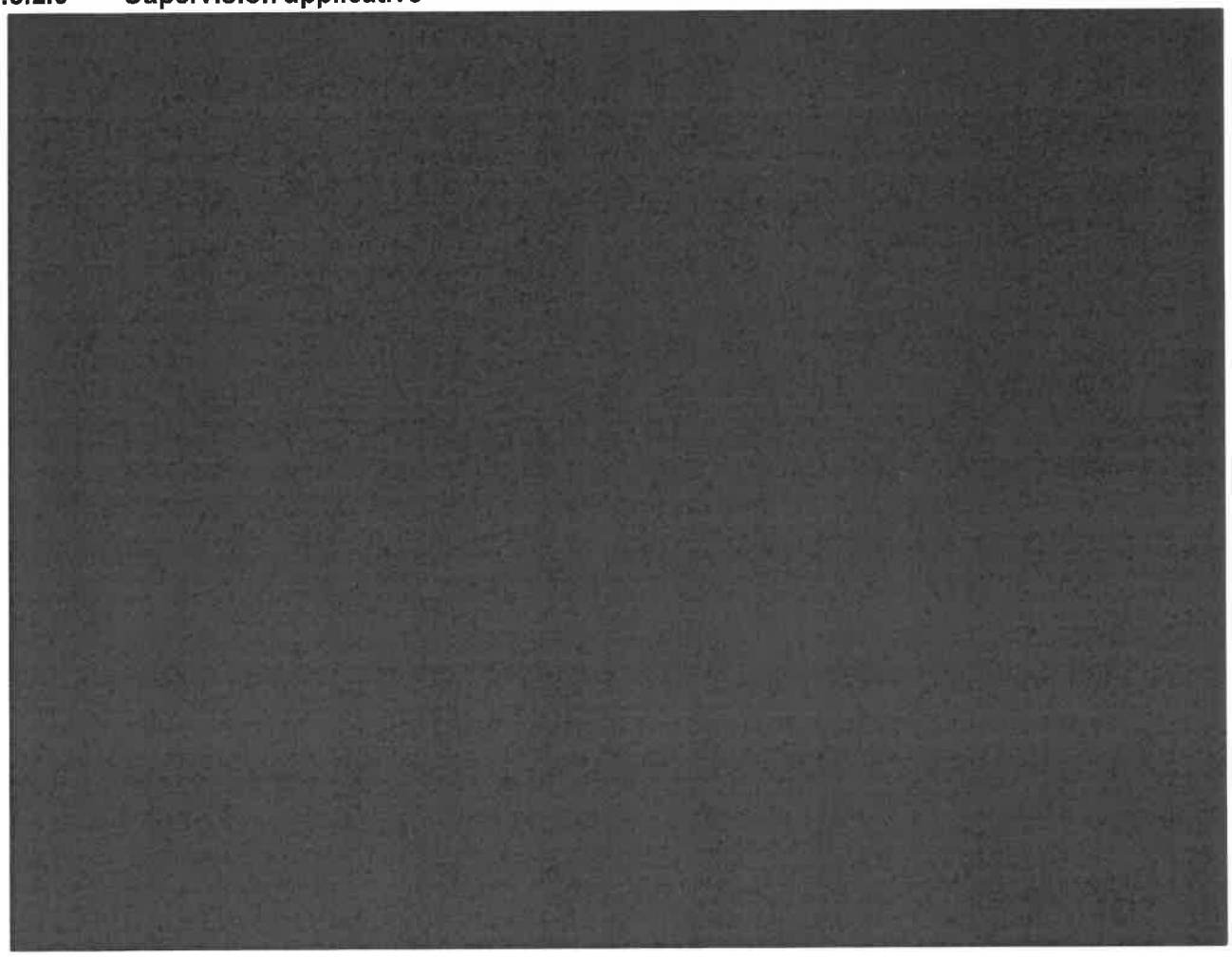
5.3.2.8 Gestion des incidents de sécurité



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



5.3.2.9 Supervision applicative



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

5.3.2.10 Sauvegardes

[redacted]

5.3.2.11 Continuité d'activité

[redacted]

5.3.2.12 Audits et contrôles

[redacted]

5.3.2.13 Synthèse des mesures de sécurité

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

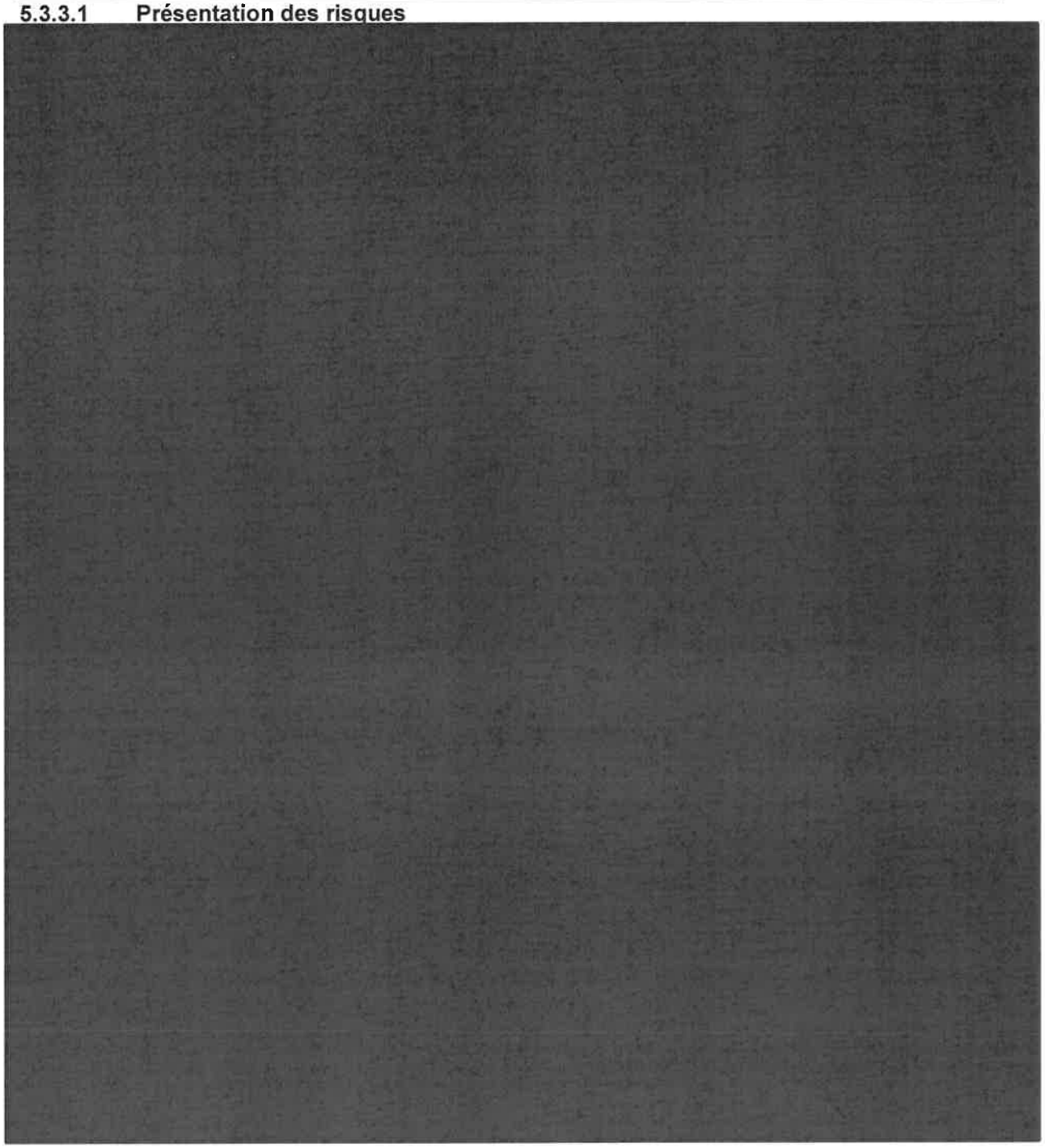
[redacted]

5.3.3 Risques

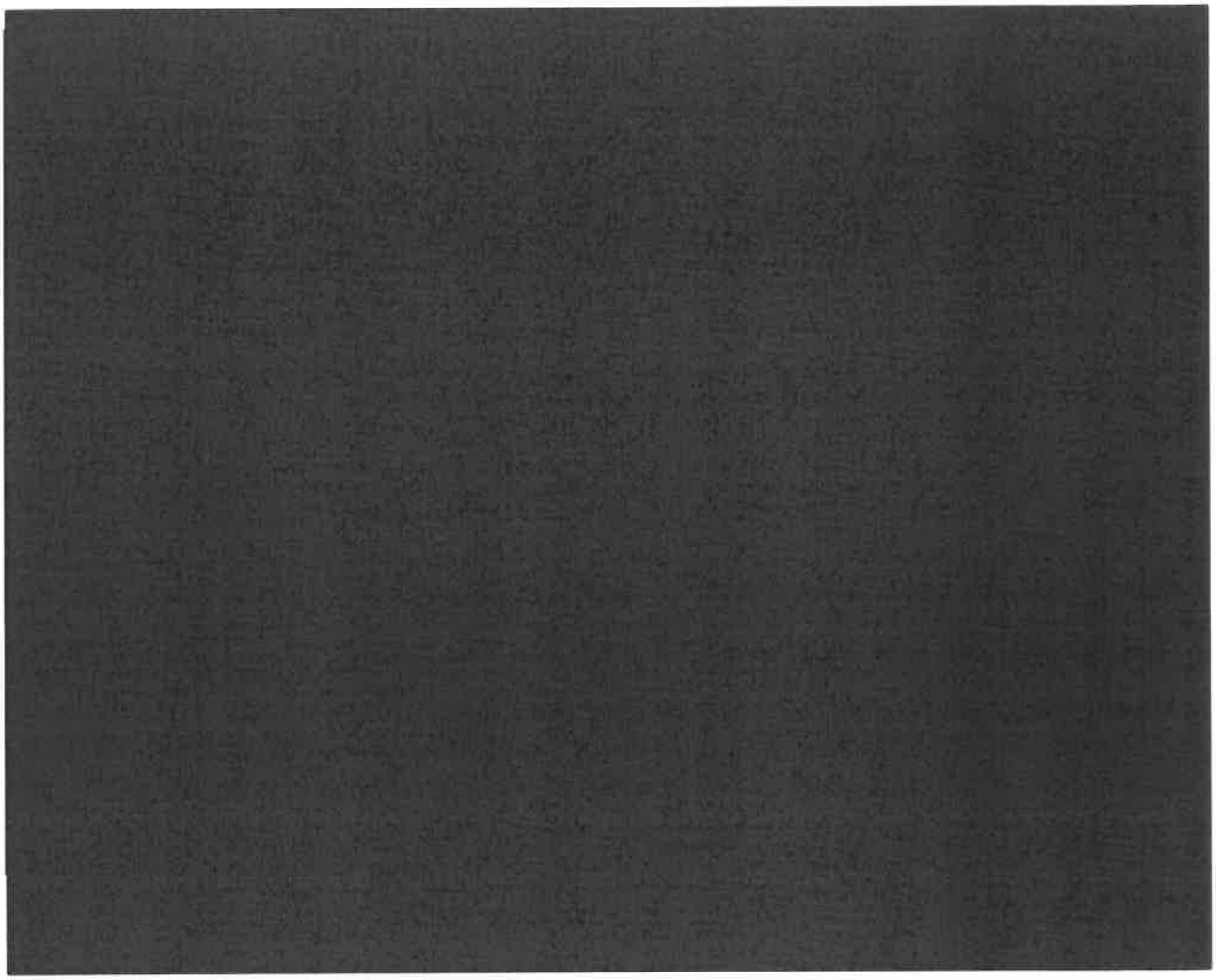
[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

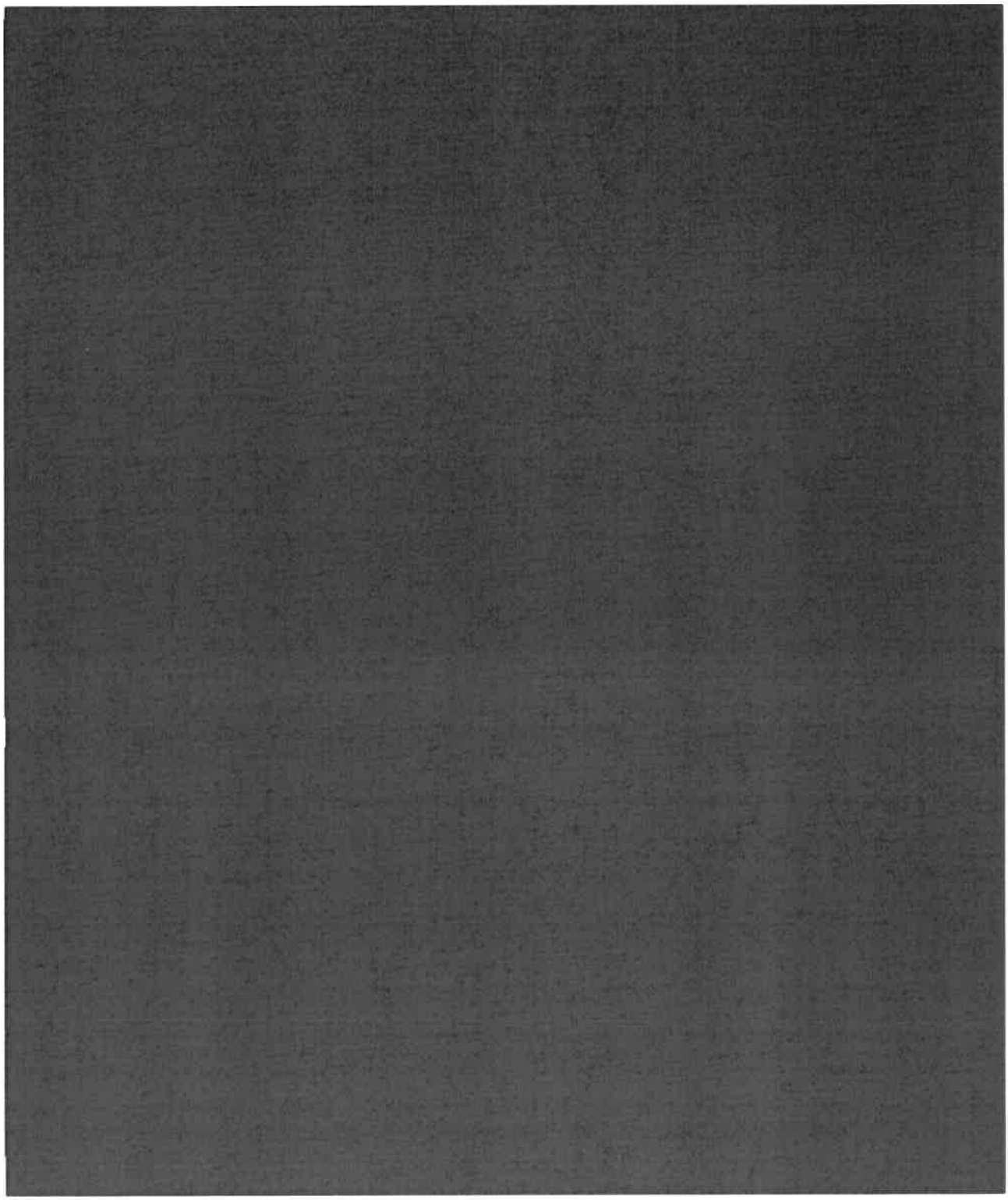
5.3.3.1 Présentation des risques



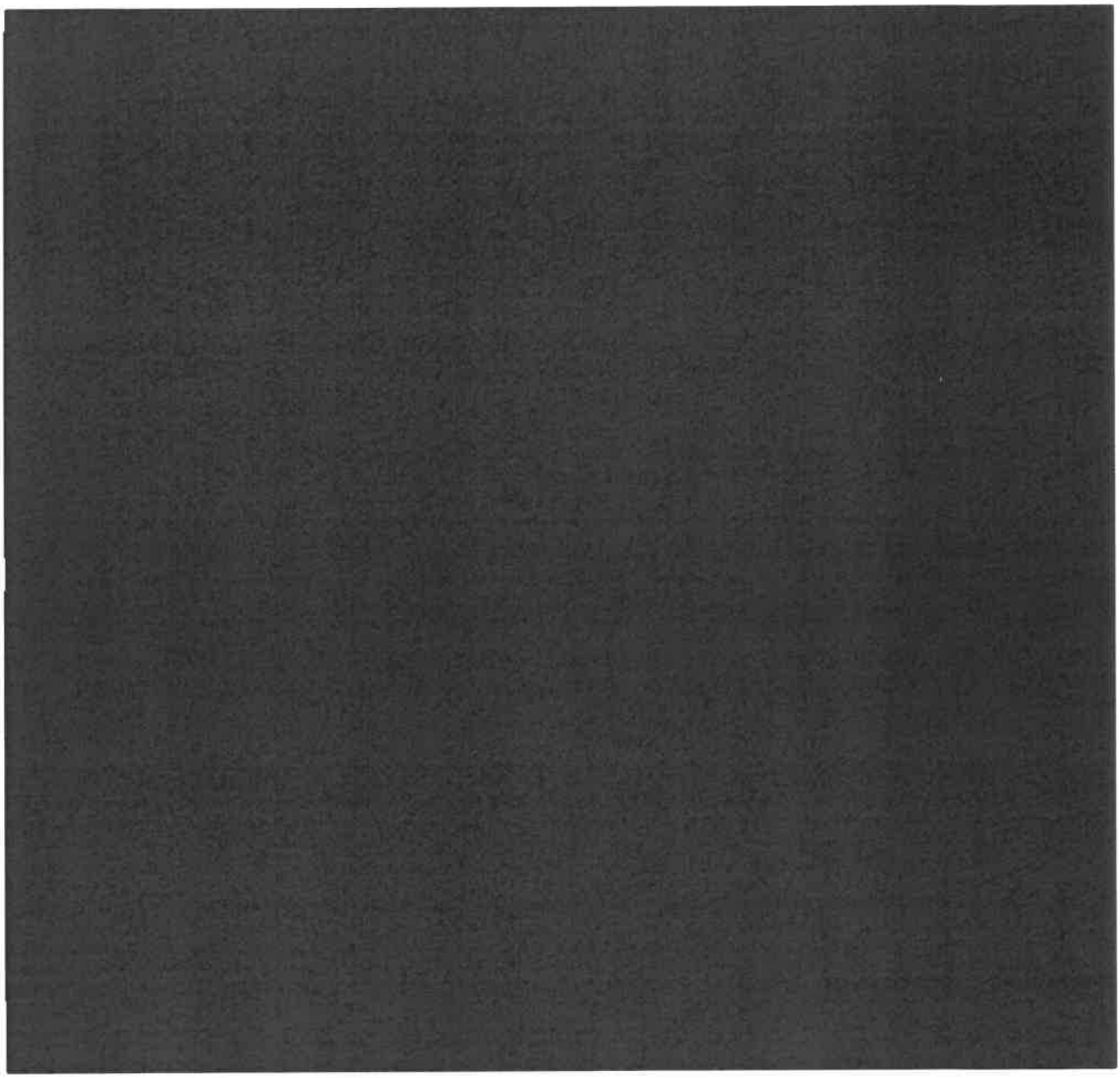
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



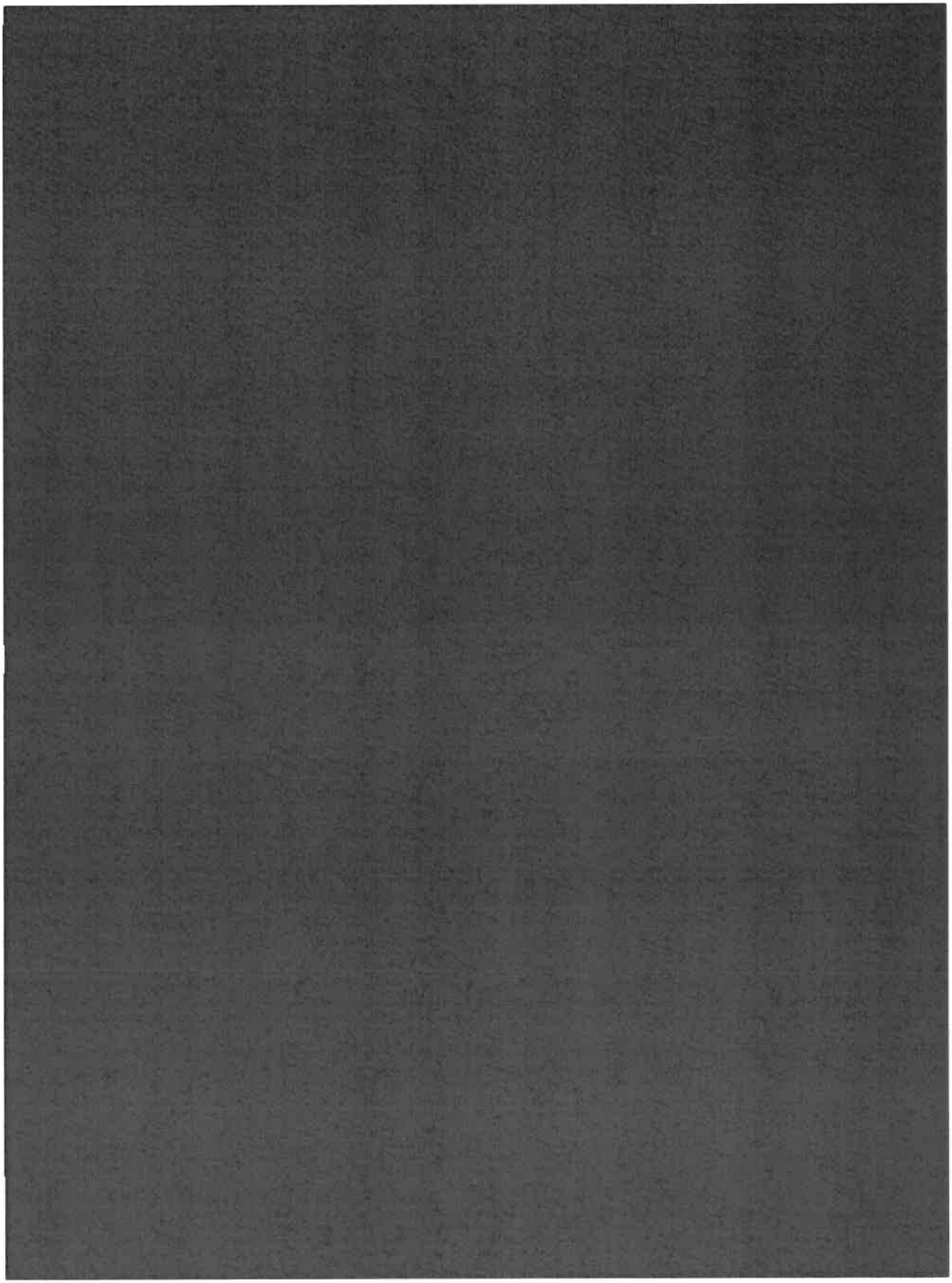
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

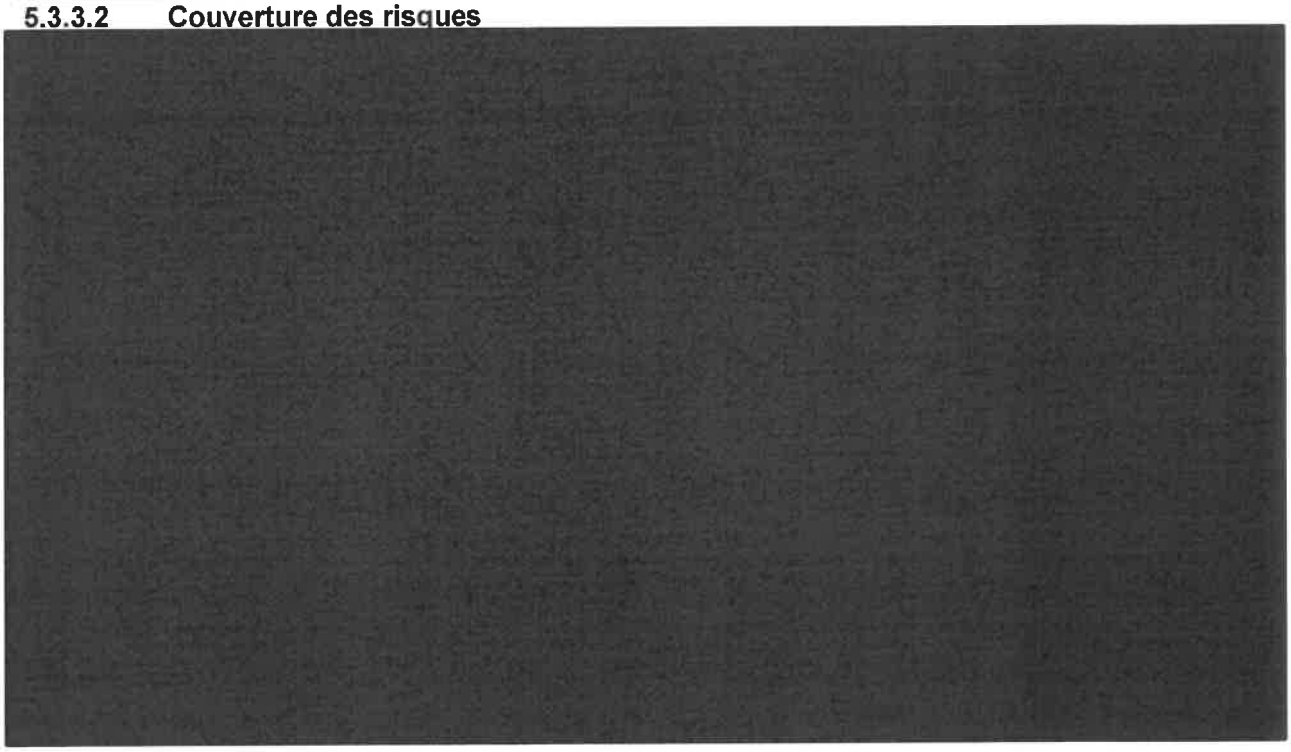


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

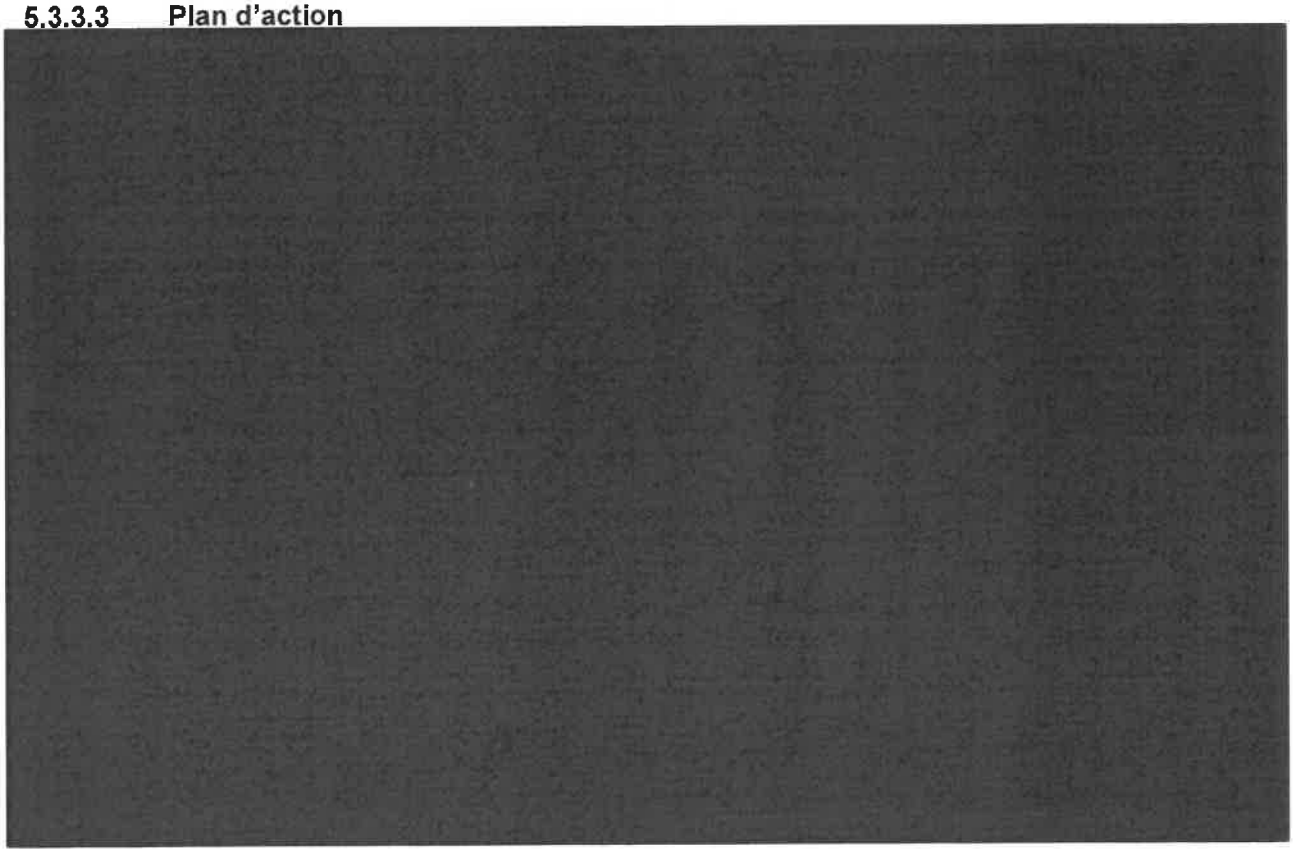


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

5.3.3.2 Couverture des risques



5.3.3.3 Plan d'action



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6 PROCESSUS LIES AU CYCLE DE VIE DU DISPOSITIF APCV

Dans cette version, deux parcours d'activation en ligne sont disponibles :

- Le parcours d'activation IVI, basé sur le recours à un Industriel de Vérification d'Identité (IVI) ;
- Le parcours d'activation France Identité, basé sur l'application France Identité et la CNIe (Carte nationale d'identité électronique).

Le parcours d'activation France Identité est proposé par défaut dès lors que l'application France Identité est détectée sur le smartphone de l'assuré.

Afin d'inciter les utilisateurs à utiliser ce nouveau parcours d'activation, si l'application France Identité n'est pas présente, un écran invite les utilisateurs disposant d'une CNIe à créer leur identité numérique :

Ces processus d'activation ont plusieurs objectifs : vérifier l'identité de l'utilisateur de l'application mobile, collecter sa photo, associer de manière forte son smartphone et cette identité vérifiée.

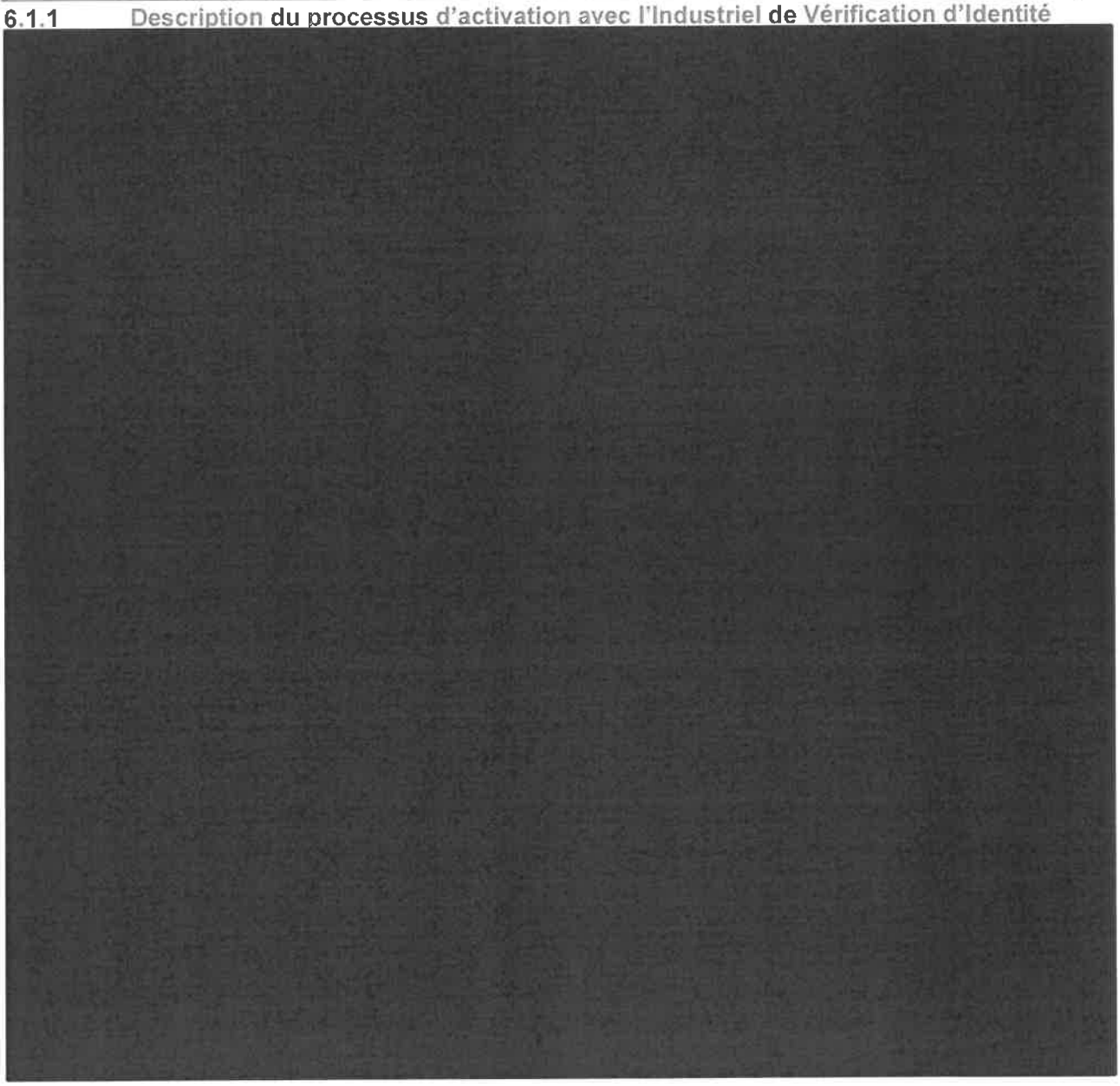
Ils se déroulent complètement en ligne, depuis l'application ApCV. En cas de difficulté, l'utilisateur a la possibilité de contacter sa Caisse de rattachement : l'agent Caisse consulte le portail AMO pour connaitre l'état d'activation de l'ApCV et assister l'assuré dans la finalisation de l'activation [MES111].

Dans une version ultérieure de l'ApCV, un parcours d'activation en Caisse sera également disponible. Il sera décrit dans une future version de l'AIPD.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.1 Parcours d'activation IVI

6.1.1 Description du processus d'activation avec l'Industriel de Vérification d'Identité



Le processus d'activation se décompose en 4 grandes étapes :

1. L'assuré fournit son NIR et saisit le code d'activation reçu par mail ;
2. Il réalise le parcours de vérification d'identité en présentant successivement sa pièce d'identité et son visage ;
3. Il définit le mot de passe de déverrouillage de l'appli carte Vitale et patiente le temps que son identité soit validée ;
4. Une fois l'identité validée, il reçoit un mail l'invitant à finaliser l'activation.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Etape 1 :

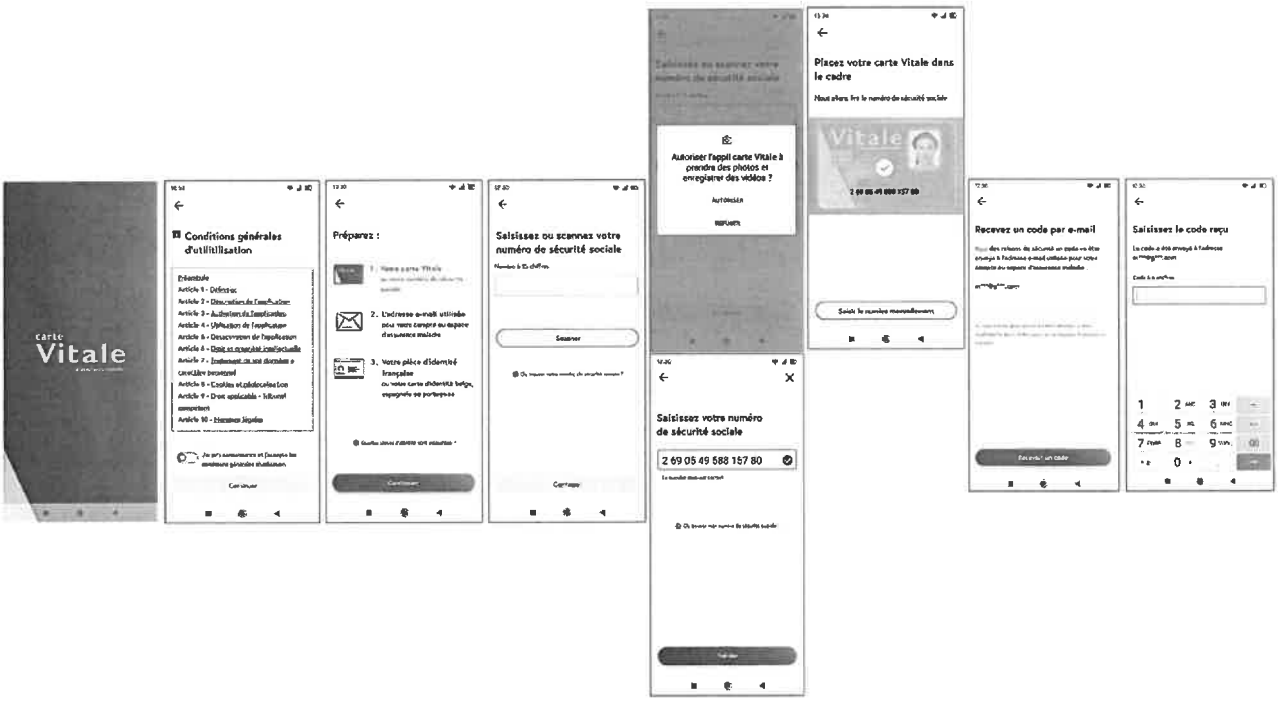


Figure 9 : processus d'activation (étape 1 – NIR et code d'activation)

1. L'utilisateur installe l'ApCV sur son smartphone. [MES06] Au premier lancement, il prend connaissance des CGU et de la Politique de protection des données personnelles. Il déclare en avoir pris connaissance, sans quoi il ne peut pas démarrer l'activation.
2. Il saisit ensuite son NIR ou utilise la lecture automatique du NIR sur sa carte Vitale (voir complément d'information ci-dessous) : une vérification de l'éligibilité de l'assuré est opérée [redacted] Si l'assuré n'est pas éligible, il est informé qu'il ne peut pas poursuivre l'enrôlement [redacted]
3. Si l'assuré est éligible, [redacted]
   - Si l'adresse mail de l'assuré n'est pas connue de l'AMO, l'assuré est informé qu'il ne peut pas poursuivre l'activation ;
   - Sinon, [EX16] le SI-ApCV envoie un mail contenant un code d'activation à 6 chiffres à l'utilisateur. Ce code est valide pendant 1 heure. L'adresse mail à laquelle le code est envoyé est présentée masquée à l'utilisateur [redacted]
4. A réception du mail, l'utilisateur saisit le code de vérification dans l'ApCV. [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Etape 2 :

Figure 10 : processus d'activation (étape 2 – vérification d'identité)

5. Les informations relatives au traitement biométrique à venir sont présentées à l'utilisateur.
6. L'utilisateur choisit sa pièce d'identité. Les pièces d'identités françaises, espagnoles, belges et portugaises sont acceptées.
7. L'utilisateur est informé qu'une vidéo va démarrer. Il doit autoriser l'appli carte Vitale à enregistrer des contenus audios, photos et vidéos
8. Un flux vidéo démarre sur son smartphone.
9. L'utilisateur est invité à présenter successivement le recto et le verso de sa pièce d'identité. L'IVI vérifie l'authenticité de la PI présentée (vérification automatique par un algorithme).
    - Si le contrôle est positif, la photo de la PI est extraite et un dossier est ouvert (conservé 3 jours afin de reprendre un enrôlement sans perdre le bénéfice d'une pièce d'identité authentique).

[redacted]

10. L'utilisateur est ensuite invité à présenter son visage. L'IVI procède à un rapprochement biométrique automatique entre le visage de l'assuré et la photo figurant sur la PI.

[redacted]

11. Un challenge du vivant (sourire) est demandé à l'utilisateur.

[redacted]

12. Les traits d'identité de la PI authentifiée sont extraits automatiquement.
13. Un rapprochement entre l'identité extraite de la PI avec le NIR puis avec l'INS est réalisé. En cas d'échec, le processus d'activation est interrompu.
14. Si le résultat des contrôles automatiques est positif, un opérateur de l'IVI doit valider systématiquement la décision d'acceptation de l'authenticité de la PI, du test du vivant et du rapprochement de la photo de la PI avec le selfie. Cette opération peut prendre jusqu'à 48h. En cas d'échec, le processus d'enrôlement est interrompu.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

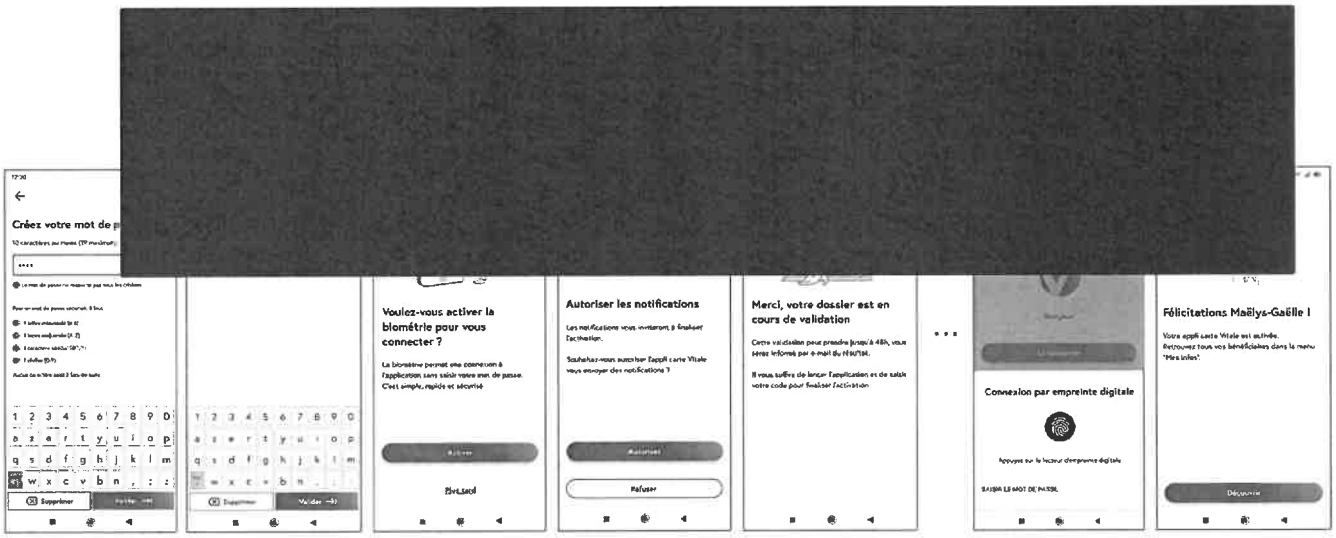


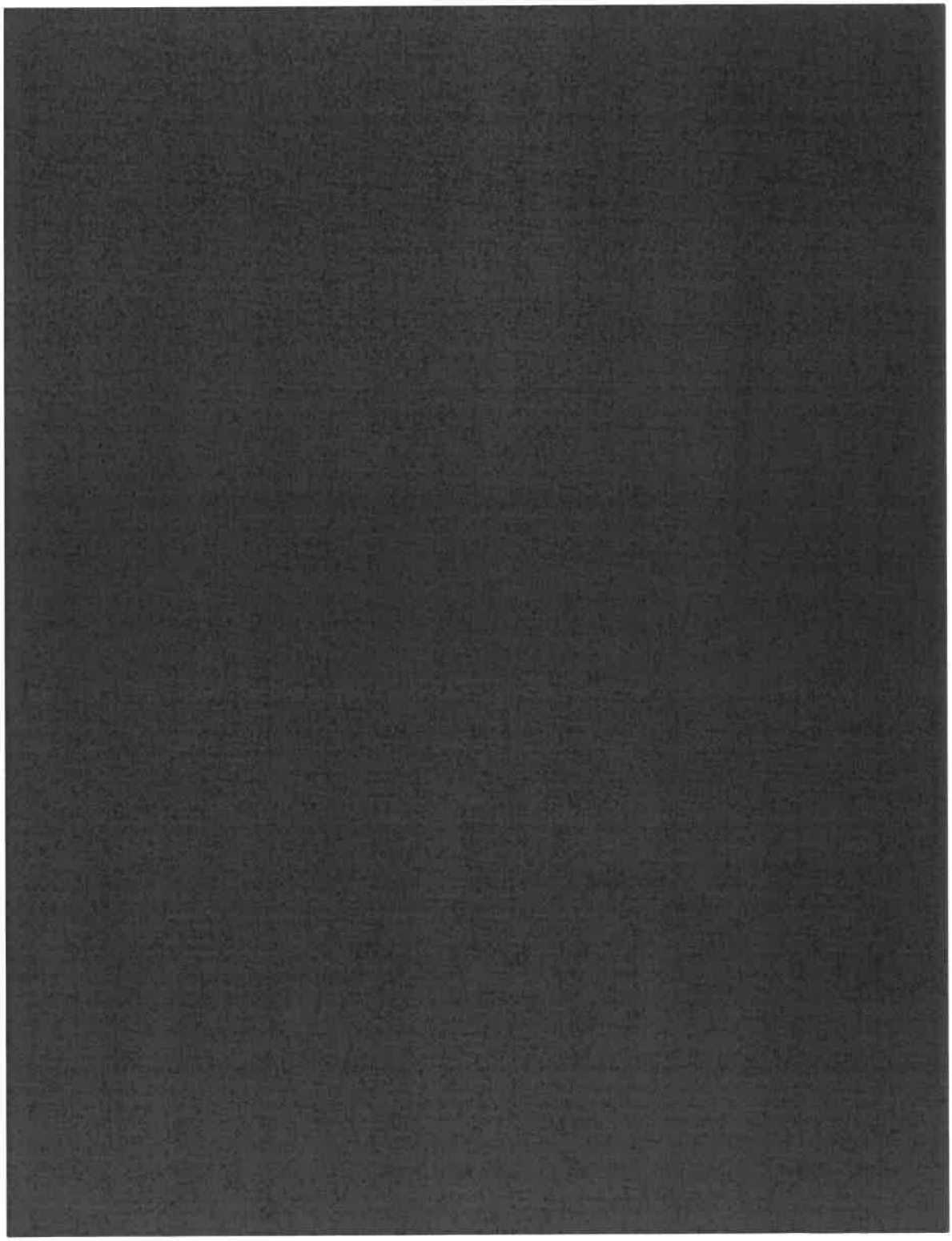
Figure 11 : processus d'activation (étape 3 et 4 – finalisation de l'activation)

15. Pendant que l'opérateur de l'IVI procède à la validation, l'utilisateur choisit un mot de passe de déverrouillage et le saisit dans l'ApCV.
16. S'il le souhaite, l'utilisateur peut ensuite activer la biométrie, qu'il pourra utiliser en substitution du mot de passe pour déverrouiller l'application.
17. Il est ensuite informé qu'il pourra finaliser son activation ultérieurement après les vérifications de l'opérateur de l'IVI.
18. Une fois ces vérifications réalisées, un dossier de preuve est mis à disposition par l'IVI et consultable sur son portail avec données d'identité, copie de la pièce utilisée, score authenticité pièce et score de la comparaison biométrique (ce dossier n'est pas transmis au SI ApCV).
19. L'utilisateur est informé par mail qu'il peut lancer l'ApCV pour finaliser son enrôlement.
20. Les traits d'identité de l'assuré (Nom, prénom, date de naissance) sont récupérés auprès du service de rapprochement d'identités de l'inter-régime et comparés avec ceux extraits de la PI.
21. Les données métier AMO [redacted] et les données d'identité (Etat civil, adresse mail, photo, identité AMO et Patient) sont envoyées [redacted]
22. Si une autre ApCV était déjà associée à l'assuré dans le SI ApCV, elle est révoquée. Si cette ApCV tente de se connecter au SI ApCV, elle sera alors supprimée.

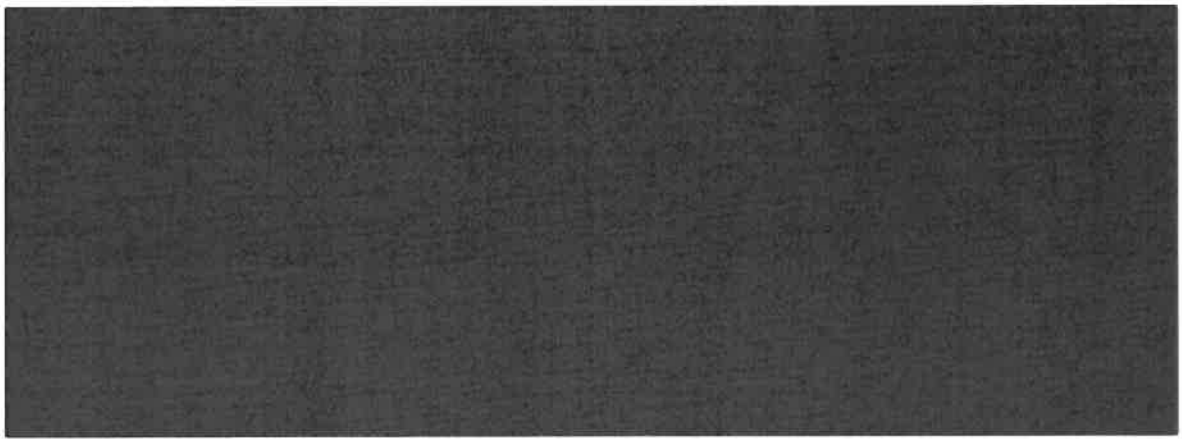
6.1.2 Description du circuit de la donnée

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



6.1.3 Respect des principes fondamentaux

6.1.3.1 Caractéristiques du traitement

	Enrôlement
Finalité principale	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Sous-finalité	Initialiser et activer une ApCV pour un bénéficiaire identifié au moyen d'un traitement biométrique (rapprochement automatisé entre le selfie et le titre d'identité)
Informations complémentaires	Le processus d'activation permet : - A l'utilisateur de s'identifier, de valider son identité et sa photo, d'initialiser son ApCV - De disposer d'un référentiel liant les ApCV à des utilisateurs pour permettre au système ApCV d'être un fournisseur d'identité - De disposer d'une source de référence en cas de contestation, a posteriori, d'un assuré sur l'ApCV qui lui a été délivrée - De disposer des moyens de validation (par échantillonnage) du service rendu par l'IVI ; notamment la justification des traitements manuels versus automatiques
Intervention de sous-traitants ultérieurs	Infogérant du SI ApCV Industriel de Vérification d'Identité Fournisseur du SDK Sécurité et infogérant du SI Sécurité

6.1.3.2 Explication et justification de la minimisation des données

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Données capturées à l'aide de la caméra du smartphone (vidéo du titre d'identité et vidéo du visage de l'utilisateur)	DCP	Nécessaire pour valider l'identité de l'utilisateur	Données minimales nécessaires pour valider l'identité de l'utilisateur Ces données sont traitées au sein du SI IVI et ne sont pas transférées au SI ApCV.
Données utilisées lors du traitement biométrique de la photographie issue du titre d'identité de l'utilisateur et de la vue de son visage (vidéo du titre d'identité, vidéo du visage de l'utilisateur et gabarits biométriques)	DCP sensibles	Nécessaire pour valider l'identité de l'utilisateur	Données minimales nécessaires pour valider l'identité de l'utilisateur Ces données sont traitées en mémoire RAM au sein du SI IVI et ne sont pas transférées au SI ApCV.
Identité AMO (NIR, Nom de famille, Nom d'usage, Prénom, Date de naissance, Rang de naissance)	DCP perçue comme sensible (NIR) et DCP courantes	L'identité AMO est basée sur le NIR de chaque bénéficiaire de soin. Le NIR est associé à un ensemble minimal de données administratives nécessaires dans le cadre de la mission d'intérêt public pour la gestion des droits et prise en charge de l'assuré.	Données minimales nécessaires pour que le PS puisse accéder à un service en ligne concernant le bénéficiaire de soin.
Identité Etat civil et adresse mail (Prénoms, Nom, Date de naissance, Genre, code INSEE de la ville de naissance (si né en France), code INSEE du pays de naissance (si né hors de France), Adresse e-mail)	DCP courantes	L'identité « état civil » de l'utilisateur est récupérée sur sa pièce d'identité. Elle est composée des données nécessaires au statut de fournisseur d'identité sur FranceConnect.	Seules les données d'identité nécessaires au statut de fournisseur d'identité sur FranceConnect sont traitées.
Identité Patient (Matricule INS, Date de naissance, Lieu de naissance, Nom de naissance, Prénoms de naissance, Sexe)	DCP perçue comme sensible (matricule INS) et DCP courantes	L'identité patient est renvoyée par le service INSi pendant l'enrôlement. Cette identité patient permet d'accéder à des services liés au patient, comme le DMP (intégré au LPS) sur le poste du PS	Le stockage des traits d'identité associés à l'INS est imposé par la loi, ils doivent donc accompagner l'INS dans l'ApCV.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Dossier de preuve (vidéo du titre d'identité, vidéo du visage de l'utilisateur, noms et prénoms de l'utilisateur, date et lieu de naissance, numéro du titre d'identité, date de délivrance du titre d'identité, date d'expiration du titre d'identité)	DCP courantes	- Disposer d'une source de référence en cas de contestation, a posteriori, d'un assuré sur l'ApCV qui lui a été délivrée. - Disposer des moyens de validation (par échantillonnage) du service rendu par l'IVI ; notamment la justification des traitements manuels versus automatiques	Le dossier de preuve est stocké sur le SI IVI et n'est pas transféré au SI ApCV.
Données temporaires d'activation (NIR, adresse e-mail, traits d'identité extraits par l'IVI, type et n° de PI, date de délivrance et date d'expiration, selfie extrait du flux vidéo)	DCP perçue comme sensible (NIR) et DCP courantes	Permettre à l'utilisateur de finaliser l'enrôlement une fois les vérifications humaines réalisées par l'IVI.	Dans la version actuelle, les informations type, n° de PI, date de délivrance et d'expiration sont retournées au SI ApCV par l'IVI. Elles ne sont pas traitées ni conservées dans le SI ApCV et ne devraient donc pas être retournées par l'IVI.
Fichier des enrôlés (NIR, identifiant profil ApCV, code régime, code caisse, code centre, date de l'enrôlement)	DCP perçue comme sensible (NIR)	Transmettre au régime un état des assurés enrôlés	
UserID	DCP courante	Identifiant de l'utilisateur de l'ApCV dans le SI Sécurité	
Traces de fonctionnement [redacted] identifiant ApCV, identifiant profil ApCV, NIR pseudonymisé, adresse IP smartphone*)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées. Par ailleurs, pas de conservation de données directement identifiantes.

[redacted]

Le principe de minimisation n'est pas respecté ici du fait de la collecte de données non nécessaires (données temporaires d'activation). Une action de mise en conformité est prévue au plan d'action (EX147).

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.1.3.3 Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification
Signature des données d'identité à l'enrôlement.	[MES230] Les données d'identité sont stockées dans des documents signés [redacted]
Vérification de la disponibilité d'une mise à jour des données d'identité AMO et Patient à chaque lancement de l'application si la durée de validité est dépassée (24h).	La mise à jour des données s'appuie sur les référentiels des régimes qui portent la responsabilité de l'exactitude des données d'identité AMO. A noter que les données d'identité ne sont pas mises à jour post-enrôlement car elles proviennent de la pièce d'identité.

6.1.3.4 Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données capturées à l'aide de la caméra du smartphone (vidéo du titre d'identité et vidéo du visage de l'utilisateur)	96 heures		Traitement automatique
Données utilisées lors du traitement biométrique de la photographie issue du titre d'identité de l'utilisateur et de la vue de son visage (vidéo du titre d'identité, vidéo du visage de l'utilisateur et gabarits biométriques)	Données non stockées, non conservées.	Données traitées en mémoire (RAM)	N/A
Identité AMO **Identité Etat civil et adresse mail** **Identité Patient**	N/A	Données non conservées après l'enrôlement (stockées chiffrées dans l'ApCV et empreinte stockée dans le SI ApCV)	N/A

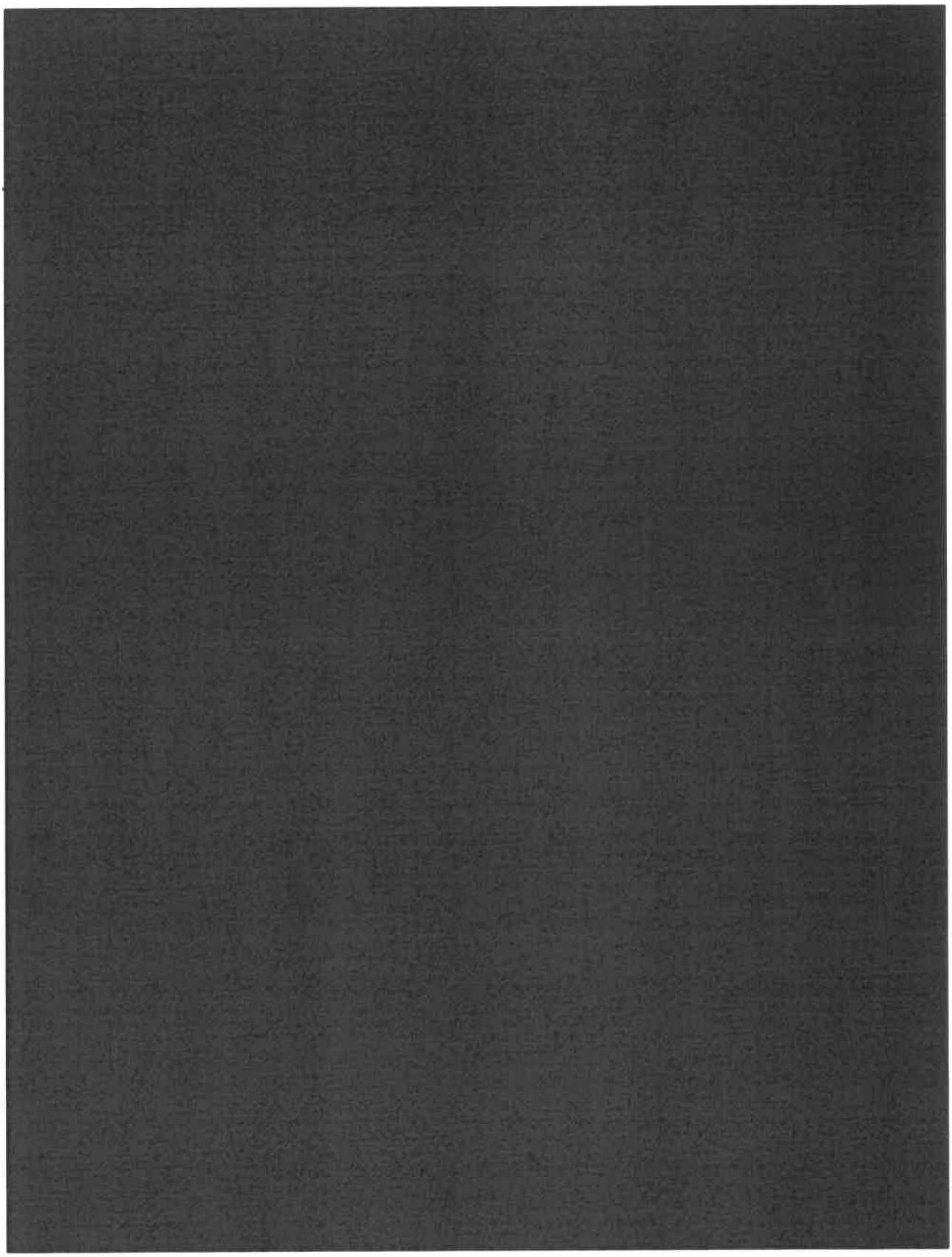
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Dossier de preuve (vidéo du titre d'identité, vidéo du visage de l'utilisateur, noms et prénoms de l'utilisateur, date et lieu de naissance, numéro du titre d'identité, date de délivrance du titre d'identité, date d'expiration du titre d'identité)	1 mois pour les dossiers en succès 3 mois pour les dossiers en échec	Suivi du marché IVI (facturation) Traitement des contestations.	Traitement automatique
Données temporaires d'activation (NIR, adresse e-mail, traits d'identité extraits par l'IVI, type et n° de PI, date de délivrance et date d'expiration, selfie extrait du flux vidéo)	7 jours, sauf type et n° de PI, date de délivrance et date d'expiration qui sont reçues mais non conservées par le SI ApCV	Donner le temps aux assurés de venir finaliser leur enrôlement une fois les vérifications humaines réalisées par l'IVI	Traitement automatique
Données permettant de constituer les fichiers des enrôlés (NIR, identifiant profil ApCV, code régime, code caisse, code centre, date de l'enrôlement)	14 jours	Envoi hebdomadaire vers les régimes (7 jours de délai pour que les assurés finalisent leur enrôlement + 7 jours maximum jusqu'au prochain envoi aux régimes)	Traitement automatique
Fichier des enrôlés (NIR, identifiant profil ApCV, code régime, code caisse, code centre, date de l'enrôlement)	30 jours	Envoi hebdomadaire vers les régimes. Conservation 30 jours pour permettre de regénérer un fichier en cas de problème.	Purge manuelle (action récurrente d'exploitation de l'infogérant [redacted]

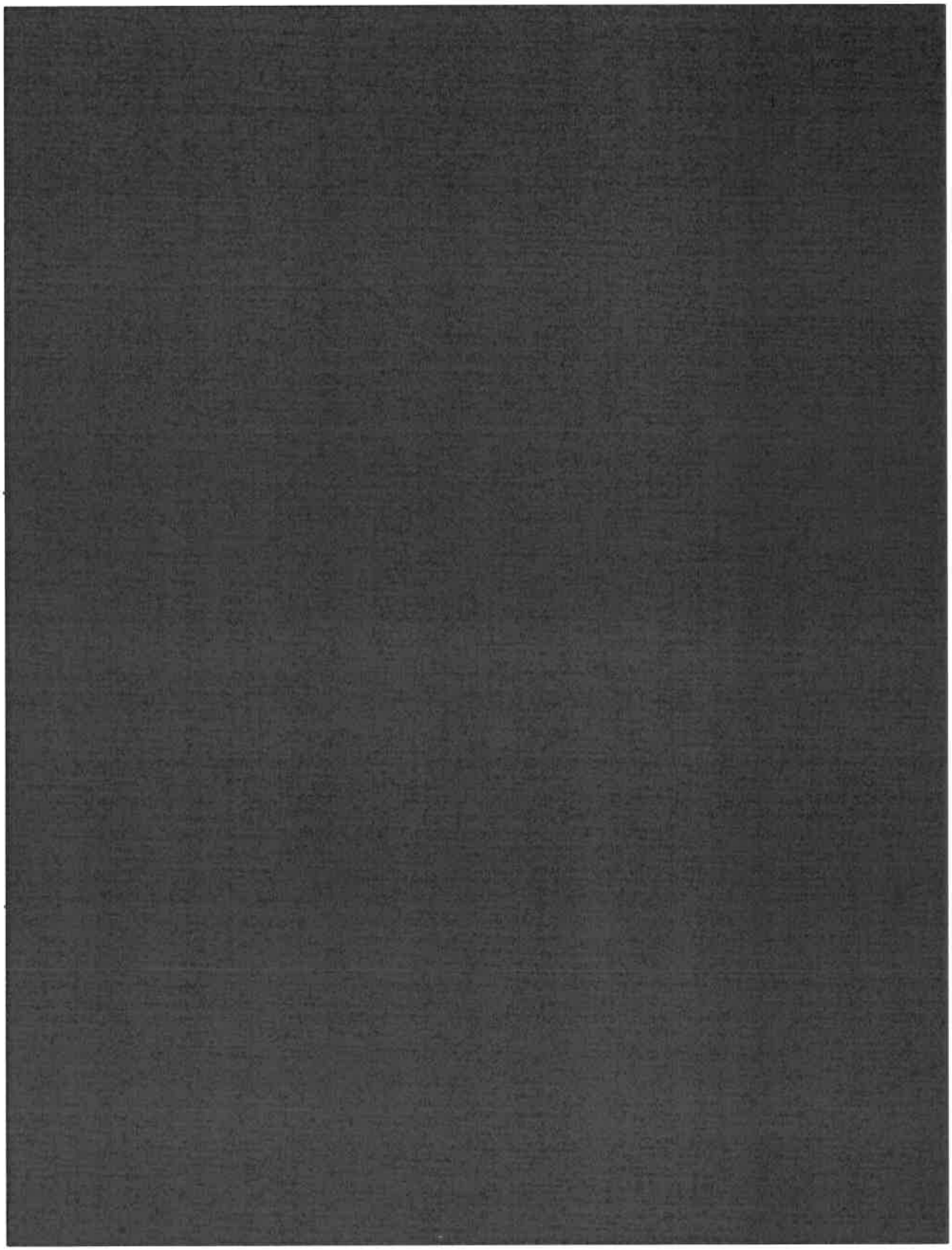
6.1.4 Mesures de sécurité

[redacted]

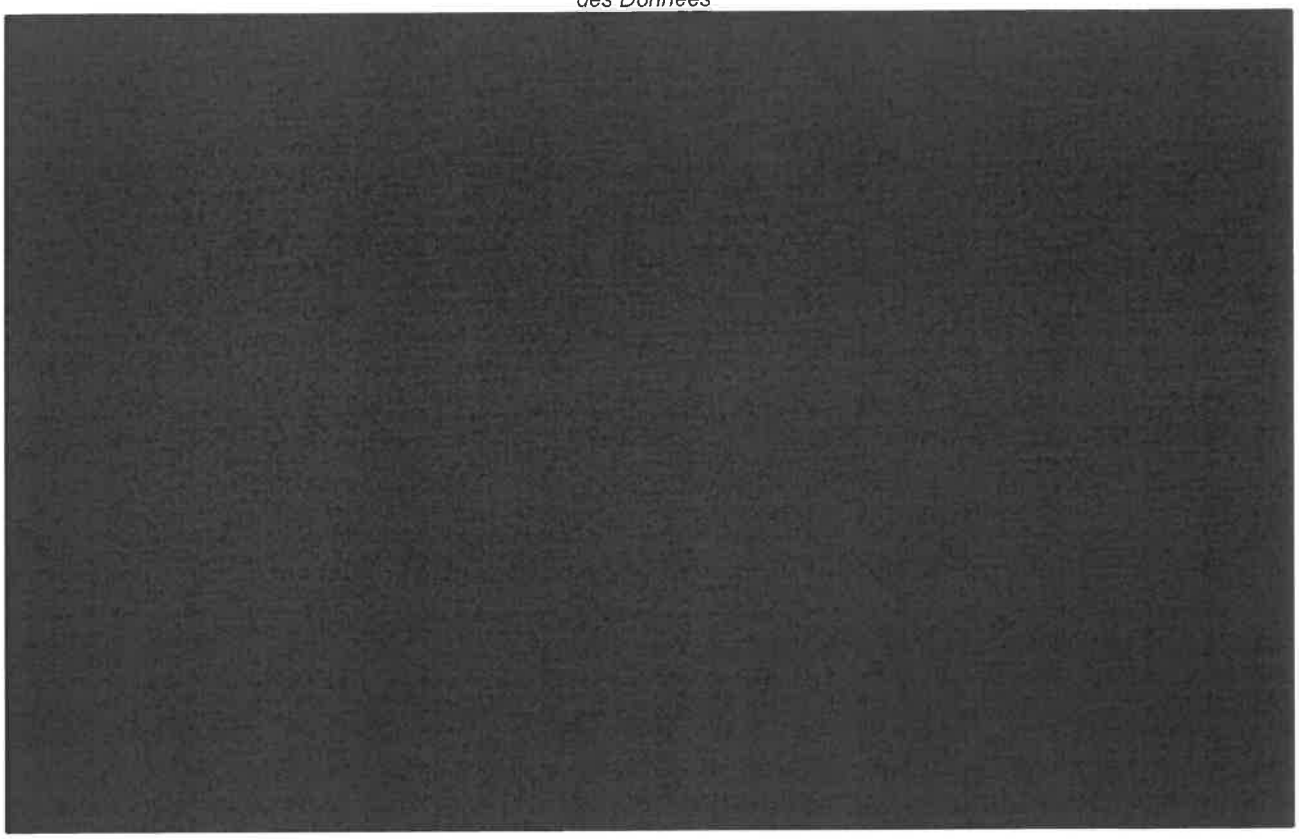
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



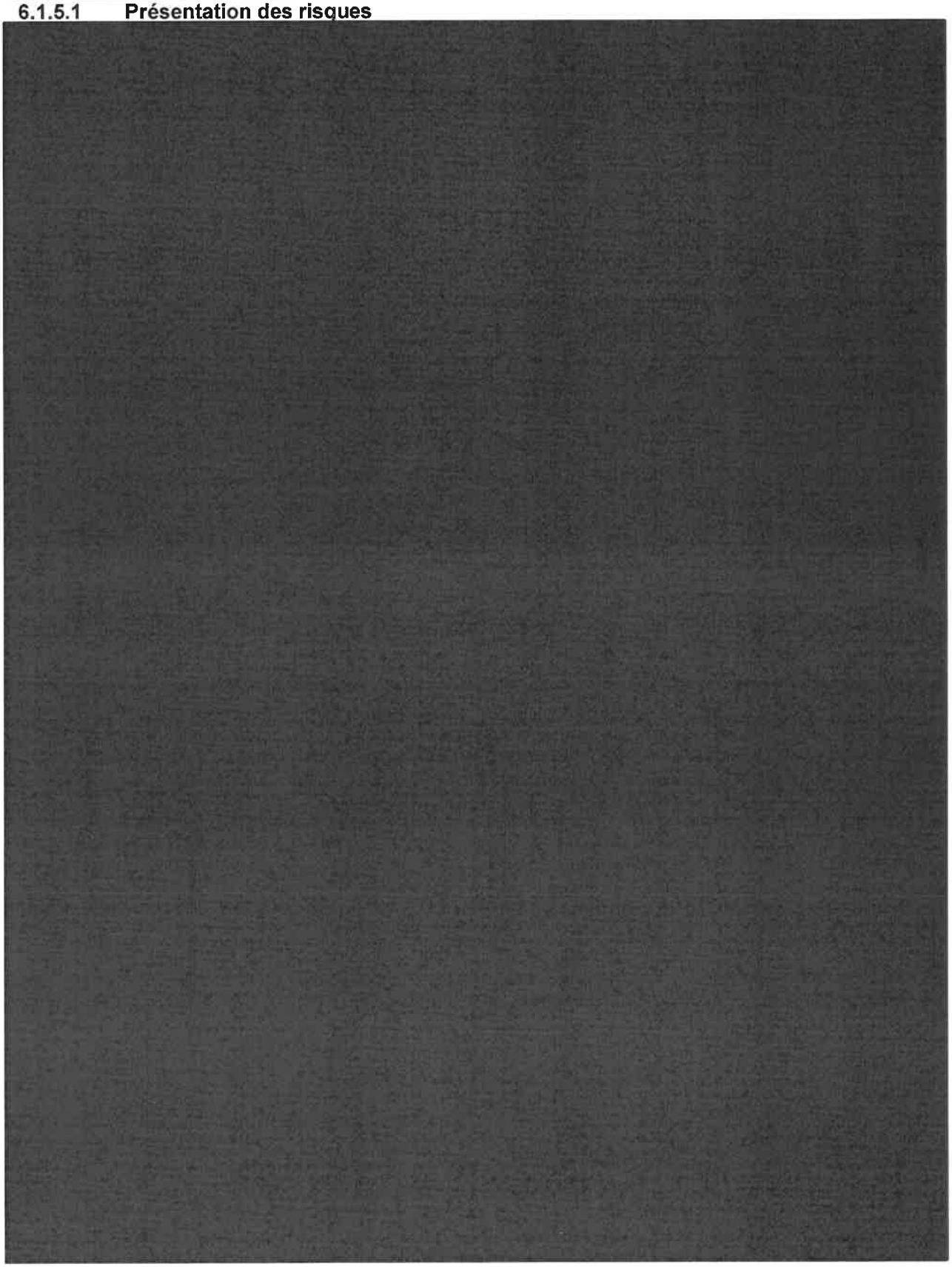
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



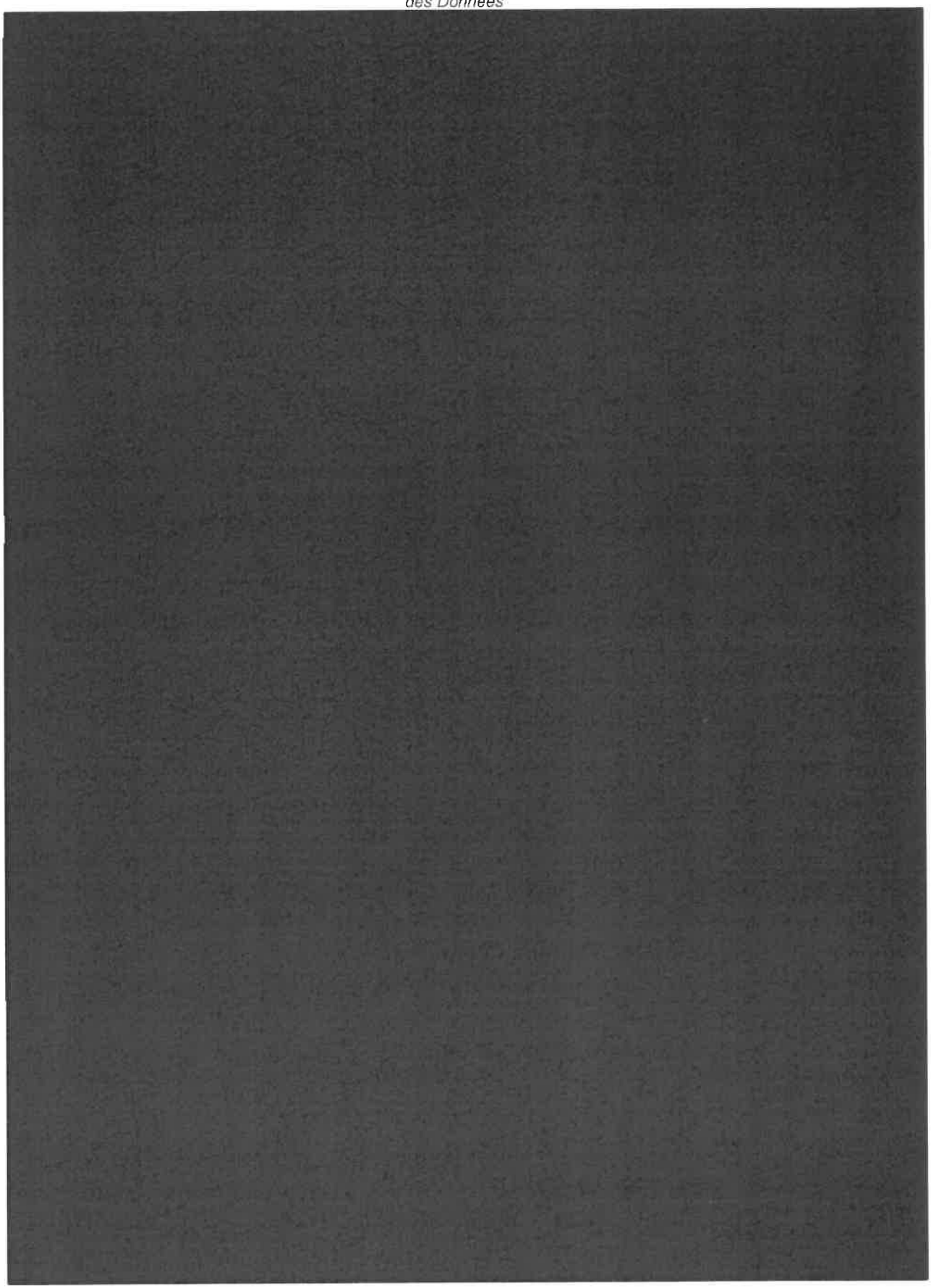
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.1.5 Risques

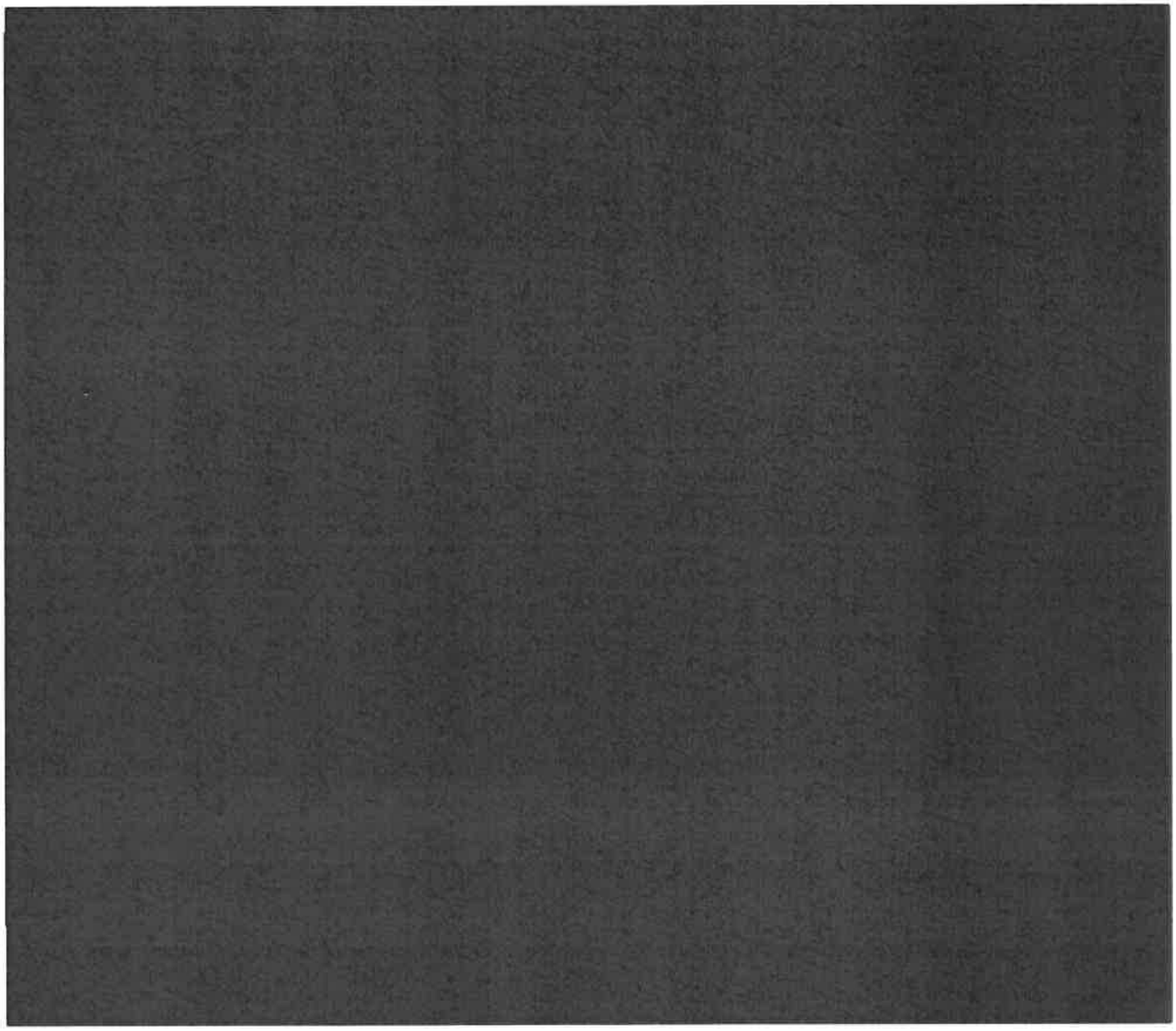
6.1.5.1 Présentation des risques



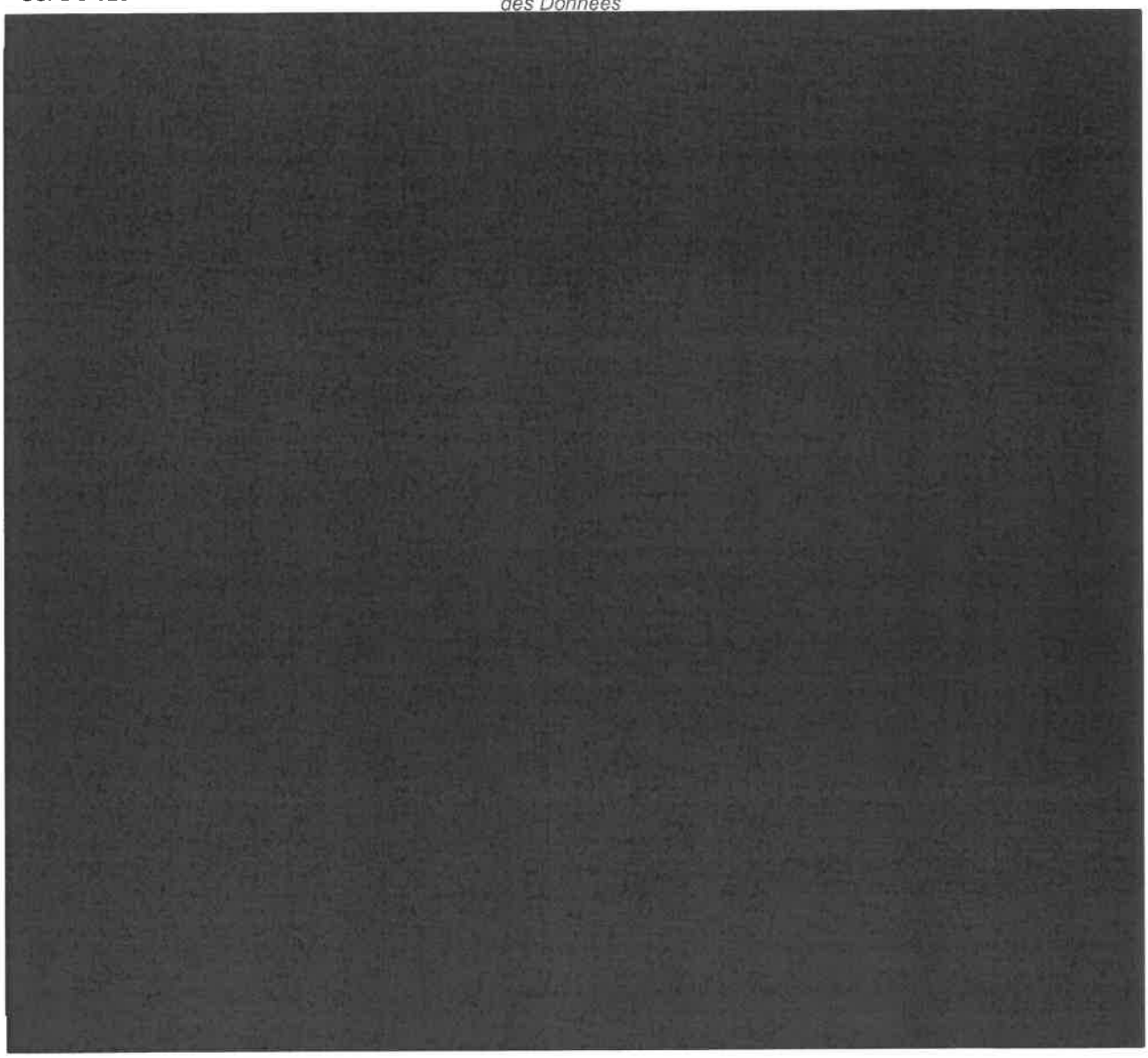
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



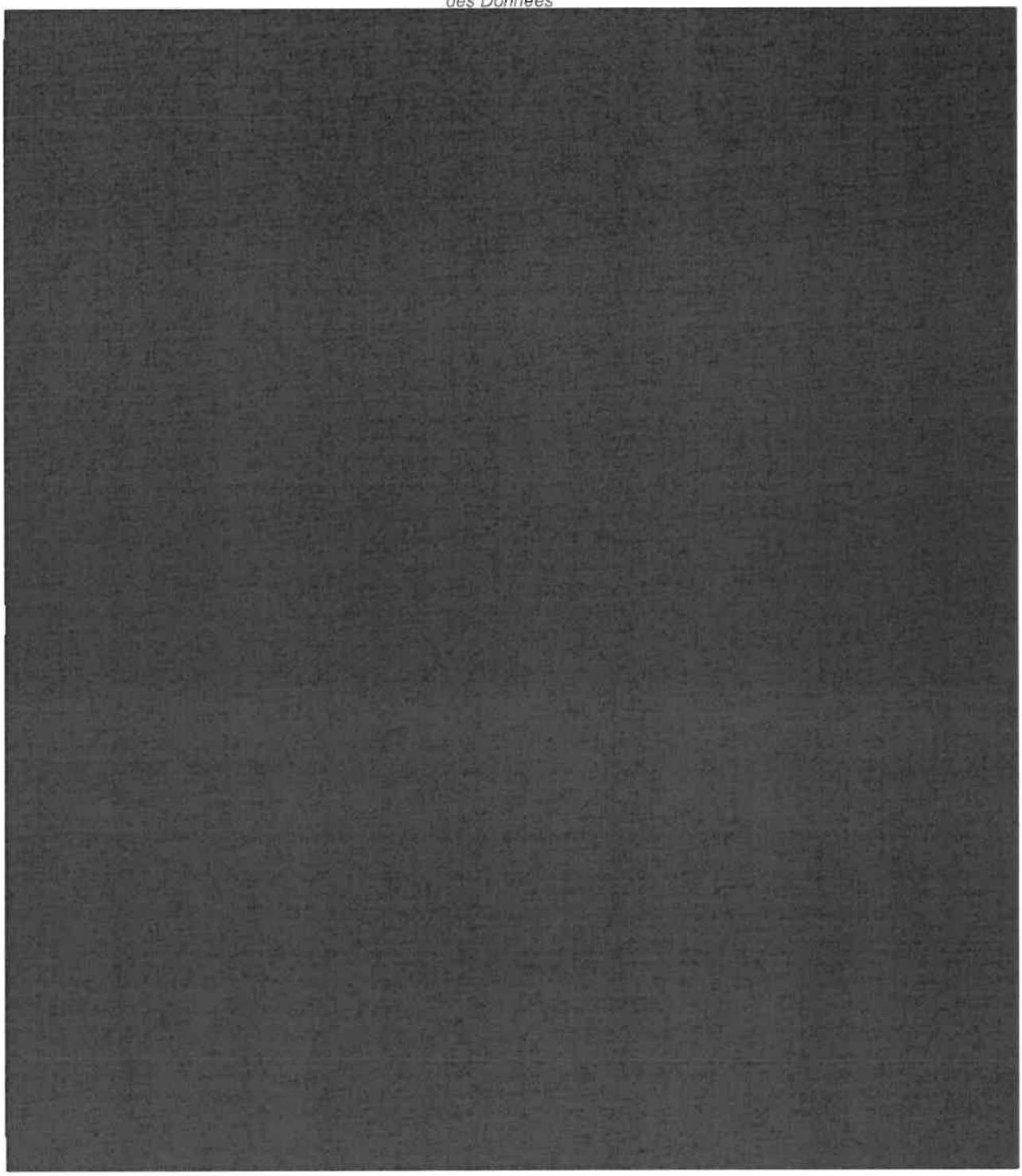
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



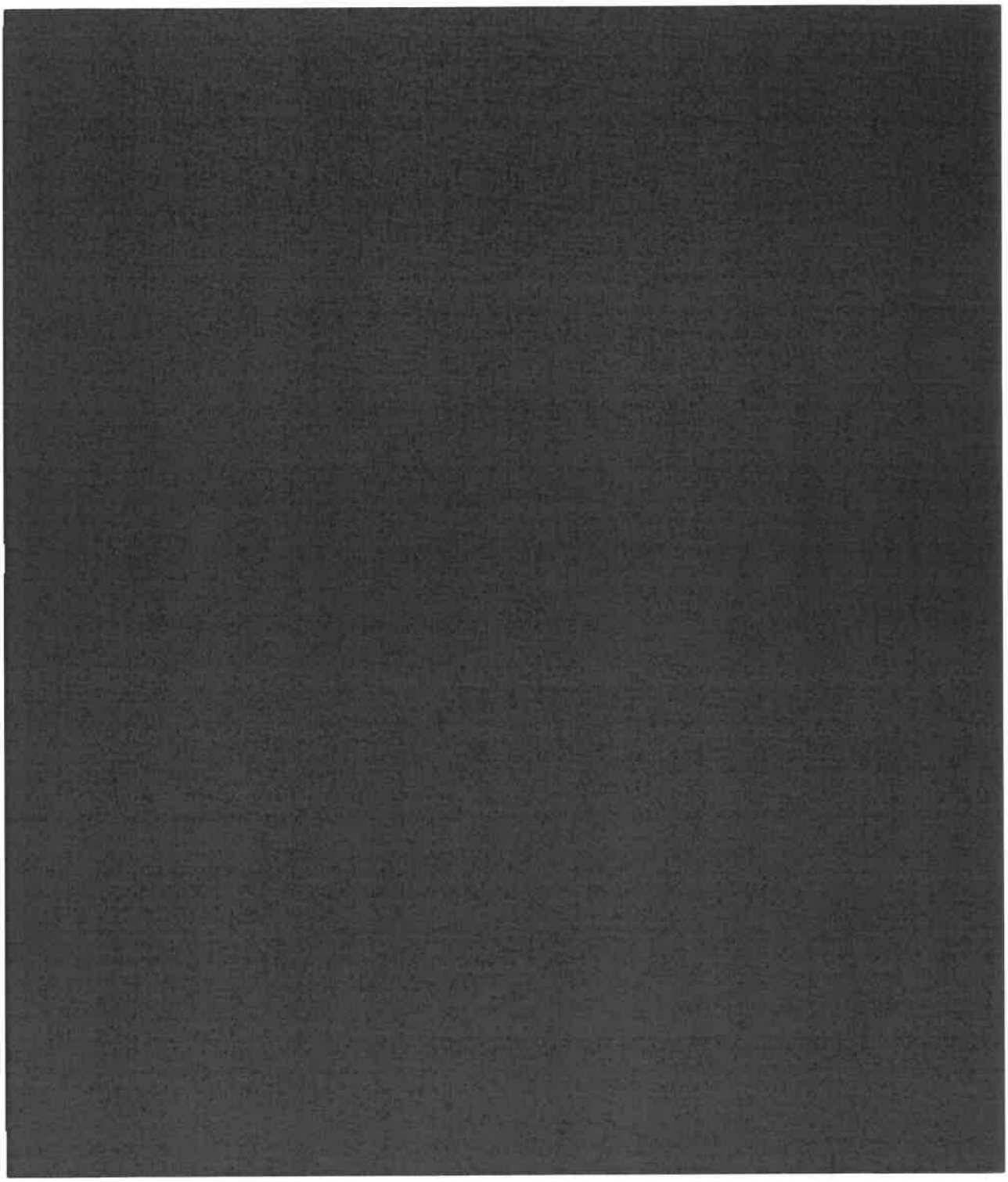
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



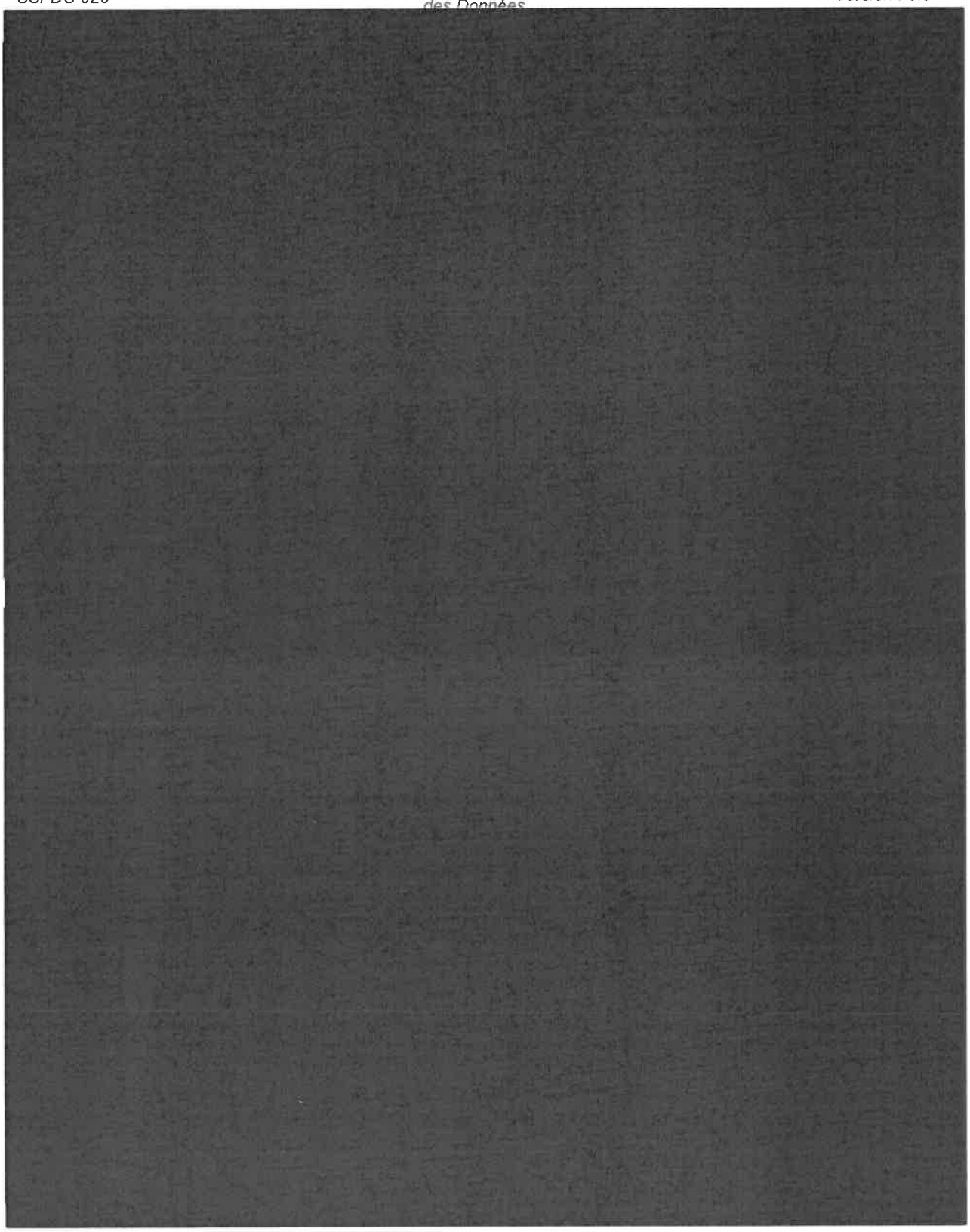
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

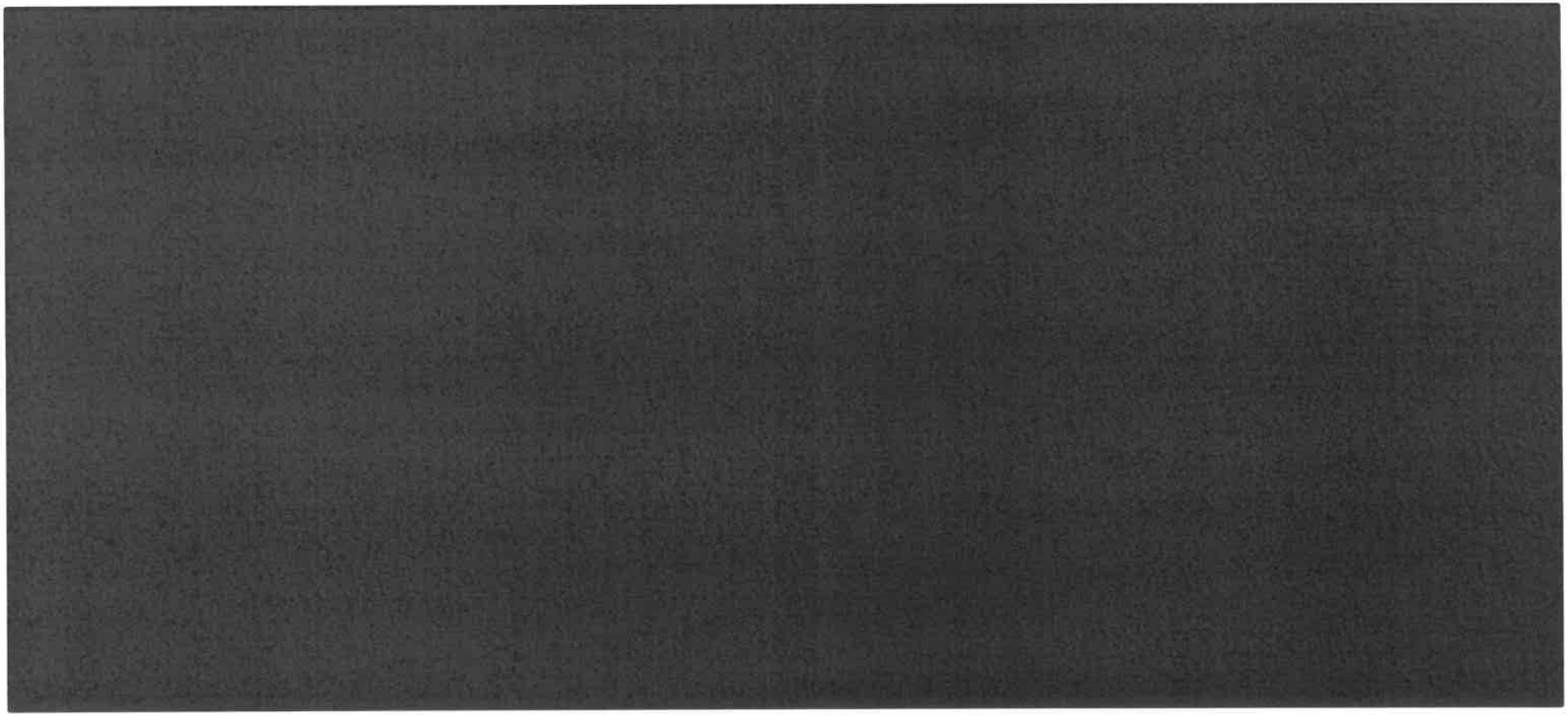


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



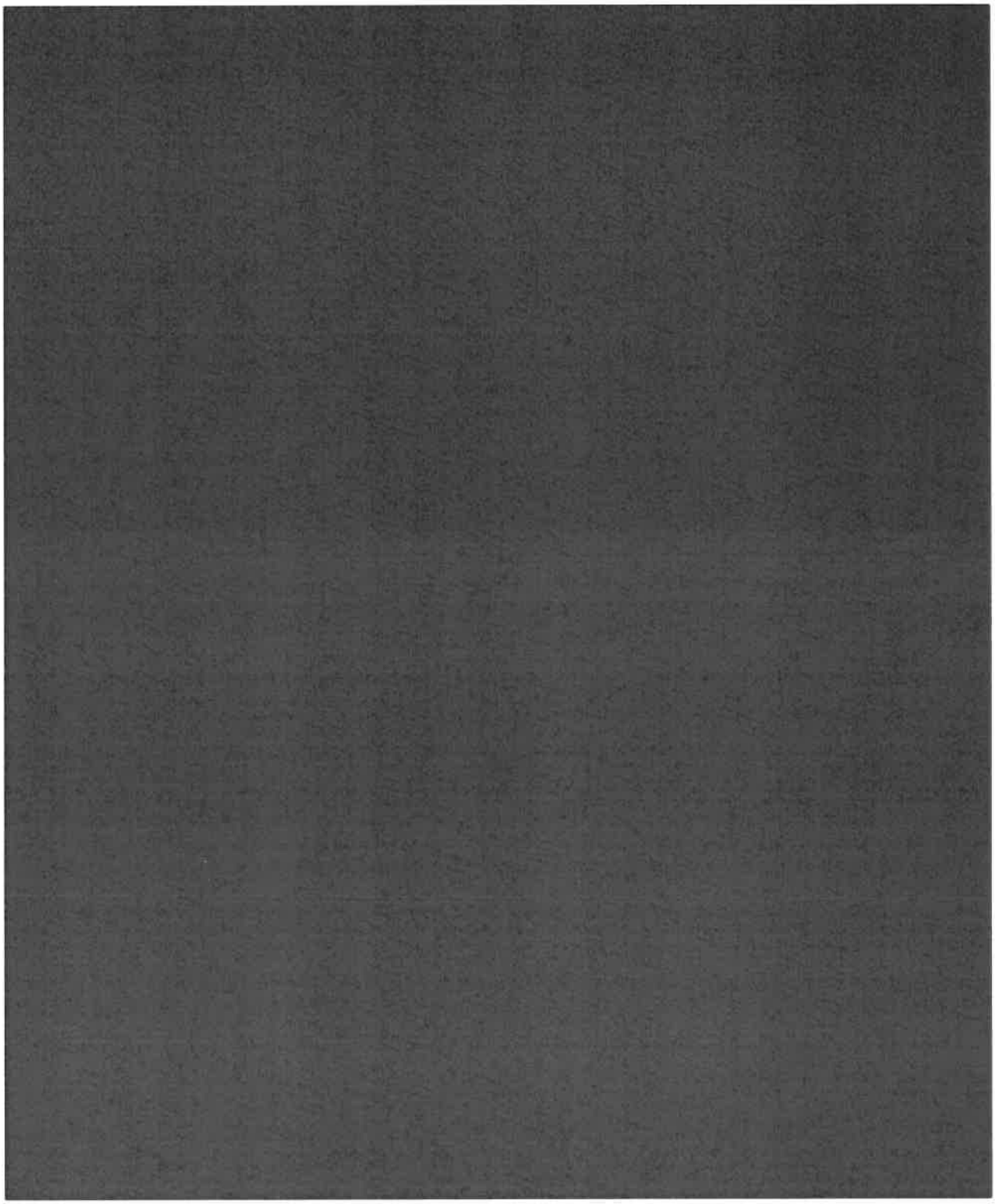
6.1.5.2 Couverture des risques

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

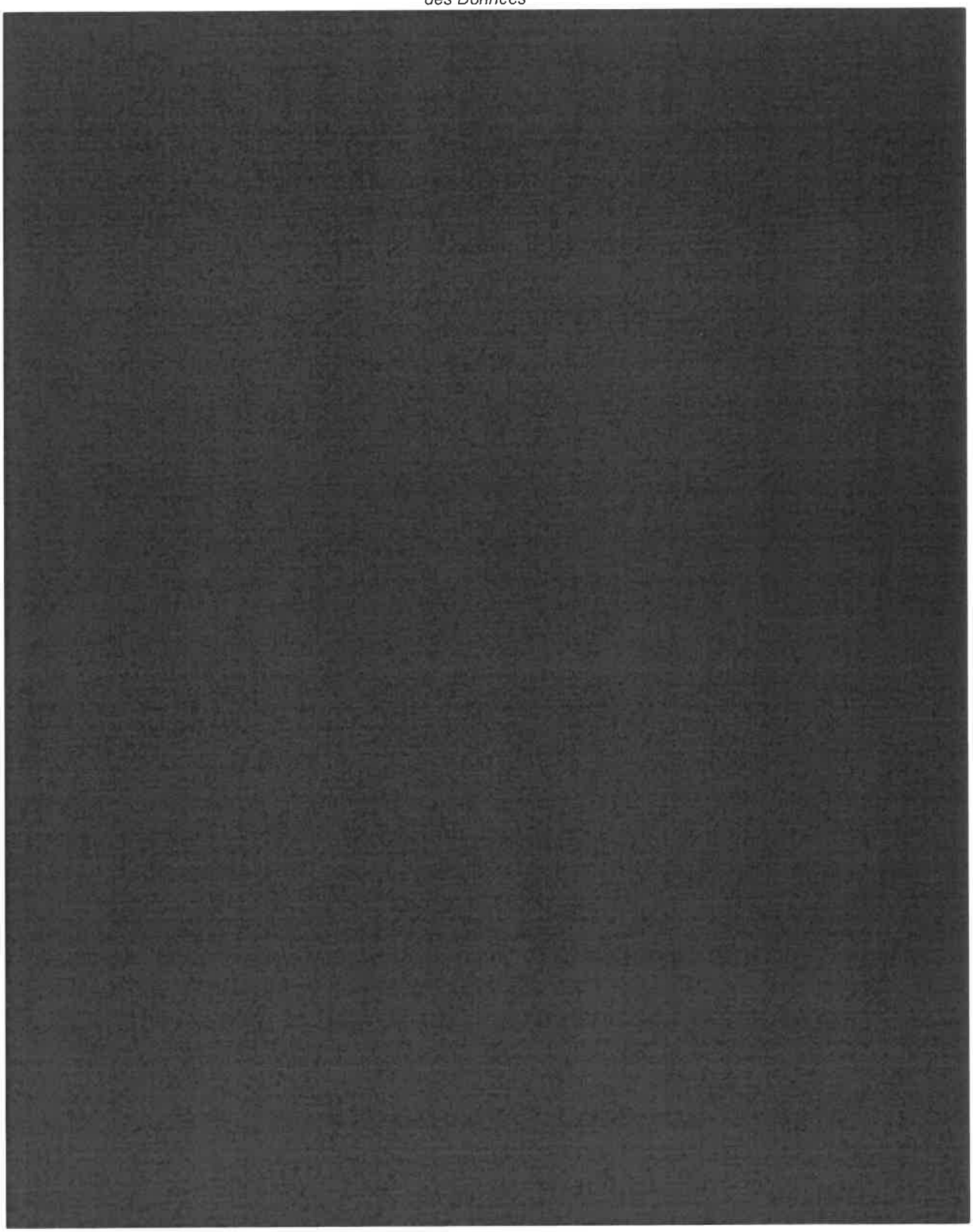


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.1.5.3 Plan d'action



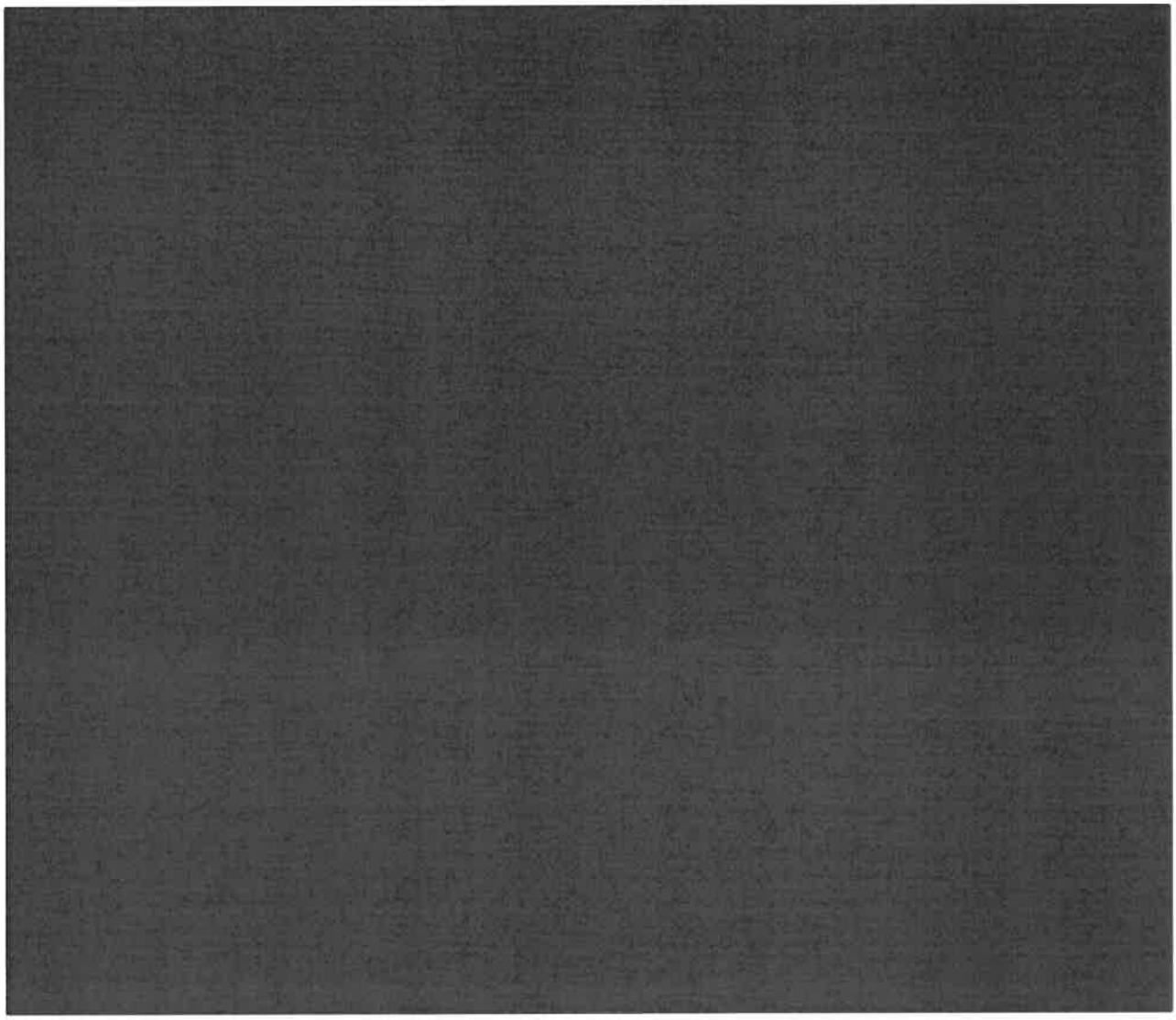
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.2 Parcours d'activation France Identité

6.2.1 Description du processus d'activation

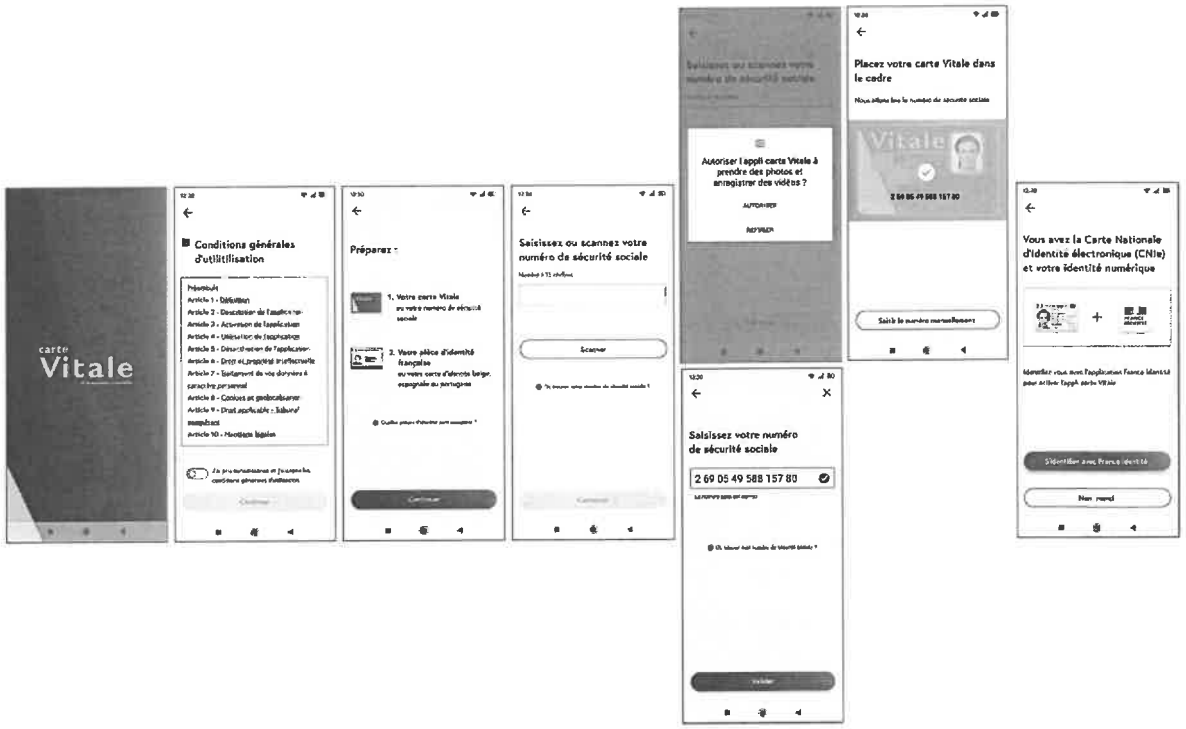


Le processus d'activation se décompose en 3 grandes étapes :

1. L'assuré fournit son NIR et choisit le parcours d'activation avec France Identité ;
2. La vérification d'identité est déléguée à l'application France Identité ;
3. L'assuré finalise l'activation dans l'ApCV en définissant son code secret.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Etape 1 :



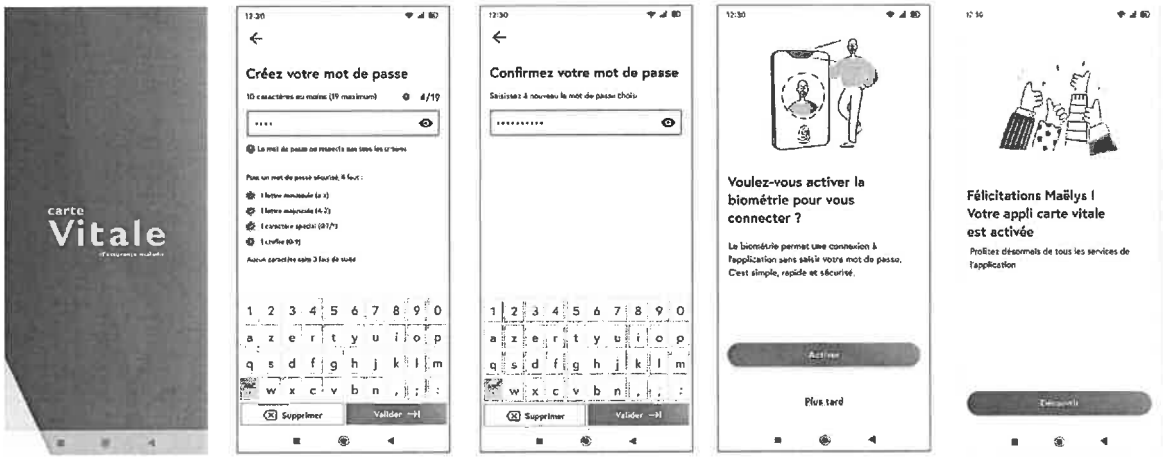
1. L'utilisateur installe l'ApCV sur son smartphone. [MES06] Au premier lancement, il prend connaissance des CGU et de la Politique de protection des données personnelles. Il déclare en avoir pris connaissance, sans quoi il ne peut pas démarrer l'activation.
2. Il saisit ensuite son NIR ou utilise la lecture automatique du NIR sur sa carte Vitale : une vérification de l'éligibilité de l'assuré est opérée par appel au service Eligibilité de l'inter-régime. Si l'assuré n'est pas éligible, il est informé qu'il ne peut pas poursuivre l'enrôlement.
3. Il choisit de poursuivre avec l'application France Identité.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Etape 2 :

4. L'application France Identité est lancée automatiquement grâce à un appel inter-applications : pour poursuivre, l'utilisateur doit accepter la transmission des données suivantes : données d'identité état civil (6 traits d'identité), adresse mail et photo.
5. L'utilisateur scanne sa CNIe pour lire le code CAN (code à 6 chiffres en bas à droite de la face avant de la CNIe) ou le saisit manuellement.
6. Il saisit son code personnel France Identité.
7. Une lecture sans fil de la CNIe démarre : l'utilisateur pose le smartphone sur sa CNIe le temps que la lecture soit réalisée.
8. Une fois la lecture réalisée, l'application France Identité envoie les données d'identité, l'adresse mail et la photo au SI ApCV.

Etape 3 :



9. L'appli carte Vitale est relancée automatiquement via un appel inter-applications.
10. L'utilisateur choisit un mot de passe de déverrouillage et le saisit dans l'ApCV.
11. S'il le souhaite, l'utilisateur peut ensuite activer la biométrie, qu'il pourra utiliser en substitution du mot de passe pour déverrouiller l'application.
12. Le SI ApCV compare les traits d'identité de l'assuré avec ceux fournis par le service de rapprochement d'identités de l'inter-régime.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

13. Les données métier AMO [redacted] et les données d'identité (Etat civil, adresse mail, photo, identité AMO et Patient) sont envoyées [redacted] dans l'ApCV [redacted]
14. Si une ancienne ApCV était déjà associée à l'assuré dans le SI ApCV, celle-ci est révoquée. Si cette ApCV tente de se connecter au SI ApCV, elle sera alors supprimée.

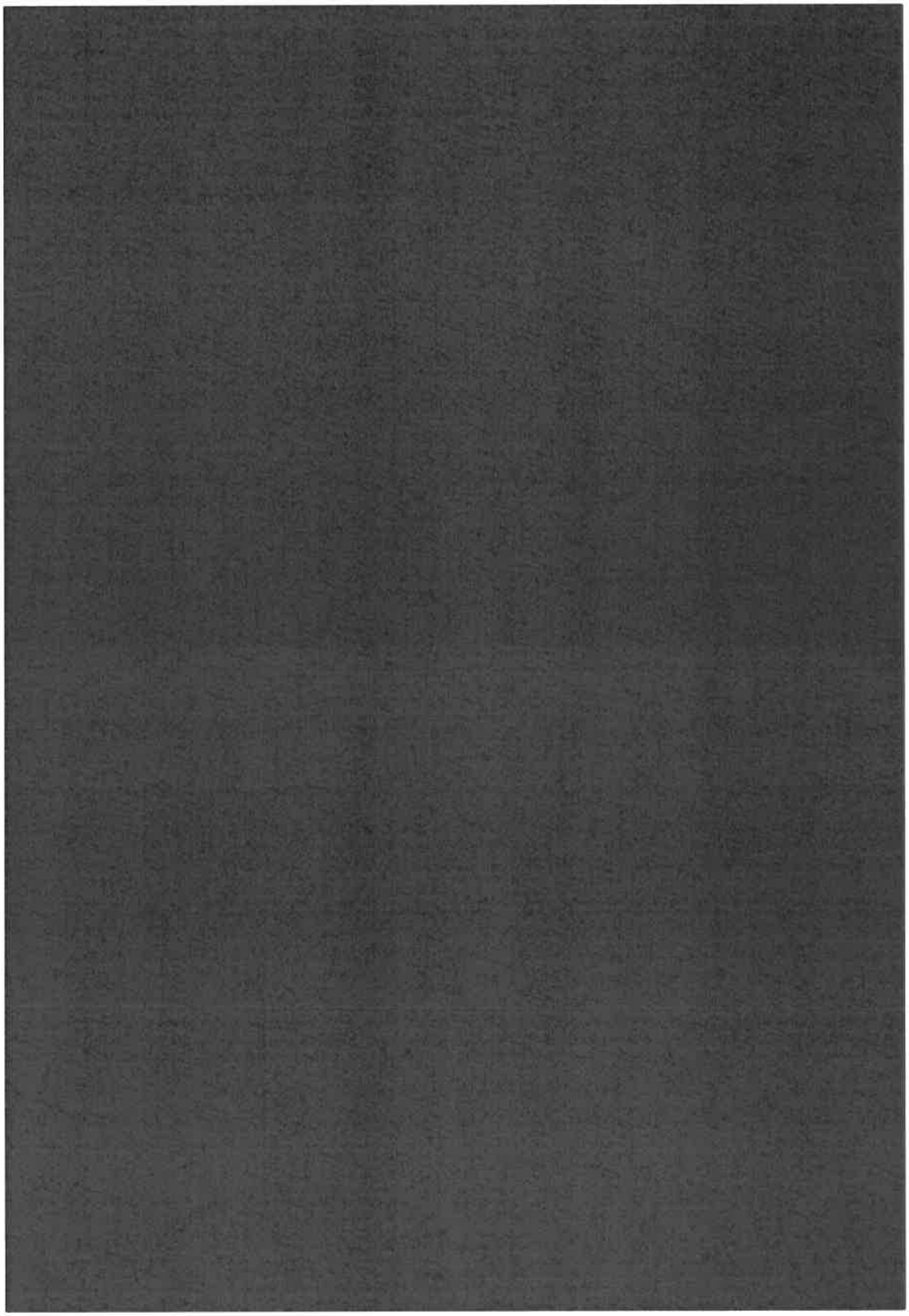
6.2.2 Focus sur le protocole de dérivation d'identité utilisé [redacted]

[redacted]

6.2.3 Description du circuit de la donnée

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.2.4 Respect des principes fondamentaux

6.2.4.1 Caractéristiques du traitement

	Enrôlement
Finalité principale	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Sous-finalité	Initialiser et activer une ApCV pour un bénéficiaire identifié au moyen de l'application France Identité
Informations complémentaires	Le processus d'activation permet : - A l'utilisateur de s'identifier, de valider son identité et d'initialiser son ApCV - De disposer d'un référentiel liant les ApCV à des utilisateurs pour permettre au système ApCV d'être un fournisseur d'identité - De disposer d'une source de référence en cas de contestation, a posteriori, d'un assuré sur l'ApCV qui lui a été délivrée
Intervention de sous-traitants ultérieurs	Infogérant du SI ApCV [redacted] Fournisseur du SDK Sécurité et infogérant du SI Sécurité [redacted]

6.2.4.2 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Identité AMO (NIR, Nom de famille, Nom d'usage, Prénom, Date de naissance, Rang de naissance)	DCP perçue comme sensible (NIR) et DCP courantes	L'identité AMO est basée sur le NIR de chaque bénéficiaire de soin. Le NIR est associé à un ensemble minimal de données administratives nécessaires dans le cadre de la mission d'intérêt public pour la gestion des droits et prise en charge de l'assuré.	Données minimales nécessaires pour que le PS puisse accéder à un service en ligne concernant le bénéficiaire de soin.
Identité Etat civil, adresse mail et photo (Prénoms, Nom, Date de naissance, Genre, code INSEE de la ville de naissance (si né en France), code INSEE du pays de naissance (si né hors de France), Adresse e-mail)	DCP courantes	L'identité « état civil », l'adresse mail et la photo sont fournies par l'application France Identité. La photo est nécessaire pour être affichée sur l'écran de présentation du QR code. Les autres données sont nécessaires au statut de fournisseur d'identité sur FranceConnect.	Seules les données d'identité nécessaires au statut de fournisseur d'identité sur FranceConnect sont traitées.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Identité Patient (Matricule INS, Date de naissance, Lieu de naissance, Nom de naissance, Prénoms de naissance, Sexe)	DCP perçue comme sensible (matricule INS) et DCP courantes	L'identité patient est renvoyée par le service INSi pendant l'enrôlement. Cette identité patient permet d'accéder à des services liés au patient, comme le DMP (intégré au LPS) sur le poste du PS	Le stockage des traits d'identité associés à l'INS est imposé par la loi, ils doivent donc accompagner l'INS dans l'ApCV.
Fichier des enrôlés (NIR, identifiant profil ApCV, code régime, code caisse, code centre, date de l'enrôlement)	DCP perçue comme sensible (NIR)	Transmettre au régime un état des assurés enrôlés	
UserID	DCP courante	Identifiant de l'utilisateur de l'ApCV dans le SI Sécurité	
Traces de fonctionnement [redacted] identifiant ApCV, identifiant profil ApCV, NIR pseudonymisé, adresse IP smartphone*)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées. Par ailleurs, pas de conservation de données directement identifiantes.

[redacted]

6.2.4.3 Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification
Signature des données d'identité à l'enrôlement.	[MES230] Les données d'identité sont stockées dans des documents signés [redacted]
Vérification de la disponibilité d'une mise à jour des données d'identité AMO et Patient à chaque lancement de l'application si la durée de validité est dépassée (24h).	La mise à jour des données s'appuie sur les référentiels des régimes qui portent la responsabilité de l'exactitude des données d'identité AMO. A noter que les données d'identité ne sont pas mises à jour post-enrôlement car elles proviennent de la pièce d'identité.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

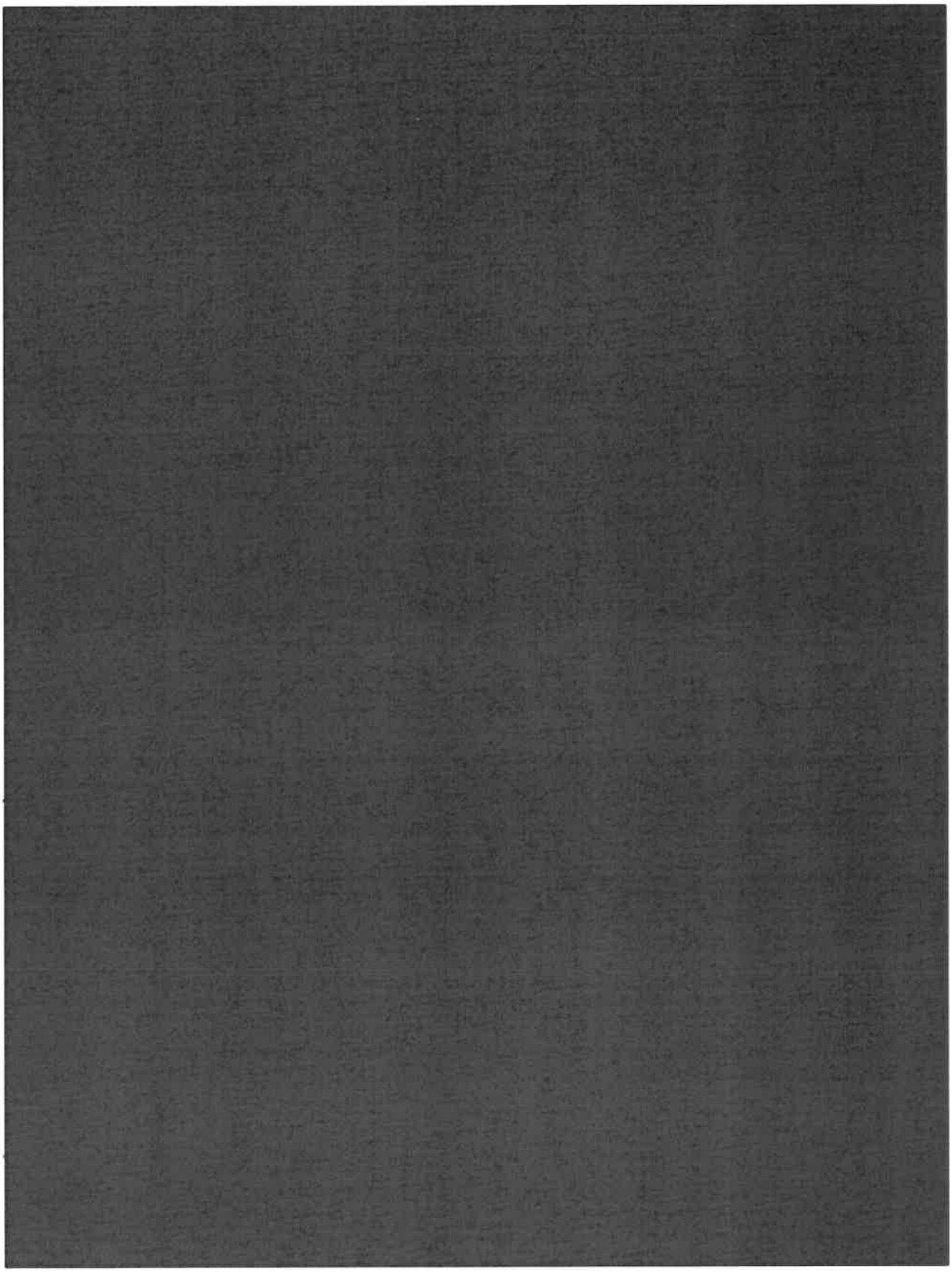
6.2.4.4 Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données temporaires d'activation (NIR, Identité Etat civil, adresse mail et photo fournies par l'application France Identité)	7 jours	La durée de rétention des enrôlements en cours est faible (puisqu'un enrôlement CNIe ne nécessite pas de temps d'attente). Cependant, un enrôlement CNIe pouvant devenir un enrôlement IVI en cas d'échec, la durée de rétention est donc alignée sur celle des enrôlements IVI	Traitement automatique
Identité AMO **Identité Patient** **Identité Etat civil, adresse mail et photo**	N/A	Données non conservées dans le SI ApCV après l'enrôlement (stockées chiffrées dans l'ApCV et empreinte stockée dans le SI ApCV)	N/A
Données permettant de constituer les fichiers des enrôlés (NIR, identifiant profil ApCV, code régime, code caisse, code centre, date de l'enrôlement)	14 jours	Envoi hebdomadaire vers les régimes (7 jours de délai pour que les assurés finalisent leur enrôlement + 7 jours maximum jusqu'au prochain envoi aux régimes)	Traitement automatique
Fichier des enrôlés (NIR, identifiant profil ApCV, code régime, code caisse, code centre, date de l'enrôlement)	30 jours	Envoi hebdomadaire vers les régimes. Conservation 30 jours pour permettre de regénérer un fichier en cas de problème.	Purge manuelle (action récurrente d'exploitation de l'infogérant [redacted]

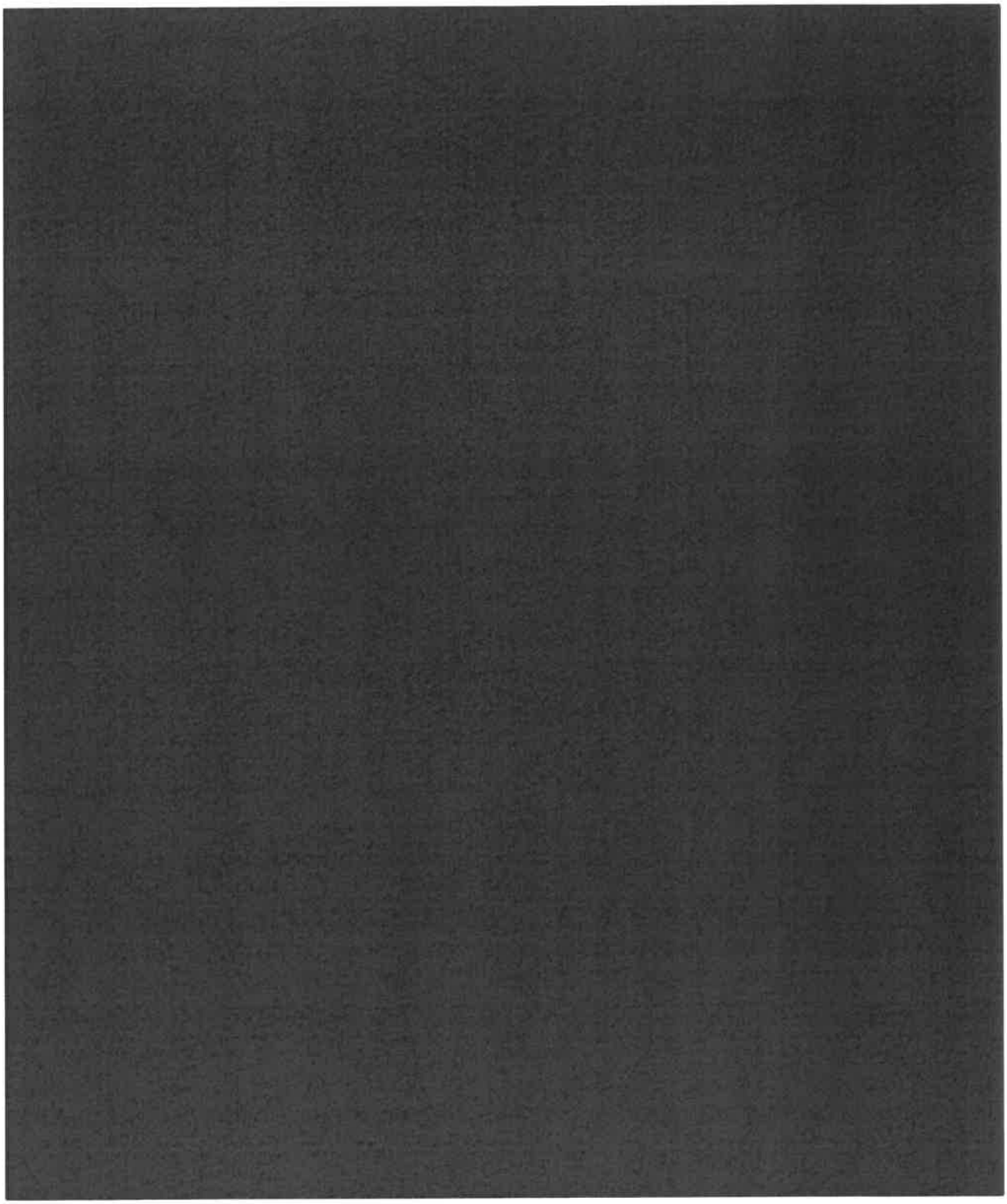
6.2.5 Mesures de sécurité

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



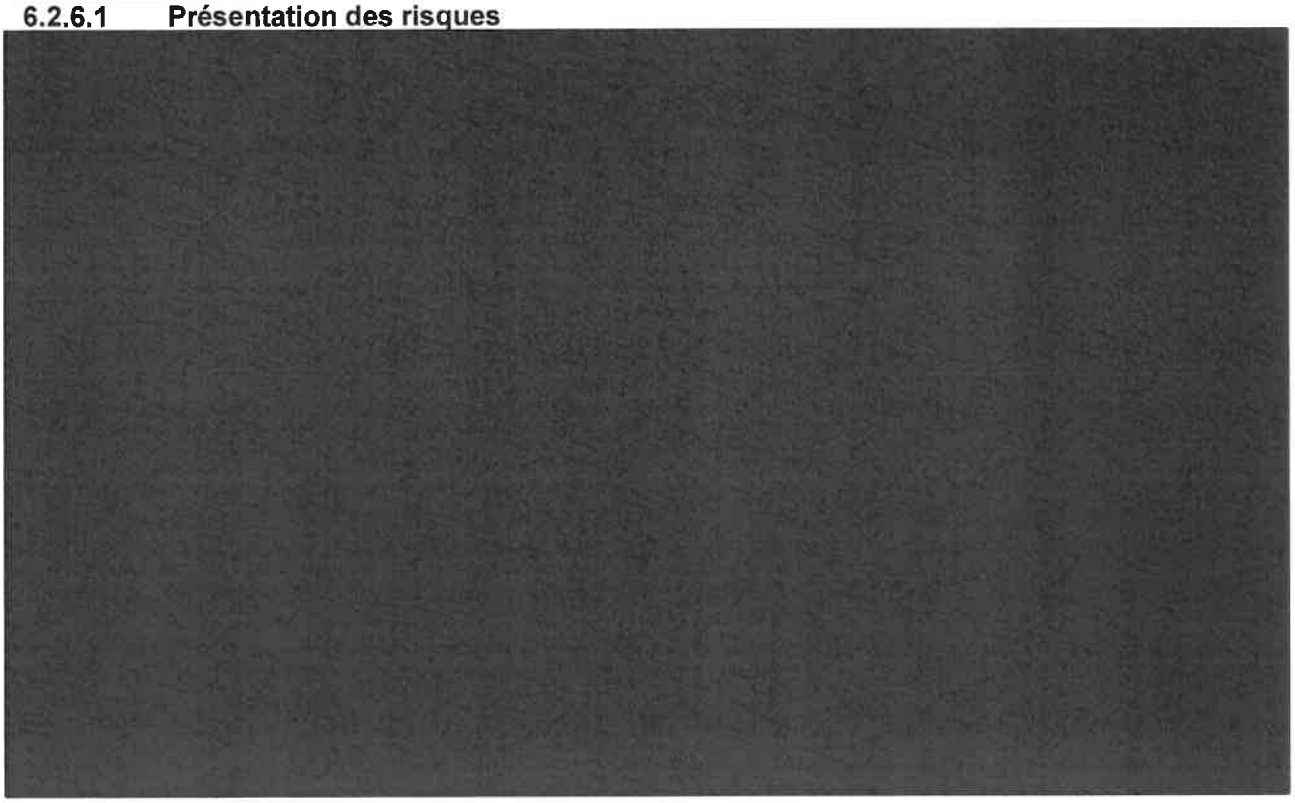
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



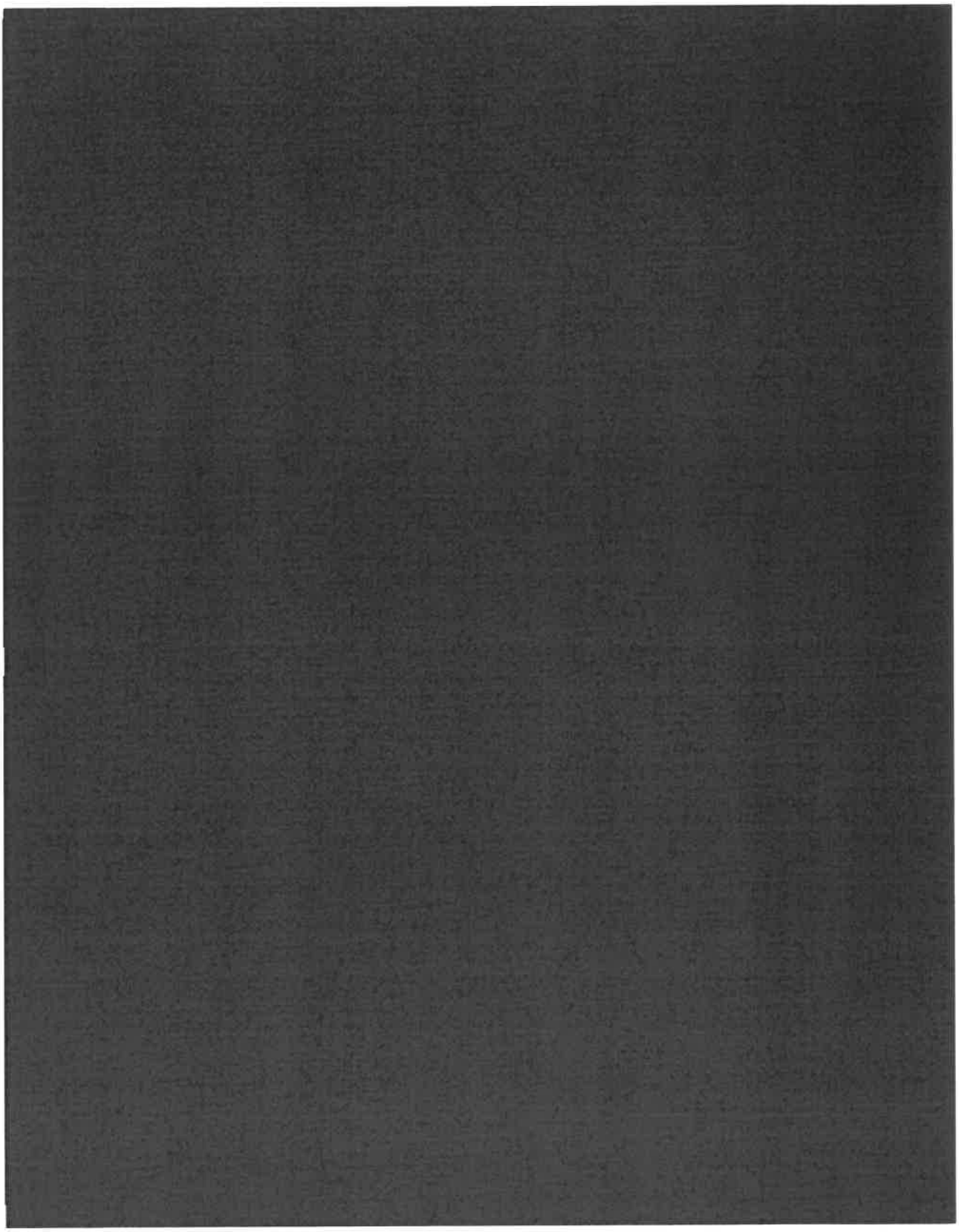
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.2.6 Risques

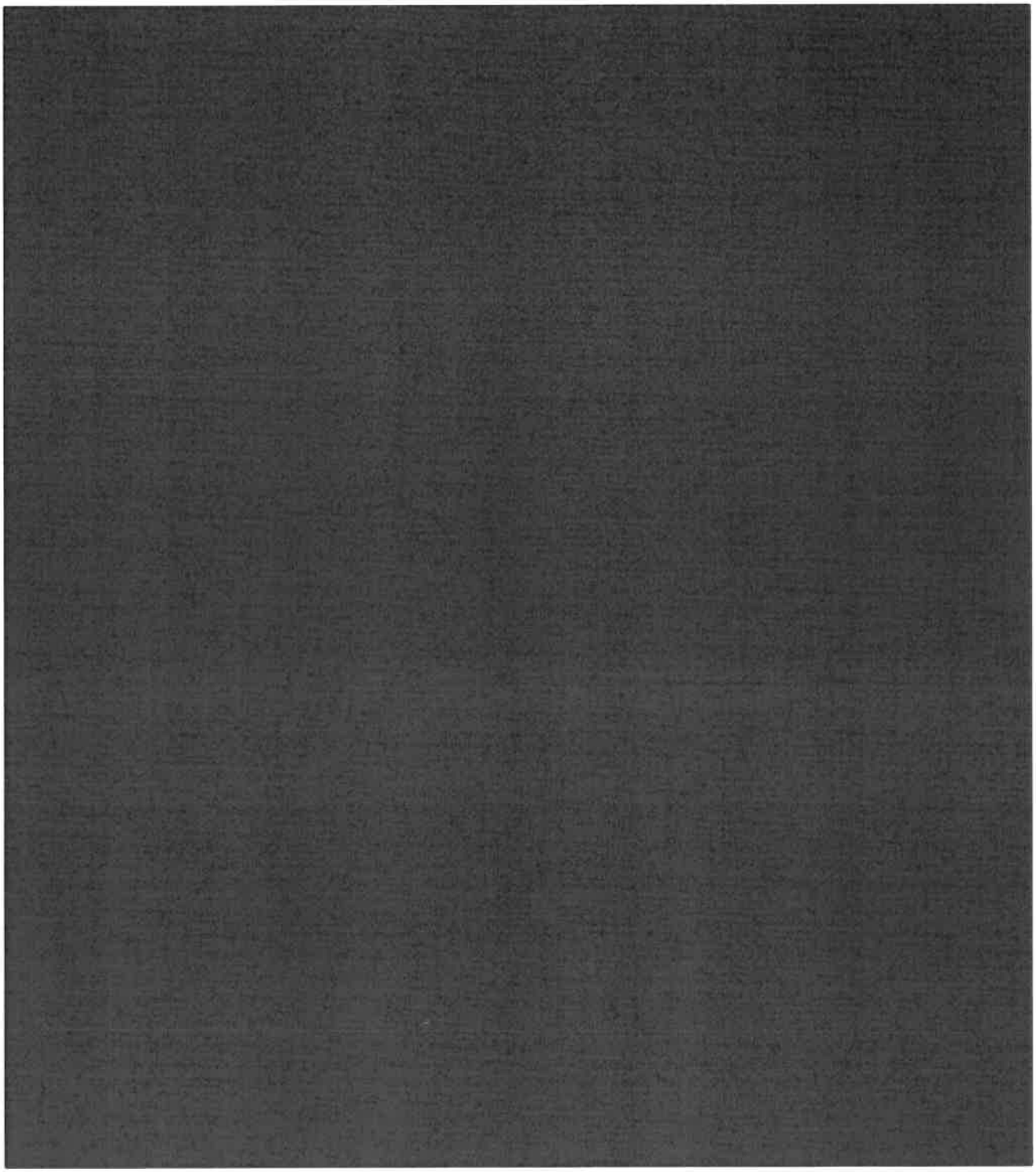
6.2.6.1 Présentation des risques



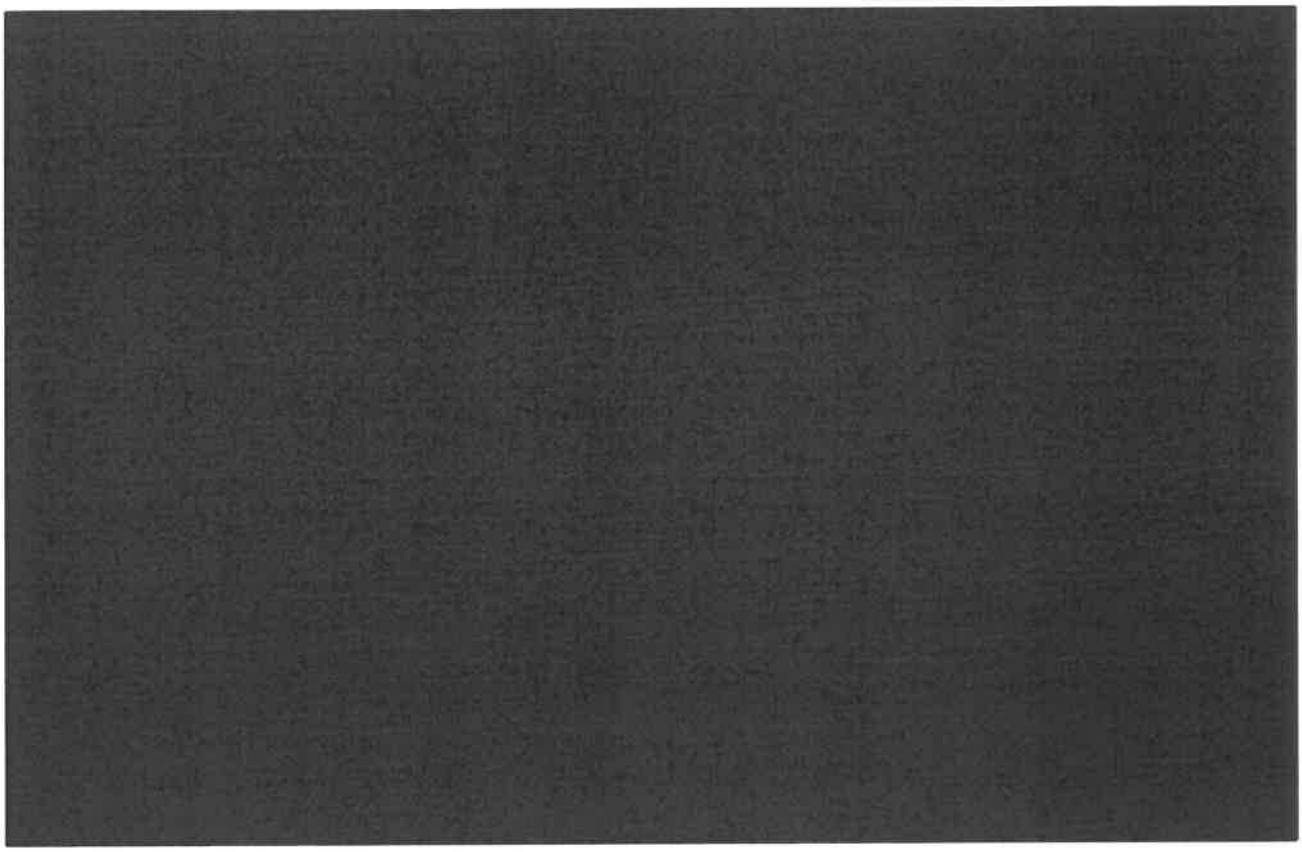
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



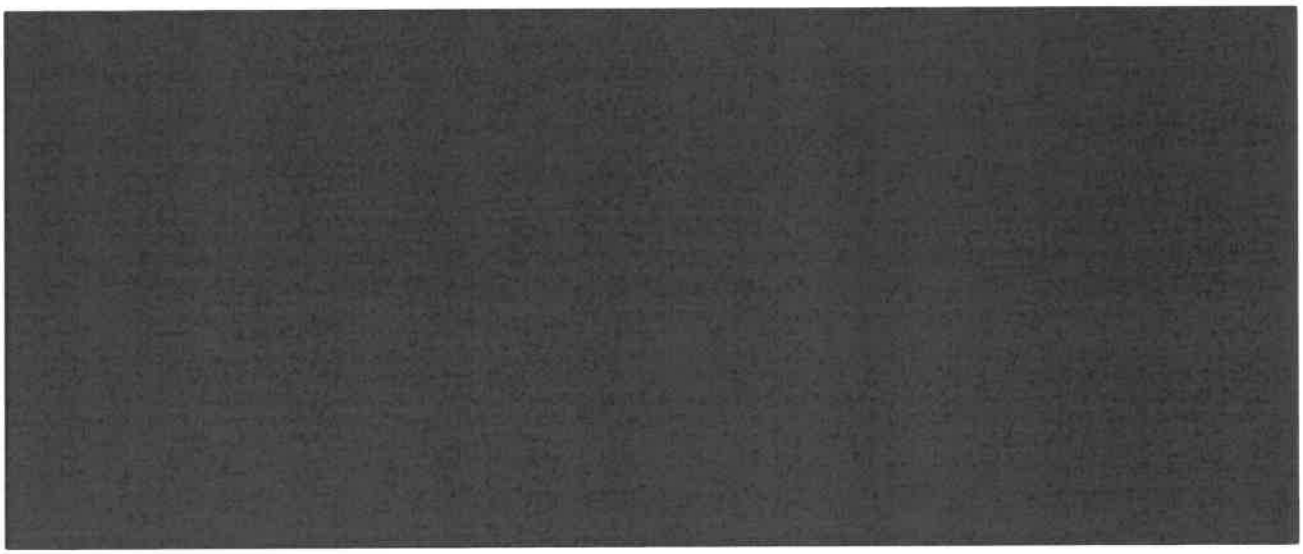
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

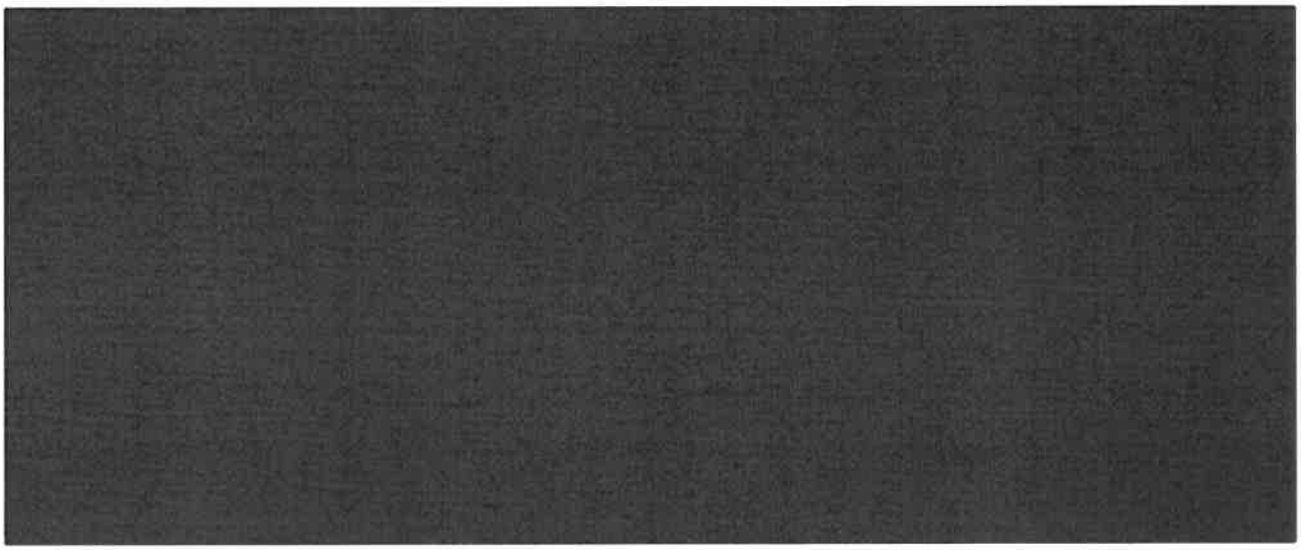


6.2.6.2 Couverture des risques



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.2.6.3 Plan d'action

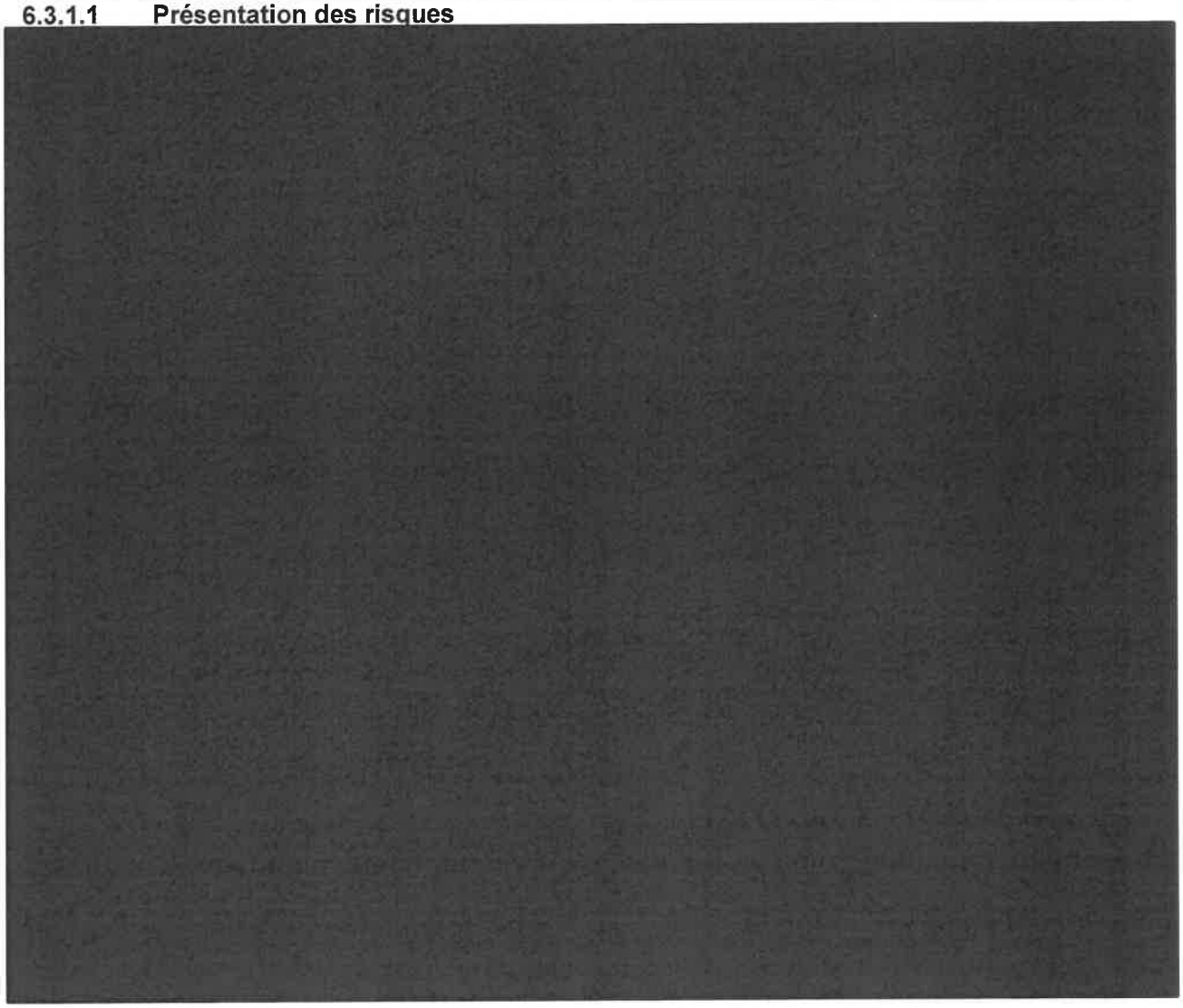


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

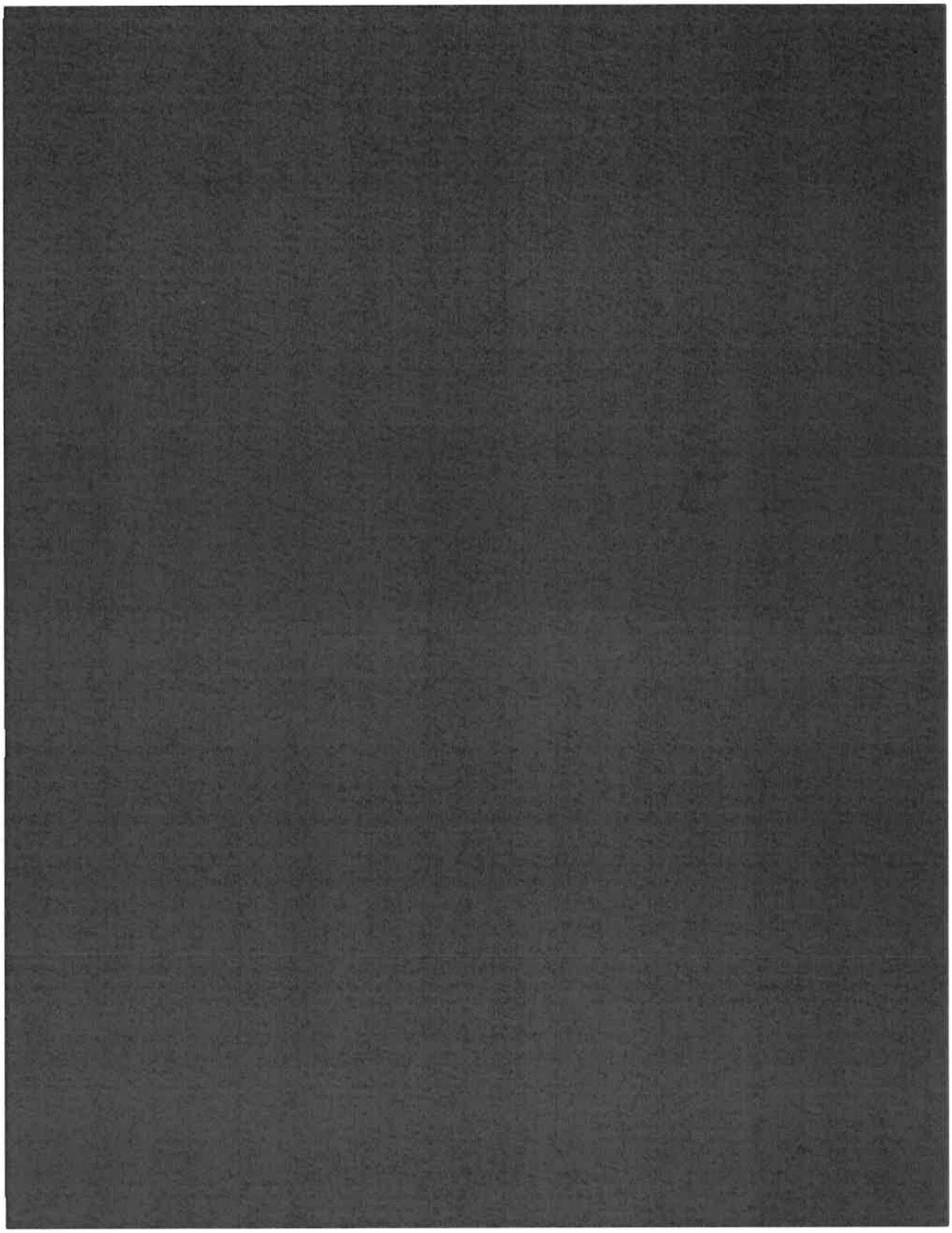
6.3 Eléments communs aux différents parcours d'activation

6.3.1 Risques

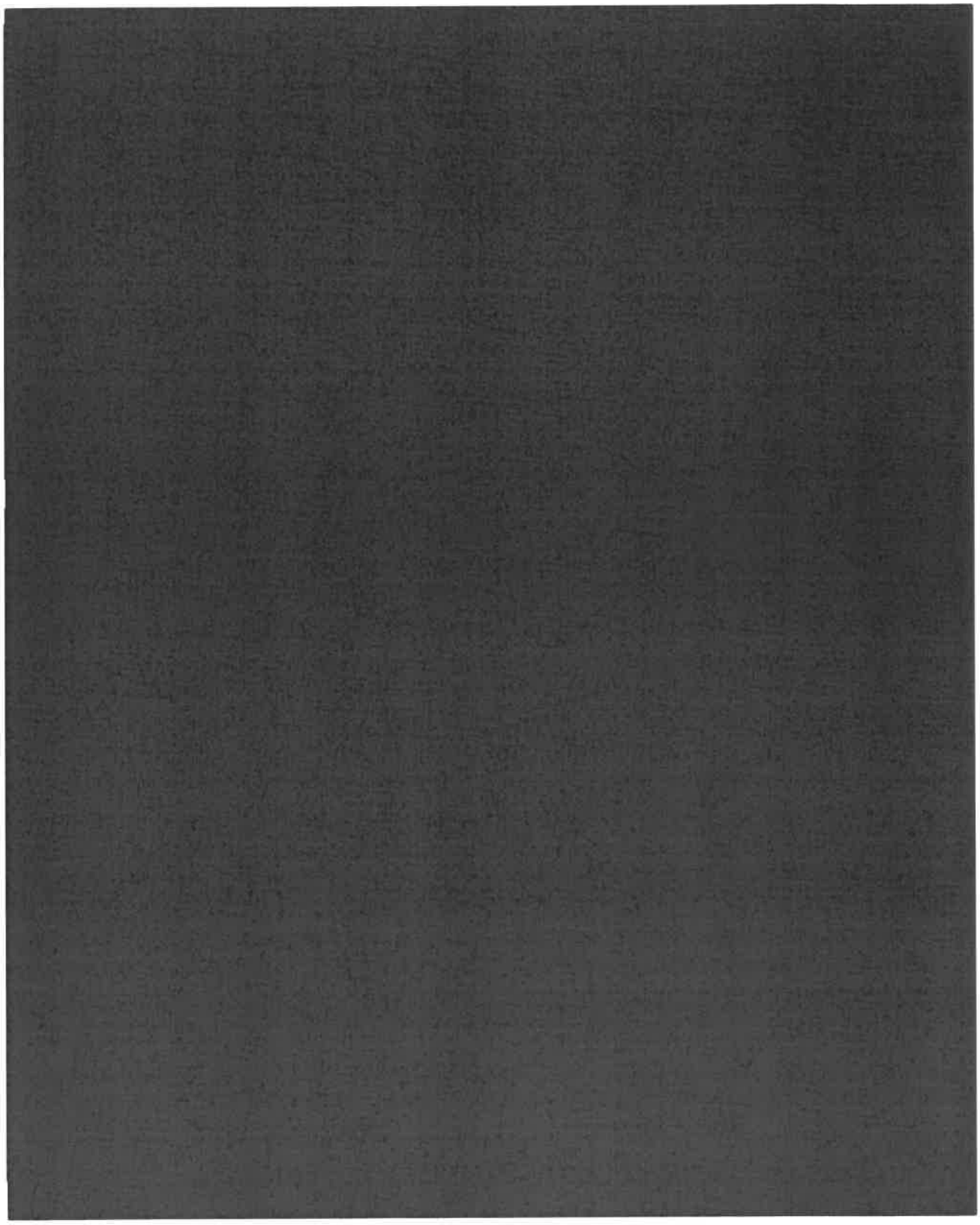
6.3.1.1 Présentation des risques



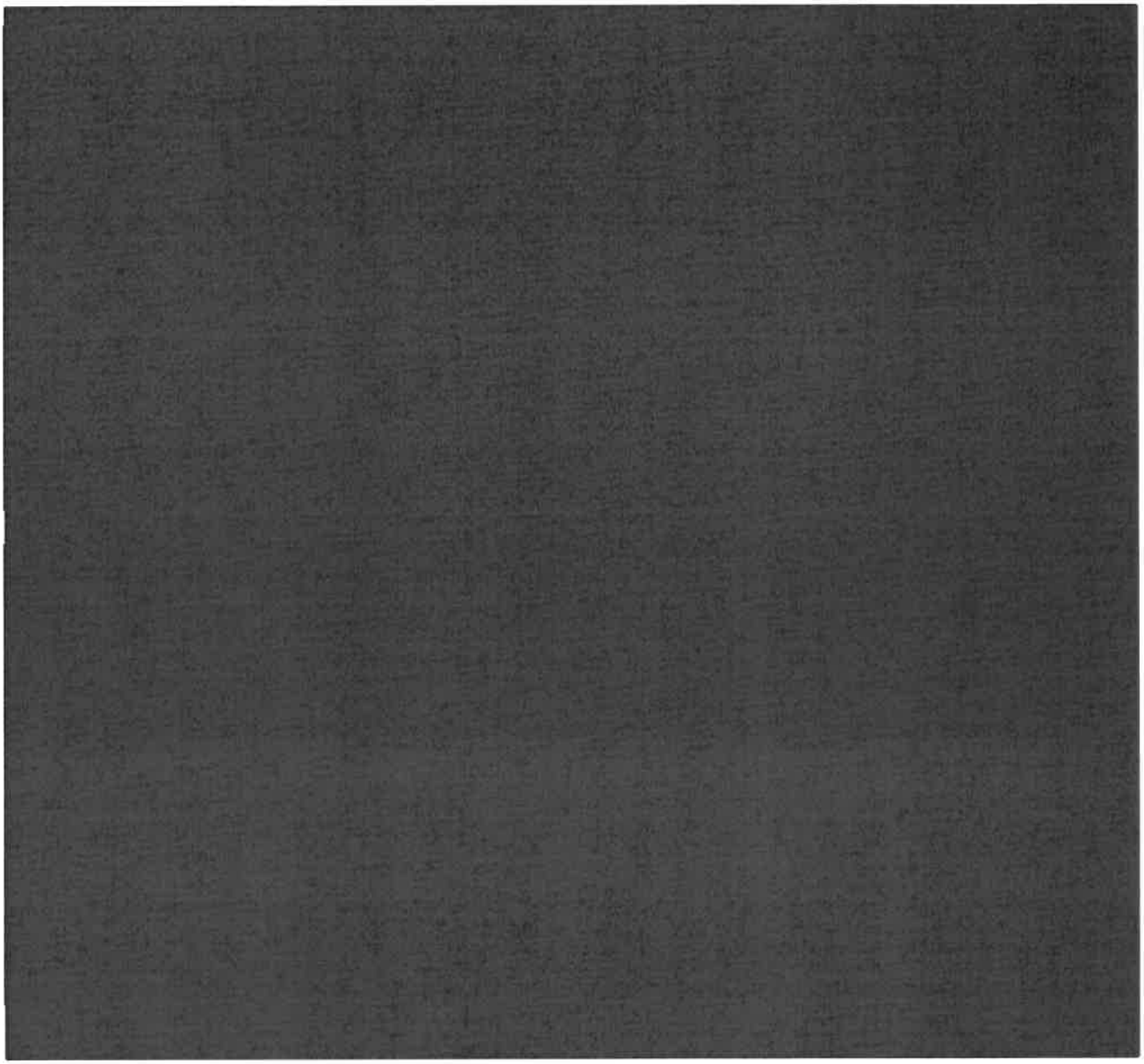
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

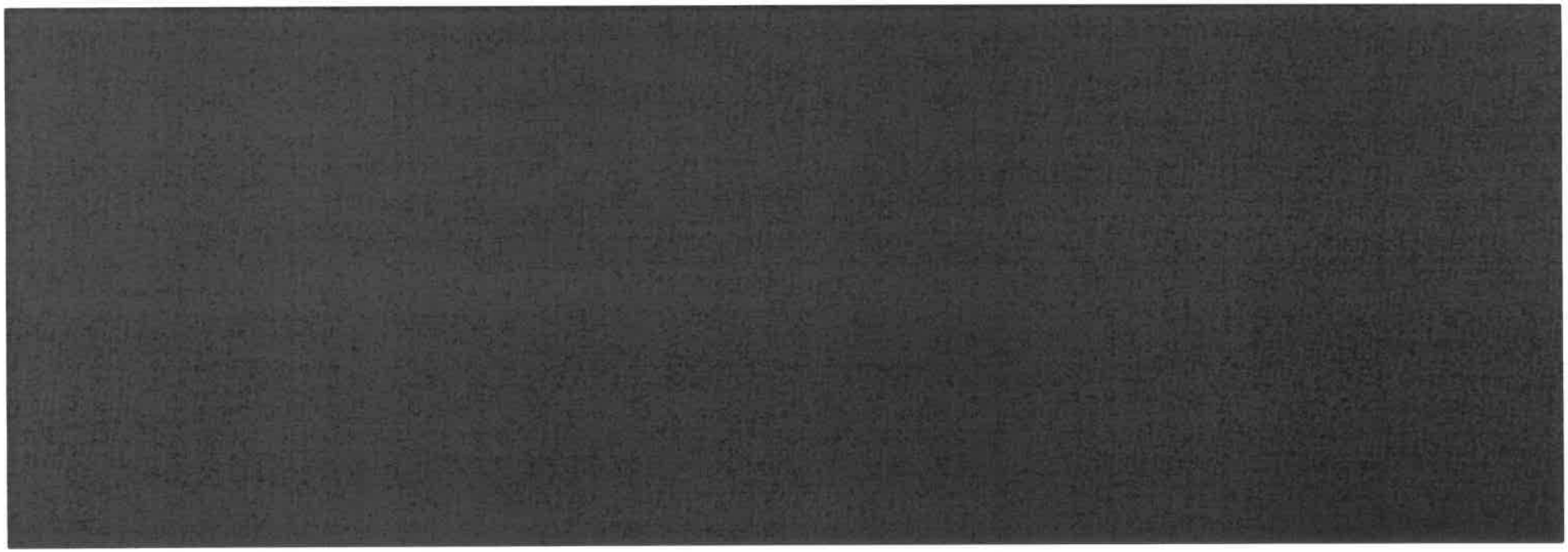


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



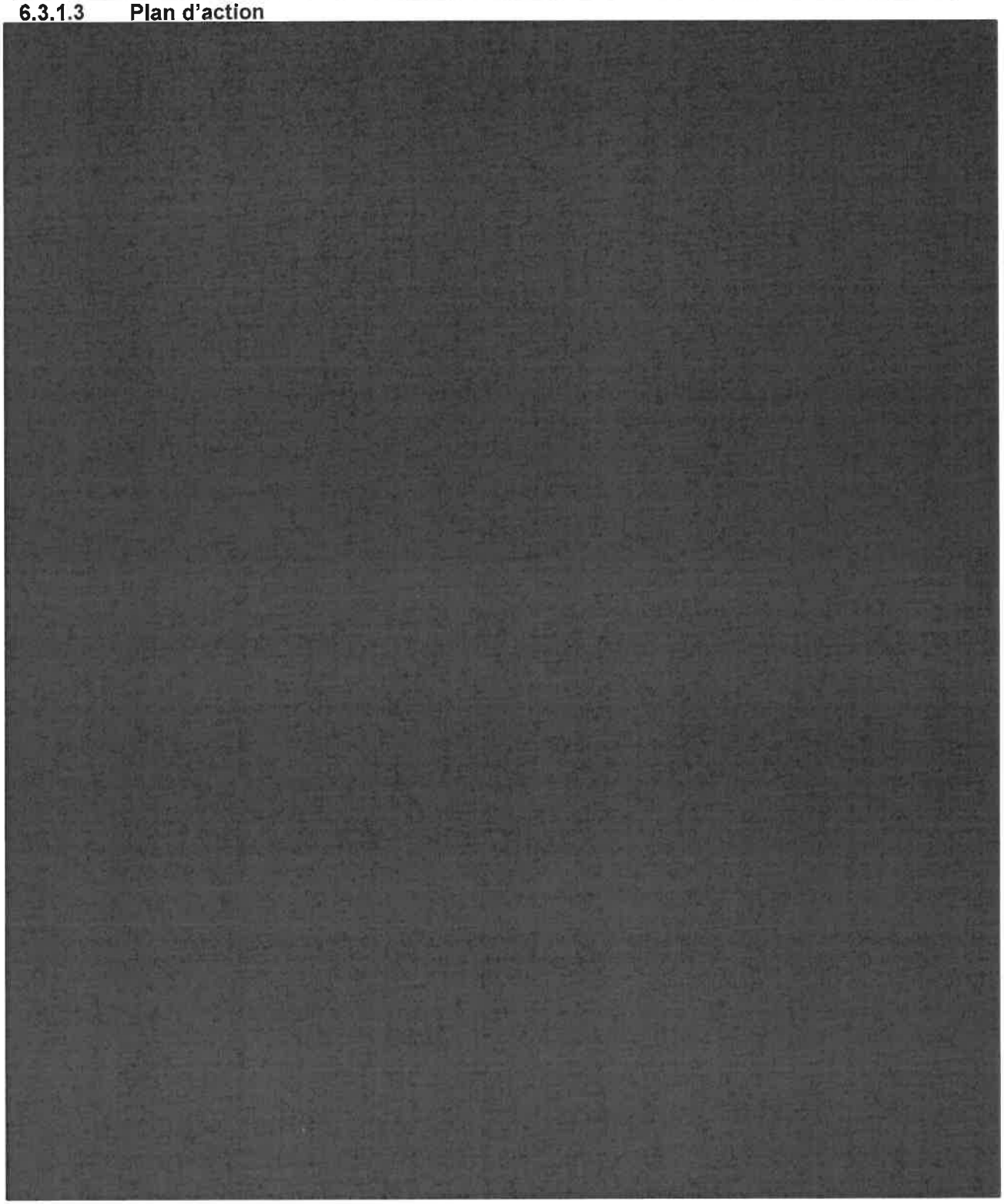
6.3.1.2 Couverture des risques

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

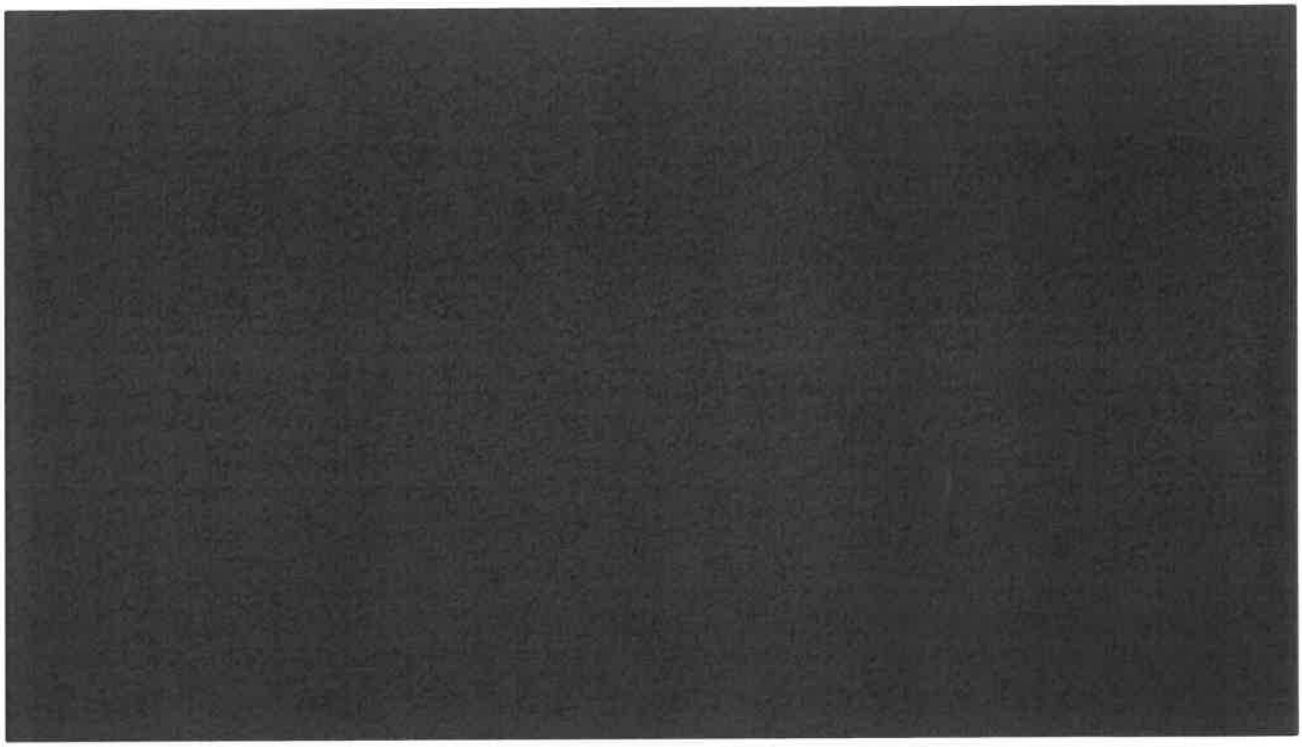


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.3.1.3 Plan d'action



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.4 Gestion de l'ApCV par les AMO

Le GIE SV met à disposition des Régimes les services suivants à destination des agents des Caisses en charge de la relation avec les assurés :

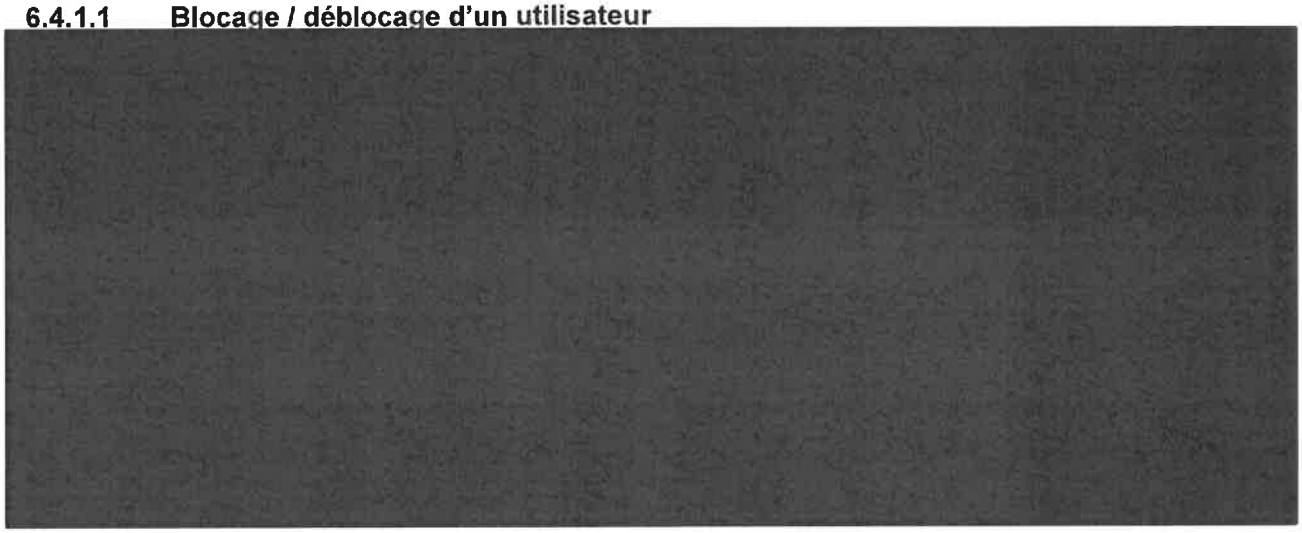
- Un portail web de gestion du support ;
- Une API permettant de réaliser le suivi de la délivrance des ApCV ;
- Une API permettant de signaler un changement de situation.

6.4.1 Portail de gestion du support

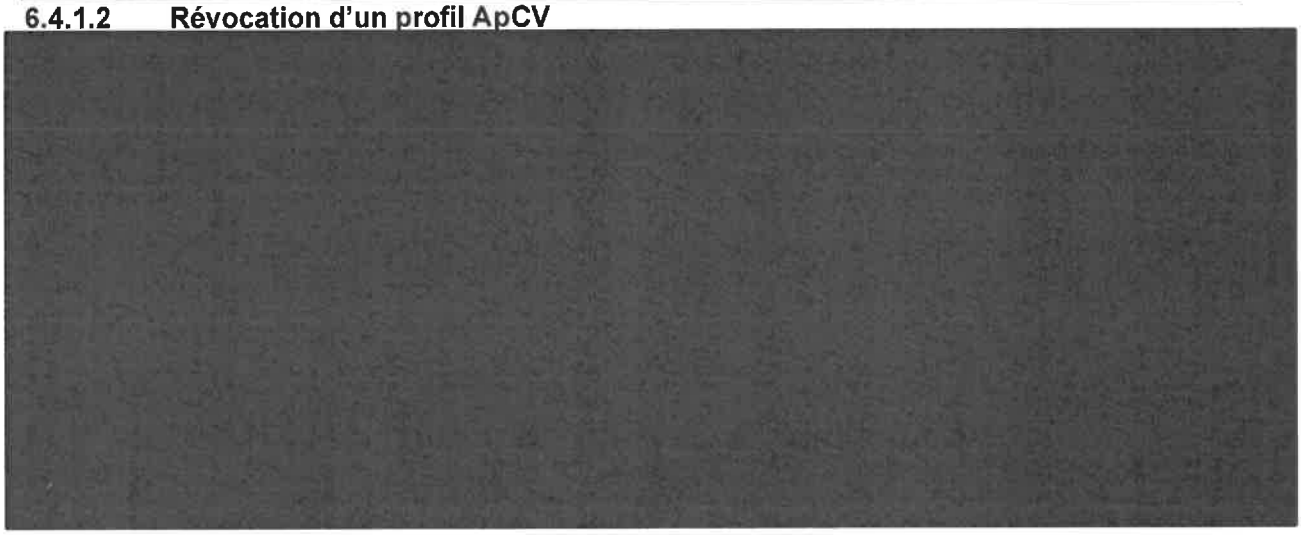
Les fonctionnalités offertes par le portail de gestion du support sont décrites dans les paragraphes ci-dessous :

- Bloquer / débloquer un utilisateur dans le cadre de la lutte contre la fraude ;
- Révoquer le profil ApCV d'un utilisateur, en cas de perte ou vol de son smartphone ;
- Suivre la délivrance de l'ApCV à un utilisateur (activation) et apporter le support nécessaire à ce dernier en consultant l'historique et les étapes d'activation de l'ApCV.

6.4.1.1 Blocage / déblocage d'un utilisateur



6.4.1.2 Révocation d'un profil ApCV



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.4.1.3 Suivi de la délivrance

Lorsqu'un assuré rencontre un problème lors de la délivrance de son ApCV (activation), il contacte sa caisse gestionnaire par les moyens habituels.

Après avoir validé l'identité de l'utilisateur, l'agent se connecte au portail de gestion du support et recherche le dossier de l'utilisateur concerné à partir :

- Soit du NIR de l'utilisateur ;
- Soit des éléments d'identification communiqués à l'utilisateur sur son ApCV (dans le cas d'un rejet avant identification de l'utilisateur).

L'agent peut alors consulter :

- L'état de la délivrance :
  - Statut de délivrance (en cours, rejeté, réalisé) ;
  - Etape où l'utilisateur s'est arrêté si le statut de délivrance est « en cours » ou « rejeté »
  - Date de délivrance si OK.
- L'ensemble des rejets survenus lors de la dernière demande de délivrance :
  - Rejet suite aux recherches IR / AMO ;
  - Rejets d'éligibilité : utilisateur bloqué, individu décédé, NIR inconnu, non-respect de la condition d'âge minimal d'utilisation (16 ans).

6.4.2 API délivrance

A partir de la version ApCV V3, une nouvelle API est mise à disposition des AMO pour leur permettre de récupérer les données relatives aux nouvelles inscriptions. Cette API remplacera à terme le fichier des enrôlés :

- Pour l'instant, les fichiers des enrôlés restent produits pour l'ensemble des régimes ;
- Prochainement [redacted] la production du fichier des enrôlés sera complètement arrêtée.

Cette API expose les services REST suivants :

- Restituer les profils ApCV nouvellement enrôlés ;
- Restituer les profils ApCV supprimés à une date donnée ;
- Restituer les individus en échec d'enrôlement à une date donnée.

6.4.3 API Changement de situation

[redacted]

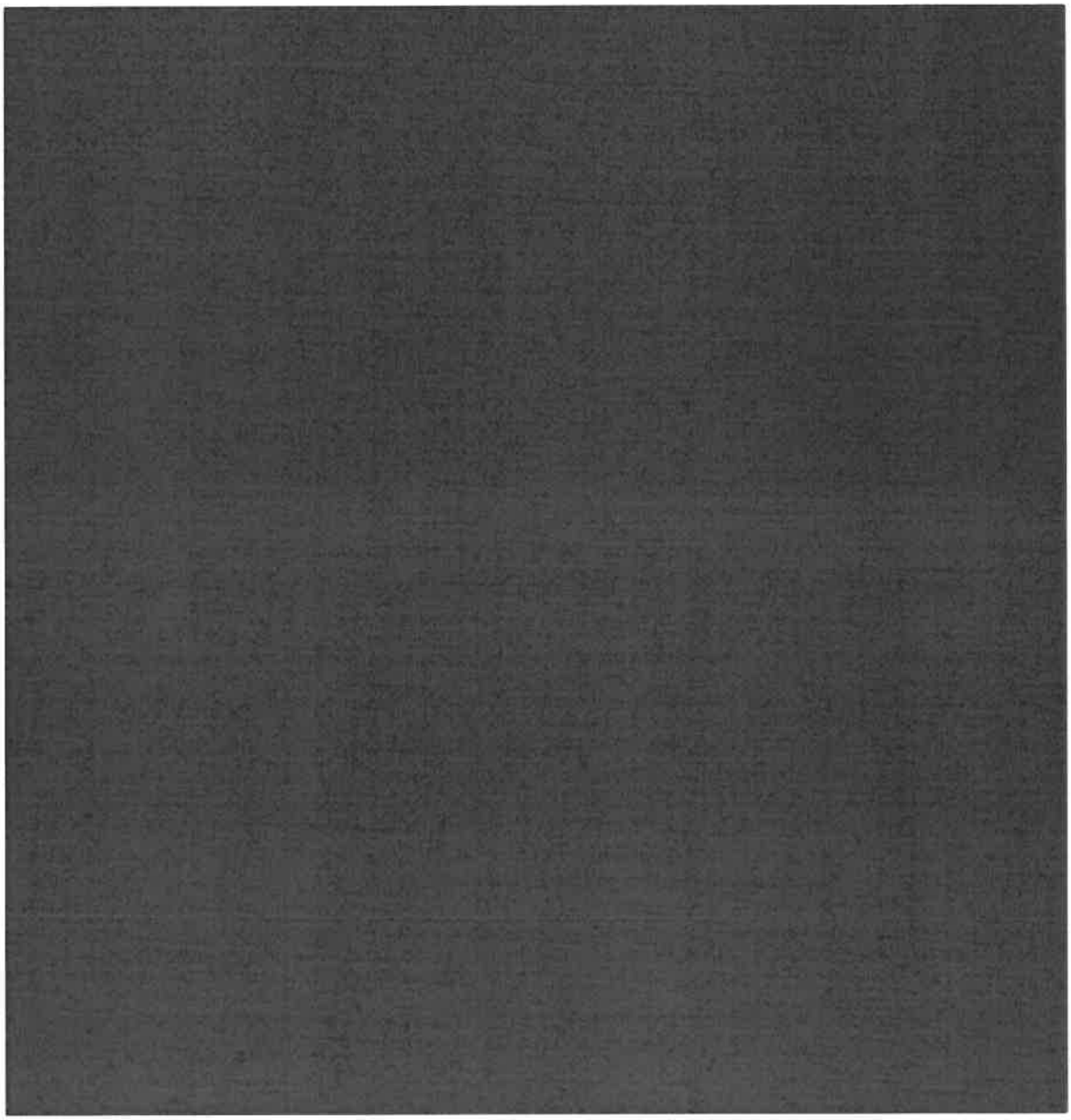
Une nouvelle API, nommée Changement de situation, est exposée par le SI ApCV à destination des AMO. A réception d'un événement (ex : décès, modification d'identité…), le SI ApCV stocke l'événement en attendant sa prise en compte à date d'application.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

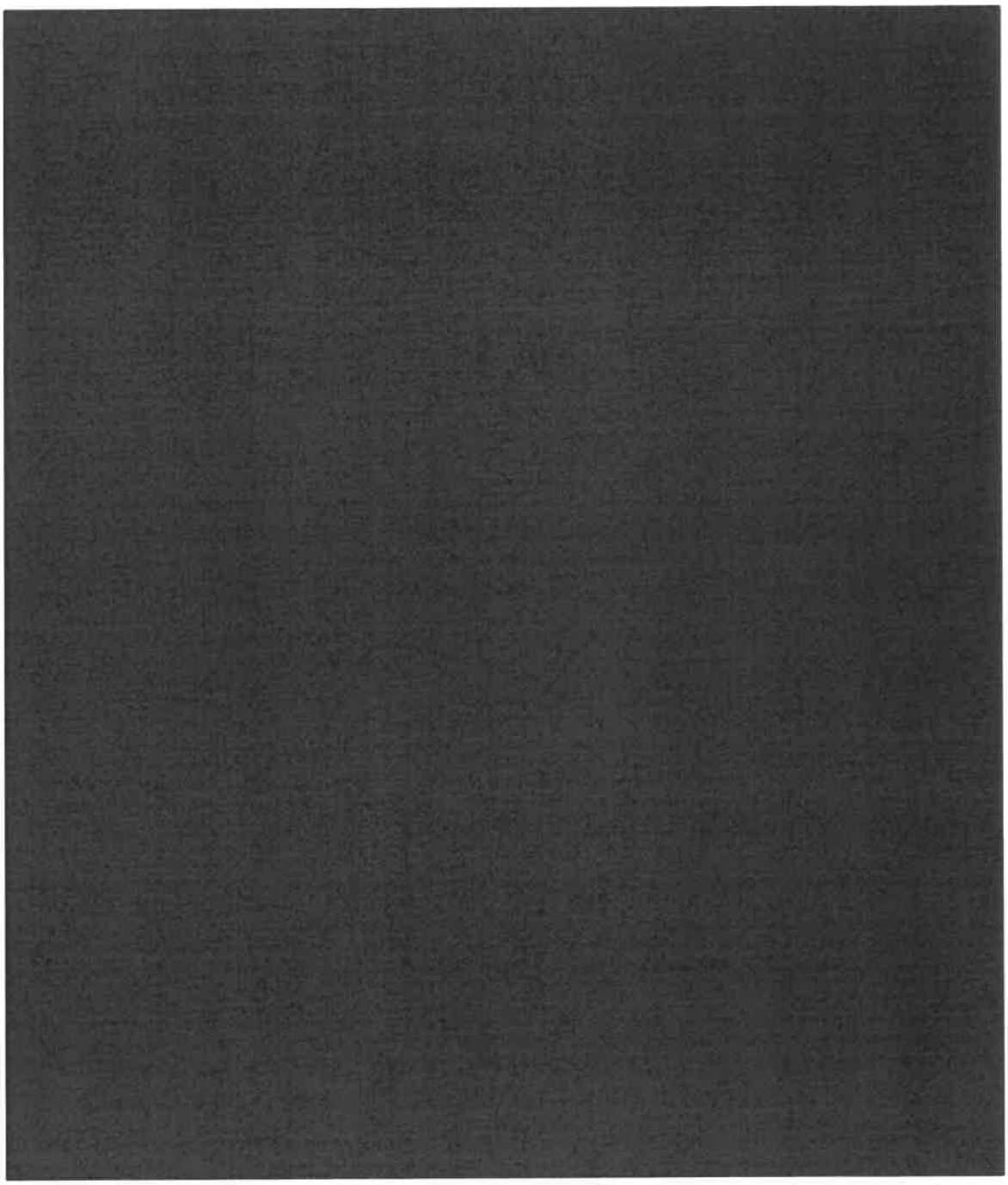
Une fois sa date d'application arrivée à échéance, le SI ApCV traite l'événement. En fonction de l'événement, le SI ApCV peut être amené à révoquer le profil ApCV correspondant ou enregistrer que l'individu est concerné par une demande de mise à jour.

Lorsque l'ApCV se connecte au SI ApCV, le SI ApCV recherche si au moins un individu hébergé dans le profil ApCV est concerné par une demande de mise à jour et si c'est le cas réalise la mise à jour des données d'identité AMO et d'identité Patient.

6.4.4 Description du circuit de la donnée



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.4.5 Respect des principes fondamentaux

6.4.5.1 Caractéristiques du traitement

	Gestion de l'ApCV par les AMO
Finalité principale	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Informations complémentaires	Le processus mis en place pour la gestion de l'ApCV par les AMO : - Expose un portail web de gestion du support aux Caisses gestionnaires permettant aux agents de : bloquer / débloquer un utilisateur dans le cadre de la lutte contre la fraude, bloquer/débloquer l'ApCV d'un utilisateur en cas de perte ou vol - Expose un portail web et une API permettant de suivre la délivrance de l'ApCV à un utilisateur (activation) et d'apporter le support nécessaire à ce dernier en consultant l'historique et les étapes d'activation de l'ApCV. - Expose une API permettant aux AMO de pousser au SI ApCV des événements relatifs aux changements de situation des assurés. - Permet de tracer les accès des agents des Caisses conformément à la norme [redacted]
Interventions de sous-traitants ultérieurs	Infogérant du SI ApCV [redacted] Fournisseur du SDK Sécurité et infogérant du SI Sécurité [redacted]

6.4.5.2 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
NIR	DCP perçue comme sensible	Identification de l'assuré	
Identifiant pseudonymisé de l'agent Caisse	DCP courante	Identification de l'agent Caisse par un pseudonymat fourni par le Régime dans le flux d'authentification	
Traces de fonctionnement (identifiant pseudonymisé agent caisse, identifiant profil ApCV, NIR pseudonymisé)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Traces fonctionnelles de sécurité (identifiant pseudonymisé agent caisse, identifiant profil ApCV)	DCP courantes	Données nécessaires pour analyser des fraudes, fautes et incidents de sécurité et disposer d'une source de référence en cas de contestation, a posteriori, de la part d'un assuré ou d'un Régime	Seules les données nécessaires sont conservées.
Traces contractuelles INTEROPS (identifiant pseudonymisé agent caisse, identifiant profil ApCV)	DCP courantes	Données dont la conservation est exigée dans la convention INTEROPS.	Seules les données nécessaires sont conservées.

6.4.5.3 Explication et justification de la qualité des données

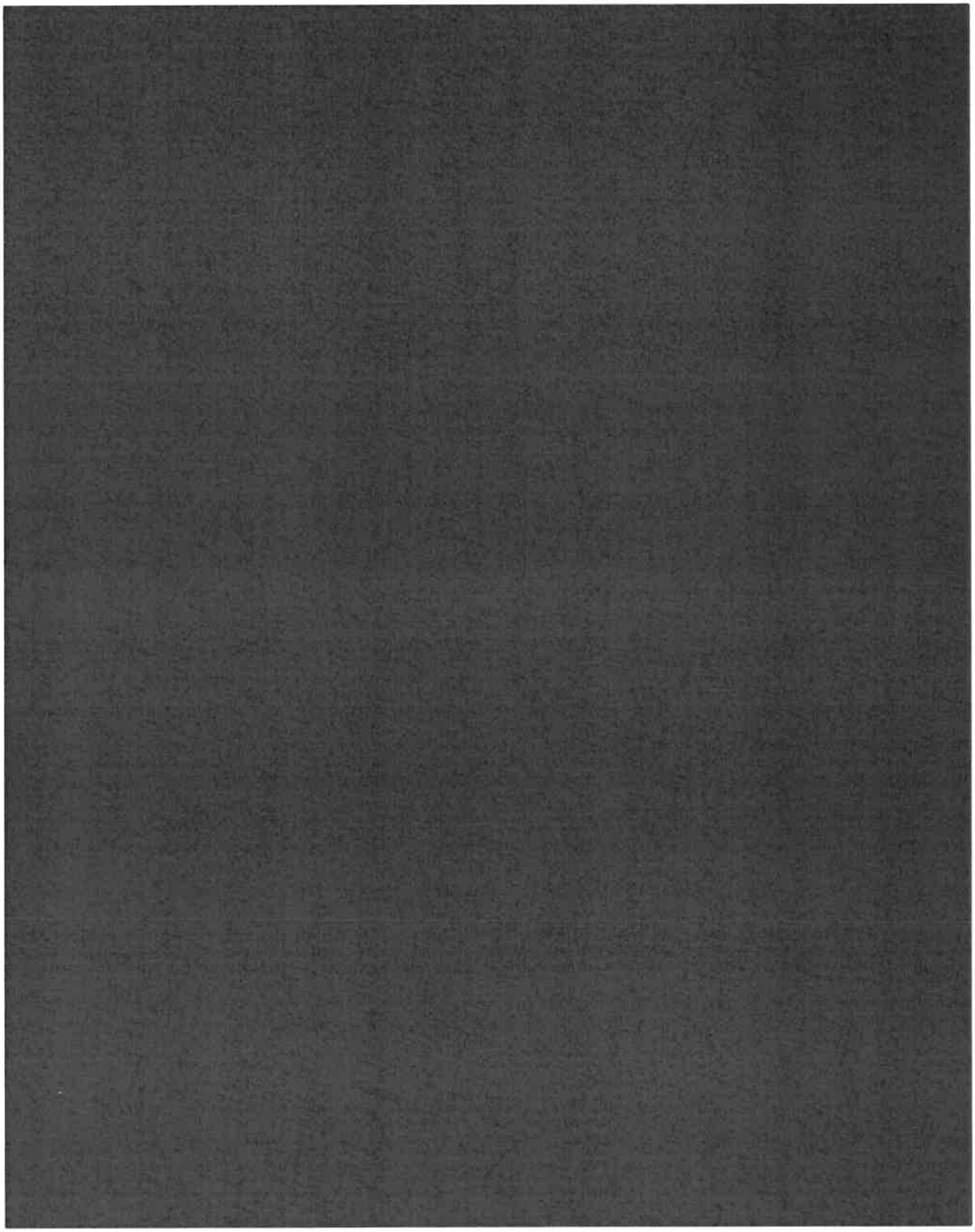
Mesures pour la qualité des données	Justification
Les données relatives au statut de l'activation sont gérées par le SI ApCV dans le cadre du processus d'activation. L'agent caisse peut les consulter mais n'a pas possibilité de les modifier.	N/A
Le statut de l'ApCV est conservé dans les bases de données du SI ApCV. Seuls les agents caisse dûment authentifiés et habilités peuvent modifier ce statut en bloquant / débloquant les ApCV.	N/A

6.4.5.4 Explication et justification des durées de conservation

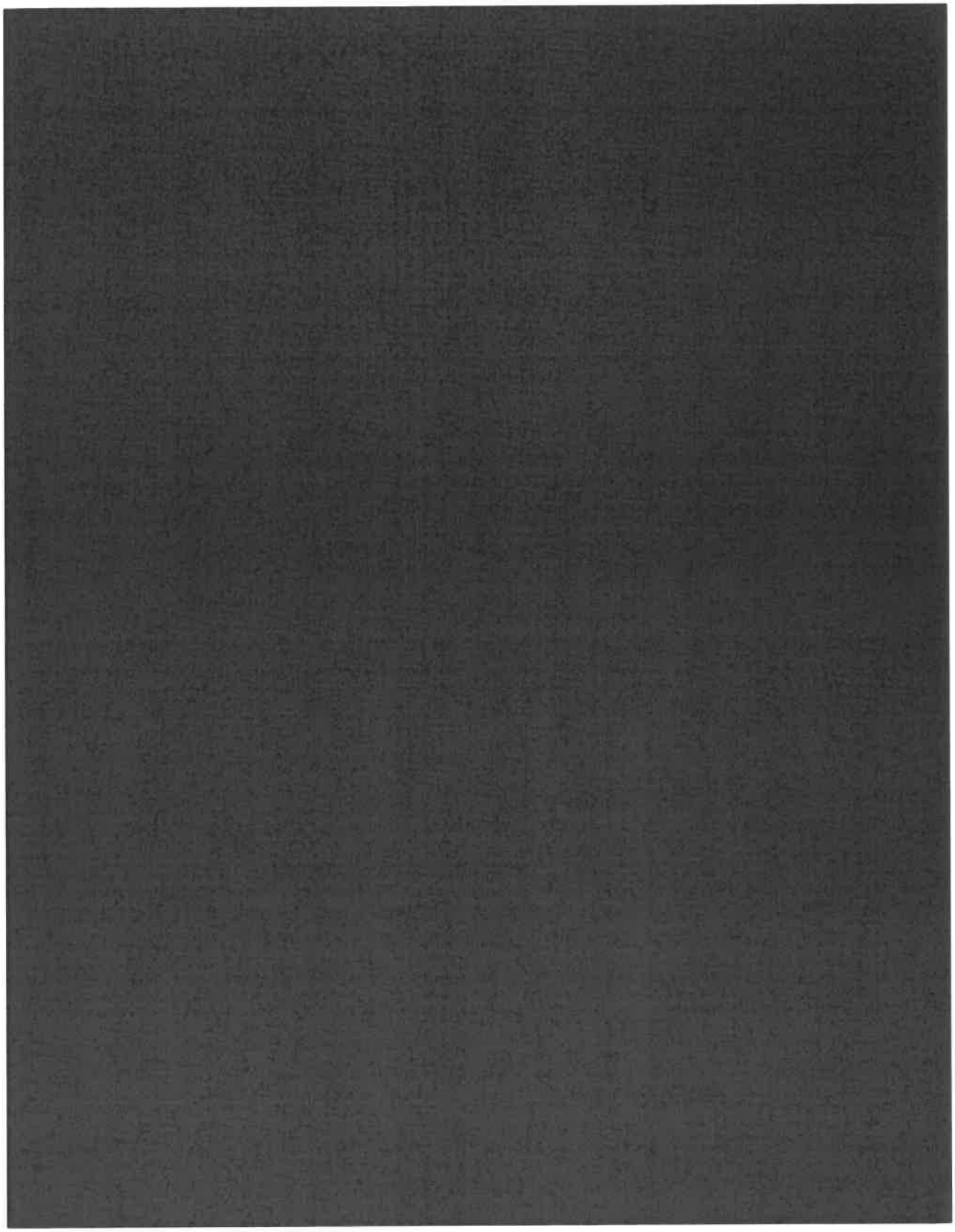
Les seules données produites sont des traces dont les durées de conservation sont précisées au §5.2.1.4.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

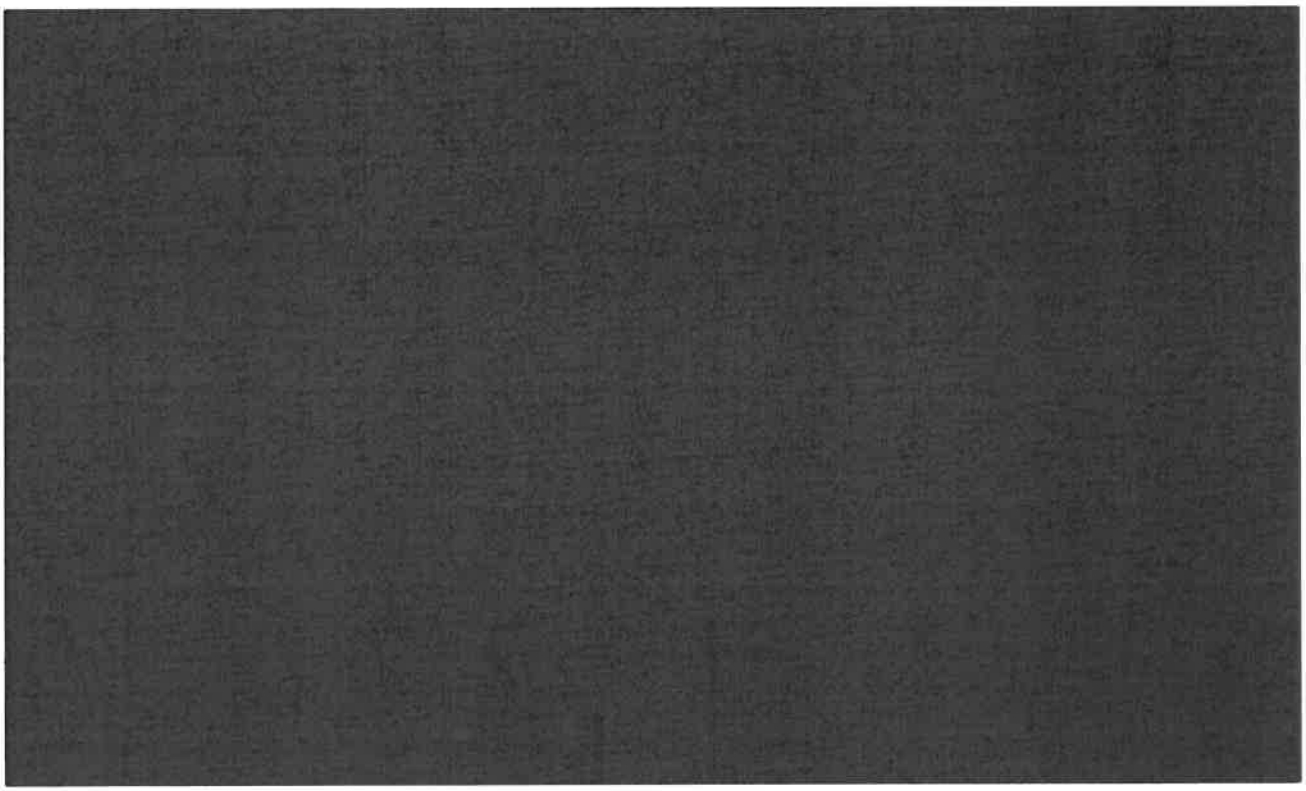
6.4.6 Mesures de sécurité



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



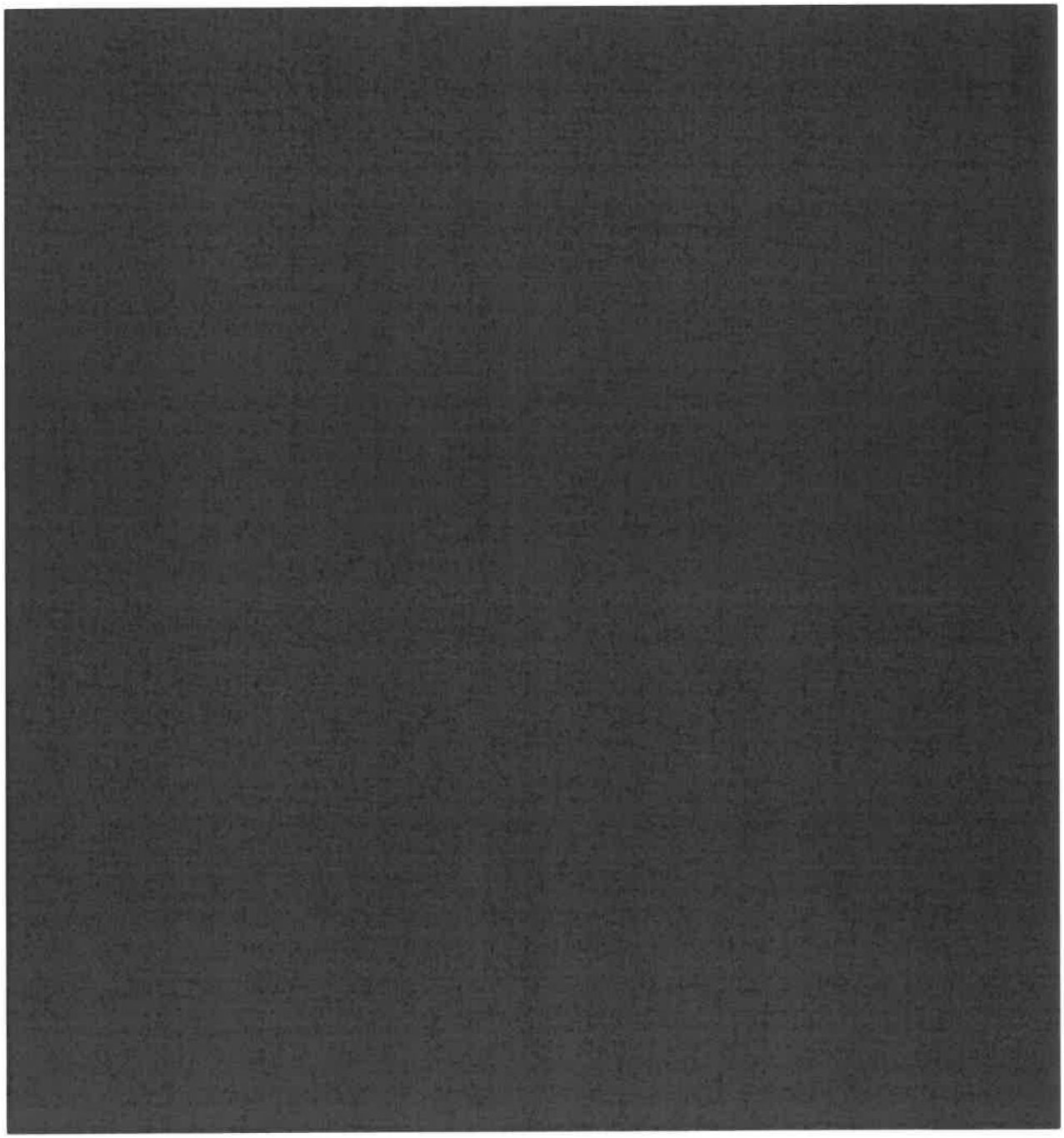
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



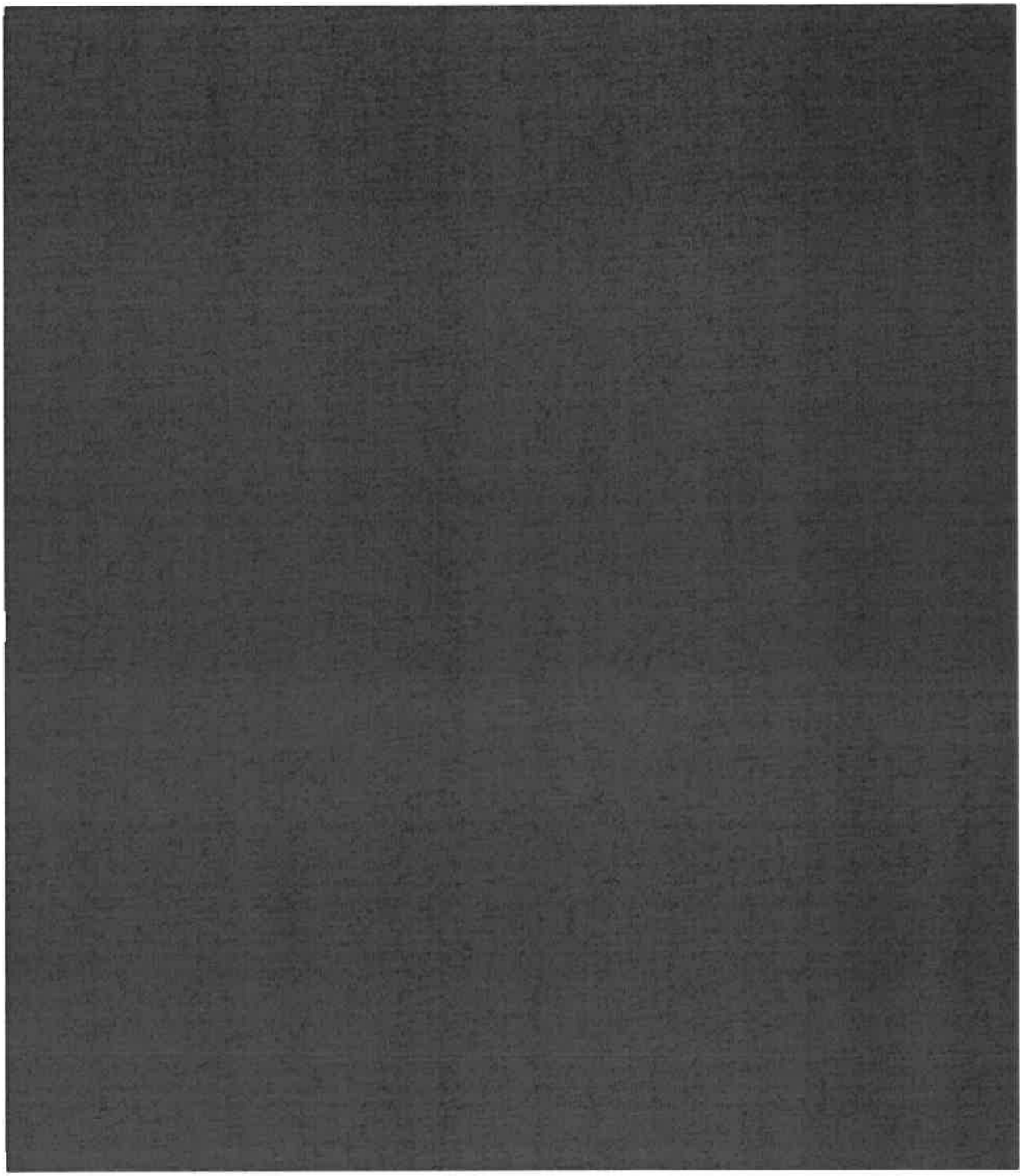
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.4.7 Risques

6.4.7.1 Présentation des risques

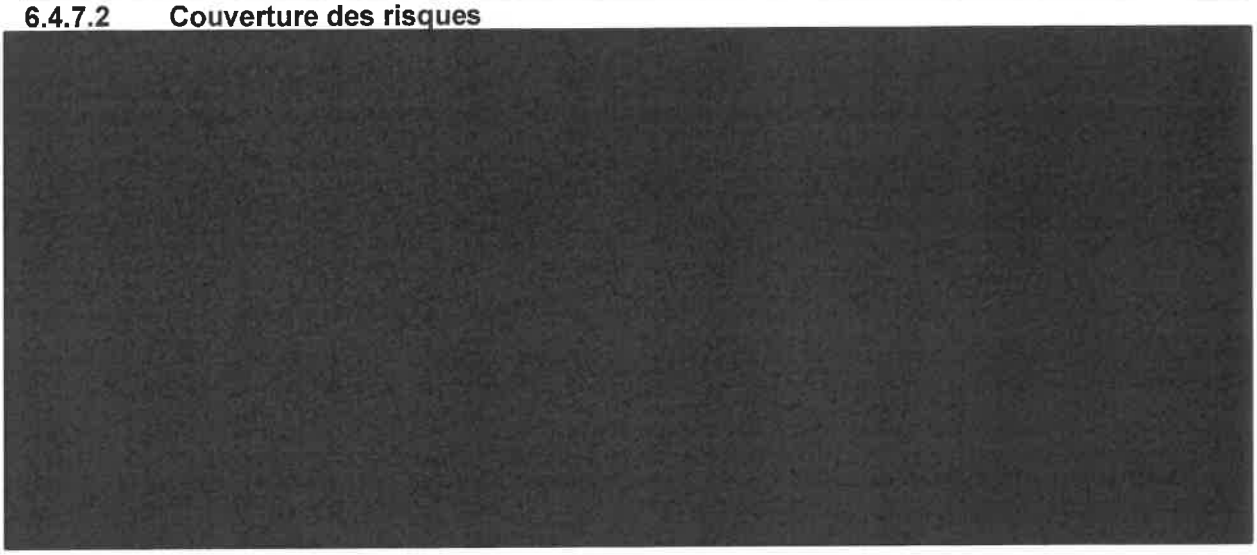


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

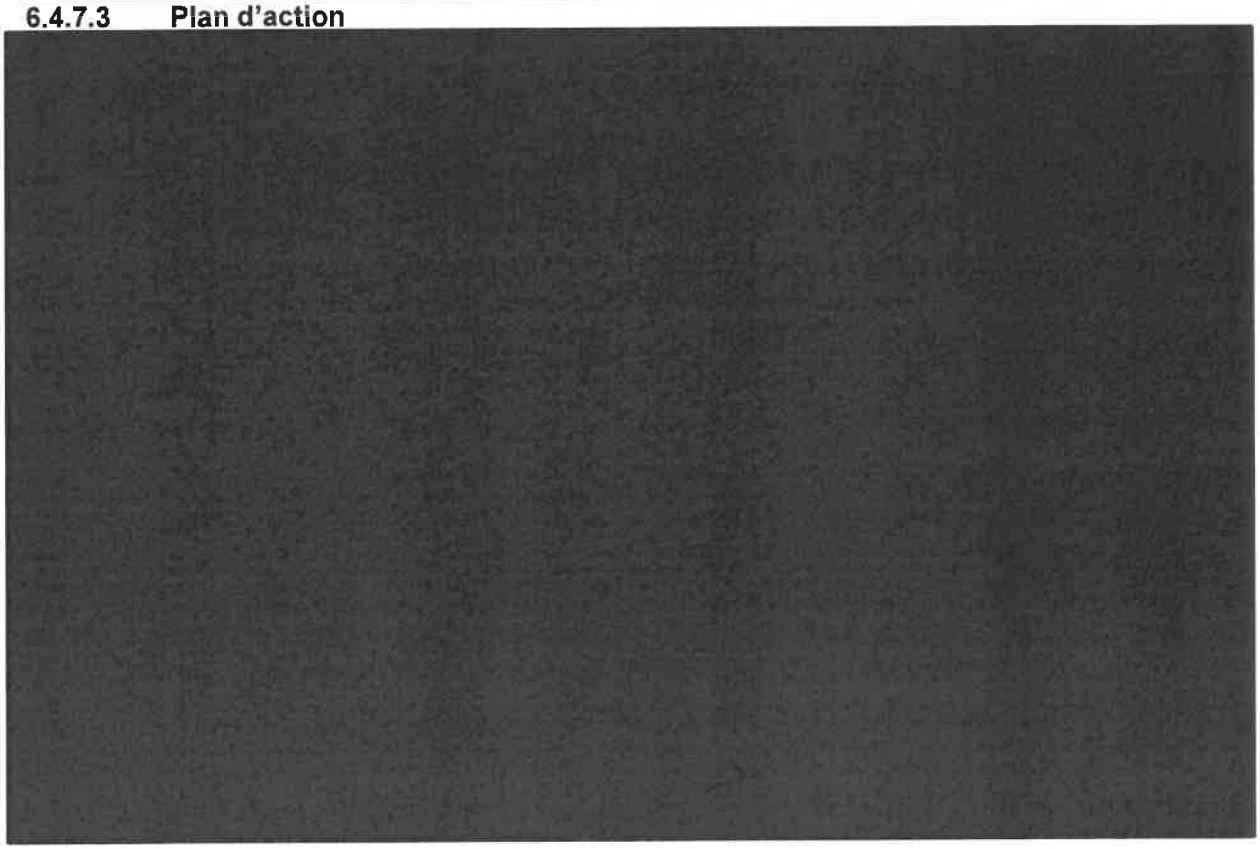


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.4.7.2 Couverture des risques



6.4.7.3 Plan d'action



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.5 Migration depuis une version antérieure de l'appli carte Vitale

6.5.1 Principe de migration

Au premier lancement de la V7, la migration des données de l'ApCV est proposée à l'utilisateur. La migration consiste à créer l'utilisateur dans le SI Sécurité et à transférer les données stockées dans l'ApCV vers le stockage sécurisé du SDK [redacted] La migration est réalisable uniquement si le smartphone est connecté à internet.

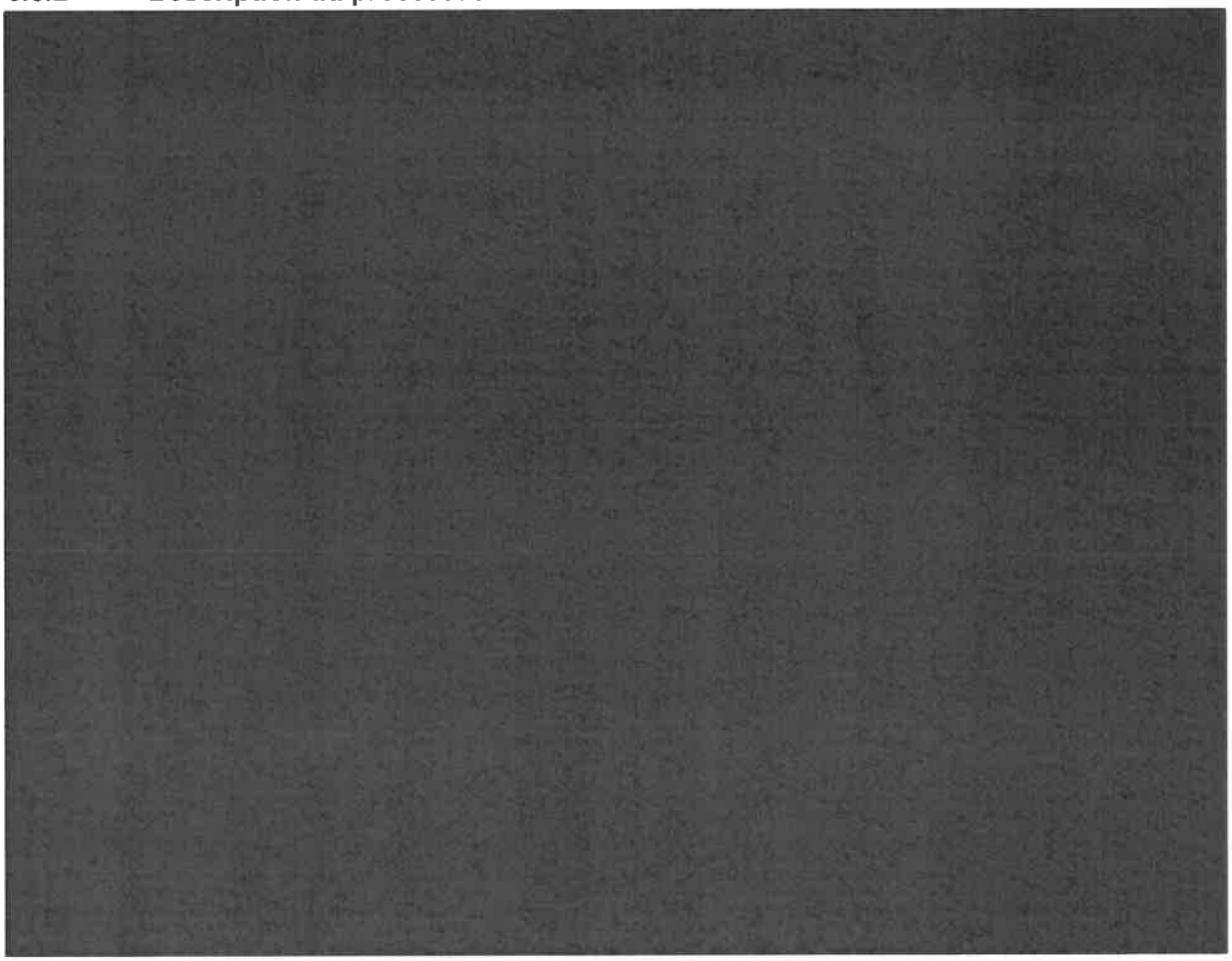
L'utilisateur a la possibilité de reporter la migration afin de ne pas être contraint de la réaliser en présence d'un PS par exemple. Cette possibilité est offerte jusqu'à une date butoir configurée dans le SI ApCV et affichée à l'utilisateur dans l'application. Lorsque l'utilisateur choisit de reporter la migration, des notifications locales lui sont envoyées (avec son accord) à la fréquence suivante :

- A J+1 du refus de réaliser la migration ;
- A J+15 ;
- Puis une fois par mois jusqu'à la date butoir.

Une fois la date butoir atteinte, la migration devient obligatoire pour continuer à utiliser l'ApCV.

Toutes les données stockées dans l'ApCV sont migrées : données d'identité AMO, données d'identité Patient, données d'identité Etat civil, adresse mail, photo et résumés de facture.

6.5.2 Description du processus



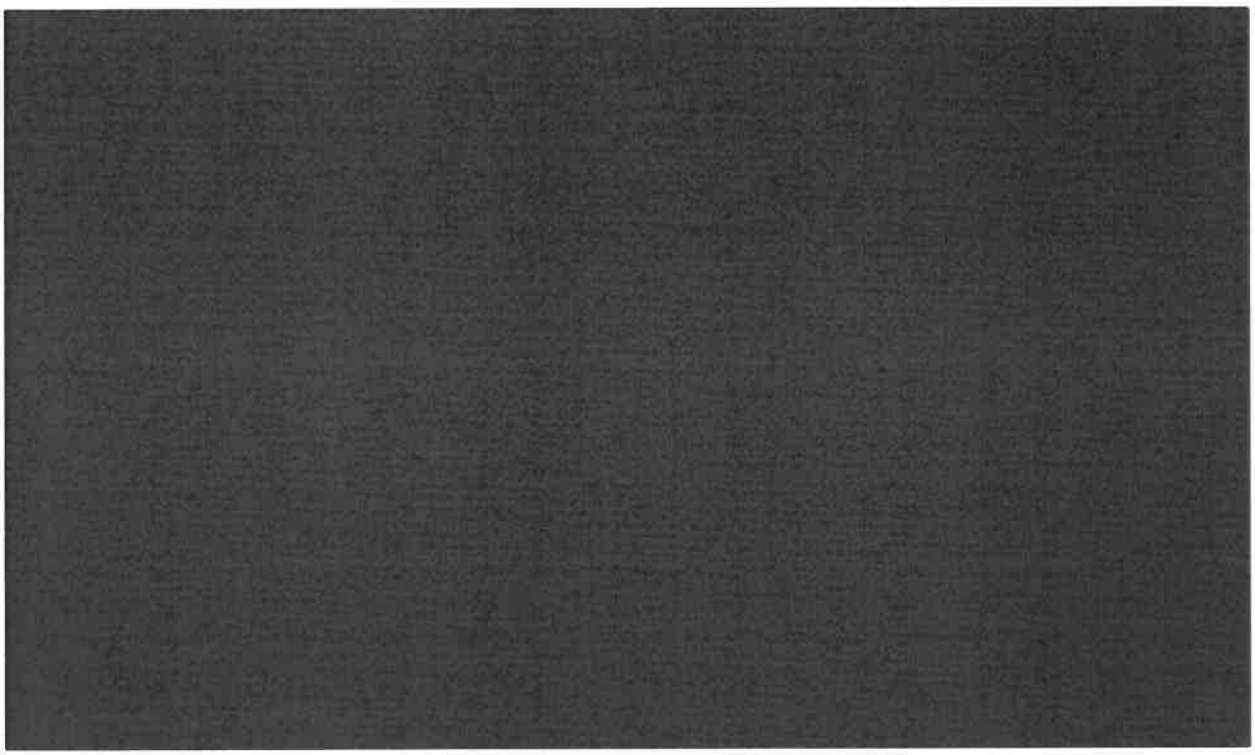
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

6.5.3 Description du circuit de la donnée

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



6.5.4 Respect des principes fondamenteaux

6.5.4.1 Caractéristiques du traitement

	Enrôlement
Finalité principale	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Sous-finalité	Migrer les données d'une ApCV d'une version précédente vers le socle de sécurité destiné à renforcer le niveau de sécurité des données stockées dans l'application carte Vitale
Intervention de sous-traitants ultérieurs	Infogérant du SI ApCV [redacted] Fournisseur du SDK Sécurité et infogérant du SI Sécurité [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.5.4.2 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Identité AMO (NIR, Nom de famille, Nom d'usage, Prénom, Date de naissance, Rang de naissance)	DCP perçue comme sensible (NIR) et DCP courantes	L'identité AMO est basée sur le NIR de chaque bénéficiaire de soin. Le NIR est associé à un ensemble minimal de données administratives nécessaires dans le cadre de la mission d'intérêt public pour la gestion des droits et prise en charge de l'assuré.	Données minimales nécessaires pour que le PS puisse accéder à un service en ligne concernant le bénéficiaire de soin.
Identité Etat civil et adresse mail (Prénoms, Nom, Date de naissance, Genre, code INSEE de la ville de naissance (si né en France), code INSEE du pays de naissance (si né hors de France), Adresse e-mail)	DCP courantes	L'identité « état civil » de l'utilisateur est récupérée sur sa pièce d'identité. Elle est composée des données nécessaires au statut de fournisseur d'identité sur FranceConnect.	Seules les données d'identité nécessaires au statut de fournisseur d'identité sur FranceConnect sont traitées.
Identité Patient (Matricule INS, Date de naissance, Lieu de naissance, Nom de naissance, Prénoms de naissance, Sexe)	DCP perçue comme sensible (matricule INS) et DCP courantes	L'identité Patient est renvoyée par le service INSi pendant l'enrôlement. Cette identité Patient permet d'accéder à des services liés au patient, comme le DMP (intégré au LPS) sur le poste du PS	Le stockage des traits d'identité associés à l'INS est imposé par la loi, ils doivent donc accompagner l'INS dans l'ApCV.
UserID	DCP courante	Identifiant de l'utilisateur de l'ApCV dans le SI Sécurité	
Traces de fonctionnement (empreinte matérielle, identifiant ApCV, identifiant profil ApCV, NIR pseudonymisé, adresse IP smartphone)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées. Par ailleurs, pas de conservation de données directement identifiantes.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

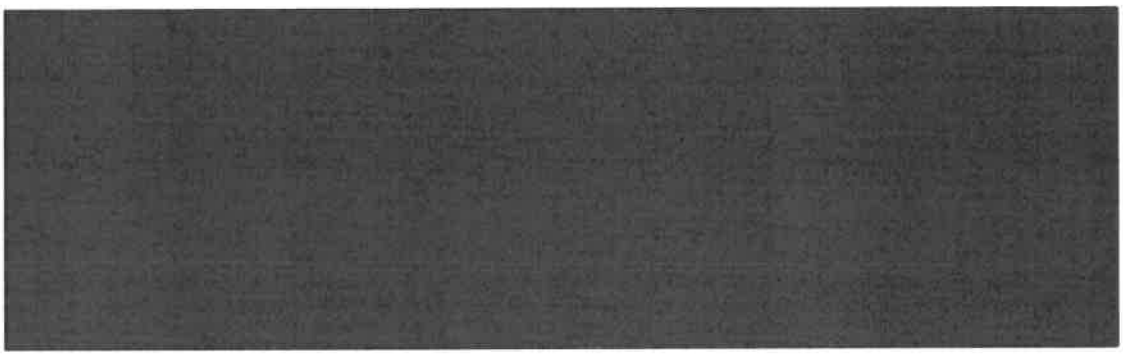
6.5.4.3 Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification
Vérification de la signature des données avant migration.	La signature des données d'identité est vérifiée avant migration. A noter que cette signature ne porte pas sur l'adresse mail ni sur la photo.
Mise à jour des données d'identité AMO et Patient à chaque lancement de l'application si la durée de validité est dépassée (24h).	La mise à jour des données s'appuie sur les référentiels des régimes qui portent la responsabilité de l'exactitude des données d'identité AMO. A noter que les données d'identité ne sont jamais mises à jour car elles proviennent de la pièce d'identité présentée lors de l'activation.

6.5.4.4 Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Identité AMO **Identité Patient** **Identité Etat civil** **Adresse mail** **Photo** **Résumés de facture**	7 jours	Données non conservées ni par le SI ApCV ni par le SI Sécurité après la migration (elles ne persistent que dans l'ApCV)	Traitement automatique de suppression si les documents du SI Sécurité n'ont pas été téléchargés par le SDK de l'ApCV dans le délai prévu.

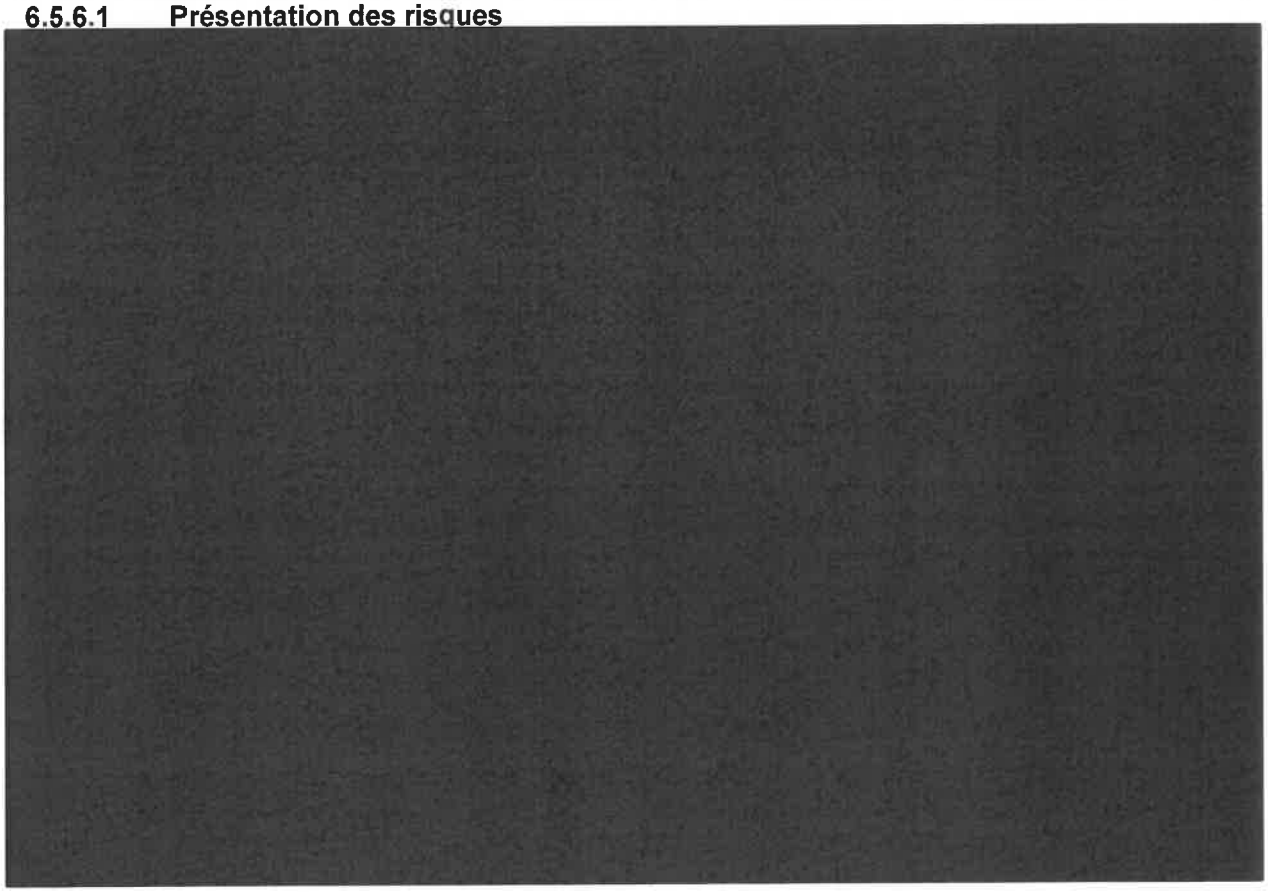
6.5.5 Mesures de sécurité



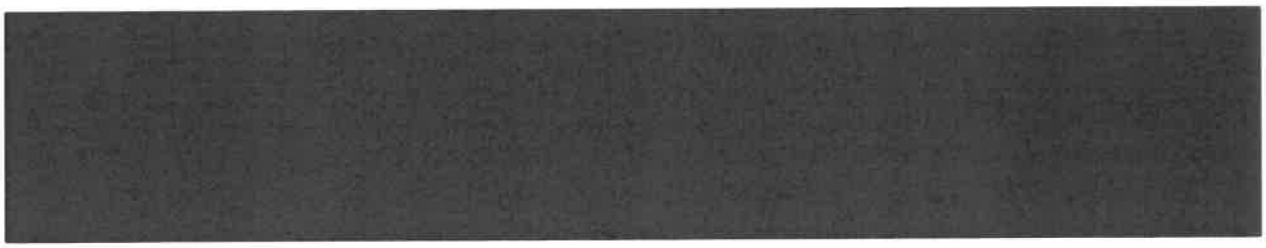
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.5.6 Risques

6.5.6.1 Présentation des risques

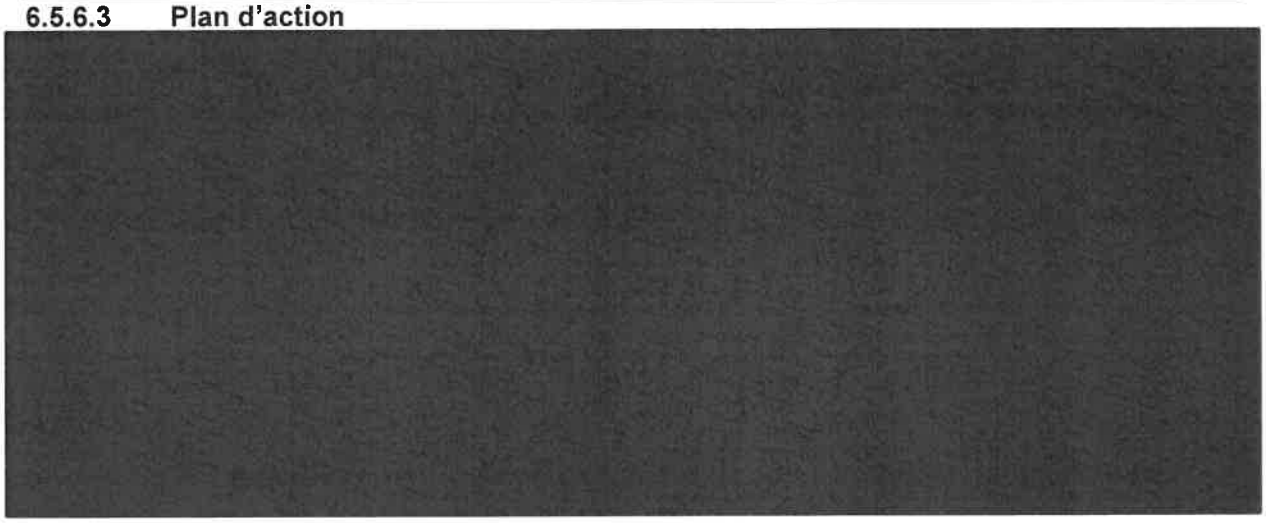


6.5.6.2 Couverture des risques



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

6.5.6.3 Plan d'action



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7 PROCESSUS SERVICES AUX PROFESSIONNELS DE SANTE

7.1 Authentification de proximité

7.1.1 Description des processus

7.1.1.1 Principes généraux de l'authentification de proximité

L'accès aux services en proximité PS nécessite une authentification préalable de l'Assuré. Pour réaliser cette authentification, l'assuré n'a pas besoin d'une connexion Internet mais le PS doit s'équiper pour exploiter l'ApCV (lecteur NFC ou lecteur de QR code).

Une fois l'authentification réalisée, un contexte ApCV est créé sur le SI ApCV. Un contexte ApCV est un groupe de données qui contient notamment :

- Les identités AMO et Patient de l'utilisateur de l'ApCV ;
- Eventuellement les identités AMO et Patient d'autres individus ;
- Des informations relatives à l'ApCV.

Une fois le contexte ApCV créé, le SI PS peut :

- Utiliser les téléservices intégrés – TLSi (cf. §7.2) ;
- Réaliser la facturation SESAM-Vitale (cf. §7.3).

Il peut également solliciter, via un navigateur, l'accès aux téléservices d'amelipro ou Web DMP PS (cf. 7.4).

Par construction :

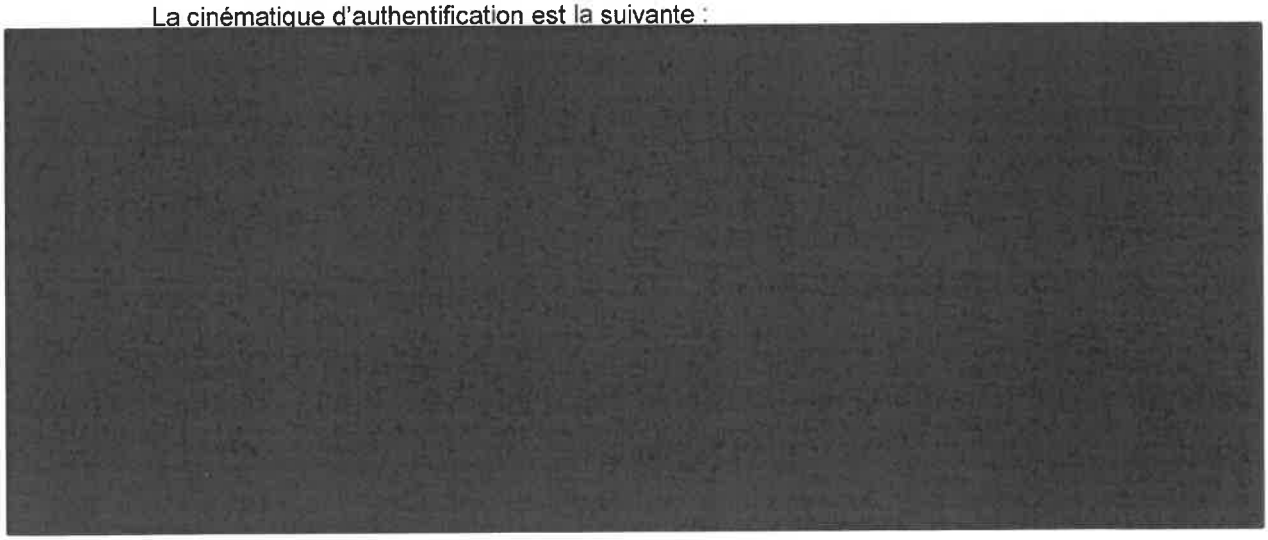
- Pour un utilisateur d'ApCV, il ne peut y avoir qu'un seul contexte ApCV actif sur le SI-ApCV à un instant donné :
- Pour un PS, il ne peut y avoir qu'un seul contexte ApCV actif sur le SI ApCV à un instant donné.

7.1.1.2 Authentification / création du contexte ApCV

Les prérequis à l'authentification sont les suivants :

- Le PS doit être authentifié et avoir obtenu une assertion PS ;
- L'assuré doit avoir déverrouillé son ApCV à l'aide de son mot de passe.

La cinématique d'authentification est la suivante :



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

1) L'ApCV demande au SDK Sécurité de générer les données d'authentification de proximité :

[redacted]

2) Le LPS récupère ces données grâce à une technologie de communication sans fil entre le smartphone de l'assuré et le SI PS (lecteur de QR code ou lecteur NFC en mode émulation de carte).

3) Le LPS envoie une demande de vérification d'identité assuré au SI ApCV

[redacted]

4) Le SI ApCV demande le contrôle de l'authentification de proximité et le déchiffrement des données au SI Sécurité.

5) Le SI Sécurité vérifie la demande d'authentification et retourne les données déchiffrées.

[redacted]

8) Le SI ApCV crée le contexte ApCV qu'il retourne au LPS.

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

7.1.1.3 Demande de contexte ApCV par le SI PS

Pendant la durée de validité du contexte ApCV, une demande de contexte peut être effectuée par un LPS pour un PS.

La cinématique est la suivante :

1) Le LPS envoie une demande de contexte [redacted]

2) Le SI ApCV vérifie que le LPS demandeur est autorisé [redacted]

3) Le SI ApCV contrôle l'assertion PS conformément aux règles définies dans le cadre d'interopérabilité des téléservices intégrés.

4) Le SI ApCV recherche un contexte ApCV valide correspondant au PS demandeur et le retourne au LPS accompagné des mêmes données que lors de la création initiale du contexte.

7.1.1.4 Destruction du contexte ApCV

Au départ de l'utilisateur, une demande de destruction du contexte ApCV doit être faite par le LPS au SI ApCV.

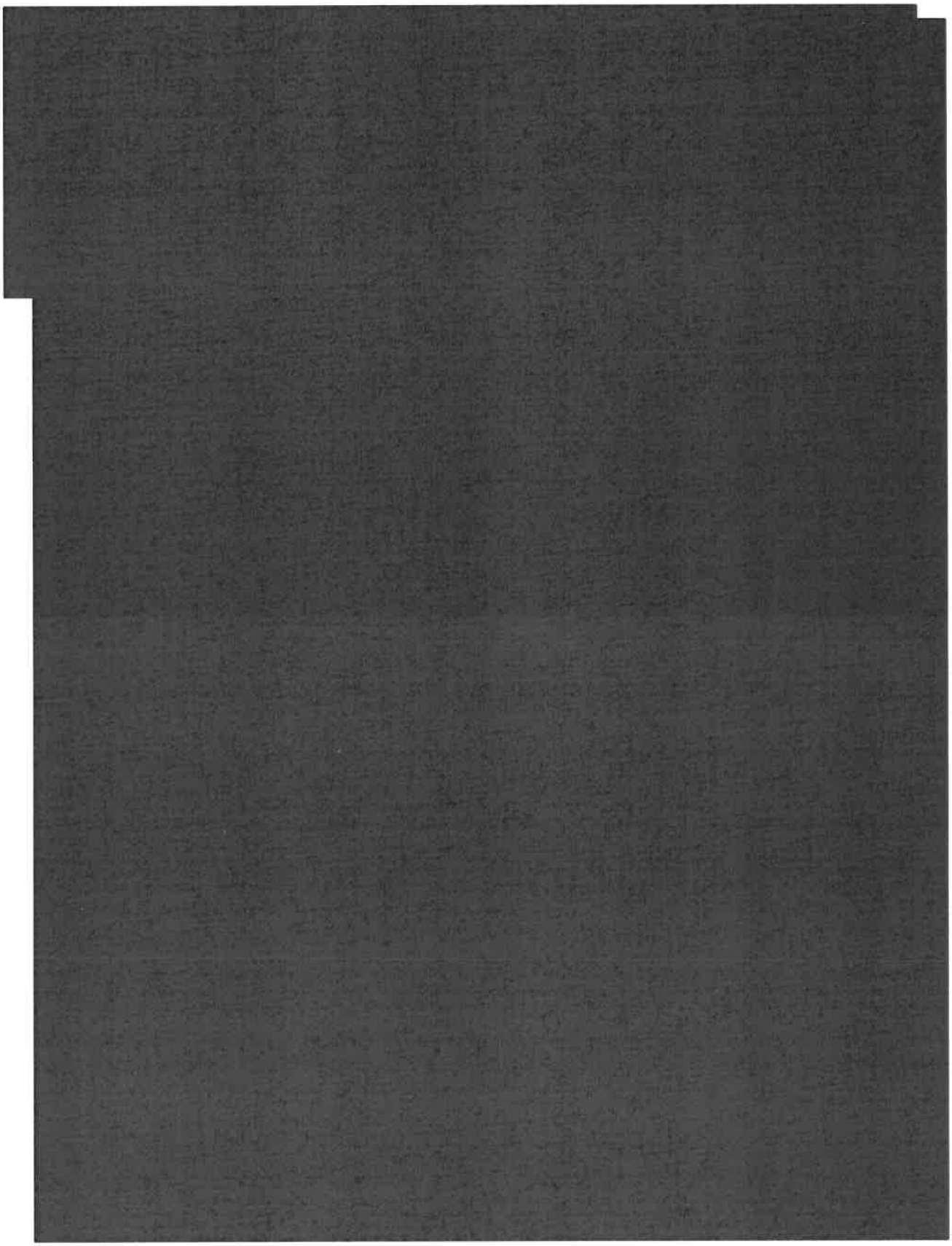
Si toutefois la destruction du contexte n'est pas demandée par le LPS, le contexte sera supprimé par le SI ApCV :

- Soit si le même PS fait une demande pour un autre utilisateur (ApCV ou carte Vitale) ;
- Soit si un autre PS fait une demande pour le même utilisateur (ApCV) ;
- Soit automatiquement à expiration [redacted]

7.1.2 Description du circuit de la donnée

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

7.1.3 Respect des principes fondamentaux

Remarque : les informations fournies ci-dessous s'appliquent au processus d'authentification de proximité, mais également à l'ensemble des processus d'accès aux services décrits dans les paragraphes suivants : appel aux TLSi, facturation et accès aux services web PS.

7.1.3.1 Caractéristiques du traitement

	Authentification de proximité
Finalités du traitement	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Sous-finalité	Renforcer la lutte contre la fraude Professionnels de Santé et assurés dans le cadre de la prise en charge des soins par l'Assurance Maladie.
Informations complémentaires	L'authentification de proximité permet l'authentification de l'utilisateur de l'application mobile et la fourniture des données permettant les usages métier PS : - Appel des téléservices intégrés (TLSi) ; - Réalisation de la facturation SESAM-Vitale avec en complément la possibilité pour l'utilisateur ApCv de consulter un résumé de sa facture ; - Accès aux services web PS : amelipro et WebDMP PS.
Intervention de sous-traitants ultérieurs	Infogérant du SI ApCV [redacted] Fournisseur du SDK Sécurité et infogérant du SI Sécurité [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.1.3.2 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Identifiant national PS Identifiant facturation PS	DCP courante	Identification du PS	
[redacted] Identifiant ApCV Identifiant profil ApCV N° de série	DCP courante	Identification de l'ApCV	
Identité AMO (NIR, Nom de famille, Nom d'usage, Prénom, Date de naissance, Rang de naissance)	DCP perçue comme sensible (NIR) et DCP courantes	Données métier nécessaires aux services pour identifier l'assuré	
Identité Patient (Matricule INS, Date de naissance, Lieu de naissance, Nom de naissance, Prénoms de naissance, Sexe)	DCP perçue comme sensible (matricule INS) et DCP courantes	Données métier nécessaires aux services pour identifier le patient	
Traces de fonctionnement (identifiant national PS, identifiant facturation PS, [redacted] identifiant ApCV, identifiant profil ApCV, NIR pseudonymisé)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées. Par ailleurs, pas de conservation de données directement identifiantes.

7.1.3.3 Explication et justification de la qualité des données

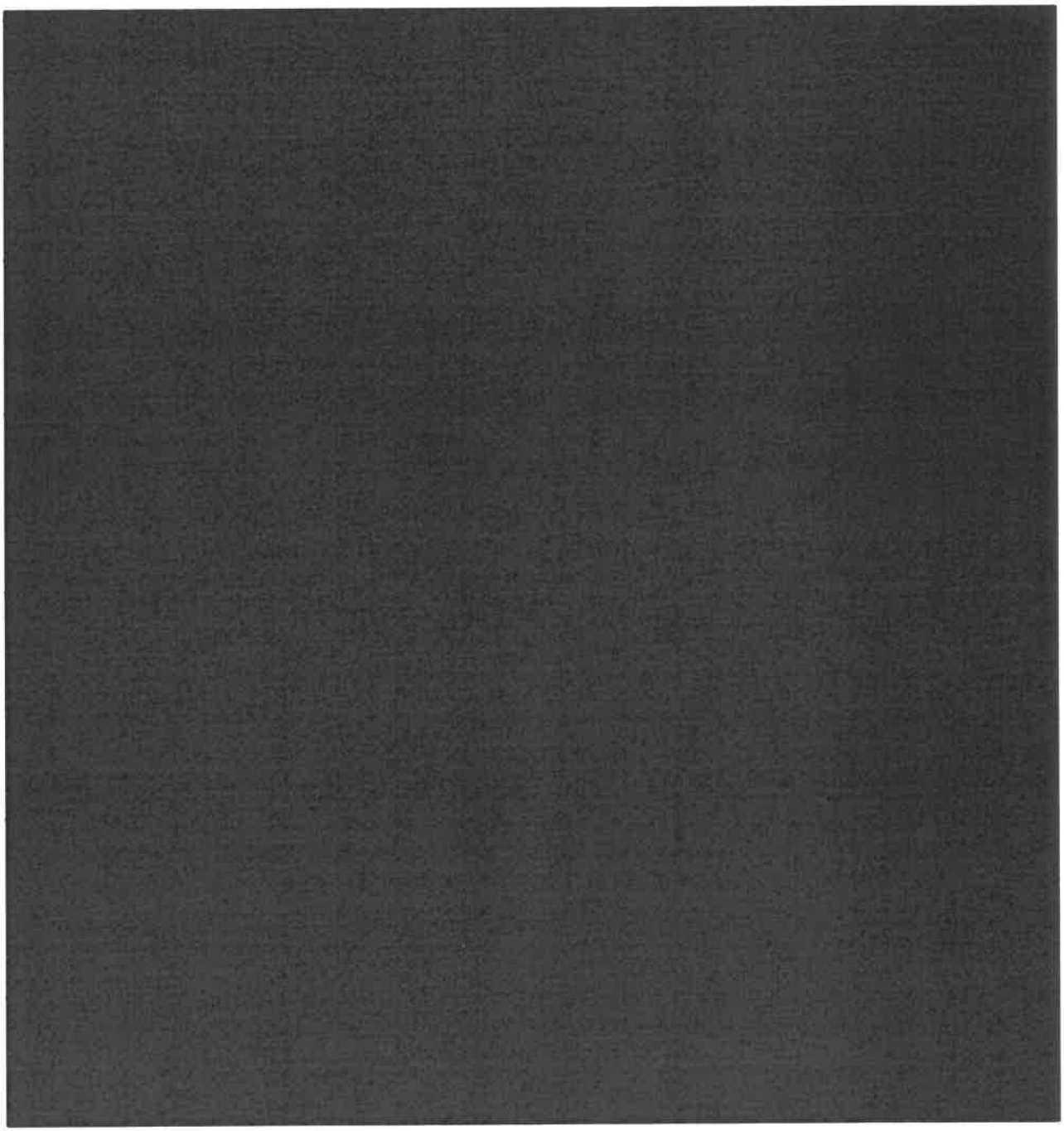
Mesures pour la qualité des données	Justification
Une signature des données d'identité est calculée par le SI ApCV à l'activation et à chaque mise à jour des données, puis descendue dans l'ApCV. Cette signature est présentée par l'ApCV et vérifiée par le SI ApCV lors de l'authentification de proximité manière à garantir d'exactitude des données fournies aux services.	N/A
Les données métier AMO sont actualisées par un appel au service FD (Famille de droits) de l'inter régime dès lors qu'un changement de situation a été signalé afin de garantir leur exactitude.	N/A

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.1.3.4 Explication et justification des durées de conservation

Les seules données produites sont des traces dont les durées de conservation sont précisées au §5.2.1.4.

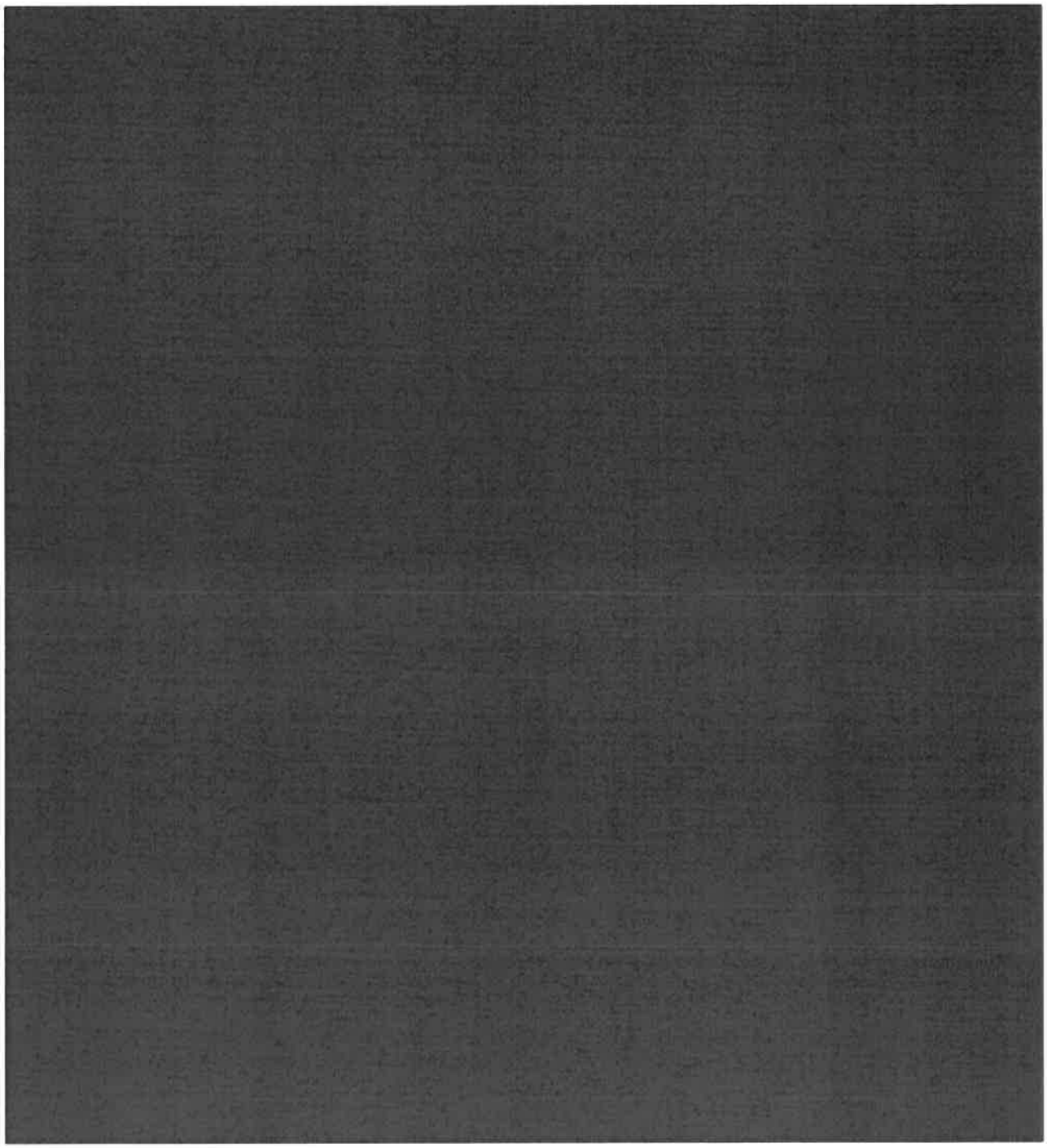
7.1.4 Mesures de sécurité



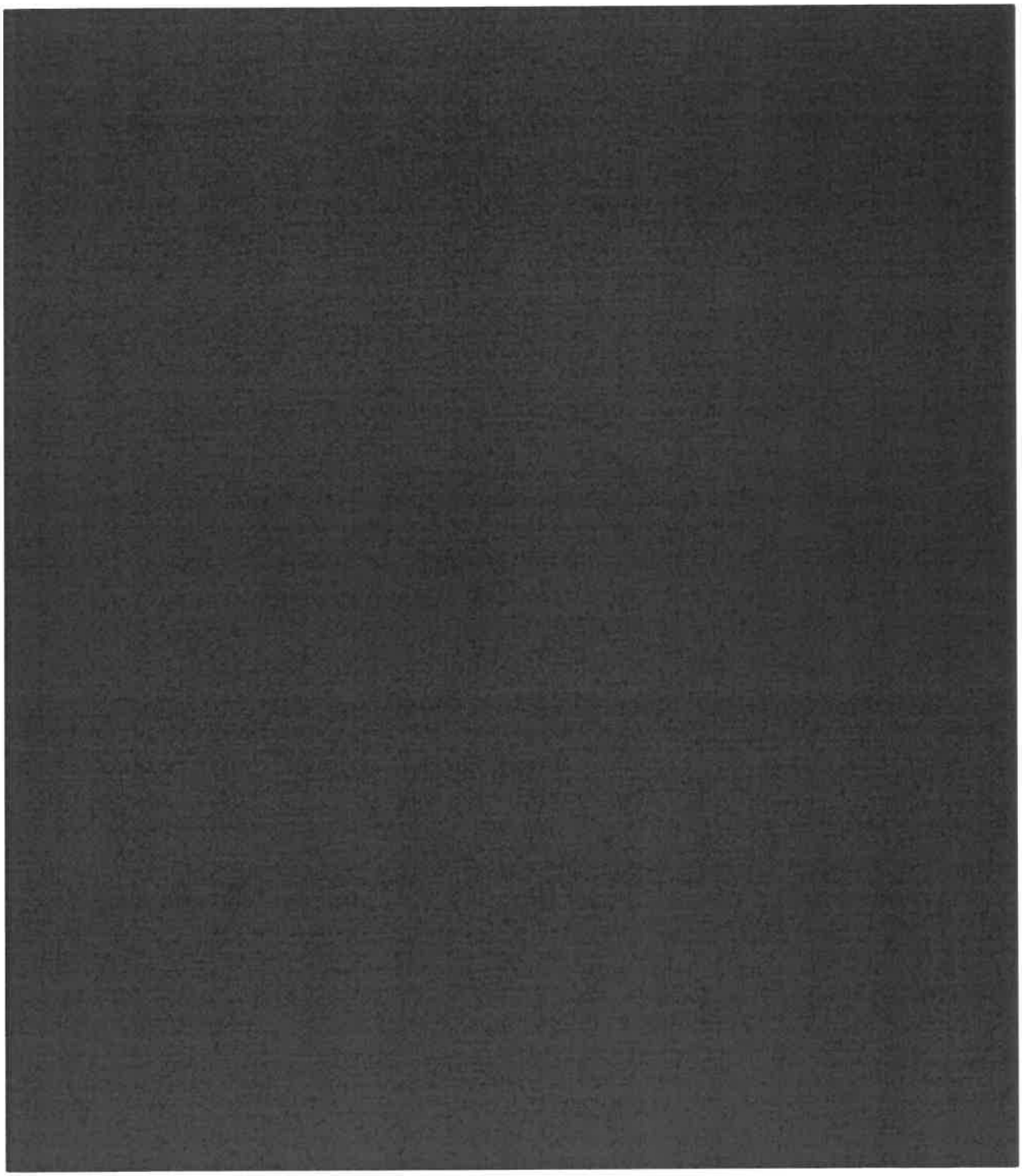
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.1.5 Risques

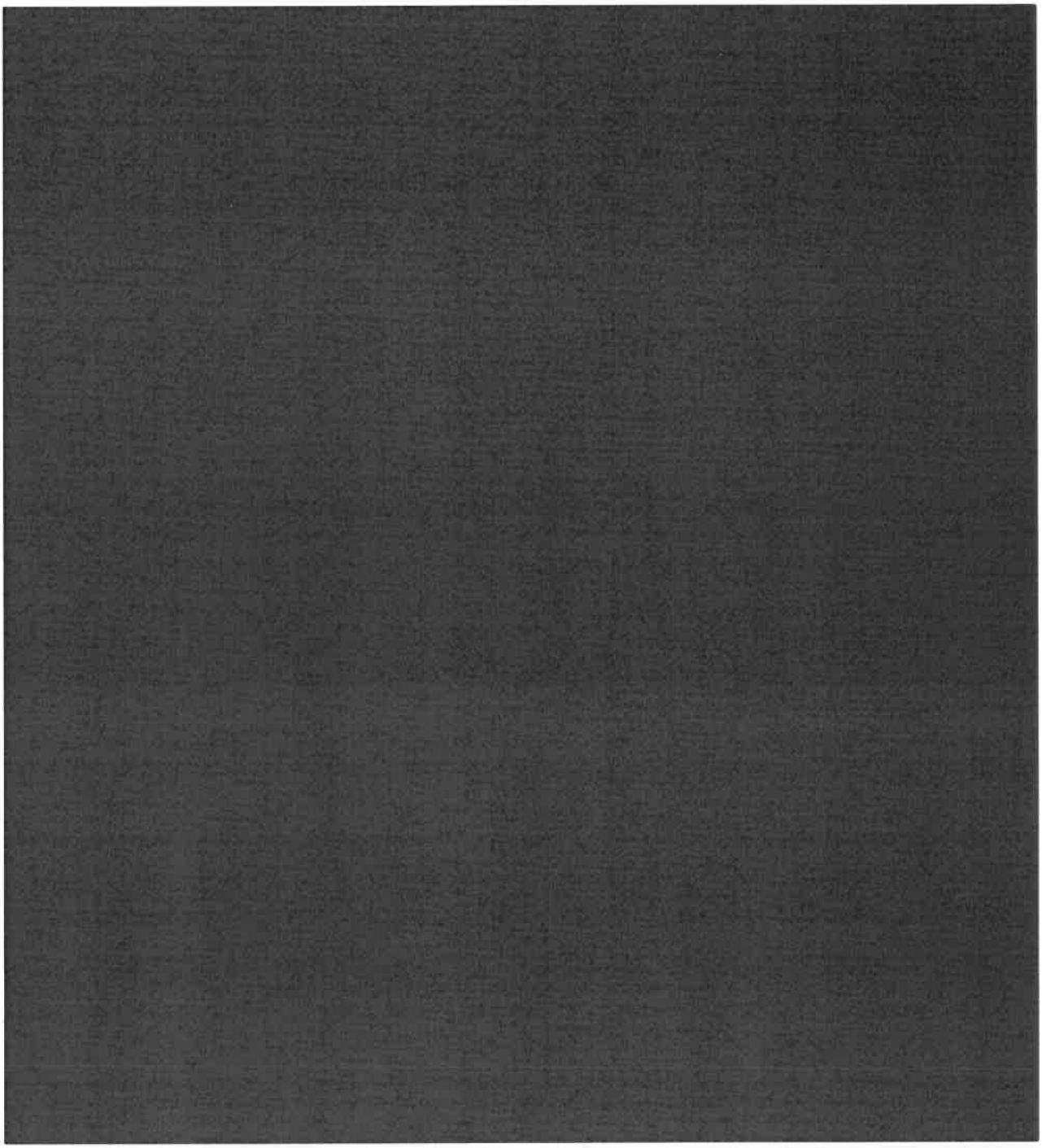
7.1.5.1 Présentation des risques



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

7.1.5.2 Couverture des risques

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.1.5.3 Plan d'action

[redacted]

7.2 Téléservices intégrés (TLSi)

7.2.1 Description du processus

[redacted]

1) [redacted]

2) [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

7.2.2 Description du circuit de la donnée

[redacted]

7.2.3 Respect des principes fondamentaux

Cf. §7.1.3.

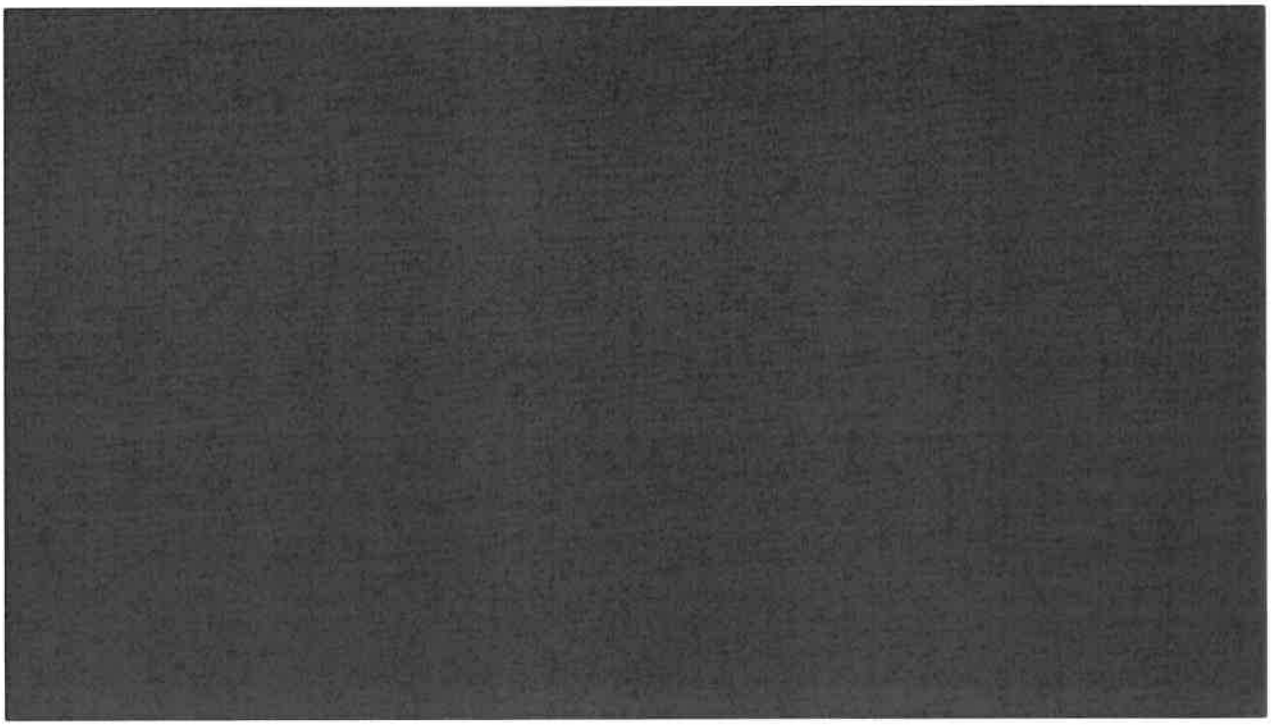
7.2.4 Mesures de sécurité

[redacted]

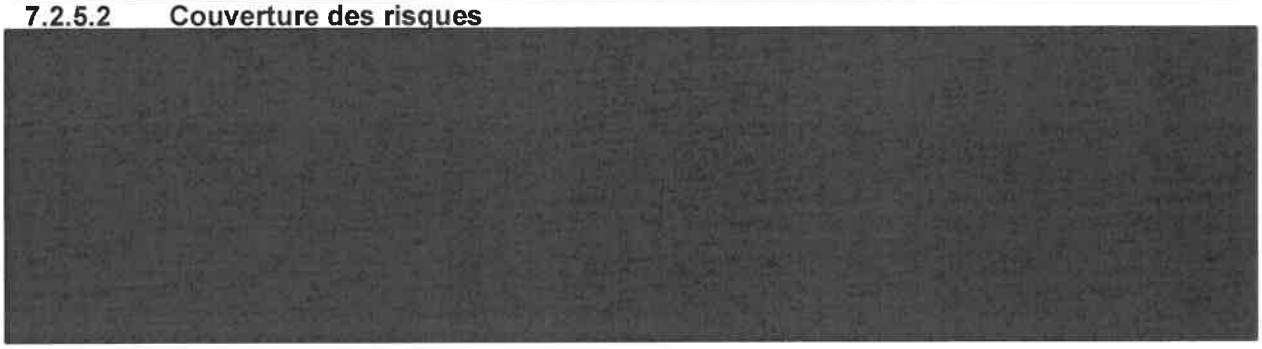
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.2.5 Risques

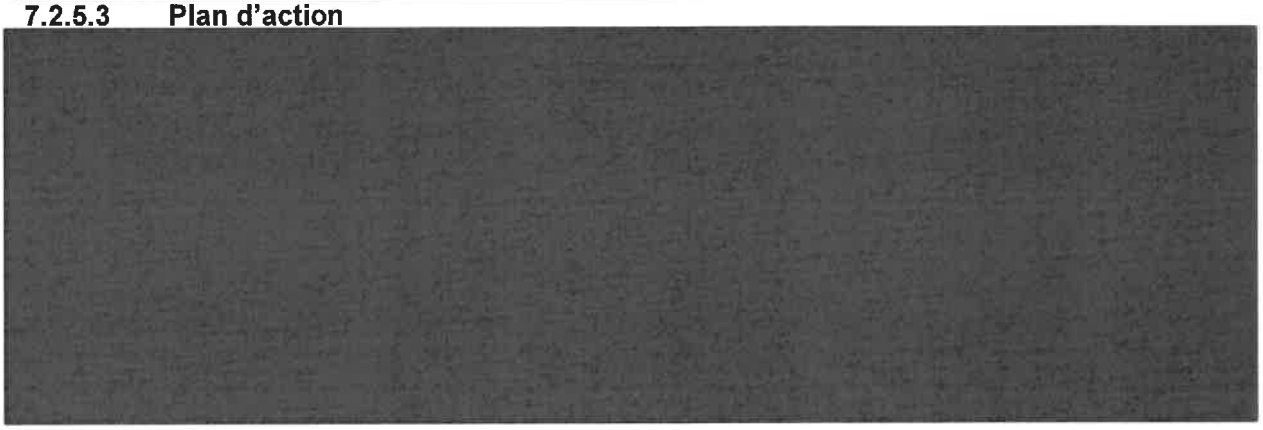
7.2.5.1 Présentation des risques



7.2.5.2 Couverture des risques



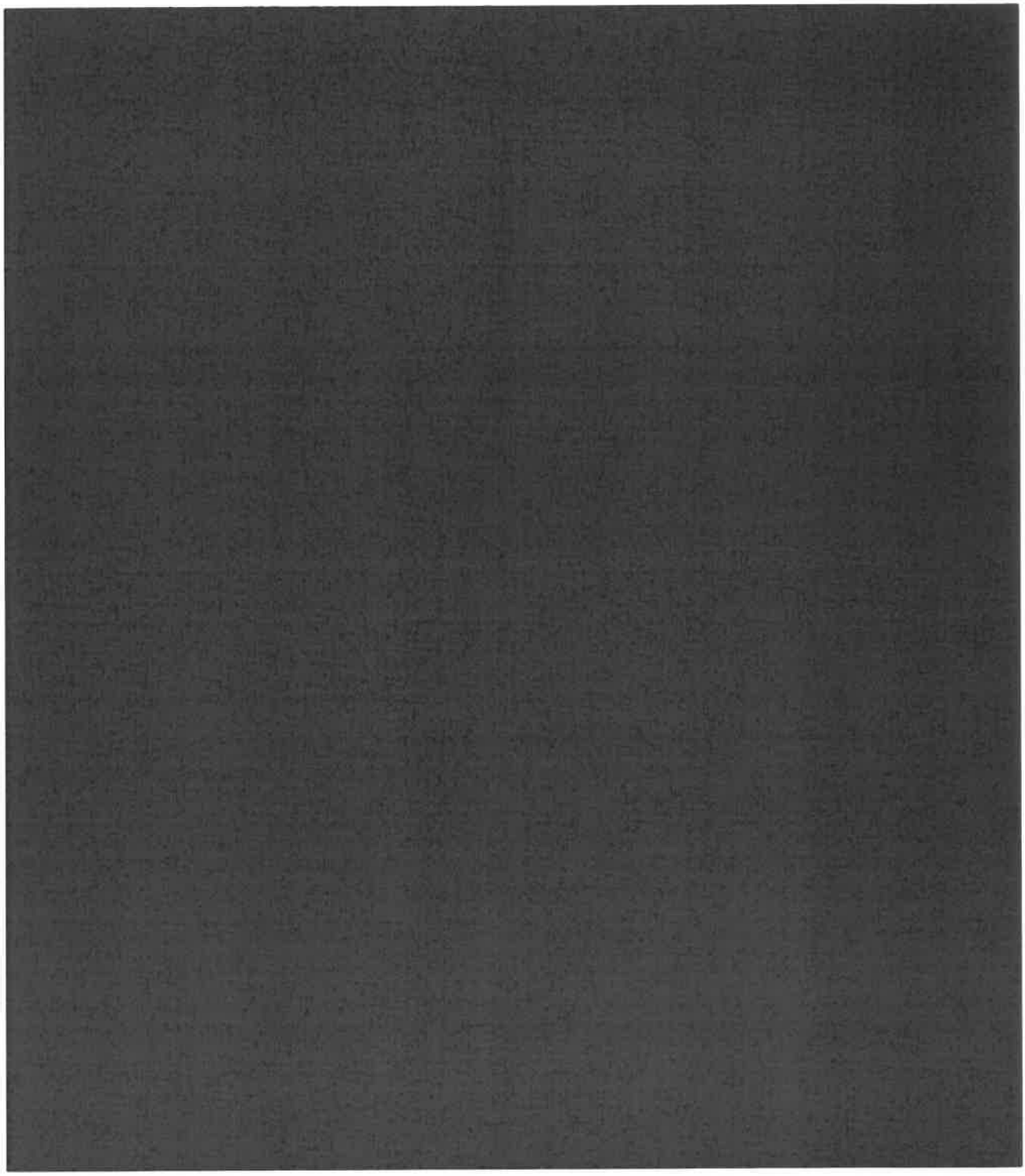
7.2.5.3 Plan d'action



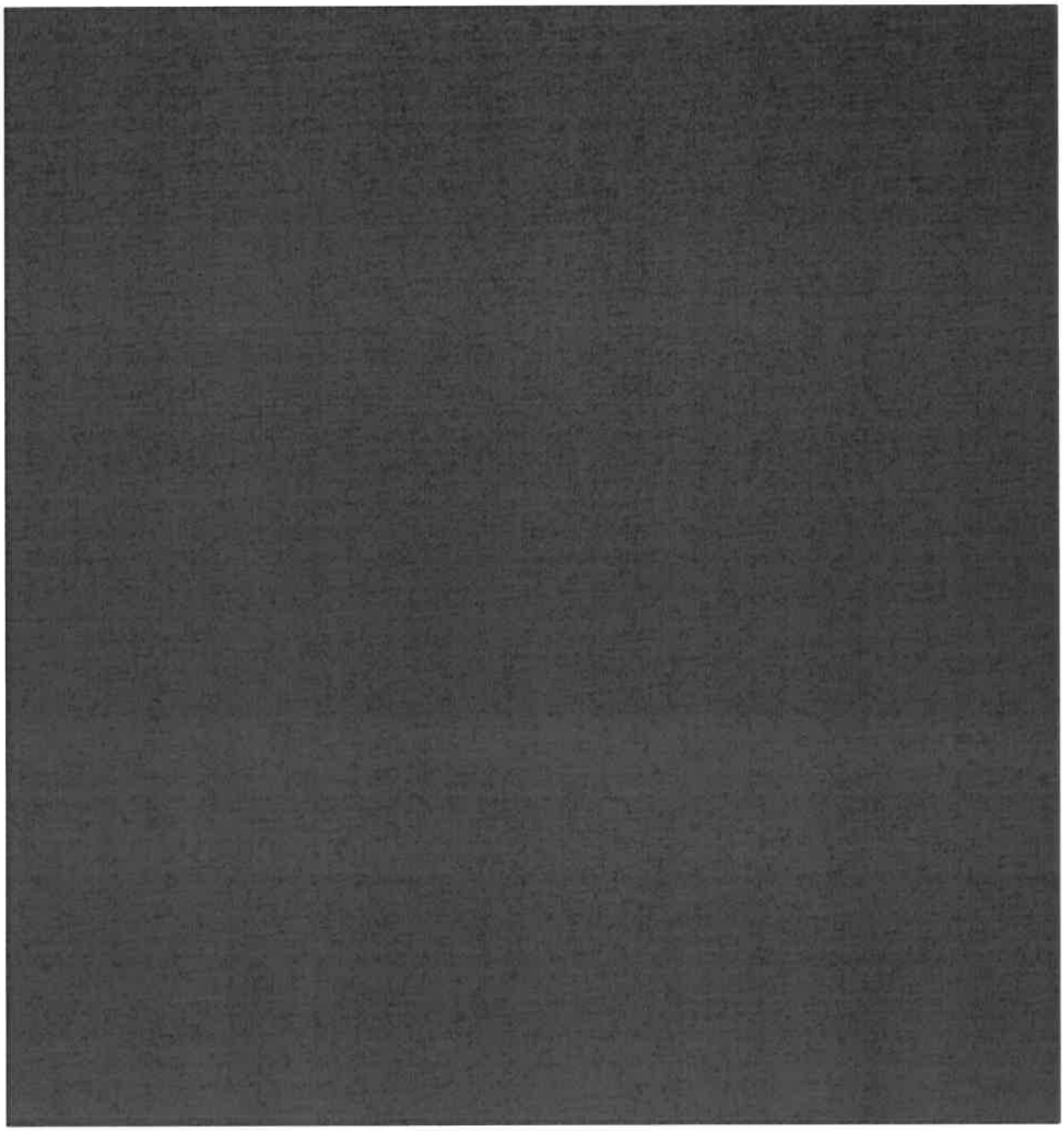
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.3 Facturation SESAM-Vitale

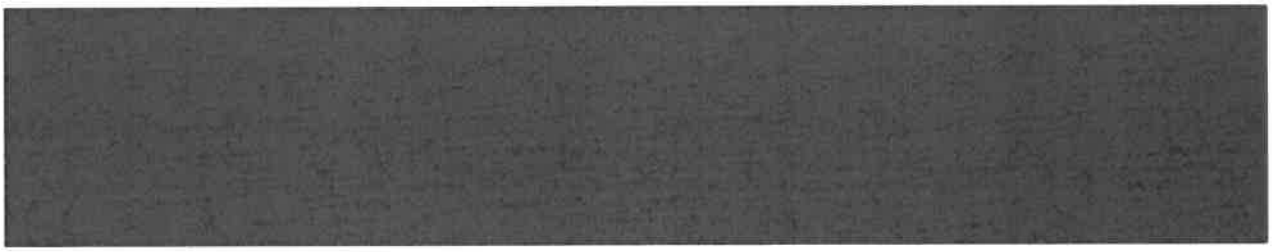
7.3.1 Description du processus



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



7.3.2 Description du circuit de la donnée

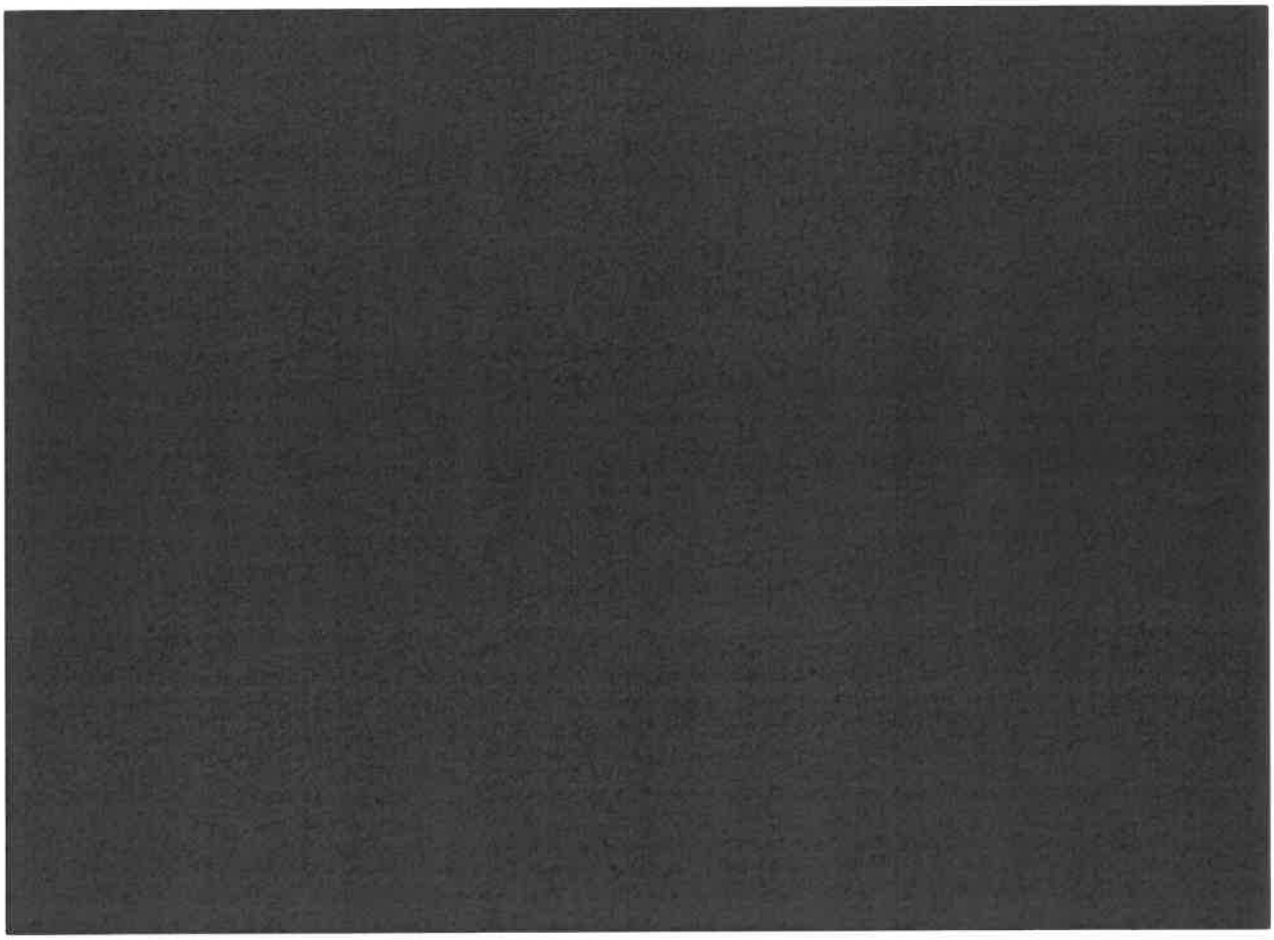


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.3.3 Respect des principes fondamentaux

Cf. §7.1.3.

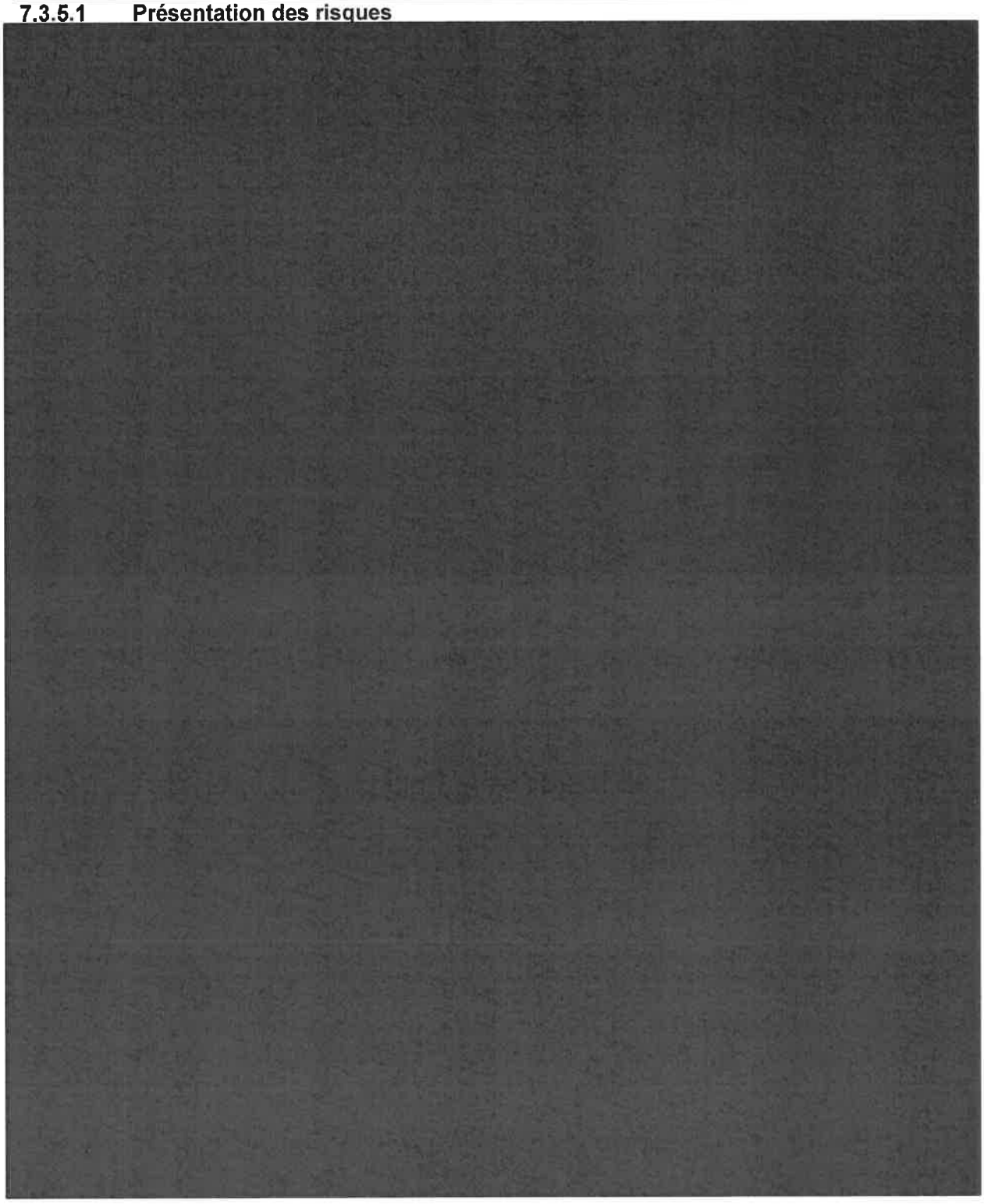
7.3.4 Mesures de sécurité



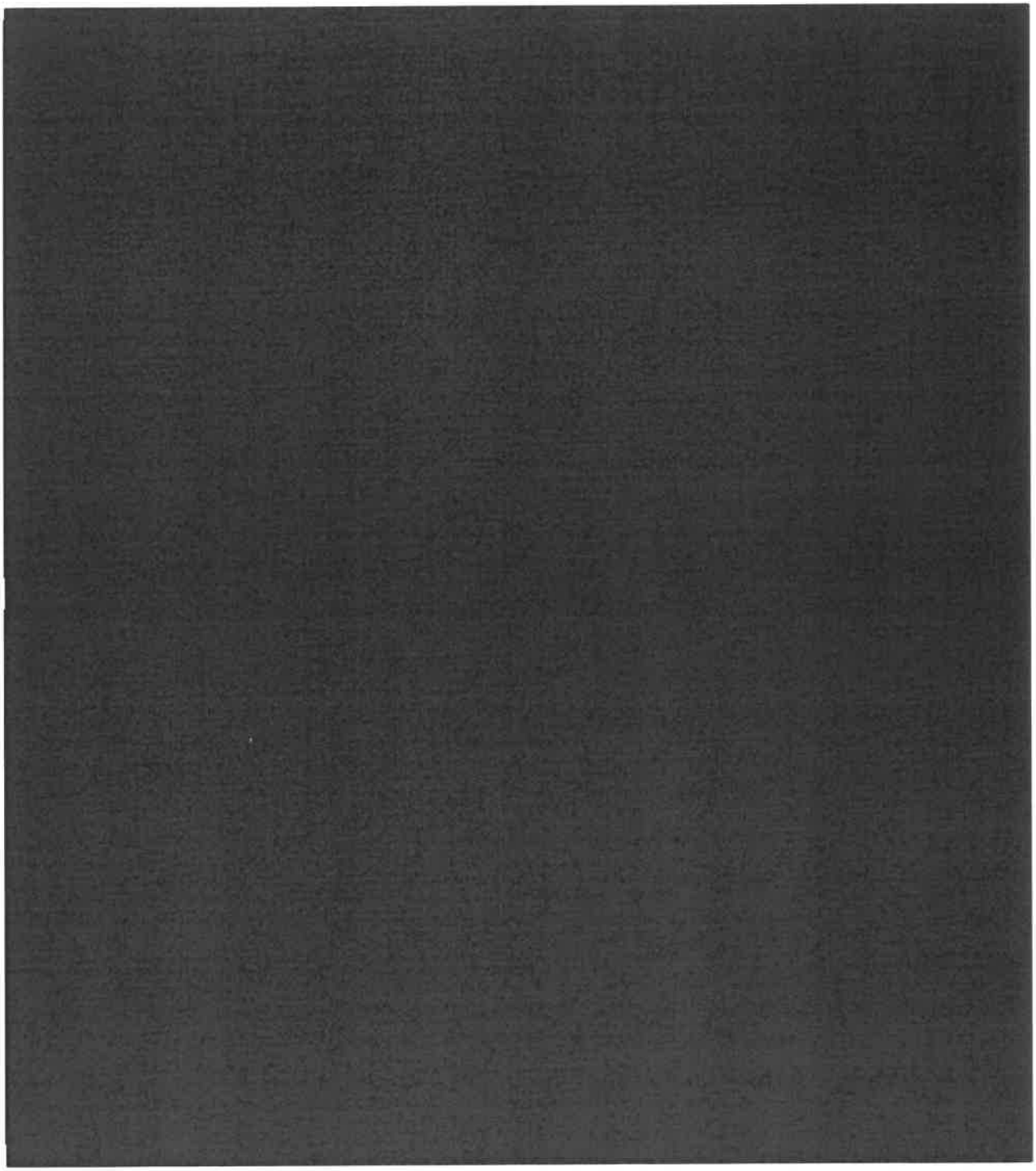
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.3.5 Risques

7.3.5.1 Présentation des risques

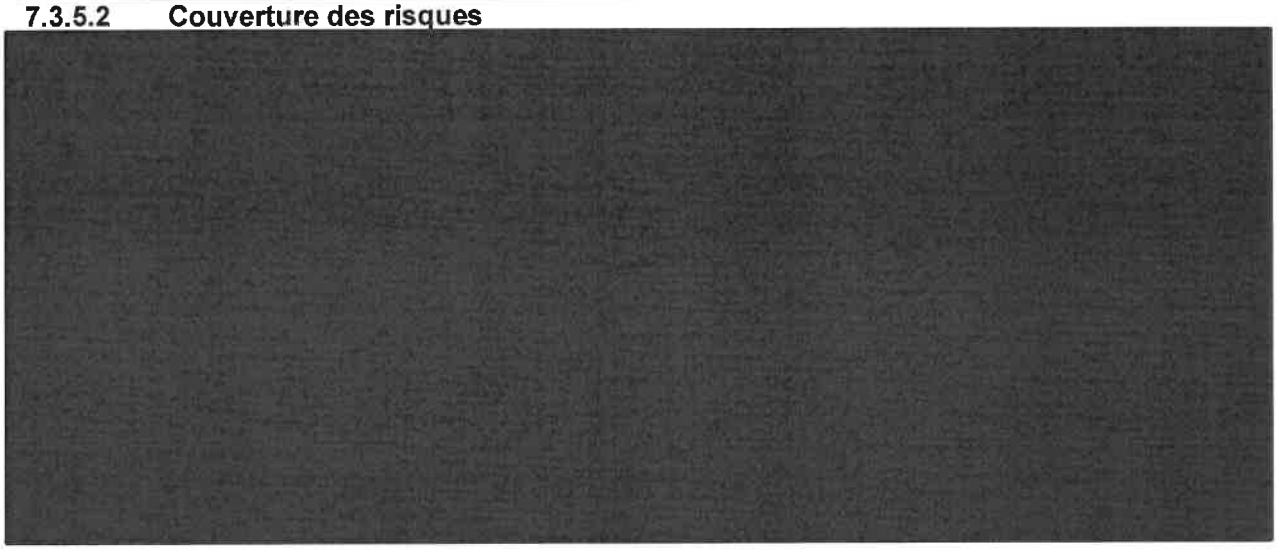


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

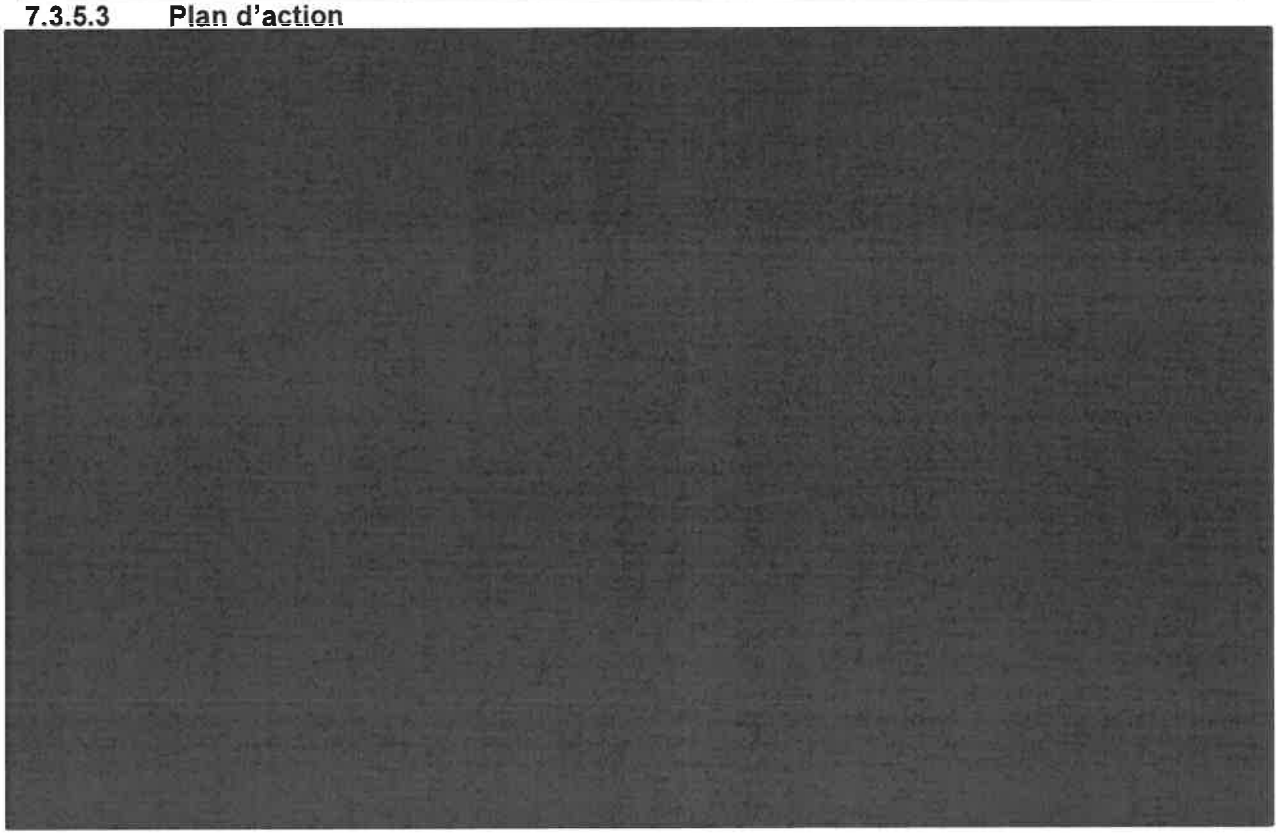


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.3.5.2 Couverture des risques



7.3.5.3 Plan d'action



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.4 Accès aux services web PS (amelipro, WebDMP PS)

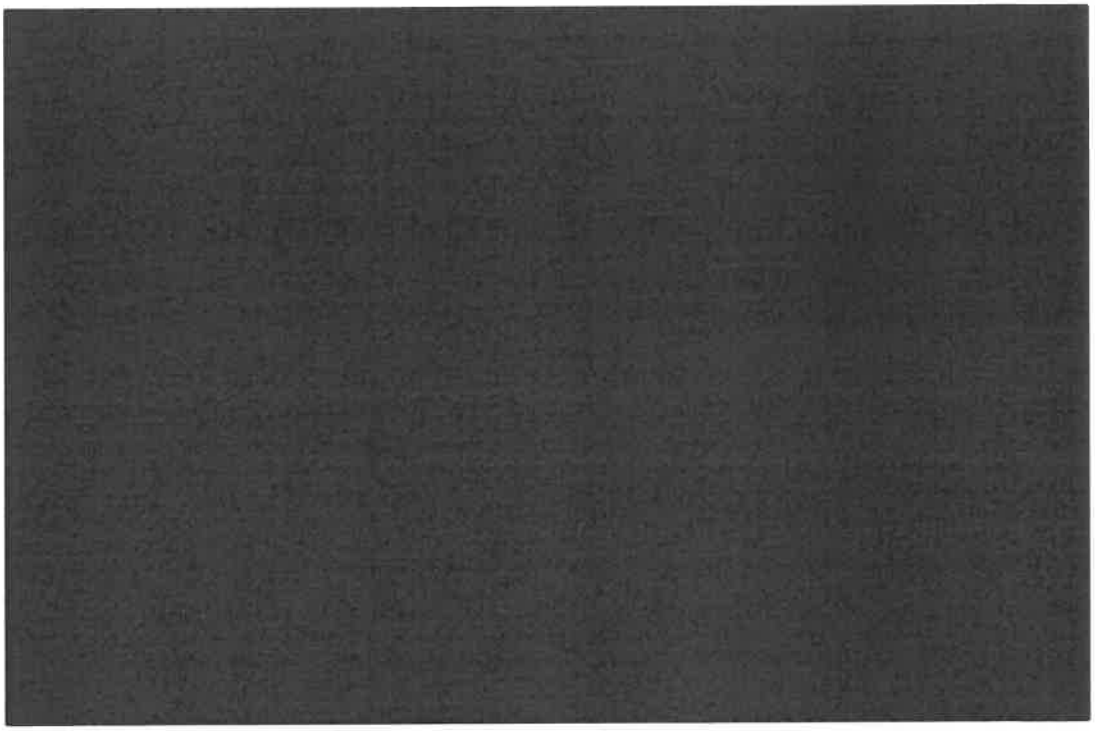
7.4.1 Description du processus

Le contexte ApCV doit avoir été créé préalablement sur le SI ApCV, via une authentification de proximité (cf. 7.1).

Le contexte ApCV a une durée de validité, durant laquelle l'accès aux services qui nécessitent la présence de l'utilisateur est autorisée. Il reste accessible sur le SI ApCV tant que sa durée de validité n'est pas dépassée. L'appel au service web PS doit être effectué dans ce délai.

Note : si le contexte ApCV expire, une nouvelle authentification de l'utilisateur de l'ApCV est nécessaire pour accéder aux services de l'Assurance Maladie. Cette nouvelle demande doit obligatoirement être réalisée via le LPS.

Le processus d'accès aux applications web amelipro et WebDMP PS est le suivant :



1) Le PS ouvre son navigateur internet et accède à l'application web d'un FS-PS comme amelipro ou WebDMP PS. Il est authentifié avec sa carte CPS. Sur la page d'accueil, il choisit d'utiliser l'ApCV du patient.
2) L'application web appelle le SI ApCV pour récupérer le contexte ApCV lié à ce PS, sachant que le SI ApCV garantit qu'à un instant donné, un seul contexte ApCV existe pour un PS donné.
3) Le SI ApCV retourne le contexte ApCV. Le contexte ApCV retourné contient :
   - Un identifiant de contexte ;
   - Les données d'identité AMO et le contrat AMO de l'utilisateur et de chacun des bénéficiaires.

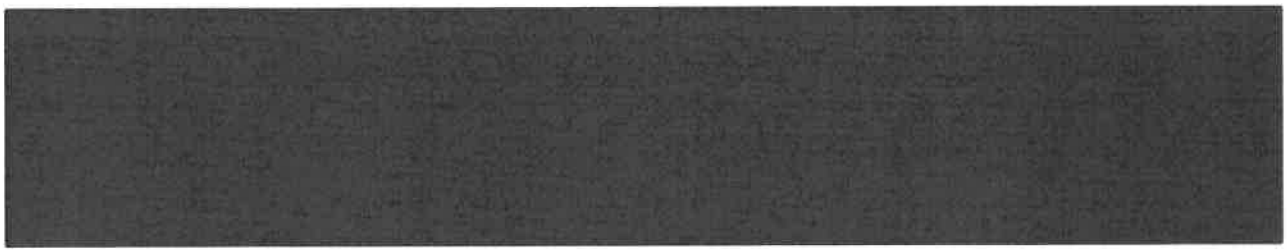
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.4.2 Description du circuit de la donnée

7.4.3 Respect des principes fondamentaux

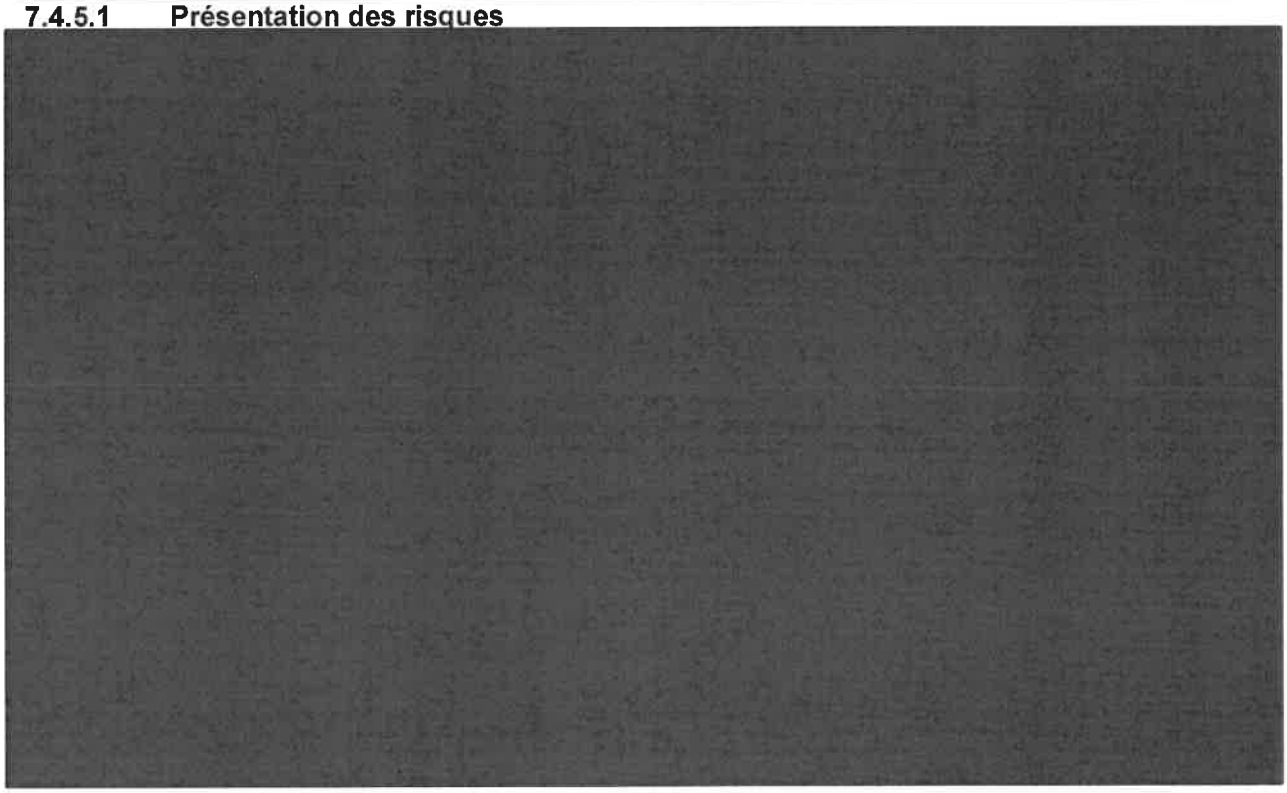
Cf. §7.1.3.

7.4.4 Mesures de sécurité



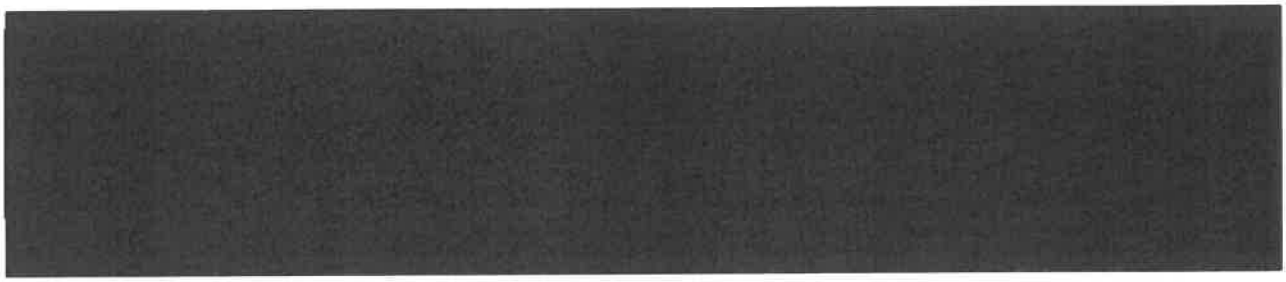
7.4.5 Risques

7.4.5.1 Présentation des risques



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

7.4.5.2 Couverture des risques



7.4.5.3 Plan d'action

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

8 PROCESSUS SERVICES AUX ETABLISSEMENTS DE SANTE

8.1 Authentification sans CPx

8.1.1 Description du processus

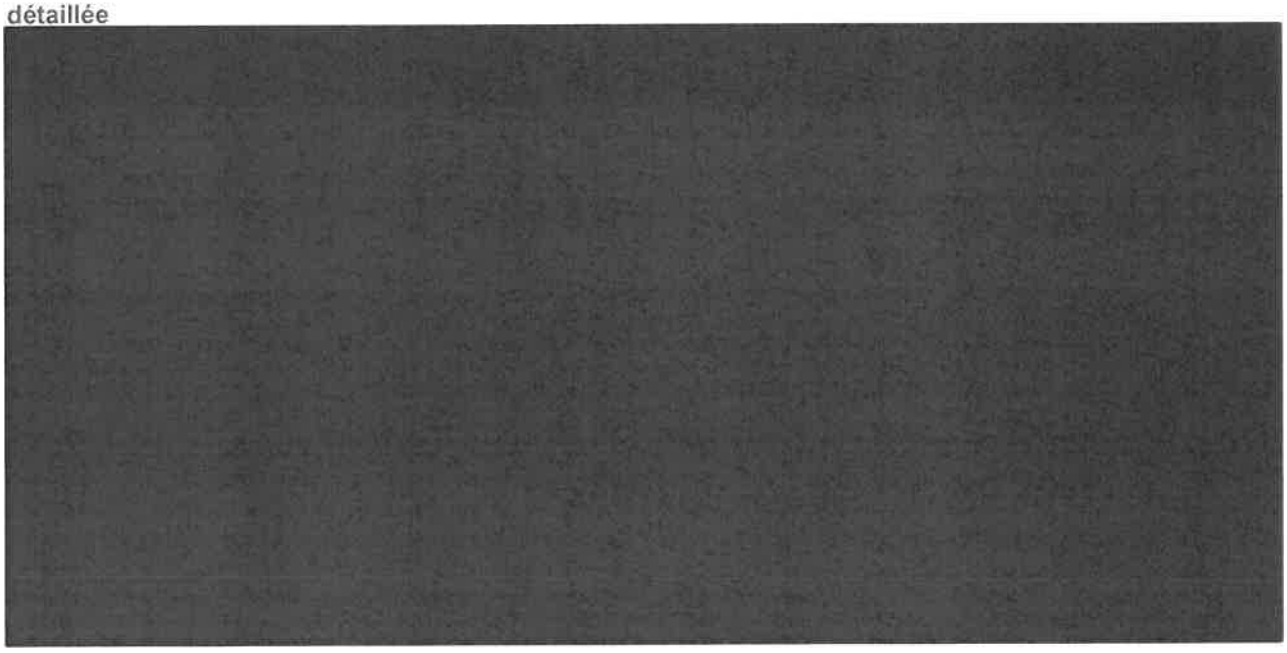
Présentation générale

Les cas d'utilisation de l'ApCV par un bénéficiaire à l'arrivée dans un établissement de Santé peuvent par exemple être :

- Le bénéficiaire est invité à utiliser les bornes d'accueil pour signaler sa présence. Si la borne reconnait un dossier complexe, elle envoie le bénéficiaire de soins à l'accueil où l'agent utilise un poste sans forcément avoir de CPx ;
- Le bénéficiaire va directement vers un agent d'accueil où l'agent utilise un poste sans forcément avoir de CPx.

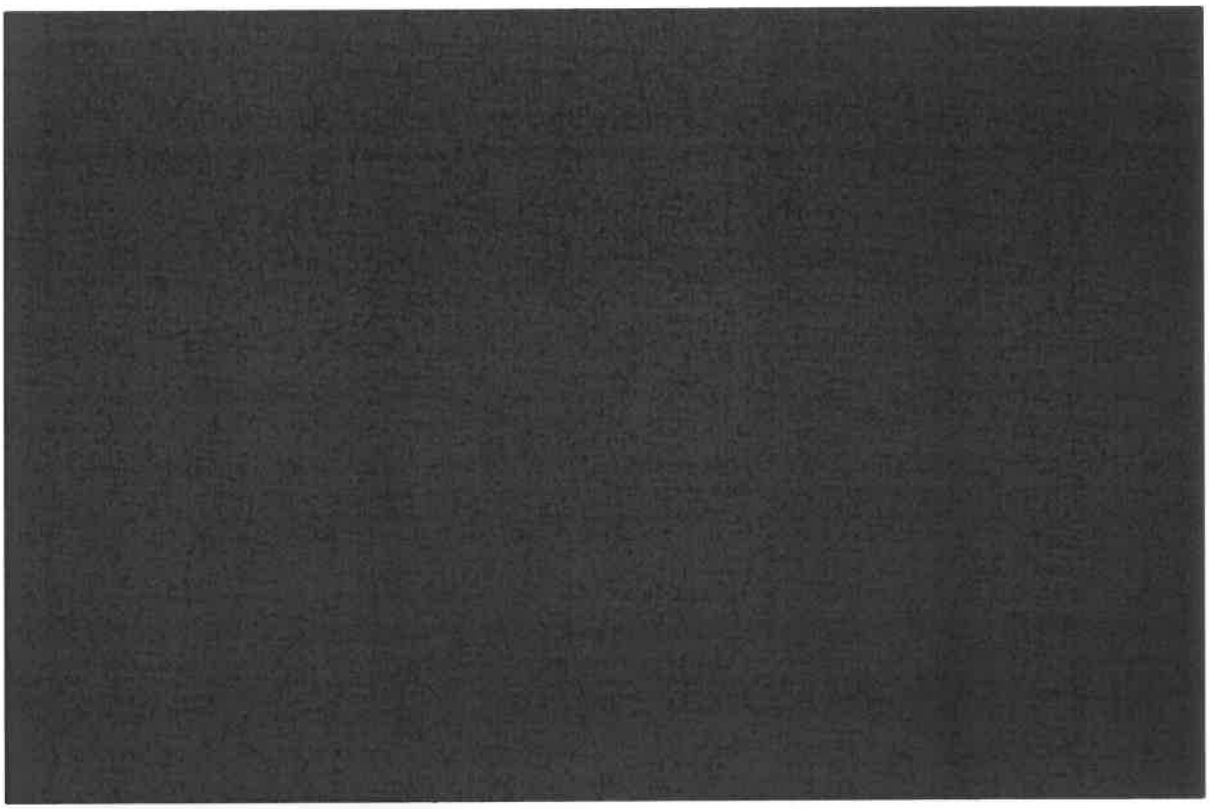
La présentation par l'utilisateur du QR Code ou du NFC à l'agent, ou la borne d'accueil, permettra de restituer à l'établissement de santé l'ensemble des données déchiffrées du profil ApCV de l'utilisateur.

Présentation détaillée



1) L'utilisateur présente son ApCV à l'agent d'accueil ou à la borne d'accueil en libre-service. La lecture de l'ApCV est réalisée par les logiciels de l'ES au moyen d'un lecteur QR Code ou d'un lecteur NFC.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

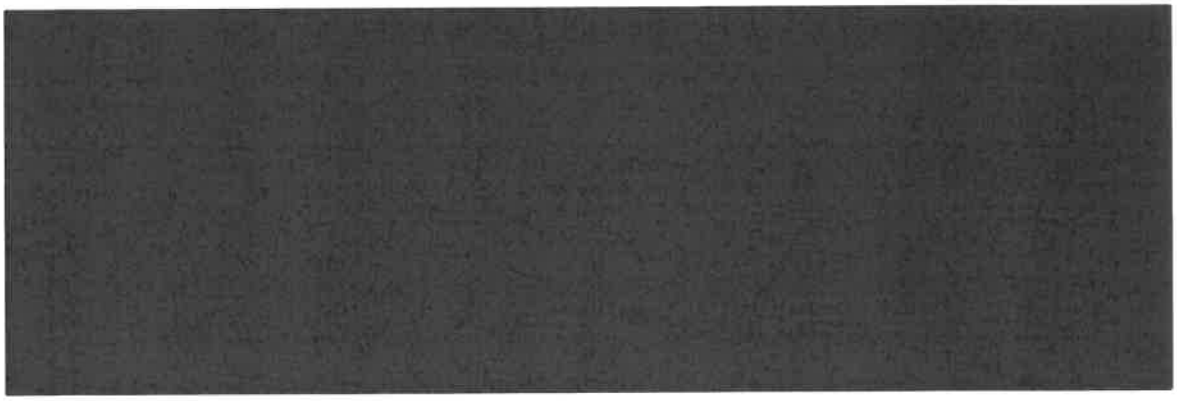


le SI ApCV restitue le profil ApCV ES qui contient :

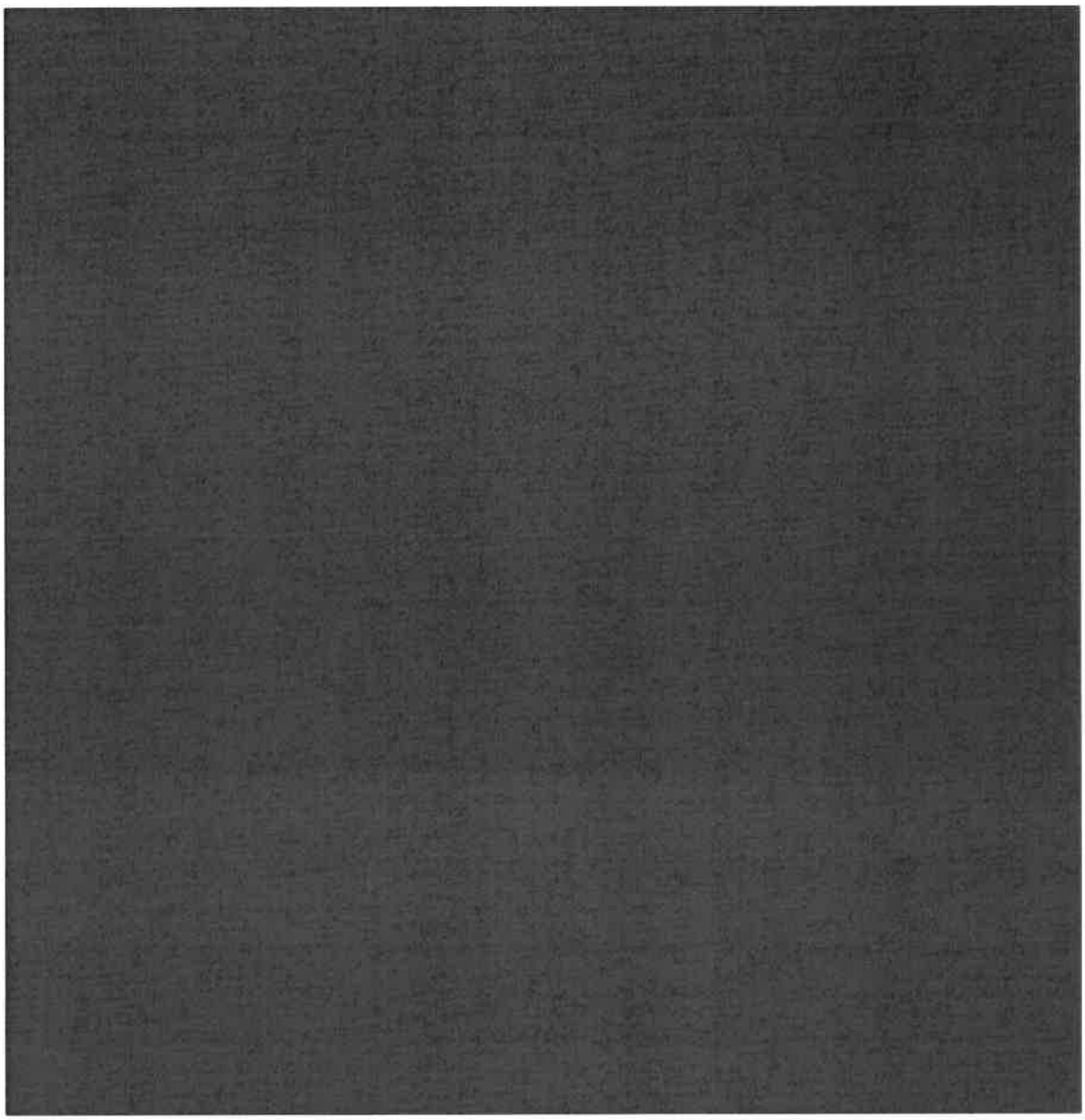
- Les données d'identité AMO et d'identité patient de l'utilisateur de l'ApCV et de ses bénéficiaires ;
- Les informations relatives à l'ApCV.

Note : contrairement à l'authentification de proximité PS, l'authentification ApCV en ES n'ouvre pas de contexte dans le SI ApCV permettant la facturation.

8.1.2 Description du circuit de la donnée



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



8.1.3 Respect des principes fondamentaux

8.1.3.1 Caractéristiques du traitement

	Authentification de proximité
Finalités du traitement	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Sous-finalité	Renforcer la lutte contre la fraude Professionnels de Santé et assurés dans le cadre de la prise en charge des soins par l'Assurance Maladie.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Informations complémentaires	L'authentification en ES permet d'authentifier l'utilisateur de l'application mobile et d'acquérir les identités du bénéficiaire lors de son admission. Les informations obtenues dans le profil ApCV sont utilisables pour l'appel à CDRi et pour la facturation des prestations effectuées par l'ES.
Intervention de sous-traitants ultérieurs	Infogérant du SI ApCV [redacted] Fournisseur du SDK Sécurité et infogérant du SI Sécurité [redacted]

8.1.3.2 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
[redacted] Identifiant ApCV Identifiant profil ApCV N° de série	DCP courante	Identification de l'ApCV	
Identité AMO (NIR, Nom de famille, Nom d'usage, Prénom, Date de naissance, Rang de naissance)	DCP perçue comme sensible (NIR) et DCP courantes	Données métier nécessaires aux services pour identifier l'assuré	
Identité Patient (Matricule INS, Date de naissance, Lieu de naissance, Nom de naissance, Prénoms de naissance, Sexe)	DCP perçue comme sensible (matricule INS) et DCP courantes	Données métier nécessaires aux services pour identifier le patient	
Traces de fonctionnement [redacted] identifiant ApCV, identifiant profil ApCV, NIR pseudonymisé)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées. Par ailleurs, pas de conservation de données directement identifiantes.

8.1.3.3 Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification
Une signature des données d'identité est calculée par le SI ApCV à l'activation et à chaque mise à jour des données, puis descendue dans l'ApCV. Cette signature est présentée par l'ApCV et vérifiée par le SI ApCV lors de l'authentification de proximité manière à garantir d'exactitude des données fournies aux services.	N/A

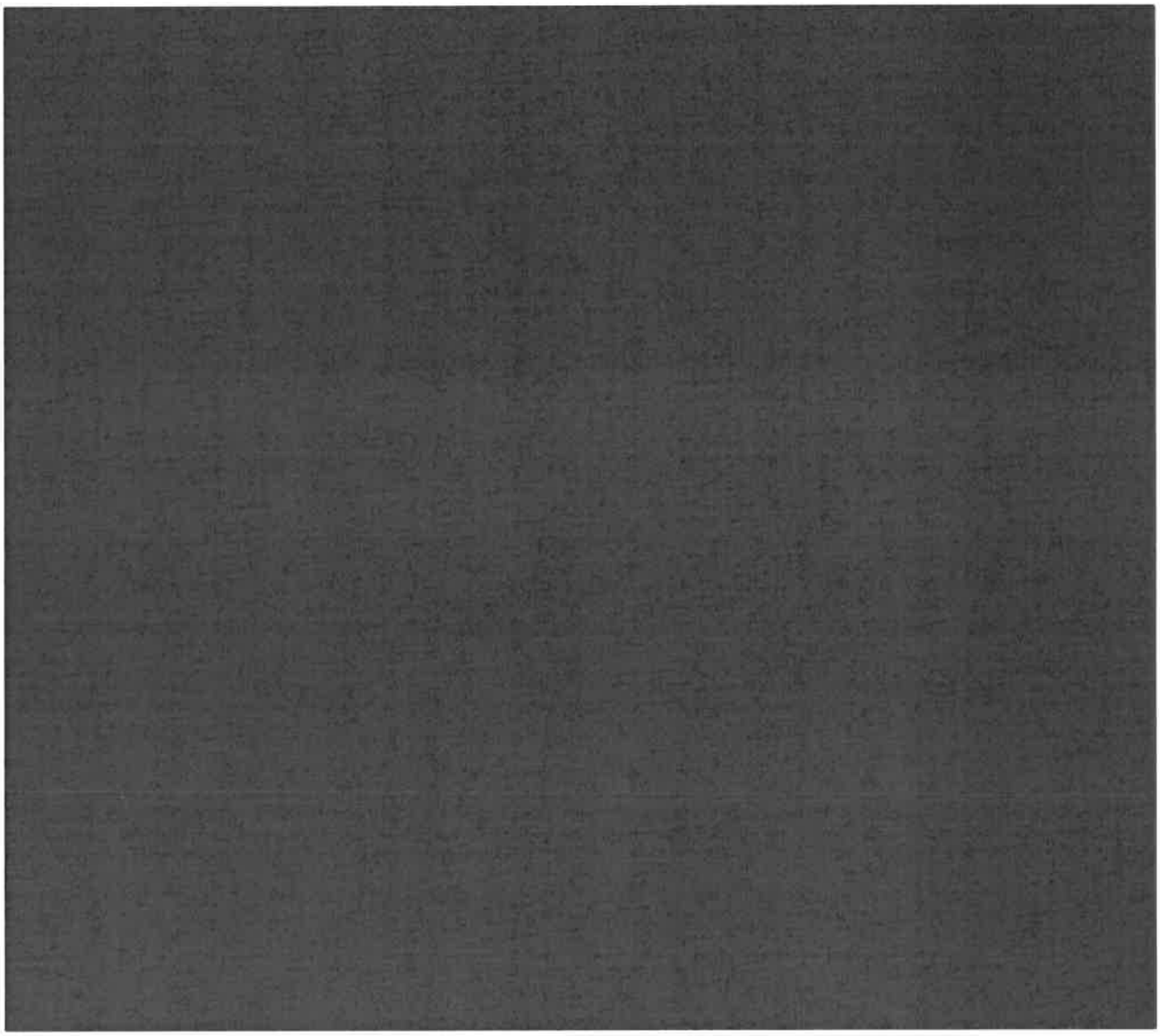
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Les données métier AMO sont actualisées par un appel au service FD (Famille de droits) de l'inter régime dès lors qu'un changement de situation a été signalé afin de garantir leur exactitude.	N/A

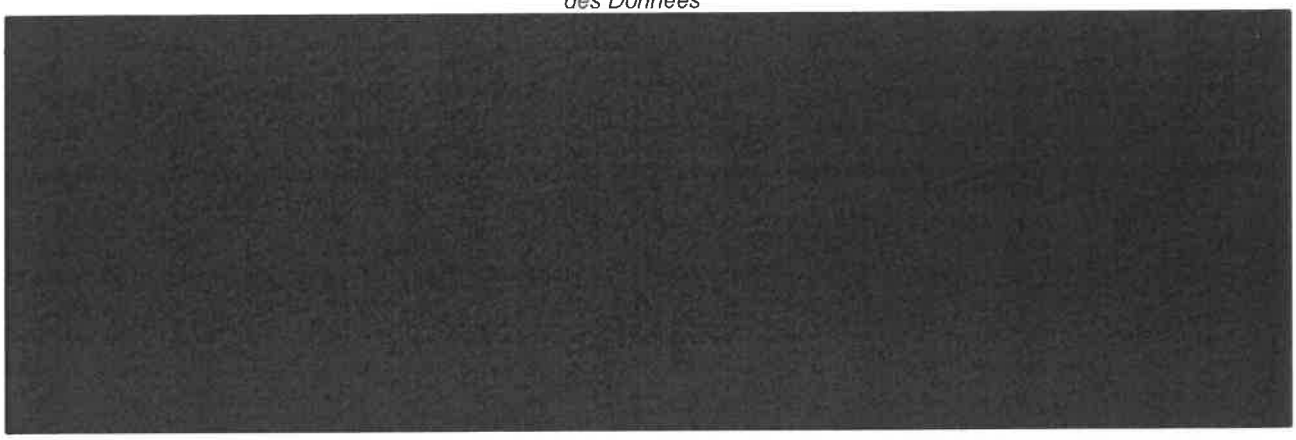
8.1.3.4 Explication et justification des durées de conservation

Les seules données produites sont des traces dont les durées de conservation sont précisées au §5.2.1.4.

8.1.4 Mesures de sécurité

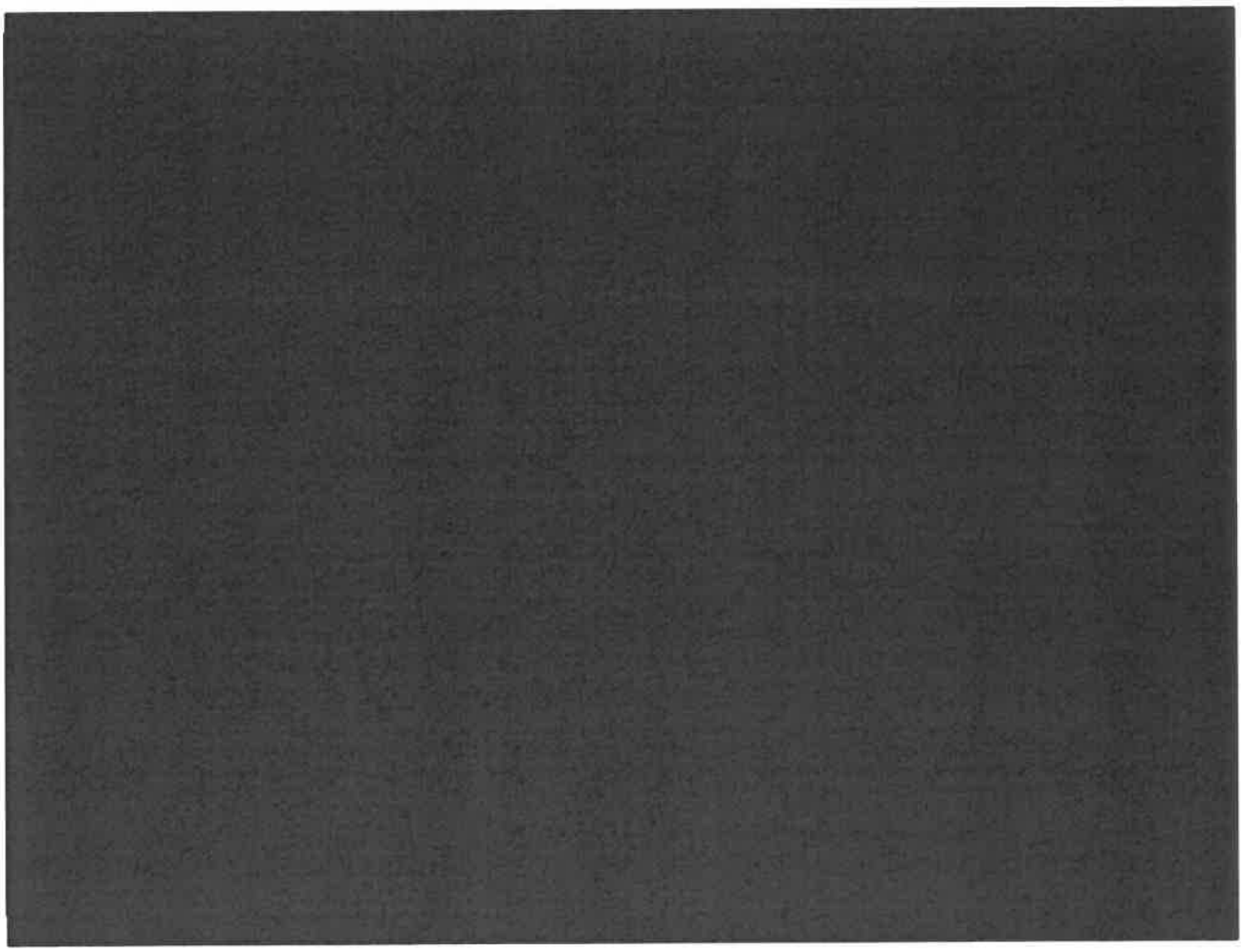


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



8.1.5 Risques

8.1.5.1 Présentation des risques



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

8.1.5.2 Couverture des risques

[redacted]

8.1.5.3 Plan d'action

[redacted]

8.2 Authentification avec CPx

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

9 PROCESSUS SERVICES AUX ASSURES

Dans l'application, l'utilisateur a accès aux services suivants :

- Changement du mot de passe de déverrouillage (cf. 5.1.2.7) ;
- Activation / désactivation de la biométrie (cf. 5.1.2.8) ;
- Modification de l'adresse mail (cf.9.2) ;
- Consultation des résumés de facture (cf. 9.1) ;
- Suppression de son profil (cf. 5.1.2.13).

9.1 Consultation des résumés de facture

9.1.1 Description du processus

L'utilisateur de l'ApCV peut consulter à tout moment ses résumés de factures depuis son ApCV.

Les résumés de facture sont des messages provisionnés dans le SI Sécurité par le SI ApCV. L'ApCV utilise un point d'entrée du SDK Sécurité pour récupérer les nouveaux messages auprès du SI Sécurité et les stocker localement [redacted]

La cinématique est la suivante :

[redacted]

1) Le SI ApCV envoie au fil de l'eau les nouveaux messages au SI Sécurité, [redacted]

Le SI Sécurité chiffre les messages dans l'attente de leur téléchargement par l'ApCV.

2) L'utilisateur déverrouille son ApCV (mot de passe ou biométrie).

[redacted]

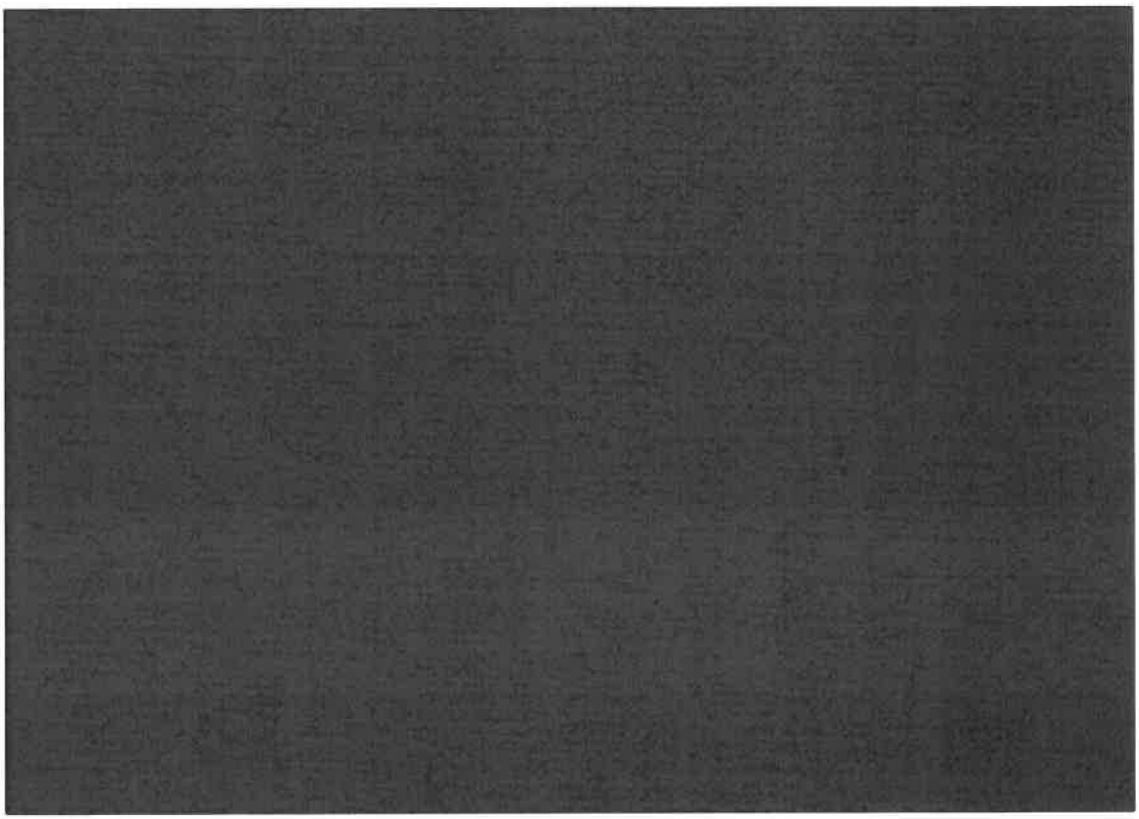
4) Le SI Sécurité envoie les messages au SDK, qui les stocke dans le Secure Storage, permettant ensuite à l'ApCV d'y accéder par un appel au SDK afin de les présenter à l'utilisateur. Chaque résumé de facture contient :
   - L'identification du PS émetteur (identifiant national et identifiant facturation),
   - Le prénom et le nom du PS émetteur,
   - La date de la facture,
   - L'identifiant de la facture,
   - Le montant payé par l'assuré,
   - Le montant facturé par l'émetteur,

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

- Le (ou les) organisme(s) d'Assurance Maladie destinataires de la (ou des) facture(s) : AMO (code régime, code caisse, code centre) et AMC,
- L'identification du bénéficiaire : NIR, prénom et nom du bénéficiaire.

5) Une fois les messages téléchargés par le SDK, le SI Sécurité les supprime immédiatement. Tout message non téléchargé dans le délai défini à la création du message est supprimé à expiration de sa durée maximale de rétention.

9.1.2 Description du circuit de la donnée



9.1.3 Respect des principes fondamentaux

	Consultation des résumés de facture
Finalités du traitement	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Informations complémentaires	Donner la possibilité à l'utilisateur ApCV de consulter un résumé de sa facture
Intervention de sous-traitants ultérieurs	Infogérant du SI ApCV [redacted] Fournisseur du SDK Sécurité et infogérant du SI Sécurité [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

9.1.3.1 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Résumés de facture : Identité du bénéficiaire (NIR, prénom et nom) Identifiant national PS Identifiant facturation PS Prénom et nom PS **Date et montant de la facture (montant total et montant payé par l'assuré)**	DCP sensibles (l'association des données d'identité PS et d'identité bénéficiaire peut donner des indications sur la santé de la personne) DCP perçue comme sensible (NIR) DCP courantes (prénom et nom)	Données métier présentes dans le résumé de facture	Le code acte de la prestation (lettre clé) qui fait partie de la facture n'est pas conservé dans le SI ApCV ni transmis dans le résumé présenté à l'assuré dans l'appli carte Vitale.
UserID	DCP courante	Identifiant de l'utilisateur de l'ApCV dans le SI Sécurité	
Traces de fonctionnement (identifiant national PS, identifiant facturation PS, [redacted], identifiant ApCV, identifiant profil ApCV, NIR pseudonymisé, adresse IP smartphone*)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées. Par ailleurs, pas de conservation de données directement identifiantes.

[redacted]

9.1.3.2 Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification
Les données constituant le résumé de facture sont collectées par le LPS, logiciel faisant l'objet d'une validation par le CNDA.	

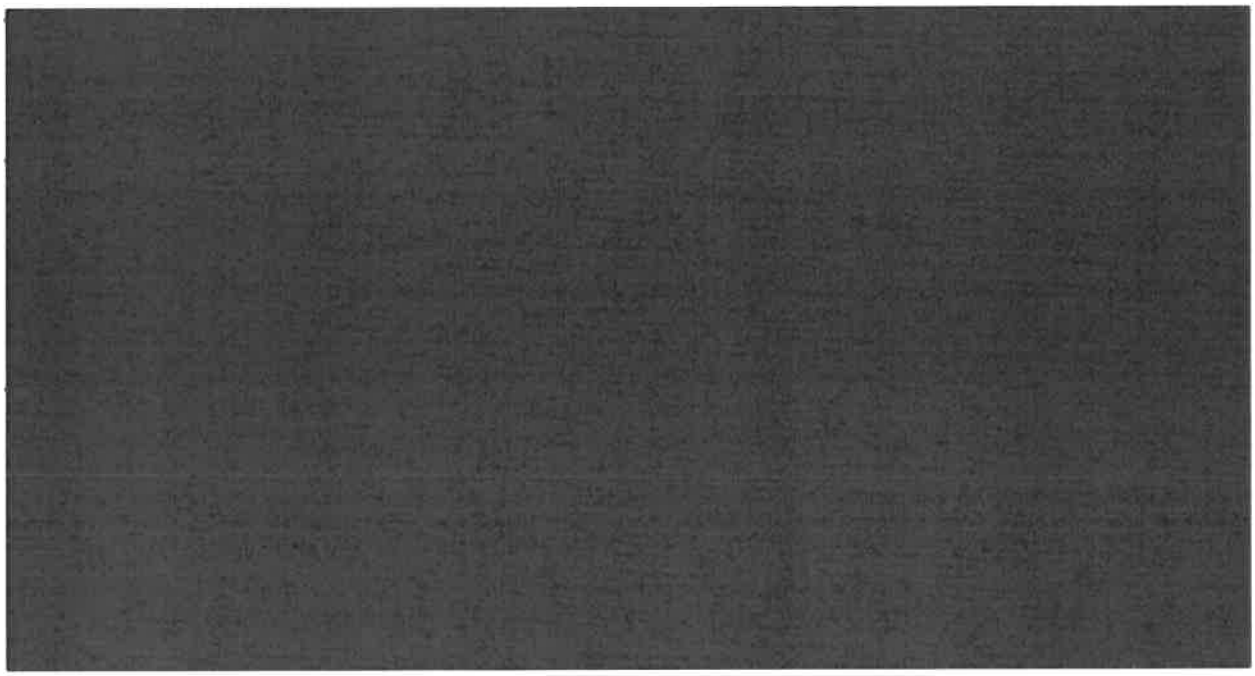
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Les résumés de facture sont stockés en base de données et bénéficient des mécanismes d'intégrité du SGBD.	

9.1.3.3 Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Résumés de facture (Identifiant national PS, identifiant facturation PS, prénom et nom PS, Identité du bénéficiaire (NIR, prénom et nom), date et montant de la facture (montant total et montant payé par l'assuré))	7 jours	Durée de mise à disposition du résumé de facture à l'assuré.	Traitement automatique

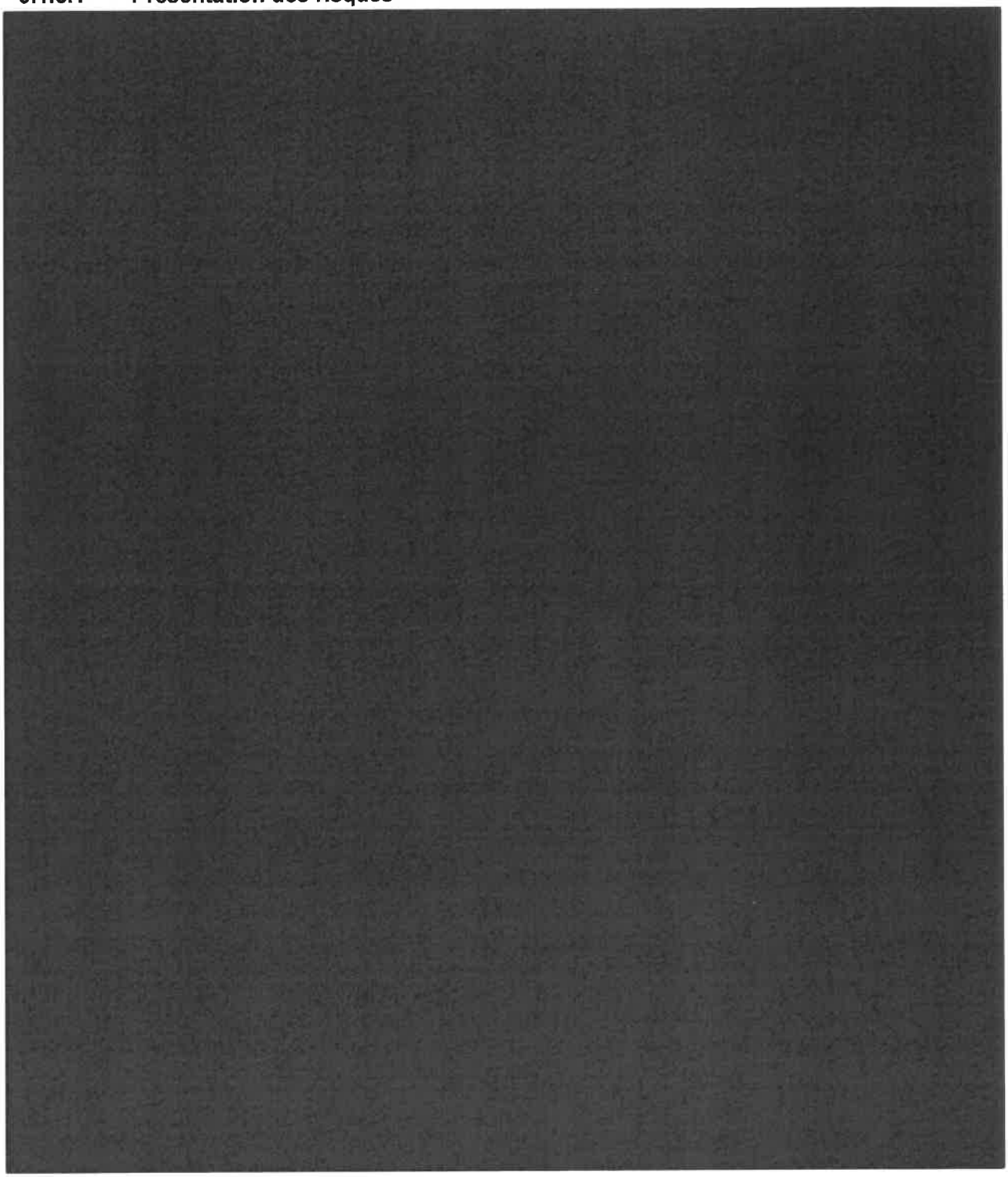
9.1.4 Mesures de sécurité



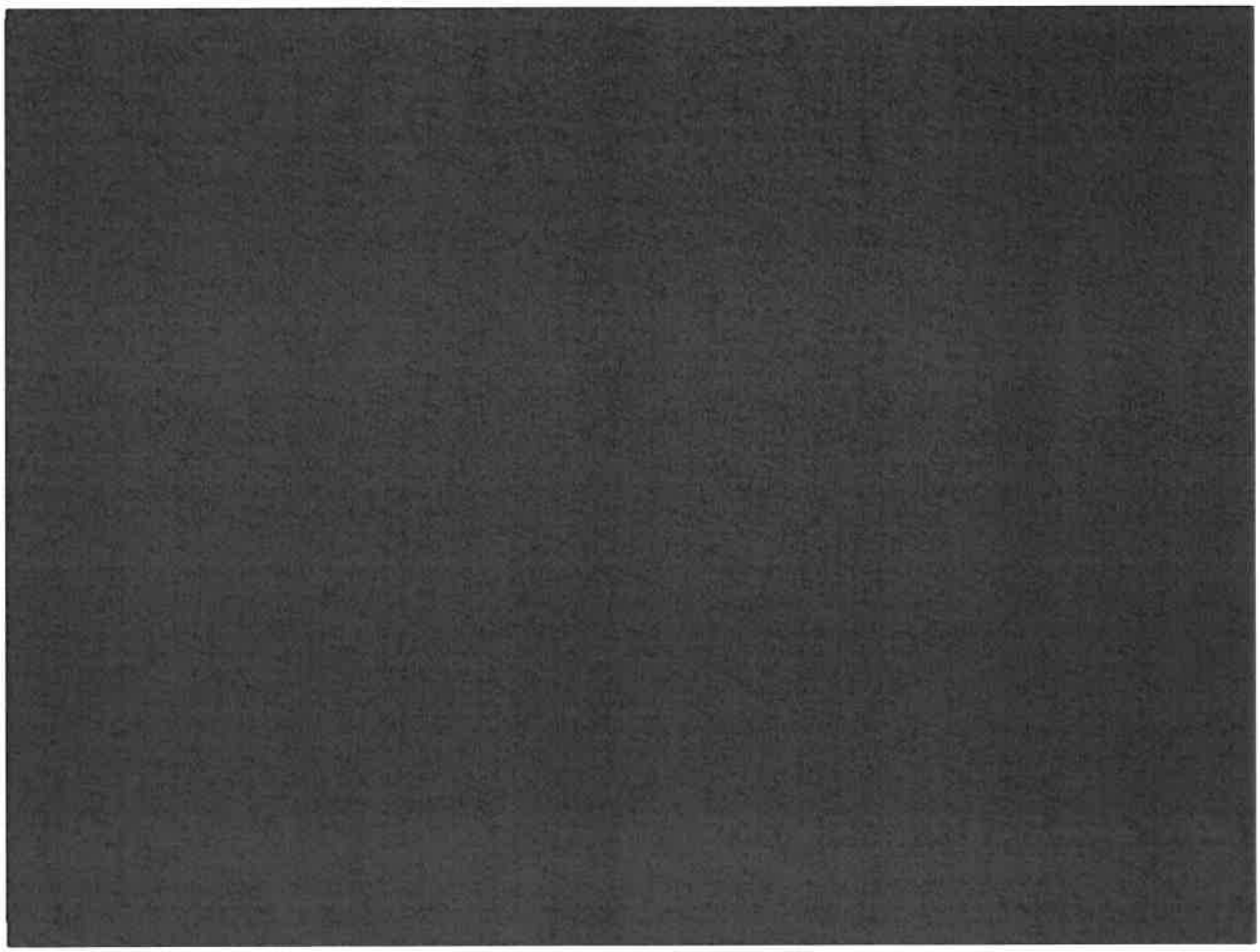
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

9.1.5 Risques

9.1.5.1 Présentation des risques



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

9.1.5.2 Couverture des risques

[redacted]

Tableau 29 : Couverture des risques liés à la consultation des résumés de facture

9.1.5.3 Plan d'action

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

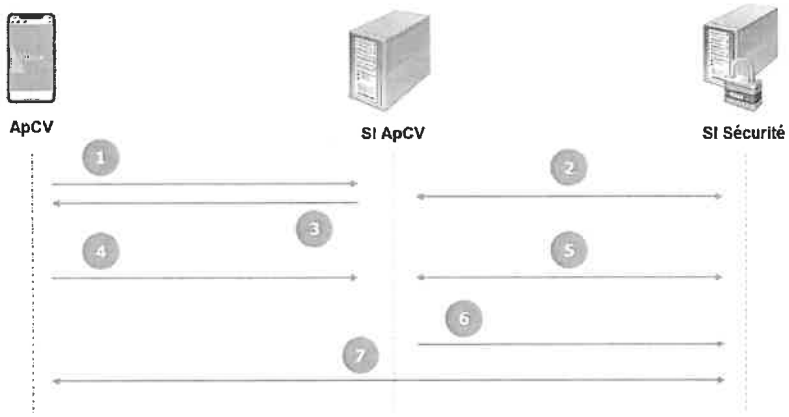
[redacted]

9.2 Changement d'adresse mail

9.2.1 Description du processus

L'utilisateur de l'ApCV peut à tout moment changer son adresse mail depuis son ApCV.

La cinématique est la suivante :



1) L'utilisateur déverrouille son ApCV (mot de passe ou biométrie), puis choisit la fonction de changement d'adresse mail et renseigne sa nouvelle adresse.

[redacted]

3) Le SI ApCV contrôle que le nom de domaine de la nouvelle adresse mail n'est pas blacklisté et envoie un code de vérification à cette nouvelle adresse ;

4) L'utilisateur saisit le code de vérification dans l'ApCV.

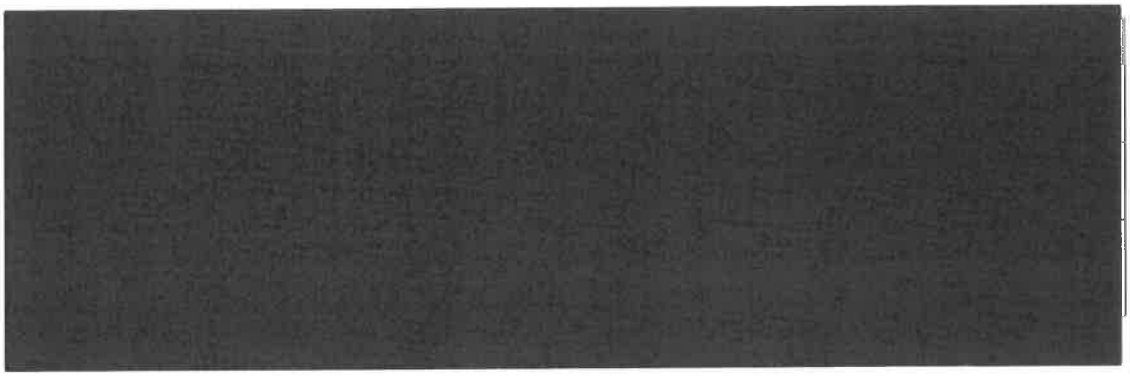
[redacted]

6) Le SI ApCV demande la mise à jour du document COORD avec la nouvelle adresse mail au SI Sécurité :

7) Le SDK récupère le nouveau document COORD auprès du SI Sécurité.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

9.2.2 Description du circuit de la donnée



9.2.3 Respect des principes fondamentaux

	Changement d'adresse mail
Finalités du traitement	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Informations complémentaires	Donner la possibilité à l'utilisateur de modifier l'adresse mail enregistrée dans son ApCV
Intervention de sous-traitants ultérieurs	Infogérant du SI ApCV [redacted] Fournisseur du SDK Sécurité et infogérant du SI Sécurité [redacted]

9.2.3.1 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Adresse mail	DCP courante	Nouvelle adresse mail à inscrire dans l'ApCV	
UserID	DCP courante	Identifiant de l'utilisateur de l'ApCV dans le SI Sécurité	
Traces de fonctionnement [redacted] identifiant ApCV, identifiant profil ApCV, adresse IP smartphone)	DCP courantes	Données nécessaires à la supervision, au diagnostic du système, à la lutte contre la fraude et au calcul des indicateurs décisionnels.	Seules les données nécessaires sont conservées. Par ailleurs, pas de conservation de données directement identifiantes.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

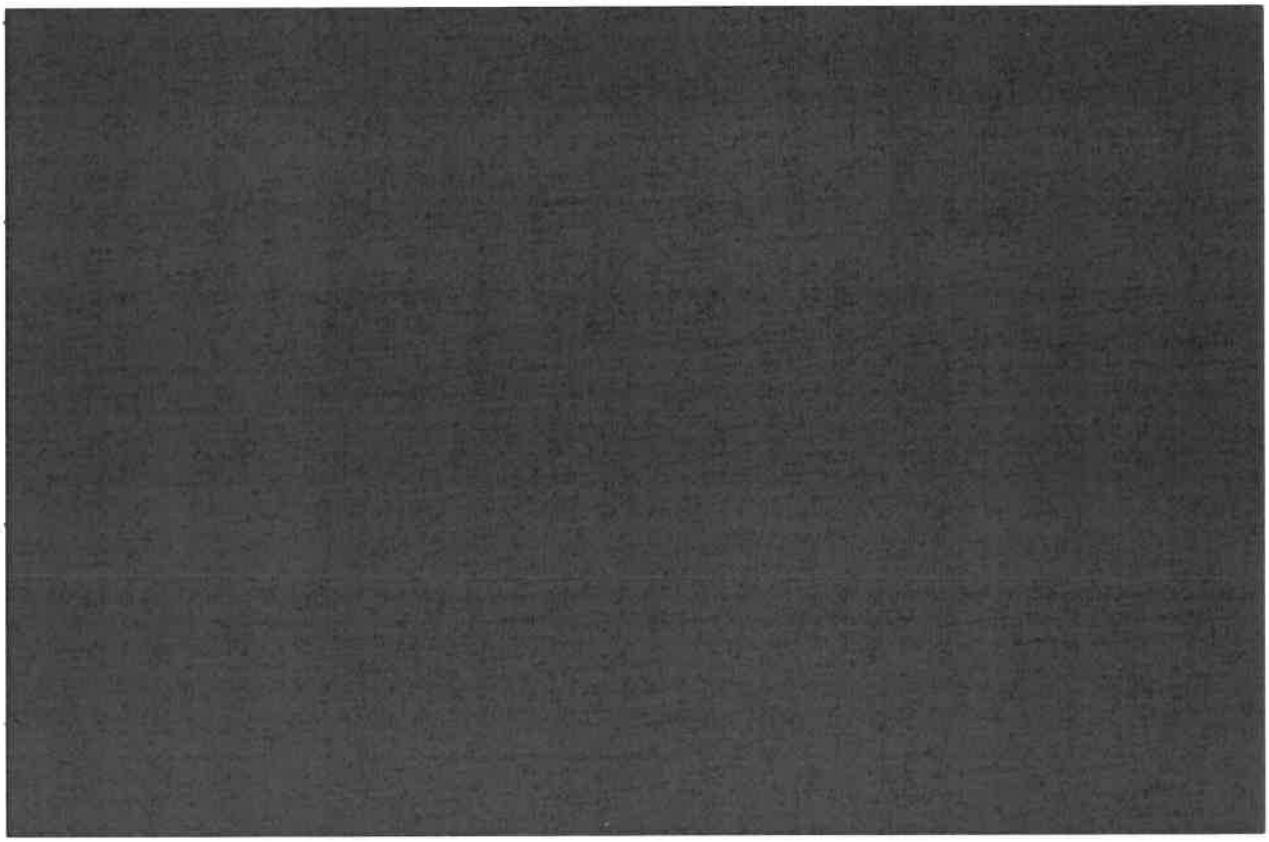
9.2.3.2 Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification
L'adresse mail est stockée dans un document signé par le SI Sécurité	

9.2.3.3 Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Adresse mail	7 jours	Durée de mise à disposition du nouveau document COORD par le SI Sécurité.	Traitement automatique de suppression si le document du SI Sécurité n'a pas été téléchargé par le SDK de l'ApCV dans le délai prévu.

9.2.4 Mesures de sécurité



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

10 PROCESSUS TRANSVERSES

10.1 Décisionnel

10.1.1 Objectifs et solutions mises en œuvre

La cible du SI Décisionnel est de permettre la consolidation dans un entrepôt de données des traces de fonctionnement des sous-systèmes du SI ApCV et l'historisation du contenu de la base des ApCV actives, avec pour objectif de réaliser :

- Le suivi du parc des ApCV ;
- Le suivi des usages.

La solution initialement envisagée, présentée dans les versions précédentes de l'AIPD et dénommée dans la suite du document « SID ApCV », était basée exclusivement sur la mise en œuvre d'un SI Décisionnel composé d'un Datawarehouse, d'un Datamart et d'une plateforme de restitution [redacted].

Afin d'offrir rapidement de la visibilité et des informations de pilotage après la mise en production de nouvelles fonctionnalités de l'ApCV, certains indicateurs sont actuellement produits directement à partir de tableaux de bord construits dans [redacted]. Dans cet [redacted], contrairement à ce qui est réalisé lors de l'importation dans le SID, la désensibilisation des données n'est pas réalisée, car cela ne permettrait plus de réaliser les actions de support et de supervision.

Il a donc été décidé de mettre en œuvre un [redacted] dédié aux usages décisionnels, dénommé dans la suite du document « [redacted] » permettant à la fois de répondre au besoin d'agilité du décisionnel tout en appliquant les mêmes règles de désensibilisation que dans le SID ApCV. Tout comme le SID ApCV, [redacted] est hébergé [redacted].

10.1.2 Tableaux de bord

A titre d'exemple (liste non exhaustive), les tableaux de bord suivants pourront être produits :

- Suivi du parc des ApCV :
  - Suivi du nombre d'ApCV par Organisme et par état dans le temps ;
- Suivi des acteurs :
  - Suivi du nombre d'utilisateurs distincts ;
  - Suivi du nombre de PS distincts (équipé, utilisateur) ;
  - Suivi du nombre d'agents caisse distincts ;
  - Suivi du nombre de fournisseurs de services PS (amelipro, DMP-PS).
- Suivi des usages :
  - Suivi du nombre et des délais d'activation (OK, NOK, rejet) ;
  - Suivi de la qualité de service de l'Industriel de Vérification d'Identité ;
  - Suivi détaillé (nombre et délais) de l'activation (nb de saisies du NIR, nb de saisie de l'email, selfie, validation des pièces d'identité...) ;
  - Suivi de la qualité et de la performance des flux (OK, erreur) ;
  - Suivi du nombre et des délais de sollicitation du portail de gestion du support ;
  - Suivi du nombre et des délais de mises à jour ApCV ;
  - Croisement avec le SID-S2F sur le numéro de facturation du PS.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

10.1.3 Description du processus

Le processus décisionnel est décrit ci-après :

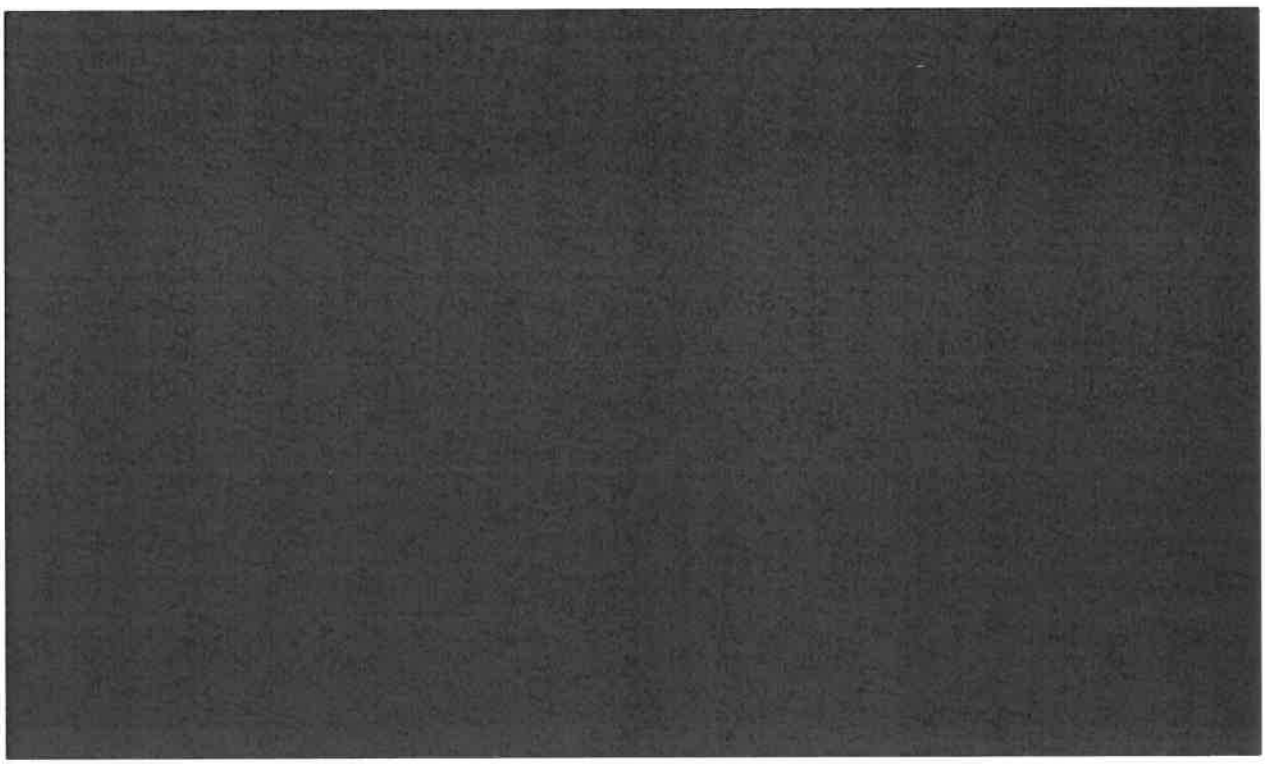
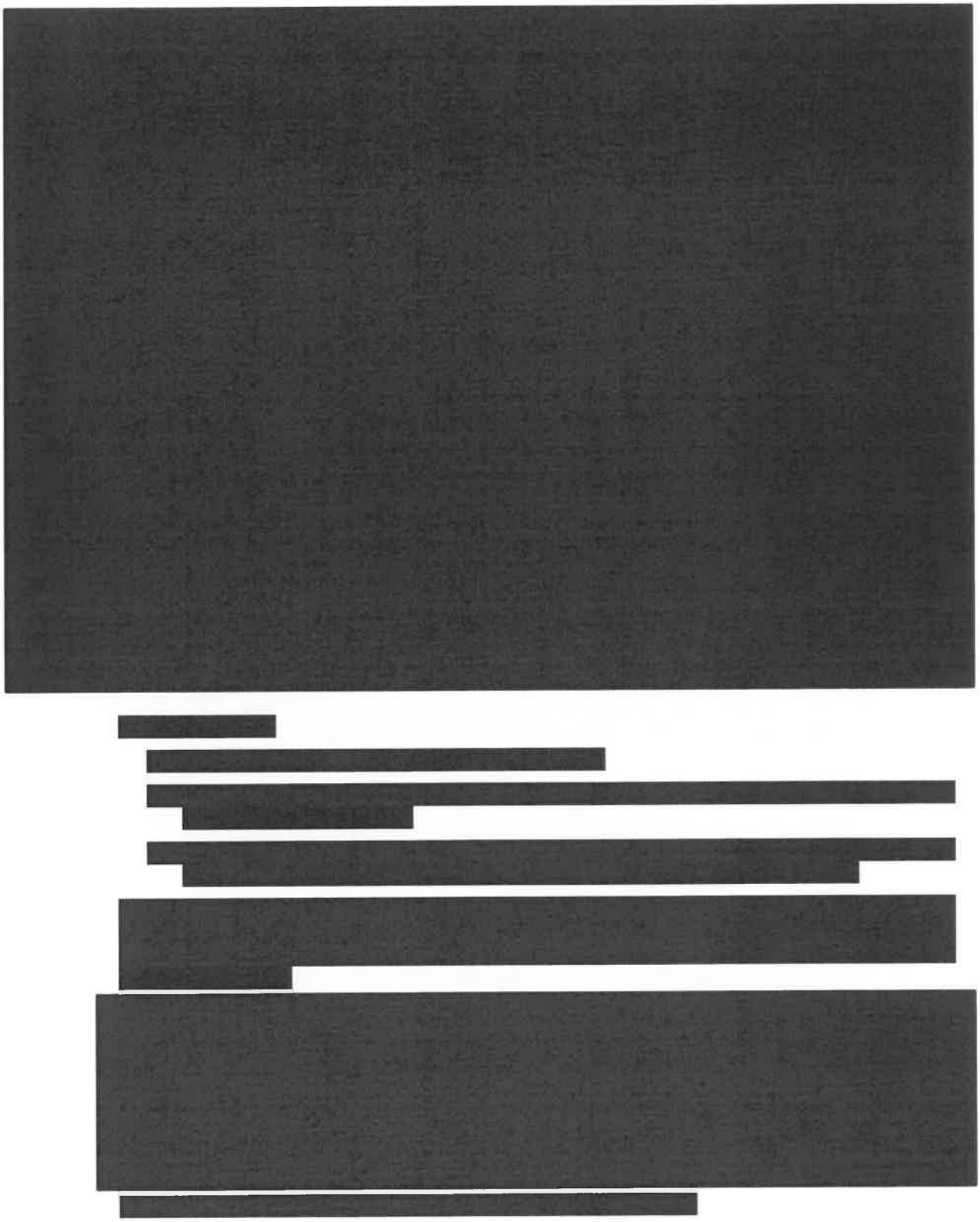


Figure 17 : Processus décisionnel

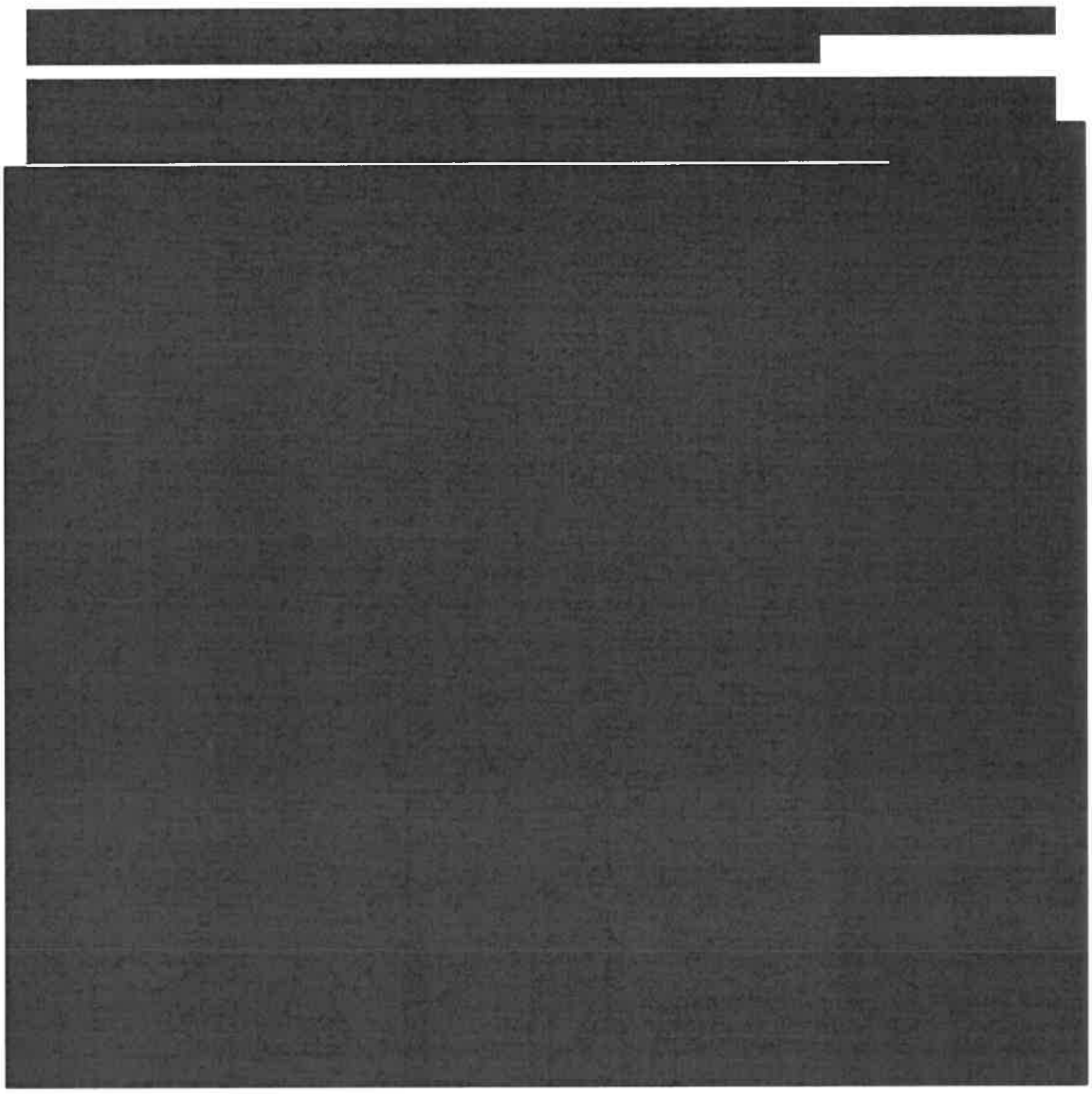
1. Chaque sous-système du SI ApCV alimente ses bases de données et produit des traces de fonctionnement à destination [redacted]
2. Le [redacted] d'extraction constitue les fichiers contenant les données de la veille nécessaires à l'alimentation du SID ApCV et [redacted]
4. Le [redacted] d'alimentation intègre les données dans le datawarehouse du SID ApCV. En parallèle, les données sont également intégrées dans l'infrastructure [redacted].
5. Un [redacted] calcule les indicateurs statistiques à partir des données du [redacted] ApCV et stocke le résultat dans le DMT SID ApCV.
6. [redacted] est la plateforme décisionnelle qui permet de créer des rapports et de visualiser des données du SID ApCV. [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

10.1.4 Description du circuit de la donnée



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



10.1.5 Respect des principes fondamentaux

10.1.5.1 Caractéristiques du traitement

	Décisionnel
Finalités du traitement	Gérer et mettre en œuvre une application permettant aux bénéficiaires comme aux professionnels de santé de disposer, a minima, des mêmes services qu'avec une carte physique
Sous-finalité	Piloter et évaluer quantitativement et qualitativement le déploiement de l'appli carte Vitale et le fonctionnement des services associés

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

Intervention de sous-traitants ultérieurs	Infogérant [redacted] Société titulaire marchés d'AT décisionnel et Réalisation logicielle

10.1.5.2 Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Identifiant ApCV Identifiant profil ApCV	DCP courante	Suivre l'évolution du nombre d'ApCV déployées	Aucune
[redacted]			
Contrat AMO (code régime, caisse, centre)	DCP courante	Suivre l'évolution du nombre d'ApCV déployées par AMO	Aucune
Smartphone (fabricant, modèle, OS et version)	DCP courante	Connaitre le modèle de smartphone pour savoir sur quel smartphone est installée l'ApCV et suivre le fonctionnement de cette dernière	Aucune
Année de naissance	DCP courante	Suivre l'installation de l'ApCV en fonction de l'âge des assurés et éventuellement repérer des tranches d'âge rencontrant des difficultés à l'installation ou utilisation de l'ApCV pour mettre en place des actions d'accompagnement adaptées pour cette population	Aucune
Identifiant national PS (RPPS, ADELI) Identifiant facturation PS (numéro Assurance Maladie)	DCP courante	Besoin fonctionnel en cours de définition (ex : suivi du nombre d'applications distinctes ayant réalisé au moins une authentification chez un professionnel de santé)	Aucune

10.1.5.3 Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification
L'intégrité technique des données est assurée par le SGBD du SID ApCV. Les utilisateurs du SID ApCV et de l'ELK Décisionnel accèdent aux données en lecture seule et avec une authentification forte.	

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

10.1.5.4 Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Identifiant ApCV Identifiant profil ApCV Contrat AMO [redacted] Smartphone (fabricant, modèle, OS et version) Année de naissance Identifiant national PS (RPPS, ADELI) Identifiant facturation PS (numéro Assurance Maladie)	5 ans	Besoin de suivre l'évolution des services ApCV dans le temps pour s'assurer de la conformité de la montée en charge (qui sera progressive sur environ 4 ans), détecter une dégradation de la qualité de service. Cette durée correspond par ailleurs à la durée de vie maximale d'un MIE eIDAS substantiel.	Traitement automatique de suppression

10.1.6 Présentation du SI Décisionnel

10.1.6.1 Hébergement du SID ApCV et [redacted]

Le SID ApCV [redacted] sont hébergés au sein [redacted]

10.1.6.2 Architecture du SID ApCV

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

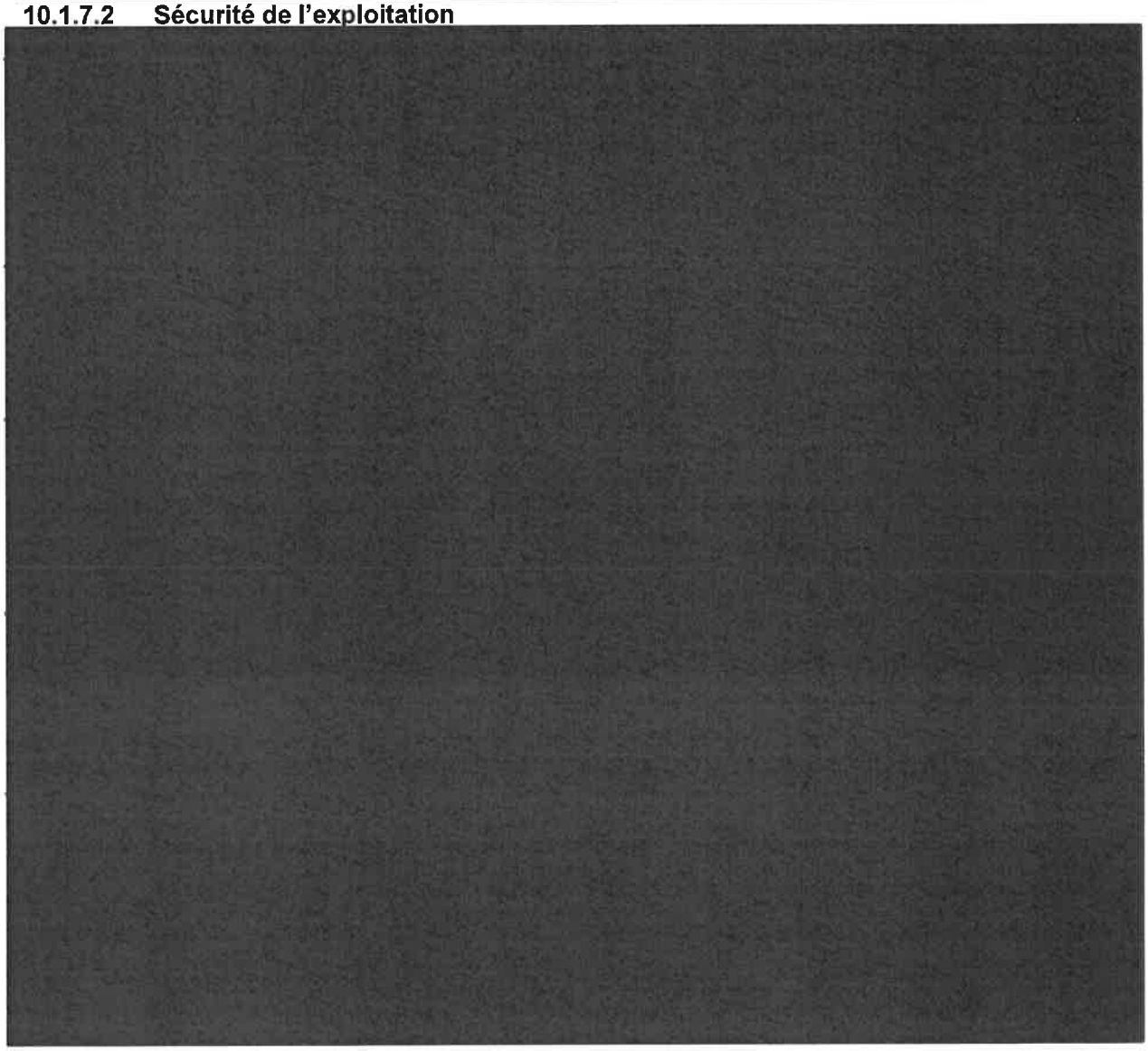
10.1.7 Mesures de sécurité

10.1.7.1 Sécurité de l'infrastructure [redacted]

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

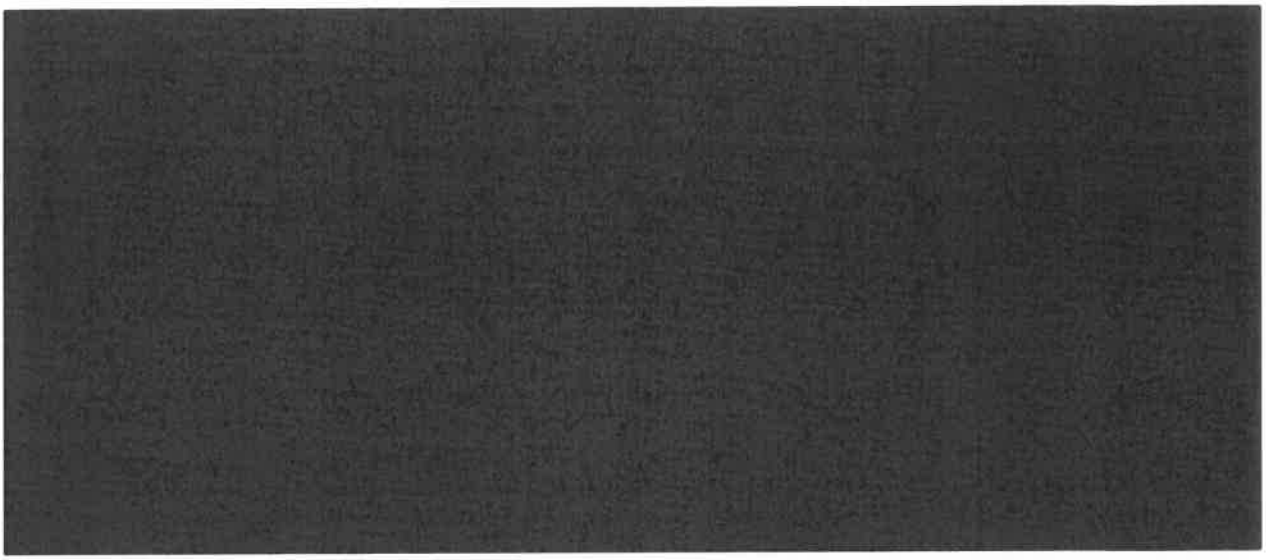
10.1.7.2 Sécurité de l'exploitation



10.1.7.3 Audit et contrôles

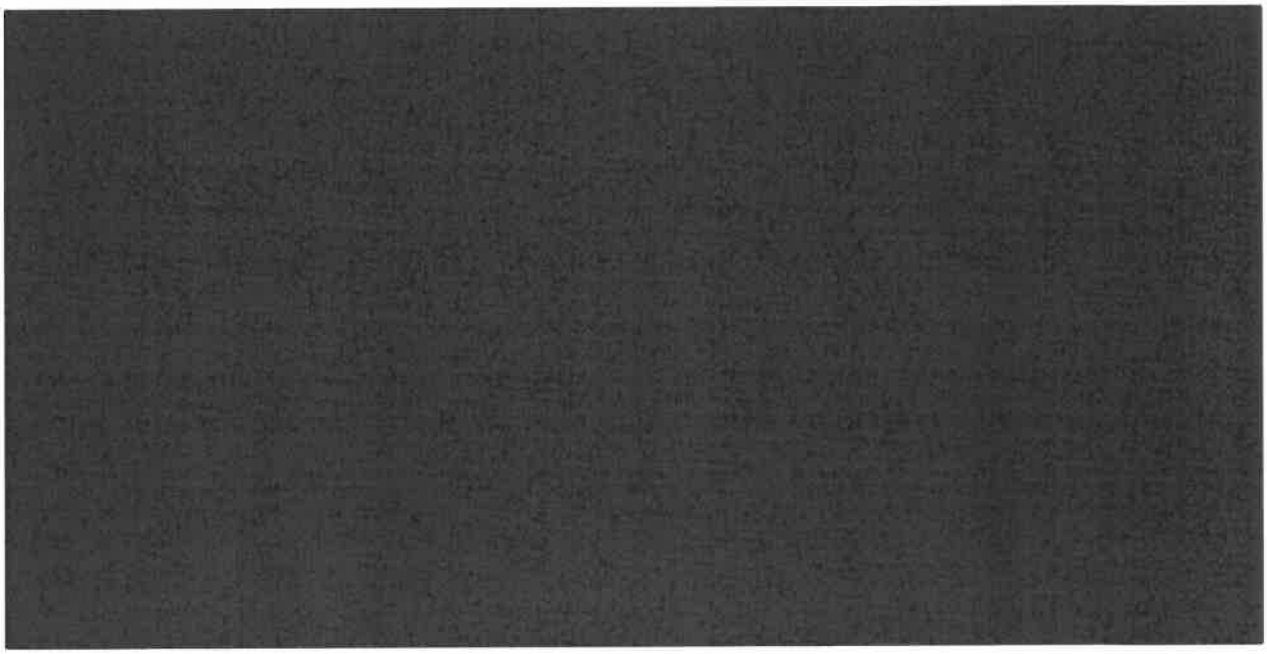
10.1.7.4 Synthèse des mesures de sécurité

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

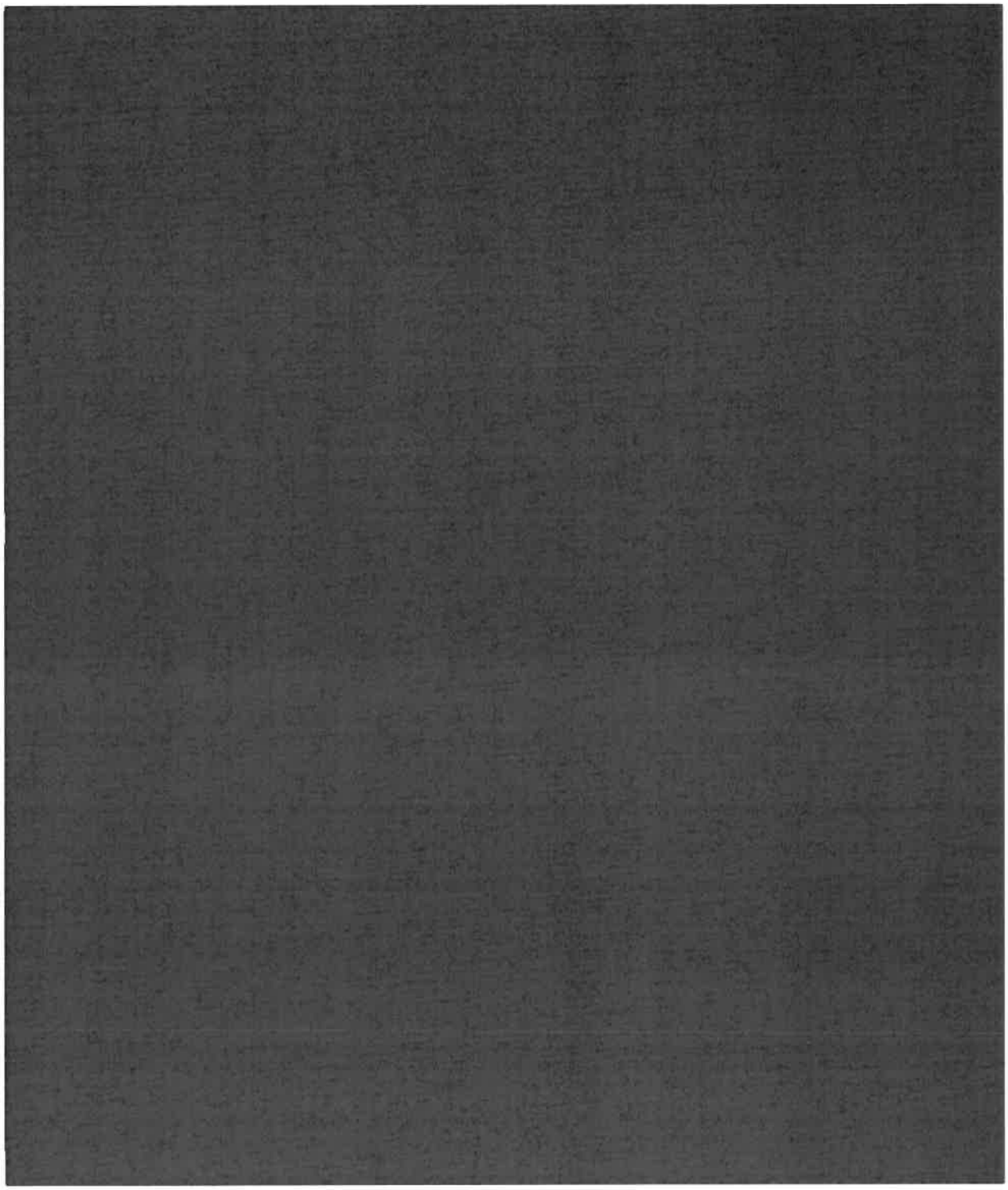


10.1.8 Risques

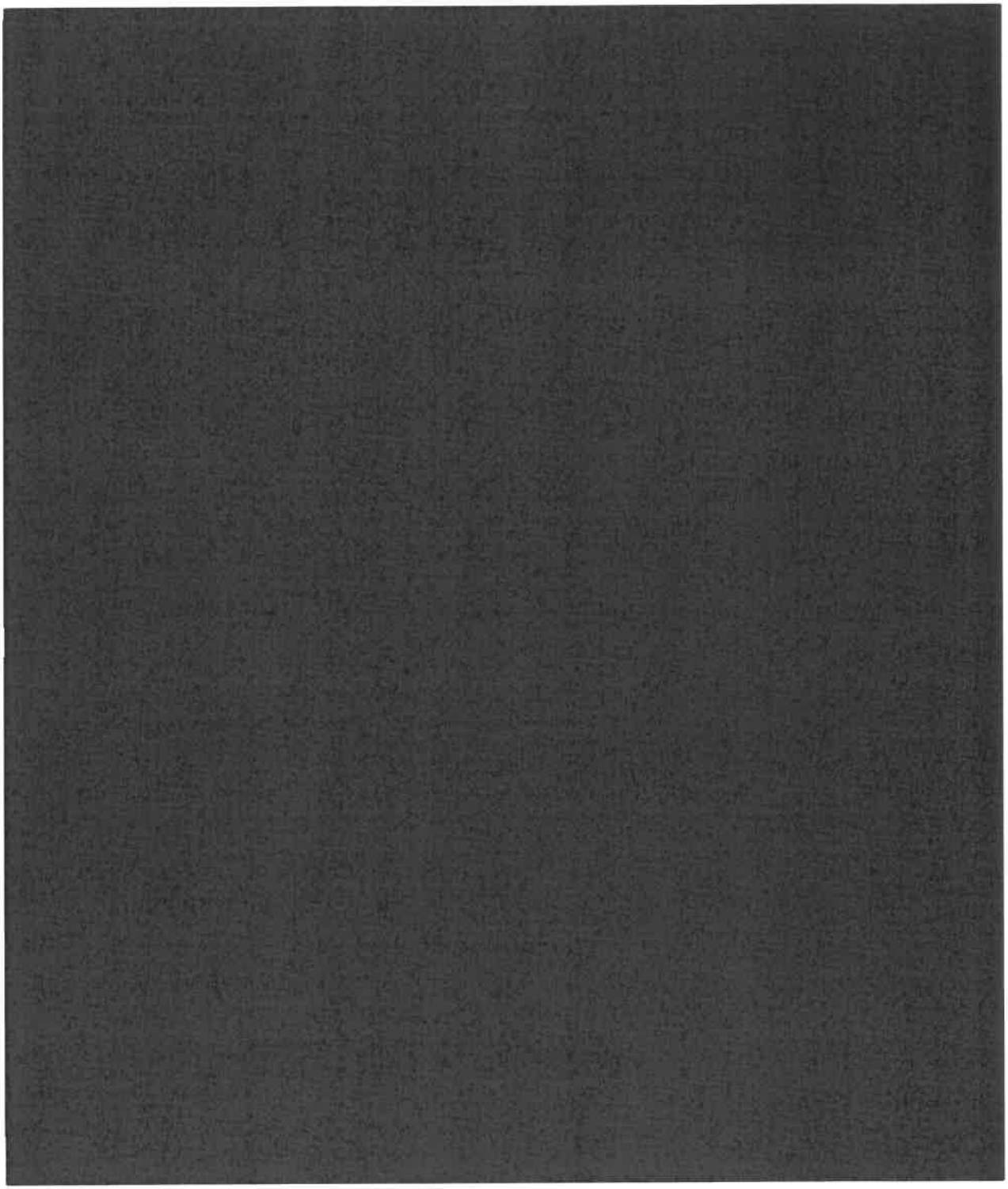
10.1.8.1 Présentation des risques



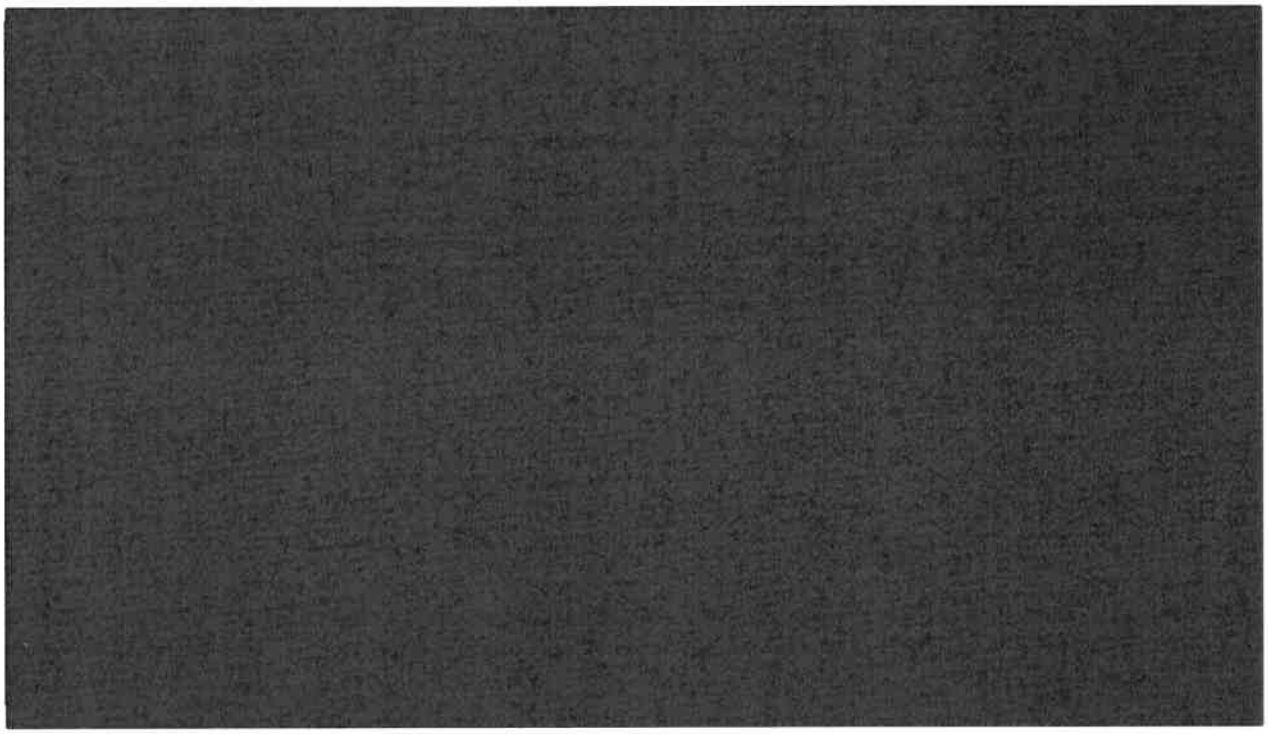
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



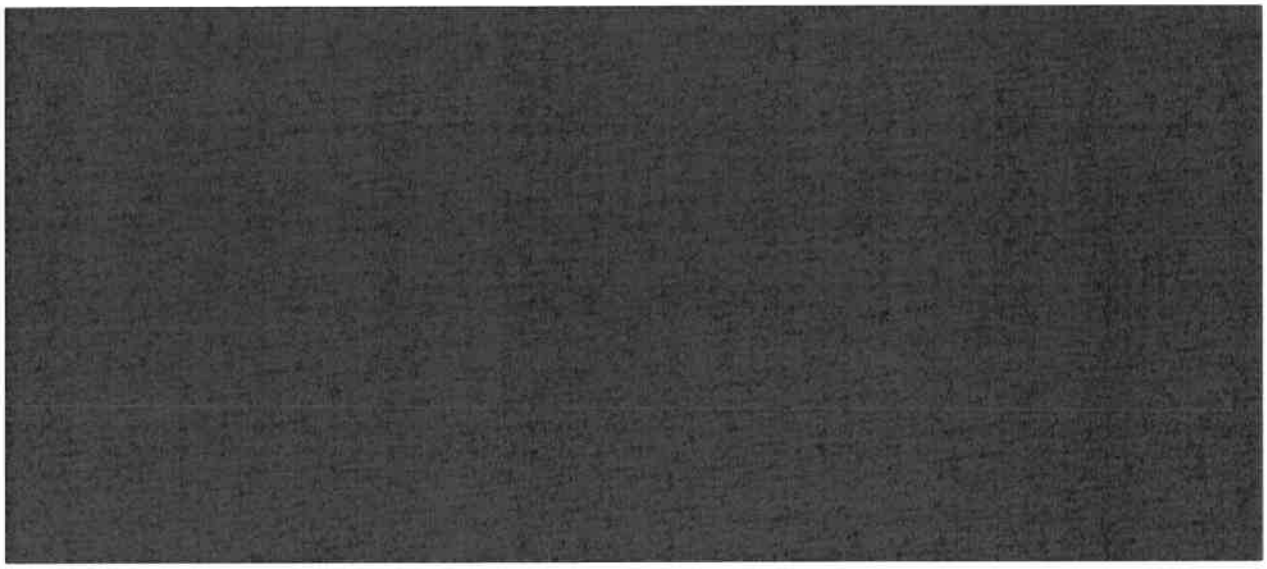
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

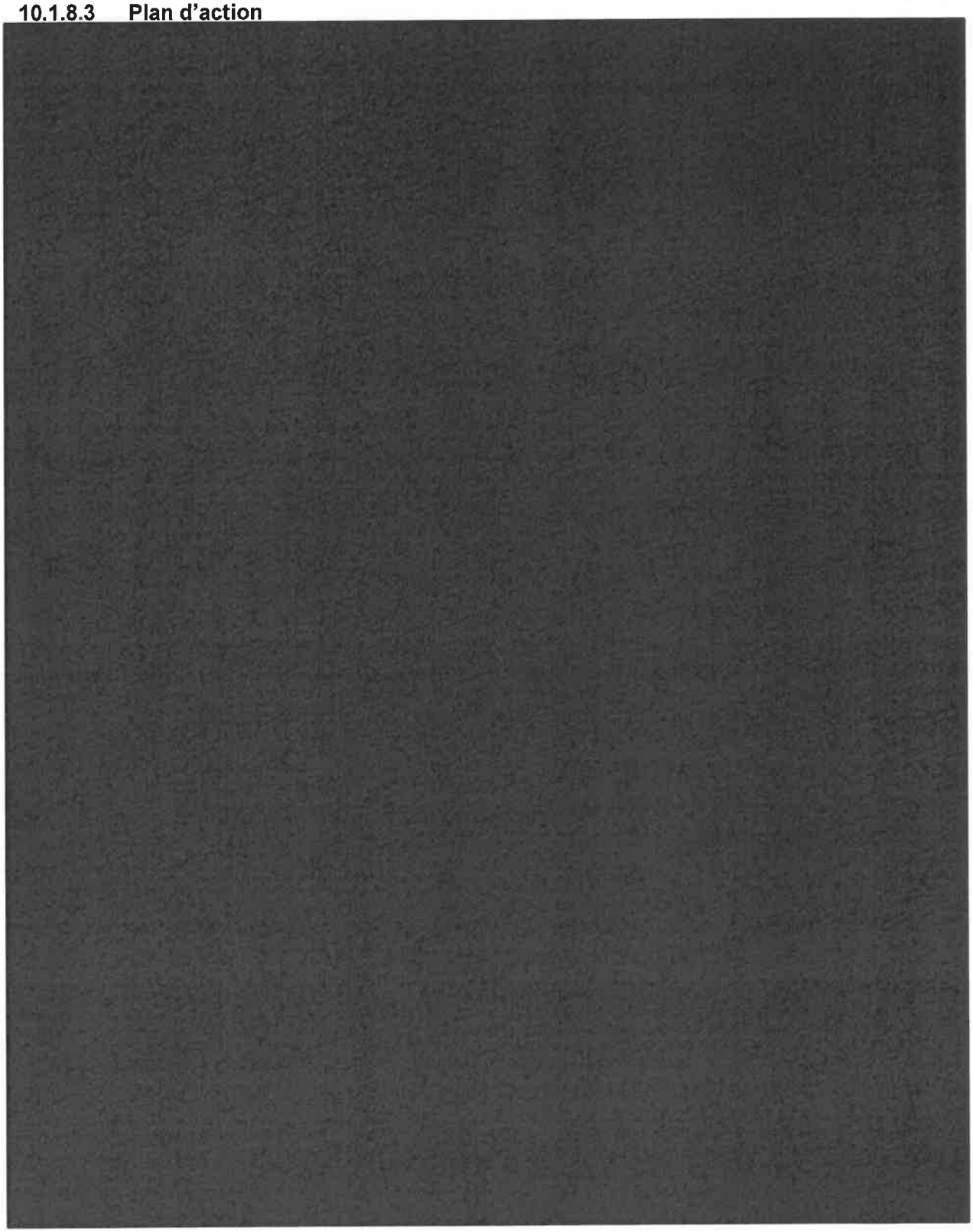


10.1.8.2 Couverture des risques

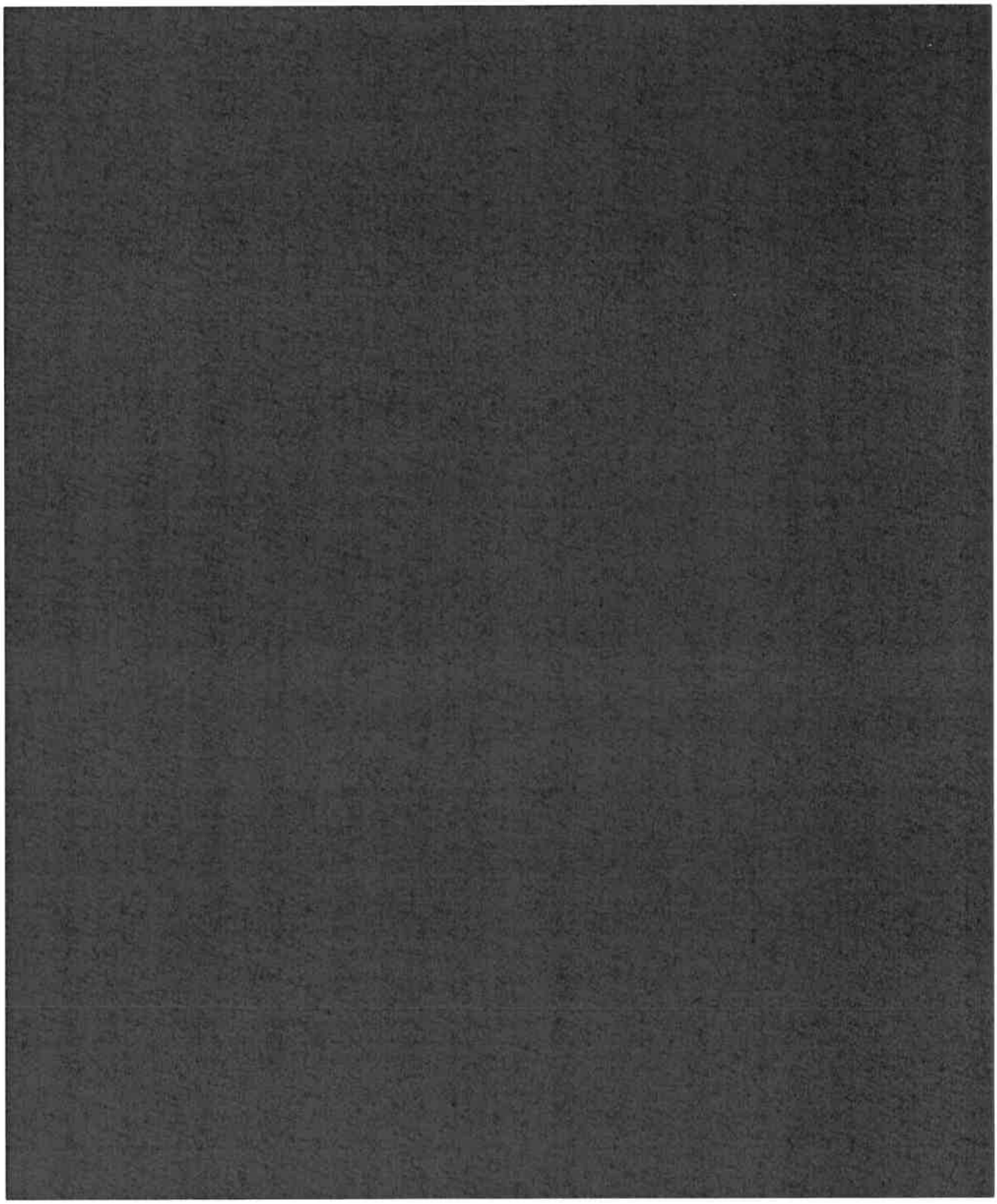


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

10.1.8.3 Plan d'action



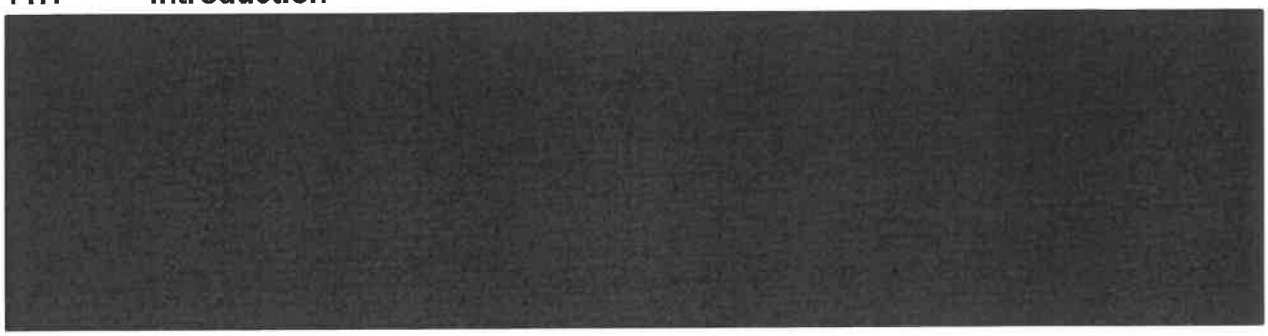
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

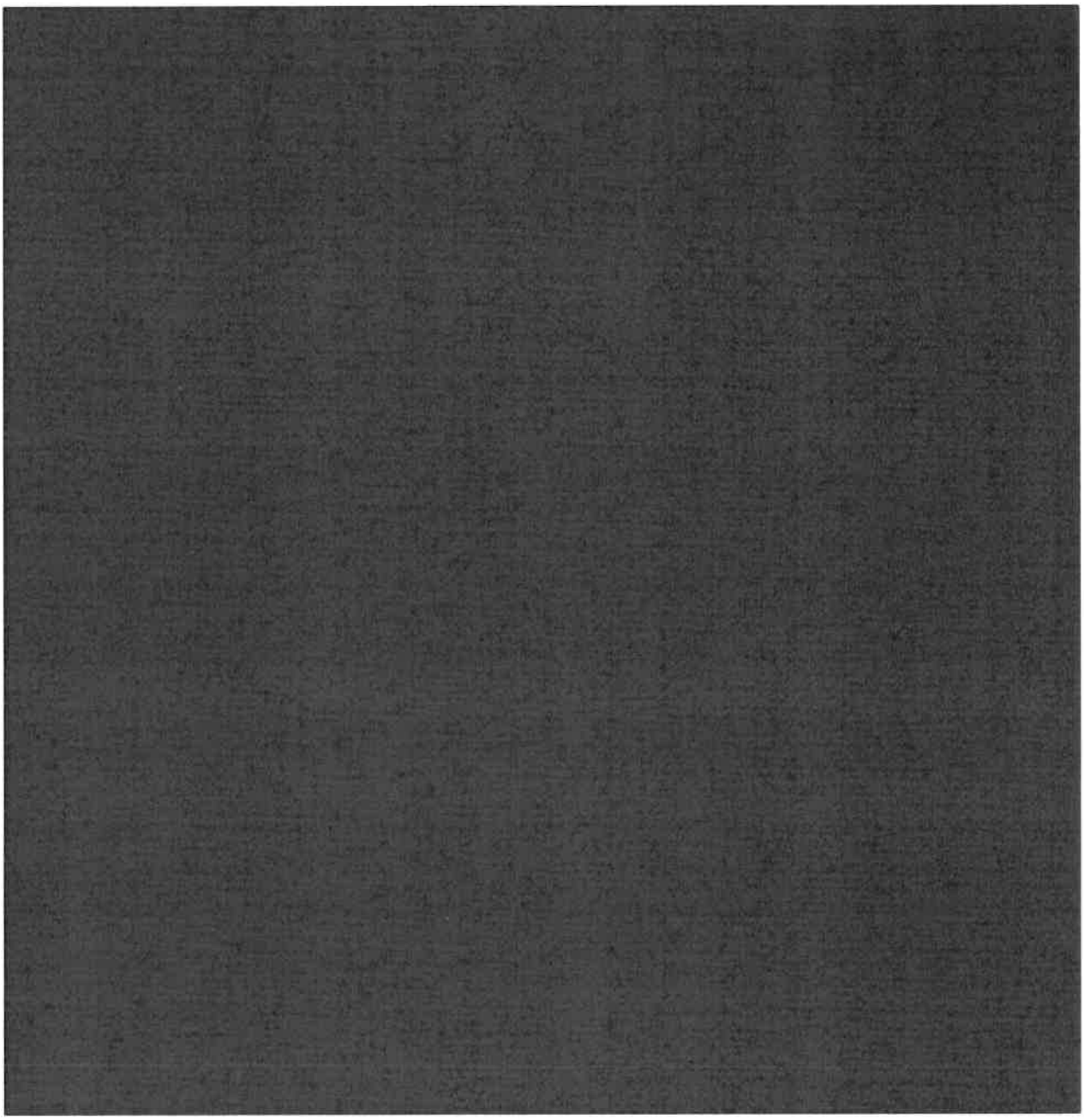
11 CONSOLIDATION / VISION GLOBALE

11.1 Introduction



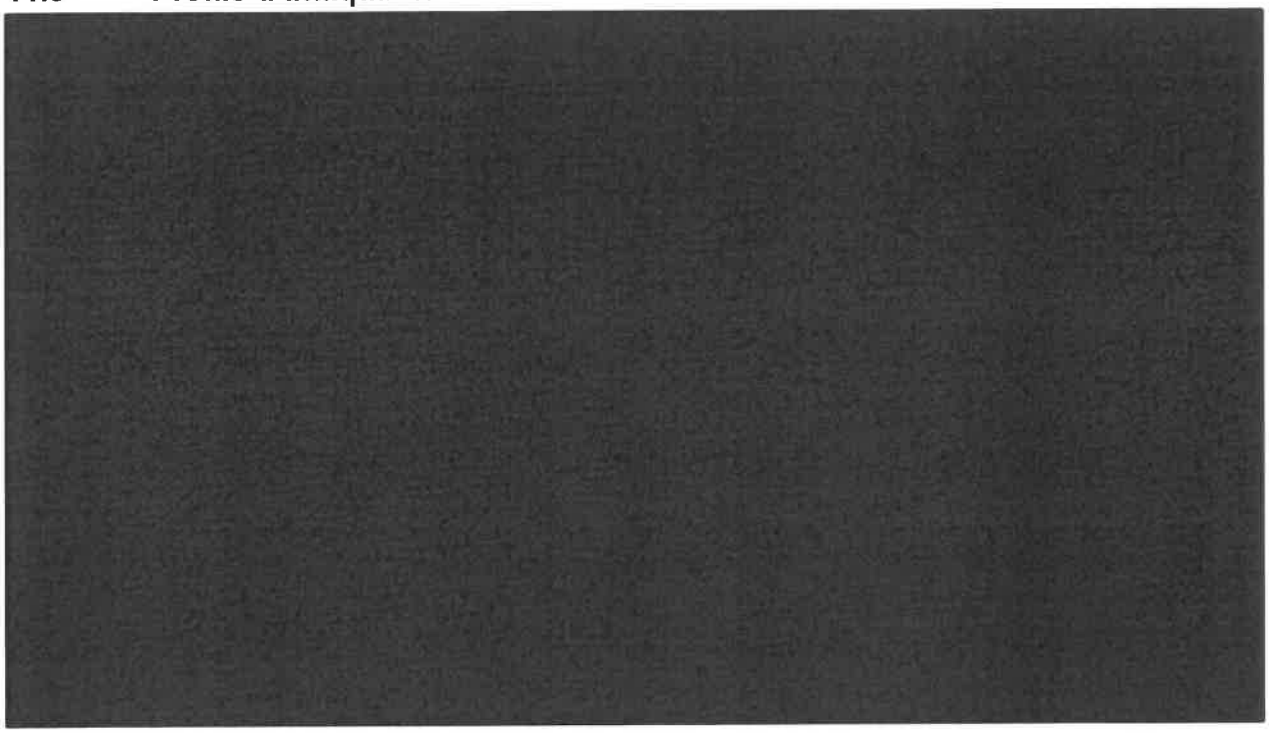
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

11.2 Identification des DCP traitées

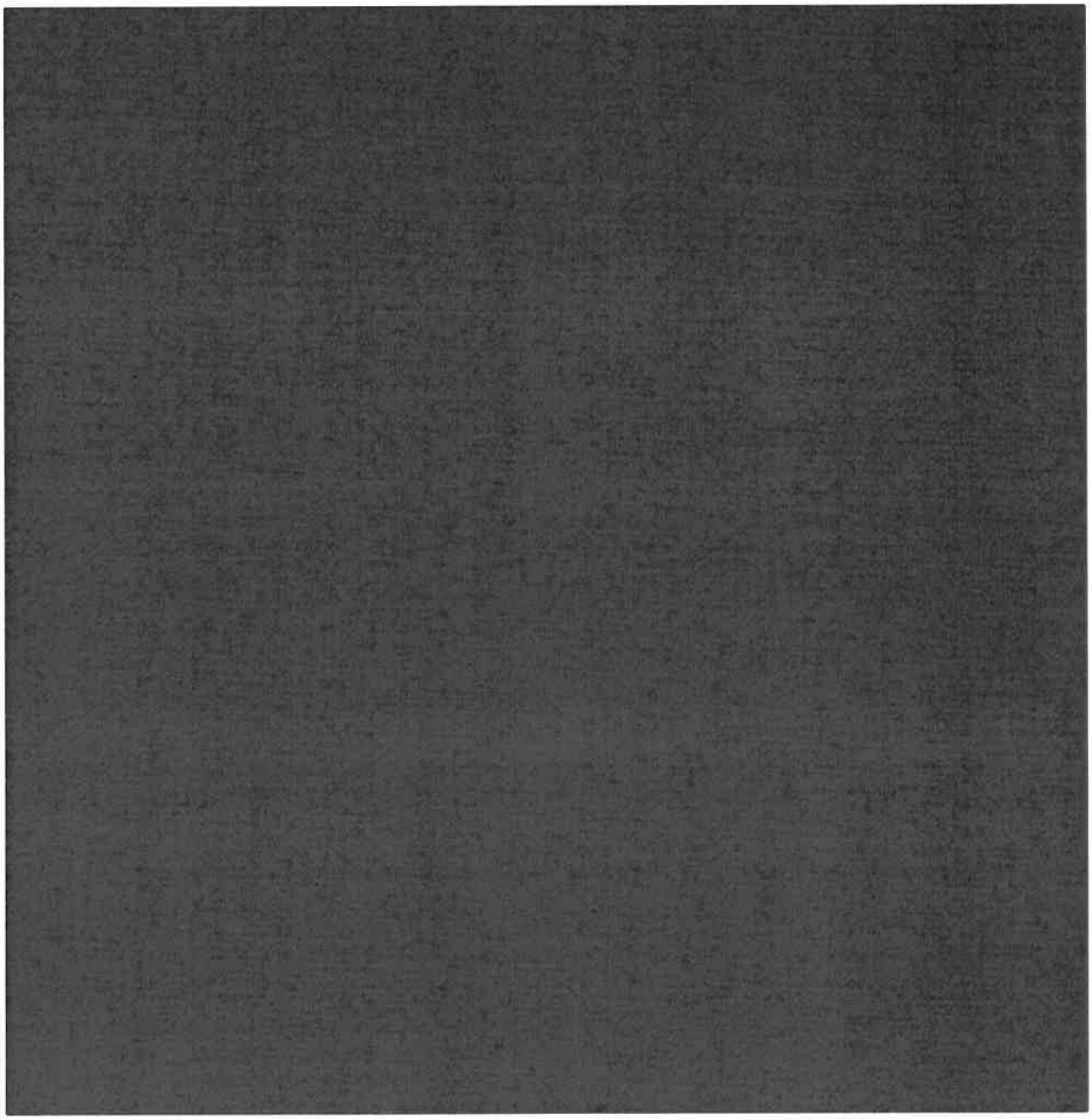


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

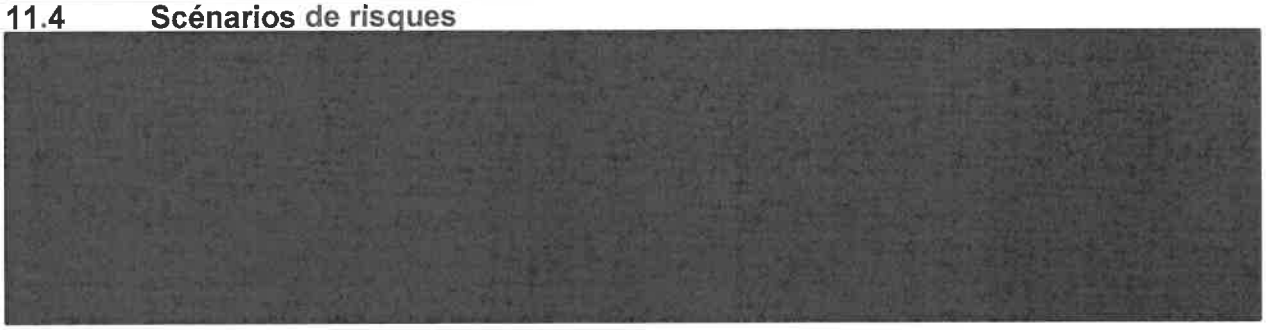
11.3 Profils d'attaquants



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



11.4 Scénarios de risques



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

11.4.1

[redacted]

11.4.2

[redacted]

11.4.3

[redacted]

11.4.4

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

11.4.5 [redacted]

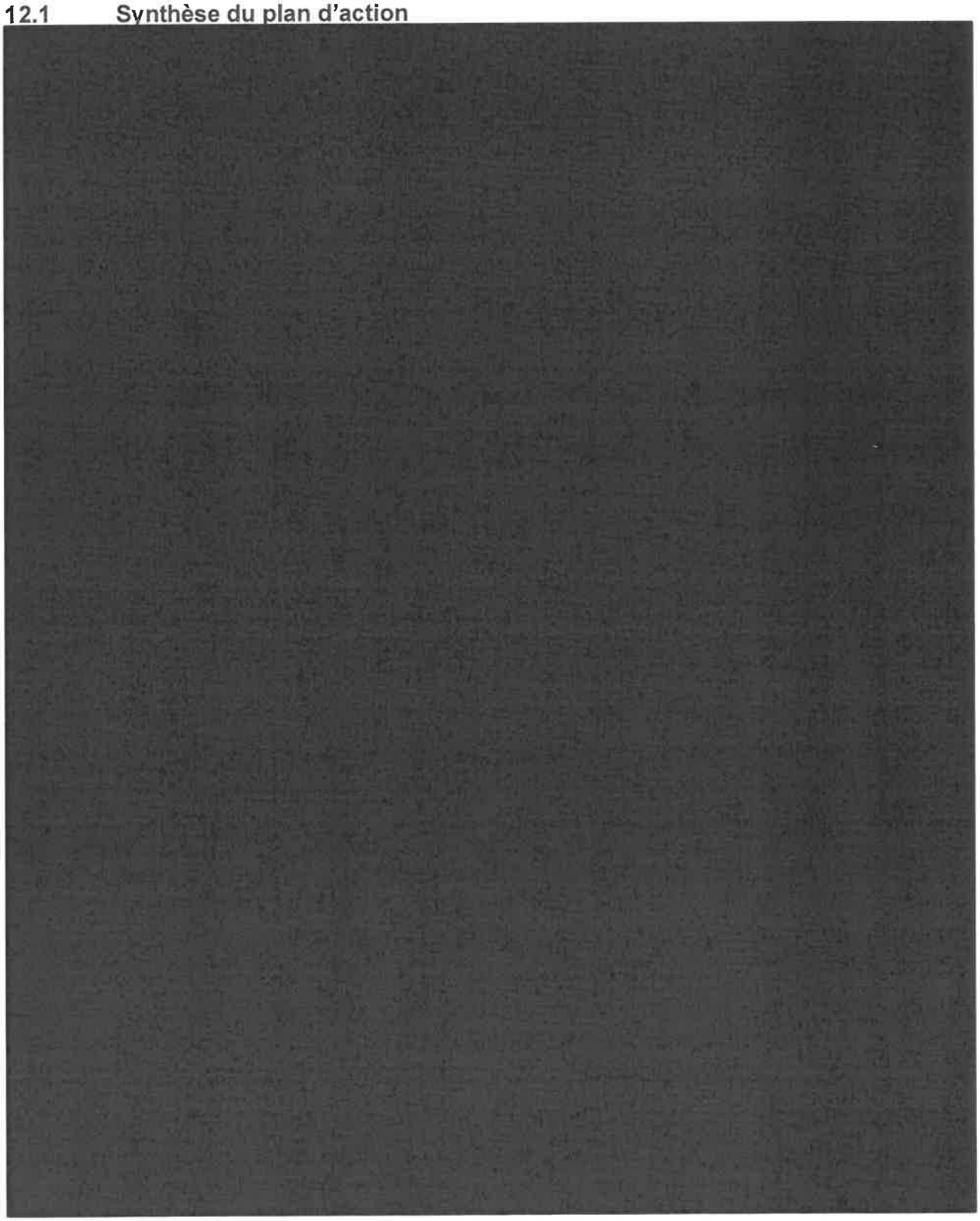
11.4.6 Matrice attaquants / risques

[redacted]

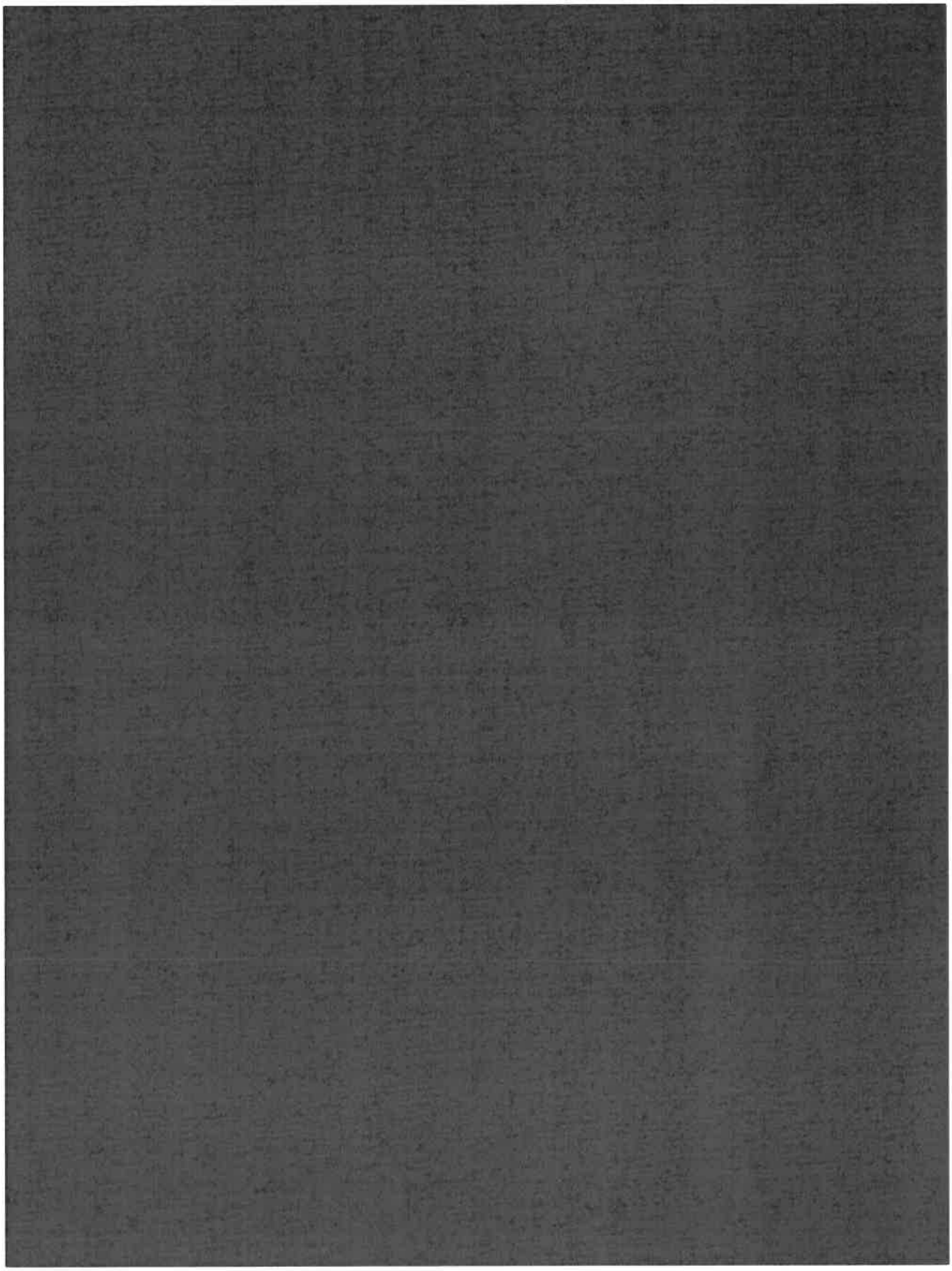
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

12 VALIDATION DE L'AIPD

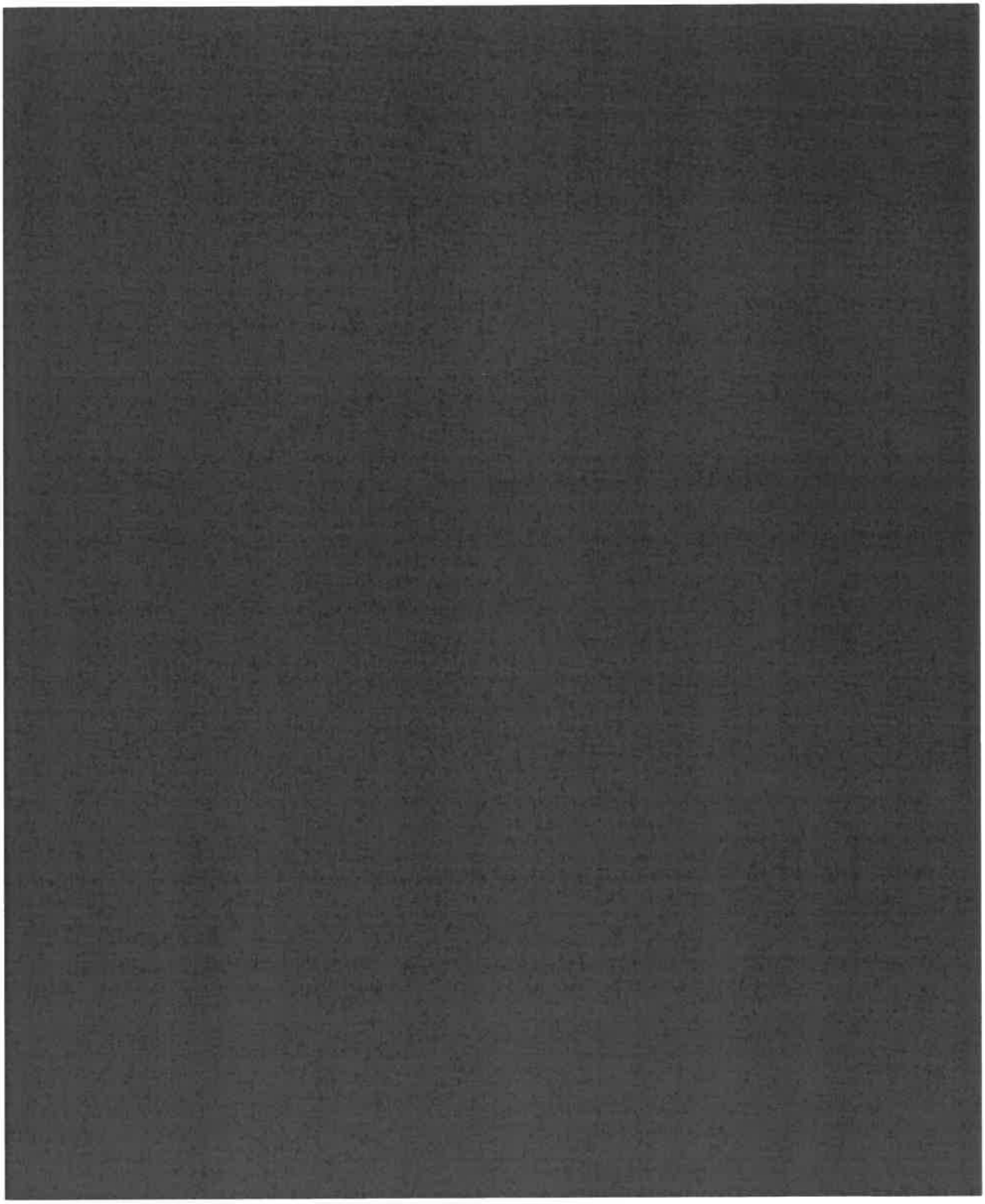
12.1 Synthèse du plan d'action



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

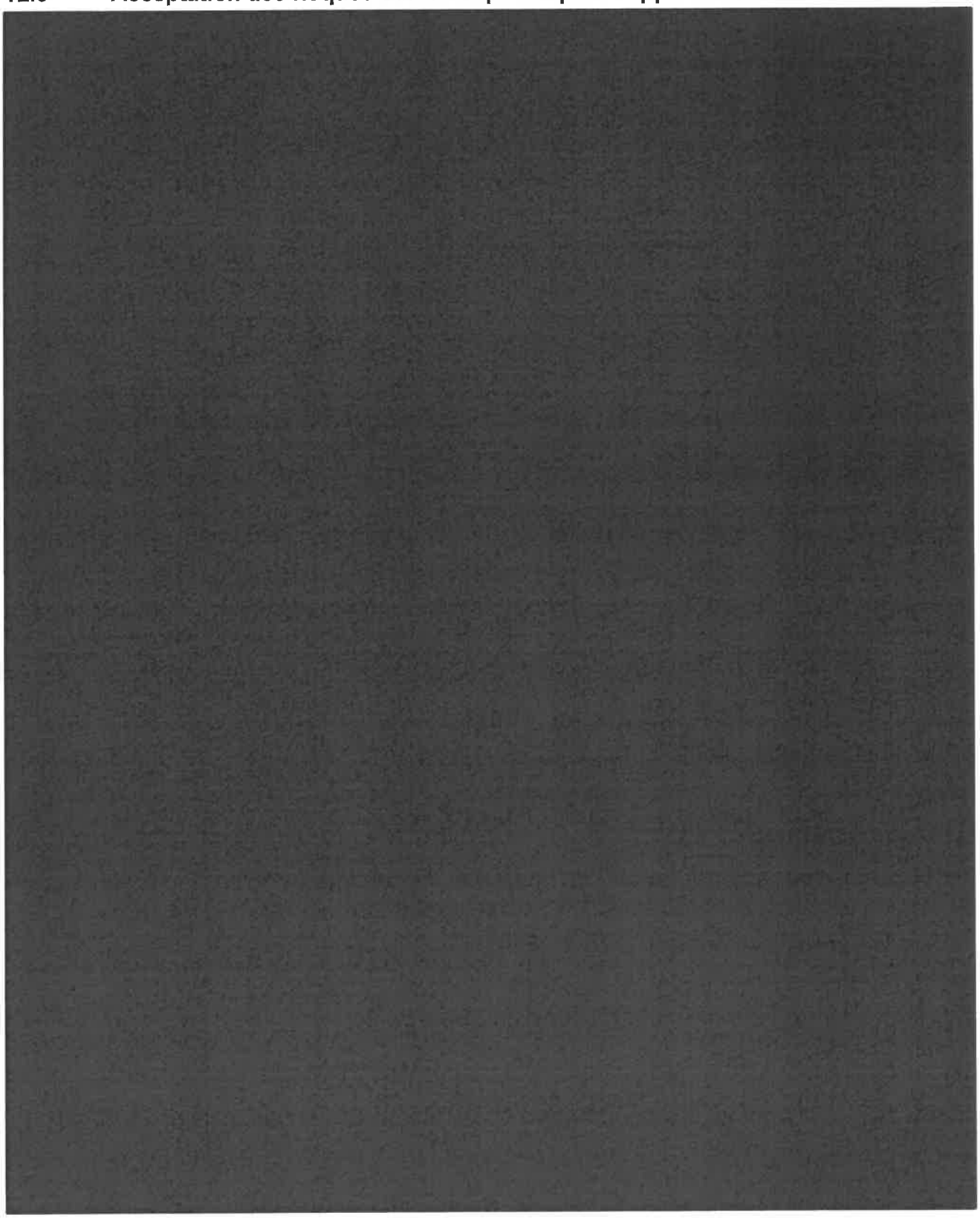
12.2 Evaluation des mesures liées au respect des principes fondamentaux

Principes fondamentaux	Acceptabilité (et arguments)
Finalité	Pas de risque résiduel
Base légale	Pas de risque résiduel
Minimisation	Risque résiduel : le SI IVI retourne au SI ApCV des données qui ne sont pas traitées ni conservées par le SI ApCV (type et n° de PI, date de délivrance et d'expiration)
Qualité	Pas de risque résiduel
Durées de conservation	Pas de risque résiduel
Information	Pas de risque résiduel
Droit d'accès	Pas de risque résiduel
Droit d'opposition / effacement	Pas de risque résiduel
Droit de rectification	Pas de risque résiduel
Droit à la limitation du traitement	En cours d'instruction pour s'assurer que ce droit peut être entièrement respecté
Mesures pour la sous-traitance	Pas de risque résiduel
Transferts hors UE	Pas de risque résiduel
Violation de données	Pas de risque résiduel

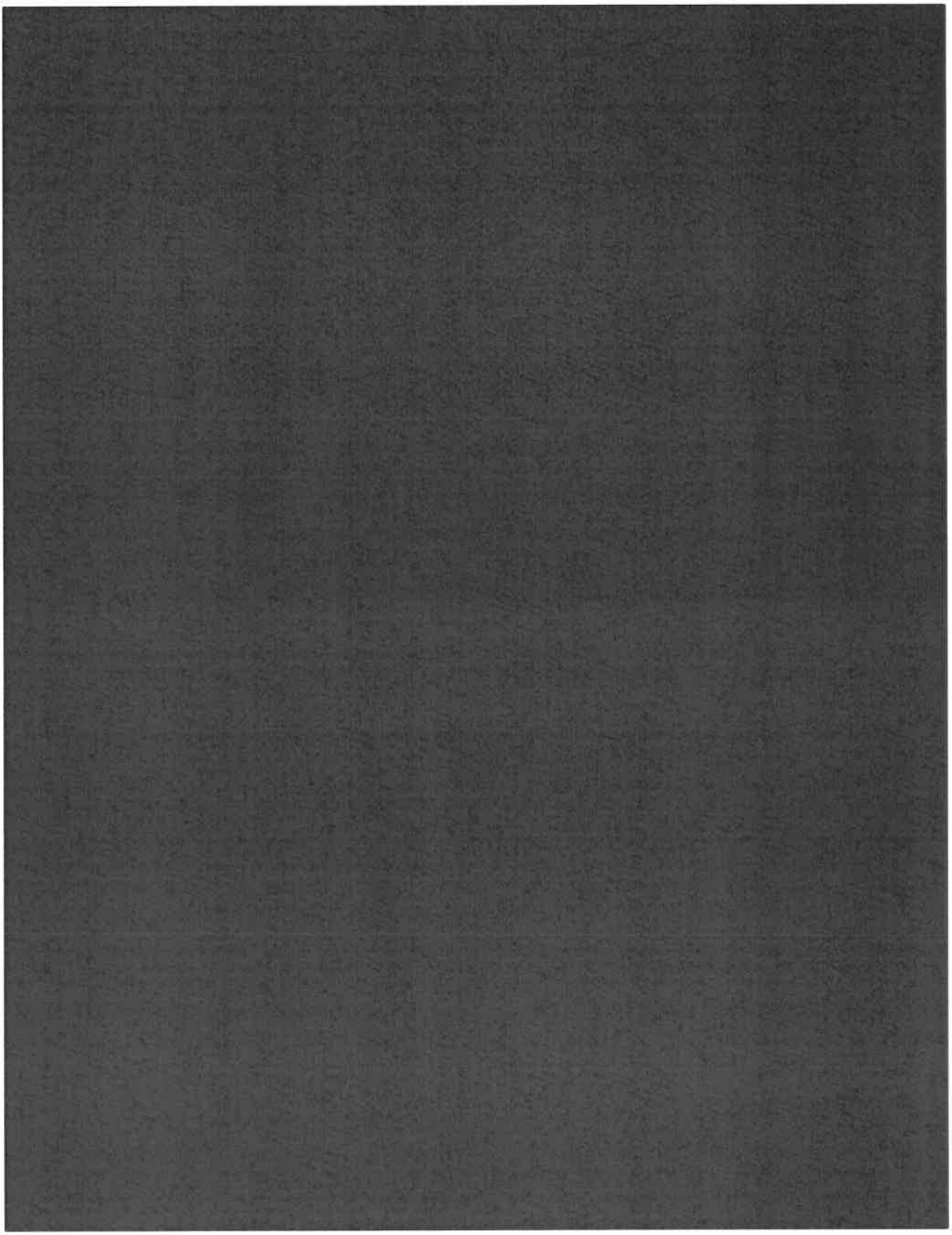
Tableau 27 : Risques résiduels liés au respect des principes fondamentaux

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

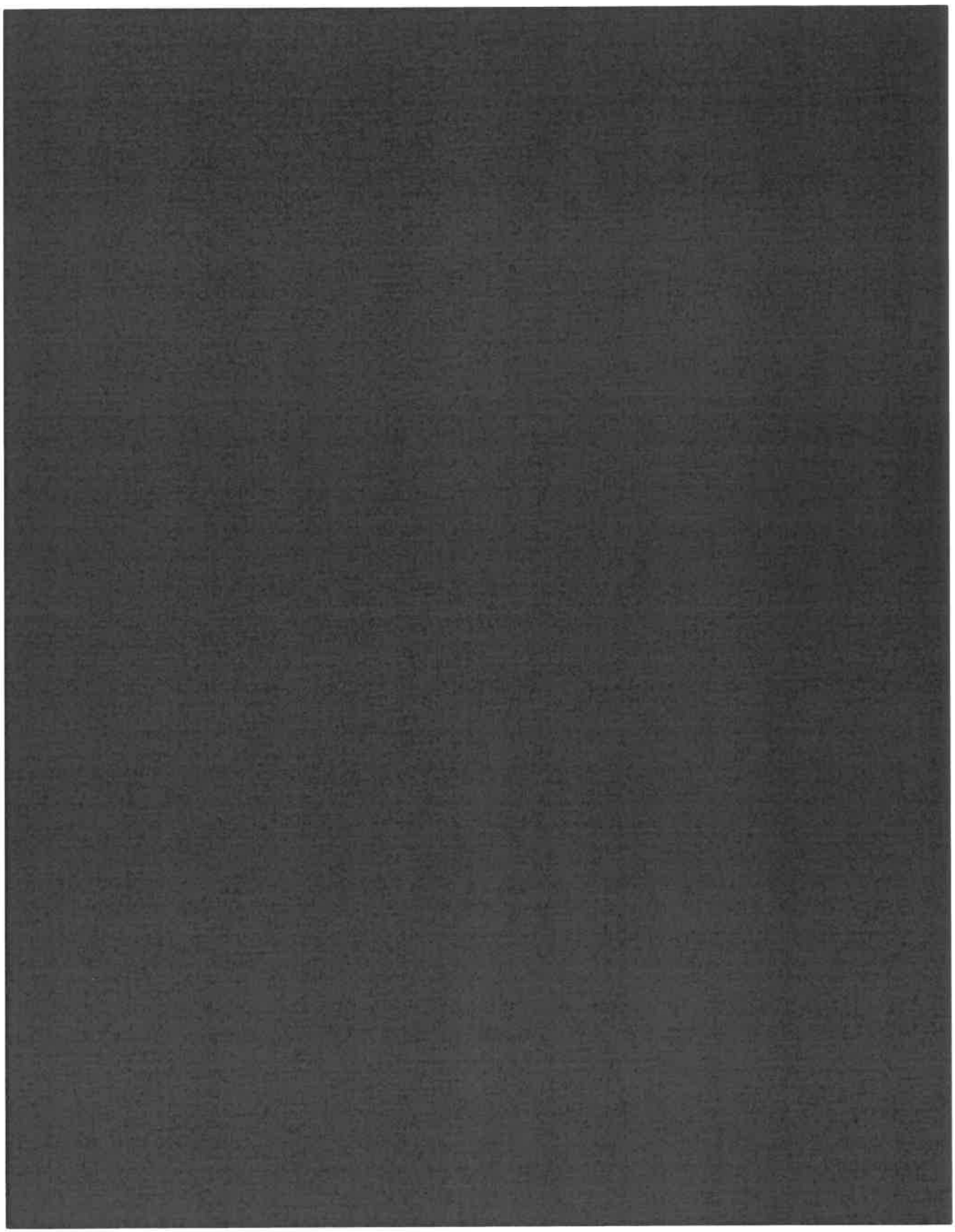
12.3 Acceptation des risques sur la vie privée pour l'appli carte Vitale V7



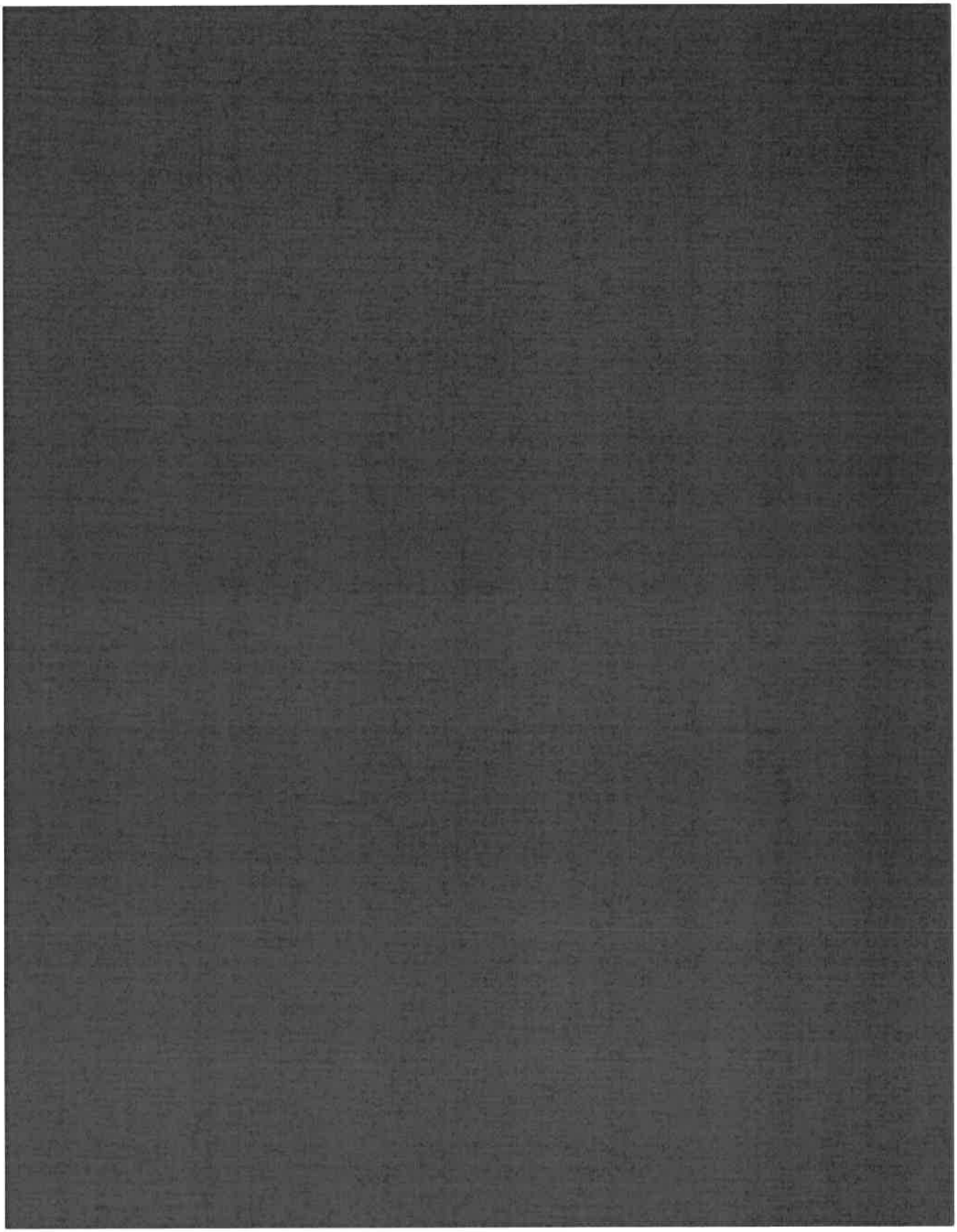
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



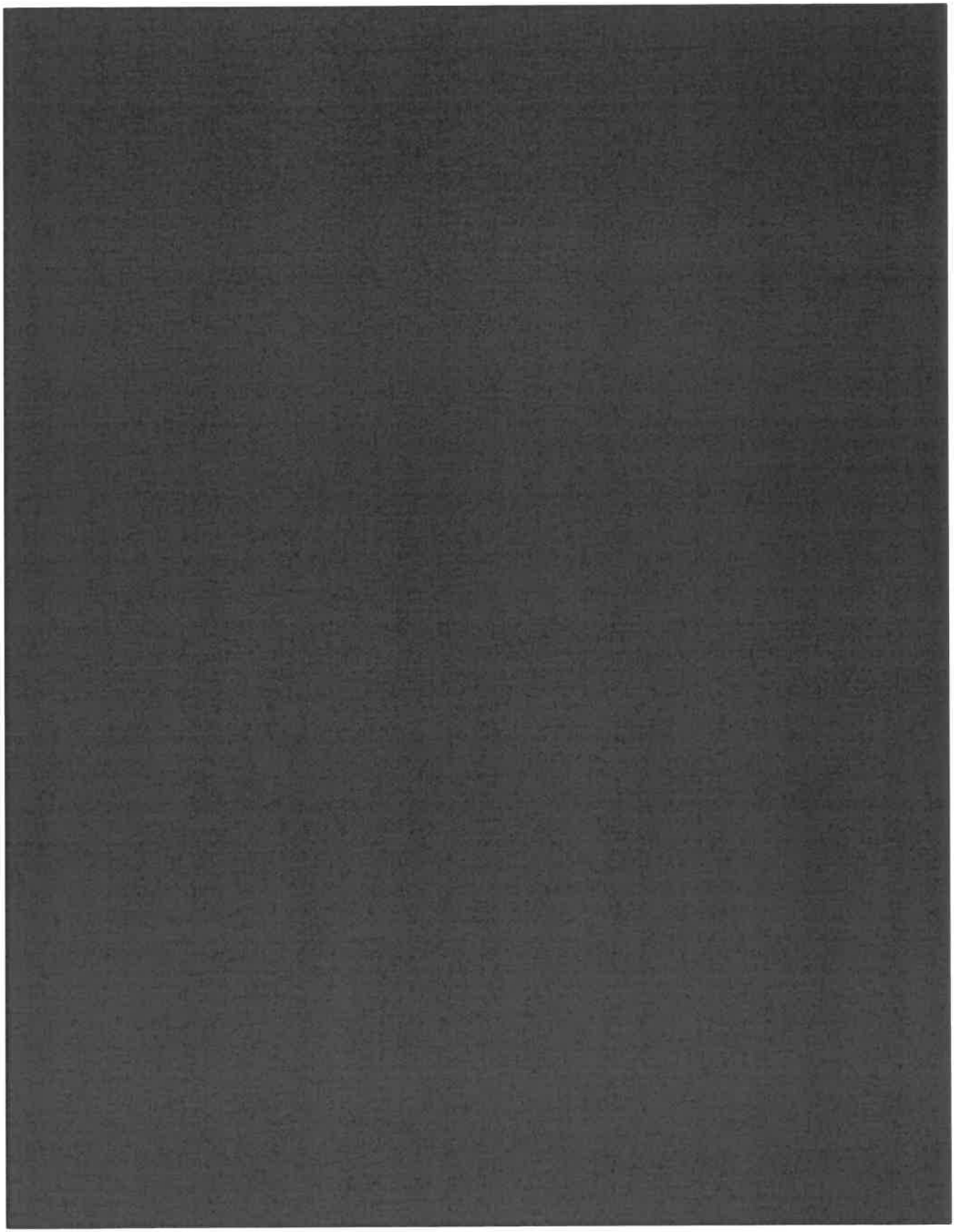
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



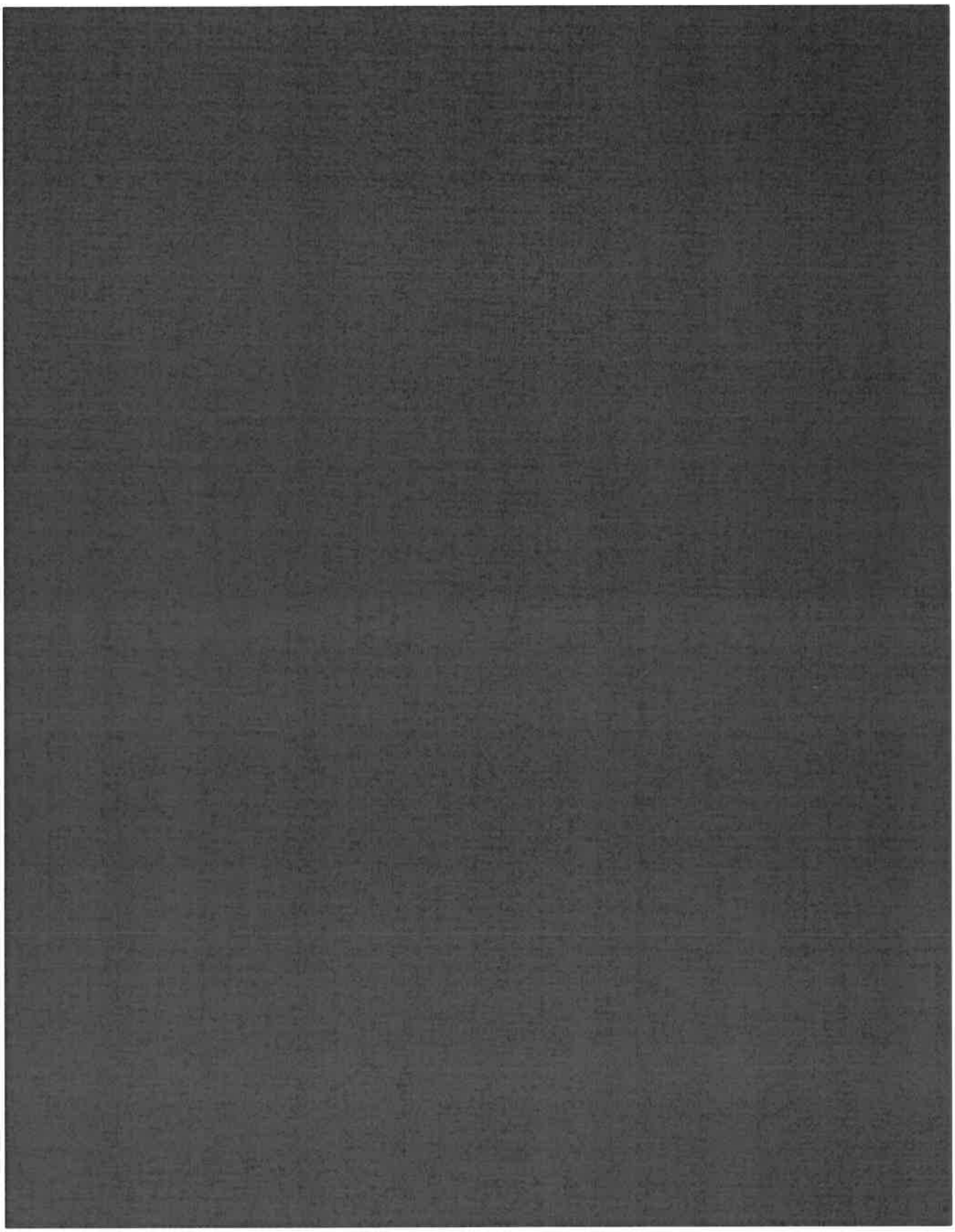
Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

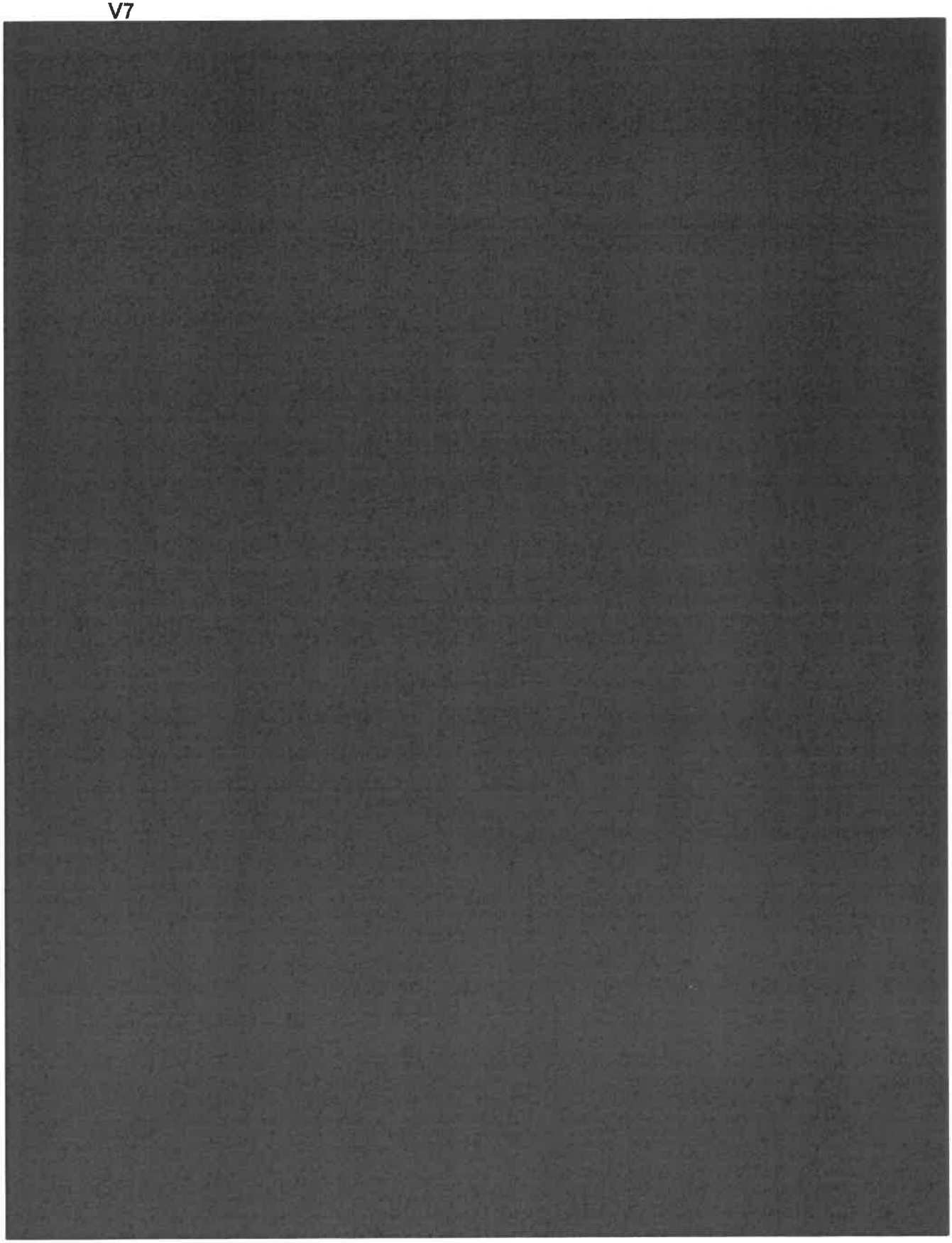


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

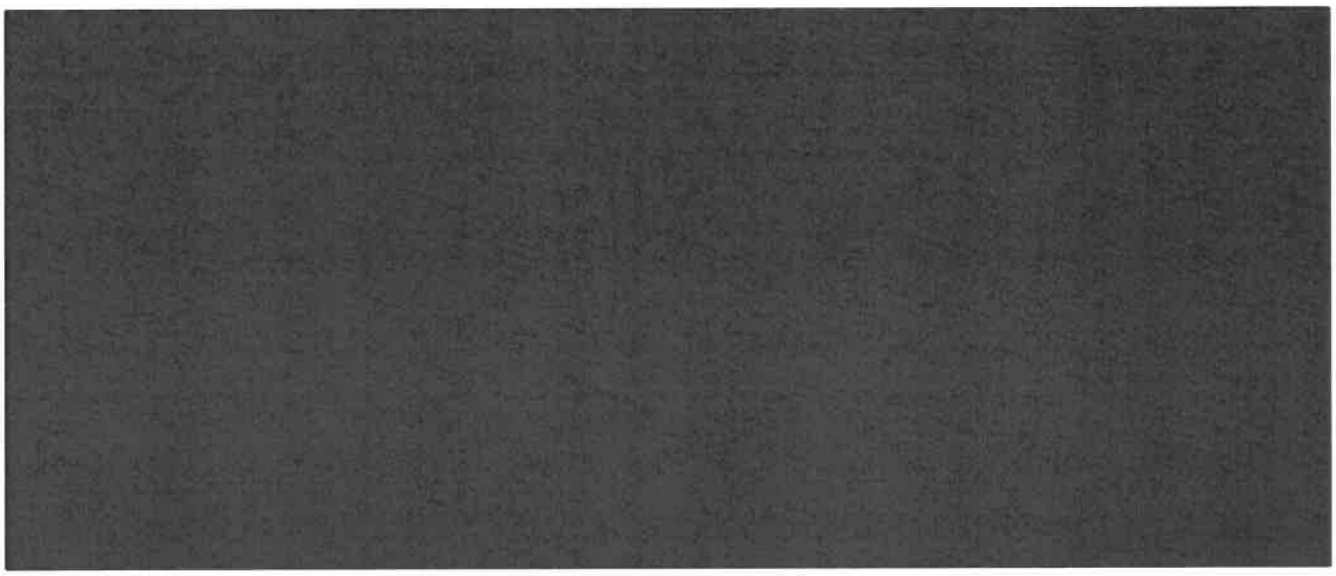


Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

12.4 Acceptation des risques sur l'Assurance Maladie pour l'appli carte Vitale V7



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



12.5 Conclusion

Les organismes AMO Cnam et CCMSA, responsables conjoints de traitement, valident l'analyse d'impact au vu de l'étude réalisée et du présent rapport.

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

13 ANNEXES

13.1 Etude cryptographique de pseudonymisation du NIR

13.1.1 Objectif

13.1.1.1 Contexte

[redacted]

13.1.1.2 Propriétés recherchées

[redacted]

13.1.2 [redacted]

13.1.2.1 [redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

13.1.2.2

[redacted]

13.1.2.3

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

13.1.3 Préconisations

[redacted]

13.1.3.1

[redacted]

13.1.3.2

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

13.1.3.3 Préconisation

[redacted]

13.1.3.4 Autres préconisations

[redacted]

13.1.4 Compromissions et mises à jour

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

13.1.4.1 Compromissions possibles

[redacted]

13.1.4.2 Mises à jour

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

[redacted]

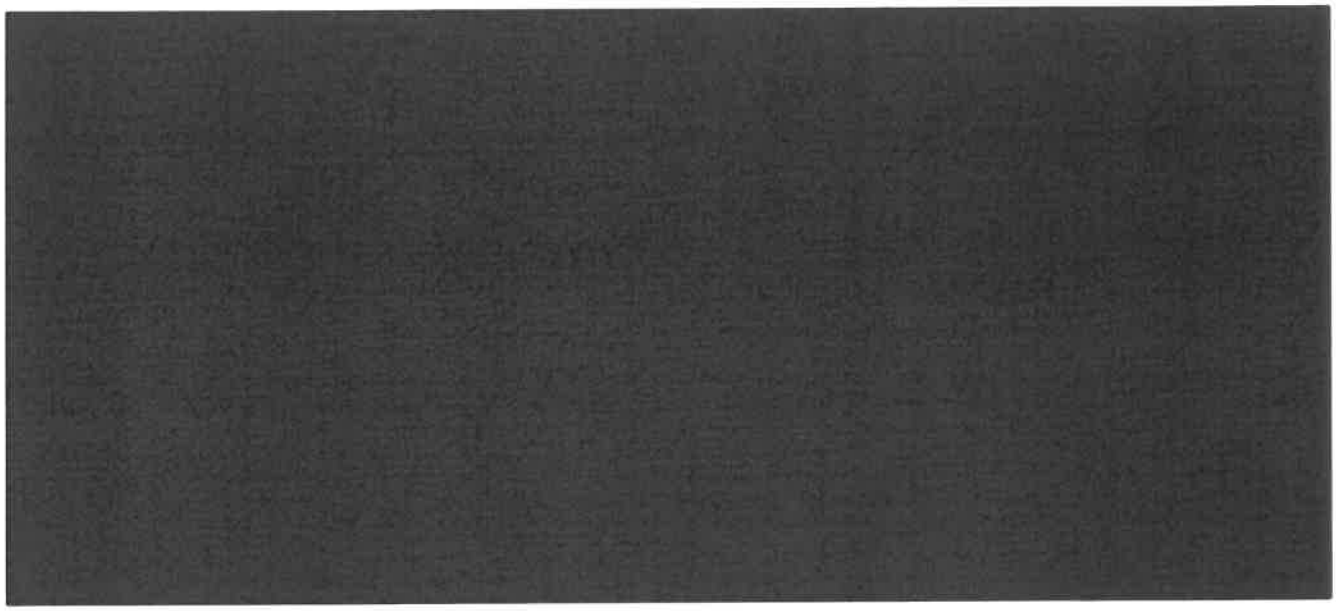
13.1.5 Références

[redacted]

13.2 Versions d'ApCV

[redacted]

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

13.3 Echelles

13.3.1 Echelle de probabilité des menaces

L'échelle de valeur de probabilité proposée pour les différentes menaces retenues par type d'acteurs est indiquée dans le tableau ci-dessous :

Niveau Dénomination	Critère compétences et moyens	Critère motivation	Profil de l'attaquant	Décision GIE
0	Impossible à mettre en œuvre dans la pratique ou possibilité extrêmement faible de se réaliser	Stratégique ou politique	Organisations criminelles ou étatiques	Non pris en compte : risque acceptable
1 Très improbable, ne surviendra probablement jamais	Demande des moyens très importants et/ou des connaissances très élevées dans le domaine considéré	Frauduleuse, stratégique, politique	Organisations criminelles ou étatiques Concurrents	À prendre en compte au cas où : zone de risque résiduel acceptable
2 Possible bien qu'improbable	Demande des matériels disponibles commercialement et/ou des connaissances de base sur le domaine considéré Pourrait arriver pendant le cycle de vie du système	Frauduleuse	Fraudeur	À prendre en compte. Toléré au cas par cas.
3 Probable, devrait arriver un jour.	Demande peu de moyens et peut être réalisé avec peu de connaissances du domaine concerné	Ludique vénale	Hacker lambda	À prendre en compte obligatoirement
4 Très probable. Surviendra sûrement à court terme	Ne demande aucun matériel particulier et peut être réalisé sans connaissances particulières du domaine concerné	Ludique occasionnel	Hacker lambda	À prendre en compte obligatoirement

Tableau 30 : Echelle de probabilité des menaces

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

13.3.2 Echelle d'impact sur la vie privée

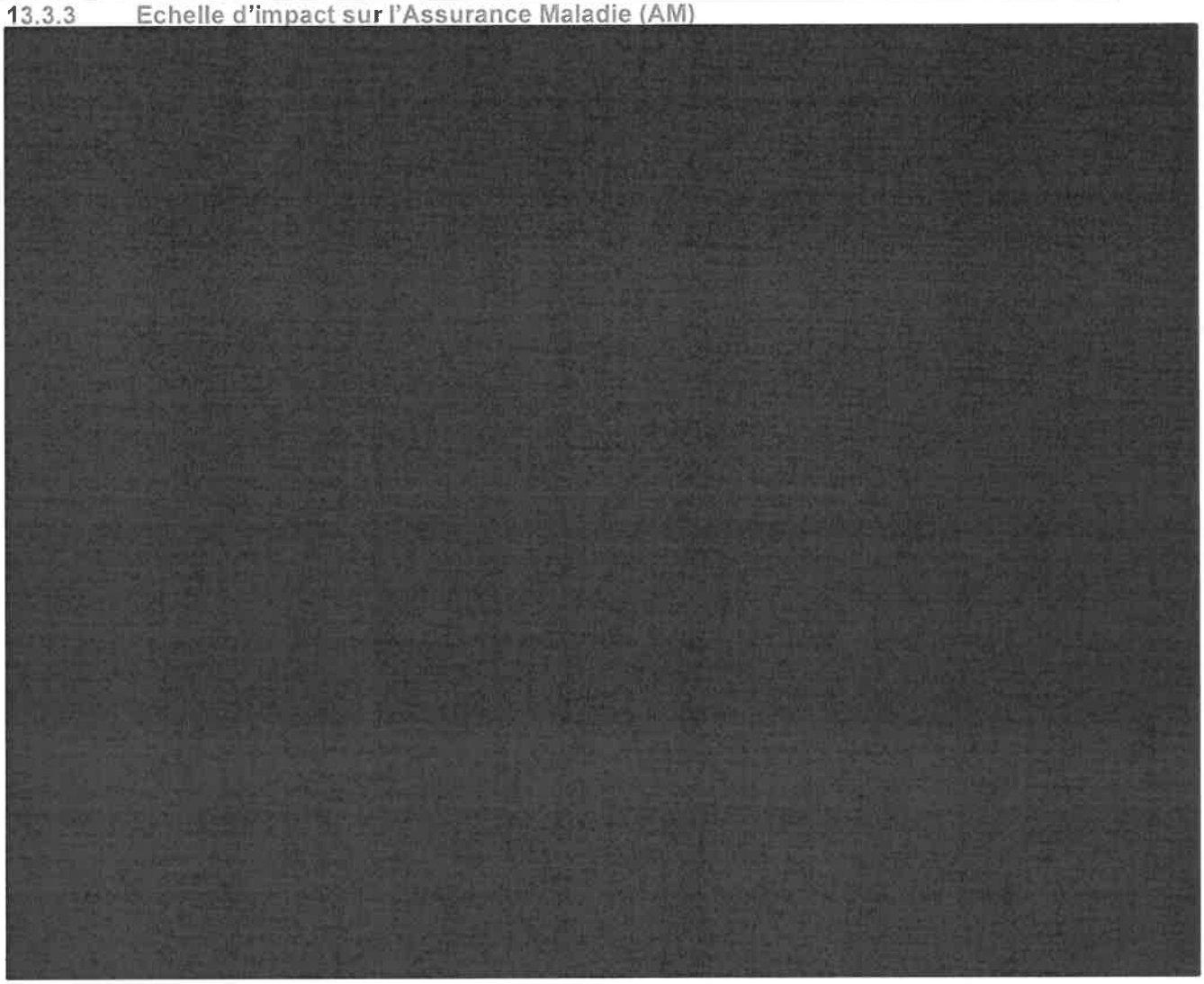
L'évaluation de l'impact des risques sur la vie privée se base sur l'échelle suivante issue des recommandations de la CNIL, à laquelle a été ajouté le niveau 0 pour assurer la cohérence avec l'échelle d'impact utilisée par le GIE SV.

	Description générique de l'impact	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemple d'impacts moraux
0 – Aucun	Les personnes concernées ne seront pas impactées	-	-	-
1 – Négligeable	Les personnes concernées pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle), maux de tête passagers	Perte de temps pour réitérer des démarches, réception de publicités ciblées non sollicitées pour des produits courants	Simple contrariété par rapport à l'information reçue ou demandée, sentiment d'atteinte à la vie privée sans préjudice réel
2 – Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	Affection physique mineure (ex. : maladie bénigne suite au non-respect de contre-indications), absence de prise en charge causant un préjudice minime mais réel (ex : handicap), diffamation donnant lieu à des représailles physiques ou psychiques	Paiements non prévus, frais supplémentaires, refus d'accès à des services administratifs ou commerciaux, promotion professionnelle manquée publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel	Affection psychologique mineure mais objective (diffamation), difficultés relationnelles avec l'entourage personnel ou professionnel (réputation ternie), intimidation sur les réseaux sociaux
3 – Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	Affection physique grave causant un préjudice à long terme (aggravation de l'état de santé suite à une mauvaise prise en charge), altération de l'intégrité corporelle par exemple à la suite d'une agression ou d'un accident	Détournements d'argent non indemnisés, difficultés financières temporaires, opportunités uniques perdues (prêt immobilier, études, emploi), interdiction bancaire, perte d'emploi, divorce	Affection psychologique grave (dépression, développement d'une phobie), , développement d'une phobie, victime de chantage, de harcèlement moral, assignation en justice, atteinte à la liberté d'expression
4 – Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	Affection physique de longue durée ou permanente, décès, altération définitive de l'intégrité physique	Péril financier, dettes importantes, impossibilité de travailler ou de se loger, perte de preuves dans le cadre d'un contentieux, perte d'accès à une infrastructure vitale (eau, électricité)	Affection psychologique de longue durée ou permanente, sanction pénale, enlèvement, perte de lien familial, changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

Tableau 31 : Echelle d'impacts sur la vie privée

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

13.3.3 Echelle d'impact sur l'Assurance Maladie (AM)



13.3.4 Echelle de gravité des risques

La gravité d'un risque est obtenue par le croisement entre la probabilité et l'impact de la menace :

Impact ⇨ Probabilité ⇩	0	1	2	3	4
0	0	0	0	1	2
1	0	1	1	2	3
2	0	1	2	3	4
3	1	2	3	4	4
4	2	3	4	4	5

Tableau 33 : Echelle de gravité des risques

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

L'échelle de gravité utilisée est présentée ci-dessous :

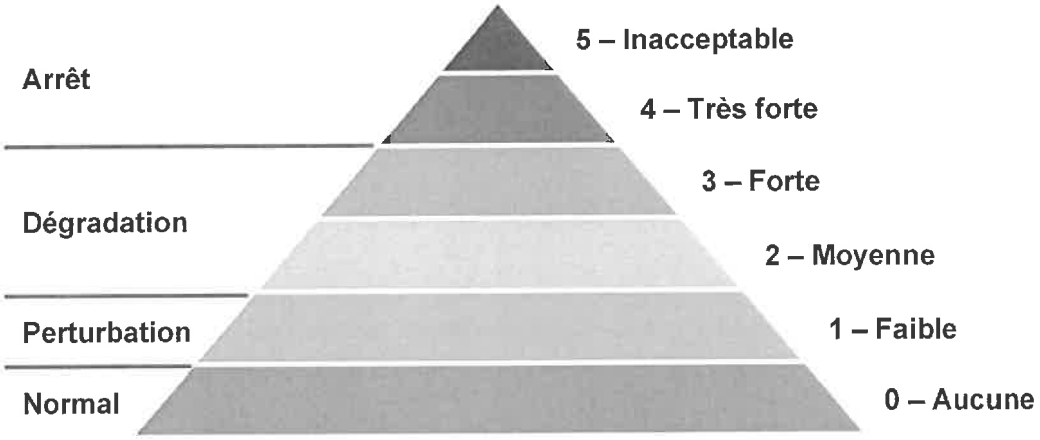


Figure 19 : Echelle de gravité

Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale

13.4 Tables des figures et tableaux

Table des Figures

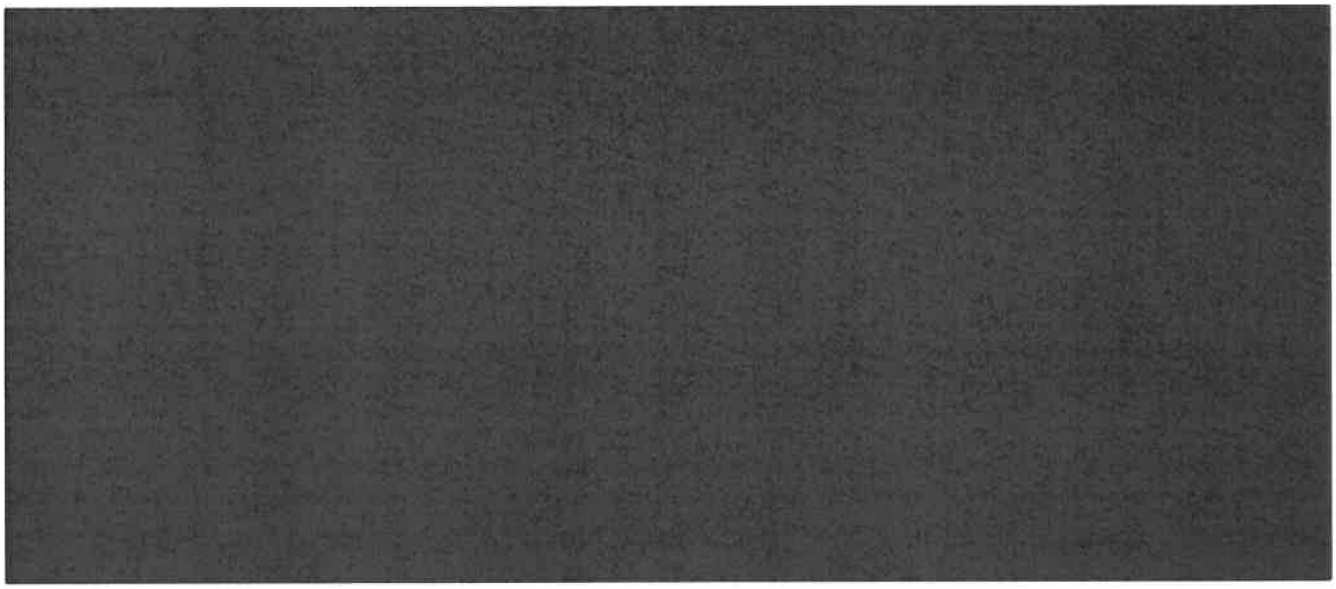
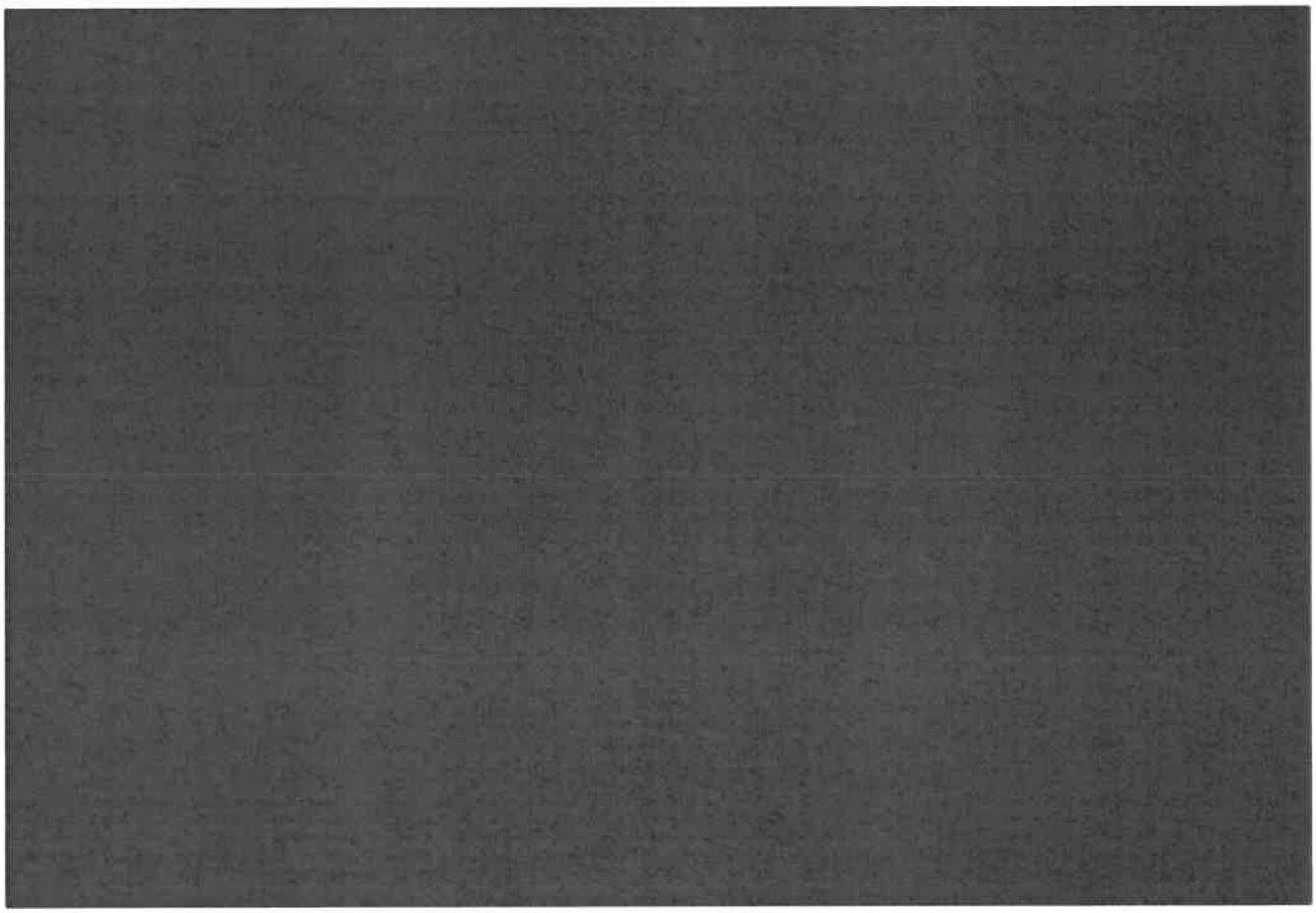
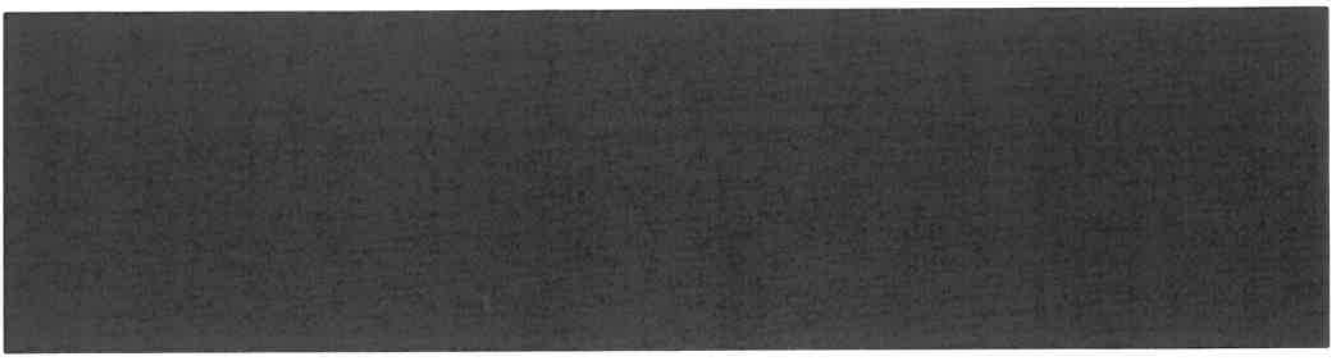


Table des Tableaux



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale



Ce document à diffusion restreinte ne peut être diffusé sans l'autorisation d'une personne habilitée au GIE SESAM-Vitale