

## **Protocole d'accord pour la destruction anticipée des documents papier numérisés et des données et documents numériques produits dans le cadre du programme « Procédure pénale numérique » (PPN)**

### **PREAMBULE**

Depuis janvier 2018, les ministères de l'intérieur et de la justice sont engagés dans un programme commun de dématérialisation de la procédure pénale. Encadré par une direction de programme « Procédures pénales numériques » (DP PPN) dédoublée, présente au sein des deux ministères, le projet vise, à l'horizon 2022, à obtenir une procédure se substituant entièrement aux dossiers sous format papier. Les autorités judiciaires et services enquêteurs seront alors en mesure de produire, échanger, consulter et conserver les documents numérisés et nativement numériques constitués dans le cadre d'une affaire pénale. Les documents sous format papier qui auront été numérisés auront vocation à être, soit éliminés, soit restitués aux justiciables et autres acteurs de la procédure.

A terme, le passage des juridictions au nativement numérique doit permettre d'automatiser les tâches les plus chronophages, faciliter la constitution et la gestion des dossiers produits dans le cadre d'une procédure pénale, générer des gains de temps dans le traitement des affaires et faciliter l'accès aux documents pour l'ensemble des acteurs de la procédure.

Le présent protocole a pour objet de définir les principes et modalités encadrant le processus de dématérialisation de la procédure pénale, afin d'autoriser par anticipation la destruction des documents sous format papier numérisés et d'assurer la mise en œuvre du cycle de vie sur les données et documents numériques dans le cadre du programme « Procédure pénale numérique ». Pour ce faire, les parties signataires du présent protocole s'accordent sur le caractère impératif des dispositifs énoncés ci-dessous et s'engagent à veiller à leur application par les services relevant de leurs responsabilités respectives.

Le présent protocole est conclu entre les juridictions participant au programme « Procédure pénale numérique » représentées par la direction de programme PPN et le service interministériel des archives de France (SIAF).



## **I. DOCUMENTS DE REFERENCE**

### **1. Cadre réglementaire et normatif**

Code du patrimoine, livre II.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique, modifiant le Code civil

Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice

Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Décret n°2014-472 du 9 mai 2014 pris pour l'application de l'article 5-2 de l'ordonnance n°45-174 du 2 février 1945 relative à l'enfance délinquante relatif au dossier unique de personnalité

Décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Décret n°2007-1388 du 26 septembre 2007 pris pour l'application de la loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance et modifiant le code pénal et le code de procédure pénale

Décret n°2007-1620 du 15 novembre 2007 modifiant le code de procédure pénale et relatif à l'utilisation des nouvelles technologies

Décret n°2010-671 du 18 juin 2010 relatif à la signature électronique et numérique en matière pénale et modifiant certaines dispositions de droit pénal et de procédure pénale

Décret n°2019-507 du 24 mai 2019 pris pour l'application des dispositions pénales de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice relatives à la procédure numérique, aux enquêtes et aux poursuites

Décret n°2020-767 du 23 juin 2020 portant création d'un traitement automatisé de données à caractère personnel dénommé « dossier pénal numérique »

Arrêté du 21 décembre 2010 modifiant l'arrêté du 16 janvier 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « numérisation des procédures pénales »

Arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale

Arrêté du 6 septembre 2019 fixant les modalités d'application des articles D 589 et suivants du code de procédure pénale relatifs à la procédure pénale numérique

Instruction DITN/DPACI/RES/2005/001 du 14 janvier 2005 sur les modalités de délivrance du visa d'élimination des documents papiers transférés sur support numérique ou micrographique, complétée et consolidée en 2014, par le vade-mecum sur la destruction de documents sur support papier après leur numérisation

Préconisation de sélection DGP/SIAF/2019/003 du 25 septembre 2019 relative aux impacts de la réforme de la prescription en matière pénale sur les archives des juridictions de l'ordre judiciaire

Fiche de présentation DGP/SIAF/2019/002 du 24 septembre 2019 relative aux impacts archivistiques de mise en œuvre du programme « Procédure pénale numérique » (PPN) dans les juridictions

Norme NF Z 42-026, 2017, Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations

Norme NF Z 42-013, 2020, Archivage électronique – Recommandations et exigences

## **2. Livrables**

Pour conseiller les juridictions dans la mise en place des nouveaux processus de dématérialisation et les accompagner dans les changements induits par ces processus, plusieurs livrables ont été réalisés et partagés entre le ministère de la justice et le service interministériel des archives de France :

- Charte qualité pour la numérisation fidèle de documents ;

- Processus de numérisation: guide pour le contrôle qualité par échantillonnage;
- Grilles de contrôle qualité pour opérateurs de numérisation et services de greffe;
- Analyse d'impact relative à la protection des données (PIA) « Traitement des dossiers pénaux numériques »;
- Vadémécum « Autoriser la destruction de documents sur support papier après leur numérisation » appliqué aux pièces de procédures pénales numériques;
- Fiche pratique: « Archivage temporaire dans NPP avant versement dans le système d'archivage électronique Axone ».

En plus de ces livrables spécifiquement créés dans le cadre de PPN, des guides, manuels utilisateurs et fiches pratiques relatifs à l'utilisation des outils et logiciels informatiques utilisés pour la gestion électronique des procédures pénales ont été produits par la DSJ. L'ensemble de la documentation est accessible sur le site Intranet du ministère de la Justice :

<http://intranet.justice.gouv.fr/site/dsj/dematierialisation-16004/>

<http://intranet.justice.gouv.fr/site/archives/>

## **II. PERIMETRE DU PROTOCOLE**

### **1. Définition des pièces et dossiers concernés par le protocole**

Les pièces concernées par le présent protocole sont les pièces numérisées pour le traitement et le suivi d'une procédure pénale :

- Les procès-verbaux et rapports dressés par les officiers ou agents de police judiciaire et les fonctionnaires et agents chargés de certaines fonctions de police judiciaire et des personnels des douanes judiciaires,
- Les actes réalisés par les experts missionnés par les services de police ou de justice,
- Les actes réalisés par les magistrats ou fonctionnaires des services judiciaires, de l'administration pénitentiaire (ex : rapports des services d'insertion et de probation, avis de la direction de l'administration pénitentiaire) ou de la protection judiciaire de la jeunesse (ex : rapports des services éducatifs),
- Tout document pouvant être apporté par le justiciable qu'il soit victime, mis en cause ou témoin,

- Toute pièce en général versée au sein du dossier de procédure.

Ces pièces viennent compléter les dossiers nativement numériques et labélisés « dossier pénal numérique » suivants, qui sont par conséquent inclus dans le périmètre du présent protocole :

- Le dossier de procédure ;
- Le dossier unique de personnalité (DUP) mineur ;
- Le minutier et/ou registre des minutes ;
- Le dossier d'exécution des peines ;
- Le dossier d'application des peines des personnes placées sous main de justice.

## **2. Définition des acteurs**

Le présent protocole s'applique exclusivement aux personnels en juridiction, fonctionnaires et agents des services judiciaires en charge de la création, de la gestion et/ou de la conservation au format papier ou numérique des actes et dossiers à valeur probante mentionnés ci-dessus.

Les actes et dossiers qui ont été numérisés pour être versés aux dossiers produits dans le cadre d'une procédure pénale, mais dont les originaux doivent être conservés par des services autres que les services de greffe en juridiction (services sous la direction de l'administration pénitentiaire ou de la protection judiciaire de la jeunesse, services enquêteurs, autres partenaires impliqués dans une procédure pénale), suivent les modalités de conservation et de destruction propres à leur service.

## **3. Périmètre applicatif**

Le programme de dématérialisation de la procédure pénale est mis en œuvre via l'application « Numérisation des procédures pénales » (NPP). Déployé depuis 2008 dans les cours d'appel (CA) et tribunaux de grande instance (TGI), le traitement informatique NPP, interfacé sur une instance de gestion électronique de documents (GED) dénommée « Alfresco », assure la gestion électronique de documents issus des pièces de procédures pénales. NPP permet de :

- Importer des pièces relatives à des procédures pénales, qu'elles soient numérisées ou nativement numériques ;

- Stocker de manière sécurisée les documents reçus ou produits par les juridictions ;
- Classer les pièces de procédures et dossiers dans une arborescence conforme à la structuration des juridictions ;
- Assurer l'accessibilité des dossiers et actes aux services gestionnaires habilités pour permettre le traitement des affaires pénales ;
- Fluidifier le partage de documents numériques et délivrer, dans les délais les plus brefs, des copies aux avocats sur support numérique ;
- Assurer la conservation des dossiers et actes de procédure jusqu'au terme de leur durée d'utilité courante (DUC) ;

La production et l'exploitation des actes de procédure passent également par l'utilisation d'autres outils informatiques :

- OEPN (outil d'exploitation des procédures numérisées), qui permet aux personnes habilitées de travailler sur les dossiers préalablement téléchargés en hors ligne. OEPN permet ainsi la consultation du dossier pénal numérique et la prise de notes et d'annotations sur les fichiers téléchargés. OEPN permet également d'importer en masse des dossiers dans NPP.
- NOE (nouvel outil d'exploitation), conçu pour les magistrats des services pénaux, l'outil permet de personnaliser l'organisation et la gestion de leurs dossiers numériques. Il permet notamment la prise de notes, l'utilisation de tags, la réalisation de schémas pour constituer une représentation graphique de l'affaire ou encore l'ajout de pièces externes à l'affaires et non conservées dans NPP (par exemple des fichiers multimédias ou des notes personnelles).

Au terme de leur exploitation courante, les dossiers et pièces de procédures seront versés dans le système d'archivage électronique hybride (SAEH) du ministère de la justice, dénommé Axone, afin d'assurer leur conservation, leur pérennité, leur intégrité et authenticité pendant toute leur durée d'utilité administrative (DUA).

### **III. ENGAGEMENTS TECHNIQUES**

#### **1. Encadrement des processus de numérisation et de contrôle interne de la numérisation**

Le programme PPN a pour objectif de dématérialiser entièrement la gestion des procédures pénales et envisage, à terme, de ne traiter que des documents nativement numériques, à l'exception de quelques pièces annexes transmises sous format papier par les justiciables, avocats, experts ou autres partenaires privés et/ou publics.

Dans l'attente de pièces de procédures intégralement créées et gérées au format numérique, des mesures et outils ont été mis en place pour encadrer et accompagner le processus de numérisation en juridiction des documents papier restant. Ainsi, une « Charte qualité pour la numérisation fidèle de documents – dossiers de la juridiction pénale », réalisée par le ministère de la justice et à destination des juridictions impliquées dans le programme PPN, définit :

- les documents concernés par le processus de numérisation ;
- les acteurs impliqués dans le processus ;
- l'organisation générale (méthode et outils employés) de la procédure de numérisation ;
- les exigences de qualité attendues ;
- les contrôles qualité à mettre en place.

Pour accompagner cette Charte, un « guide pour le contrôle qualité par échantillonnage » des documents numérisés à destination des services de greffe, ainsi que des grilles de contrôles pour les opérateurs de numérisation et services de greffe ont été réalisés.

Les juridictions s'appuient sur ces documents de cadrage afin de garantir l'intégration dans NPP de pièces de procédures fiables, complètes, authentiques et opposables en cas de litige. Le respect des procédures et mesures de contrôles décrites dans ces textes est indispensable pour autoriser la destruction de leur équivalent papier. Les parties prenantes du présent protocole et les juridictions représentées dans ce protocole par la DSJ s'engagent à faire respecter les procédures décrites et, le cas échéant, à faire remonter auprès du DADP du ministère de la justice et du SIAF, tout dysfonctionnement ou manquement au respect des procédures qui auraient été constatés.

Tout dysfonctionnement ou non-respect des procédures par les juridictions peut entraîner la suspension provisoire du droit de destruction par anticipation des

documents papier pour les juridictions concernées. L'autorisation de destruction sera rétablie après mise en place de mesures correctives et constatation, par les représentants du DADP ou du SIAF, de la levée des problèmes ayant entraînés la suspension des éliminations.

## 2. Valeur probante et fiabilité des pièces

Afin d'assurer l'authenticité et l'intégrité des documents qu'il conserve, le ministère de la justice a fait évoluer le traitement informatique NPP et lui a associé des briques de sécurité permettant de contrôler et garantir la valeur probante des documents enregistrés dans le système. Ces briques prennent la forme :

- D'un outil de signature électronique qualifiée, dénommé SIGNA qui assure la mise en œuvre de la signature sous forme numérique des pièces<sup>1</sup> dans le cadre du programme PPN. SIGNA a pour finalité de garantir l'intégrité, la non répudiation et l'authenticité des documents sur lesquels la signature est apposée. Il vise à obtenir un lien non-équivoque entre la signature et son signataire et assure la valeur probante des actes réalisés par les personnels du ministère de l'intérieur et du ministère de la justice. En fonction de la sensibilité des actes produits et de leur valeur légale, SIGNA permet d'apposer une signature électronique individuelle<sup>2</sup> ou un cachet électronique.
- D'un journal de bord intégré à NPP qui permet de tracer les opérations réalisées sur les dossiers et fichiers enregistrés dans NPP (création, modification, transfert, suppression). Pour chaque type d'opération, le journal indique la date, l'utilisateur et le fichier concerné (nom et identifiant Alfresco). A partir de ce journal, des fichiers journaliers et mensuels d'exports d'audit de sécurité au format CSV sont envoyés au coffre-fort ministériel SCORPION pour y être conservés pendant 6 ans.

En plus de ces briques, le ministère de la justice développe actuellement un système d'archivage électronique hybride (SAEH), Axone, sur lequel viendra s'appuyer NPP pour assurer la conservation pérenne des documents pendant toute leur DUA. Le SAEH déploiera un ensemble de fonctionnalités permettant de garantir l'authenticité, l'intégrité et la fiabilité des pièces archivées. Ces fonctionnalités sont :

- un outil de vérification des signatures électroniques, qui contrôlera en entrée la validité des signatures apposées aux documents versés ;

---

<sup>1</sup> Conformément à l'article R. 249-9 du code de procédure pénale.

<sup>2</sup> Les personnels disposant de la signature électronique individuelle sont les personnels des services judiciaires responsables de l'établissement des actes et possédant une carte agent (magistrats, greffiers, etc.).

- un journal des traces, qui permettra de vérifier l'ensemble des opérations réalisées sur un document conservé dans Axone et rendra l'ensemble des éléments archivés opposables, conformément aux normes en vigueur ;
- un outil de conversion de format des documents afin d'assurer la lisibilité des pièces sur le long terme et d'anticiper les risques de perte d'informations liés à la dégradation de formats trop anciens ;
- une fonction assurant la sécurité du système et de son contenu par le biais d'habilitations et droits d'accès fins aux documents et dossiers.

En attente du déploiement du SAEH Axone, l'application NPP assurera la conservation des données et documents pendant leur DUA. Les dossiers et documents clos seront extraits de la base courante NPP par les services de greffe pour être préarchivés sur une base spécifique de NPP disposant d'une arborescence propre. Ils seront ensuite versés dans le SAEH Axone dès la mise en production de la solution. Dans NPP, l'authenticité et l'intégrité des documents et données préarchivées seront assurées par les briques de sécurité définies dans les paragraphes précédents.

Ces briques de confiance sont essentielles pour garantir aux acteurs de la procédure pénale l'accès et l'exploitation de documents/dossiers fiables, intègres, authentiques et complets. Les signataires du présent protocole s'engagent à fournir ces briques de confiance aux juridictions et à en assurer la maintenance, ceci afin de prévenir tout dysfonctionnement qui pourrait altérer la fiabilité, l'intégrité ou l'authenticité des actes et dossiers de procédure.

### **3. Procédure d'archivage des pièces numériques**

La durée de conservation courante en base NPP des pièces et dossiers numériques produits dans le cadre d'une procédure pénale est strictement définie dans le PIA envoyé à la CNIL et dans la fiche pratique DUC<sup>3</sup>. Elle correspond au temps de traitement de la procédure pénale et, le cas échéant, de l'exécution de la peine :

- Les données enregistrées dans le traitement sont conservées jusqu'à ce que la juridiction saisie ait statué définitivement par une décision/ordonnance rendue sur le fond. En cas de condamnation, le dossier est conservé jusqu'à l'exécution de la mesure prononcée ;
- Dans le cadre des procédures classées sans suite y compris pour auteur inconnu, les informations enregistrées dans le traitement sont conservées jusqu'à la date d'extinction de l'action publique ;

---

<sup>3</sup> Cf. PIA Traitement des dossiers pénaux numériques et fiche pratique DUC.

- Dans le cadre de l'exécution de la peine, chaque mesure est conservée jusqu'à la fin de l'exécution de la mesure concernée.
- Dans le cas des minutiers et/ou registres des minutes, les dossiers sont conservés 8 ans dans NPP pour permettre aux services de greffe d'effectuer les annotations et modifications à la marge nécessaires pour la gestion des affaires traitées.
- Enfin, les dossiers uniques de personnalité (DUP) relatifs aux mineurs sont conservés dans NPP jusqu'aux 18 ans révolus du mineur suivi. Par dérogation, le DUP est conservé après la majorité, lorsqu'une procédure ouverte à l'encontre du mineur est encore en cours, jusqu'à ce que la juridiction ait statué définitivement par une décision rendue sur le fond, ou jusqu'au terme du suivi d'une mesure ou sanction éducative ordonnée, ou lorsque le juge des enfants exerce les fonctions dévolues au juge de l'application des peines<sup>4</sup>.

Cette durée de conservation courante est associée à une durée d'exploitation des documents qui détermine la date à partir de laquelle les dossiers, actes et pièces doivent être versés dans le futur système d'archivage électronique hybride (SAEH) du ministère de la justice, Axone, en cours de développement<sup>5</sup>. L'intégralité des pièces et données associées y seront alors conservées pendant toute leur durée d'utilité administrative. Ces durées sont définies dans la circulaire DGP/SIAF/2019/004 du 25 septembre 2019 « Préconisations de sélection relatives aux impacts de la réforme de la prescription en matière pénale ». Dans l'attente du déploiement du SAEH, NPP assure la fonction d'archivage intermédiaire afin de répondre aux exigences légales et réglementaires en la matière. Le cloisonnement sera fonctionnellement effectué par la gestion des accès dans NPP et l'archivage des dossiers clos dans un onglet dédié aux archives intermédiaires. A terme, les données ainsi conservées seront reversées dans le SAEH lors de sa mise en service et supprimées de NPP.

#### **4. Sécurisation informatique des pièces**

Dans NPP, l'authentification pour accéder à l'application s'effectue par un couple identifiant/mot de passe. Cette authentification sera, à terme, remplacée par une identification s'appuyant sur l'Active directory de Windows. Le traitement ne donne accès aux données personnelles qu'aux seules personnes ayant le droit d'en connaître par le biais d'un système d'habilitation. Ces habilitations sont fournies par

---

<sup>4</sup> Dispositions établies conformément aux durées prescrites dans le décret n°2014-472 du 9 mai 2014 pris pour application de l'article 5-2 de l'ordonnance n° 45-174 du 2 février 1945 relative à l'enfance délinquante.

<sup>5</sup> Les durées d'exploitation ont été établies par la DSJ, le DP PPN et le DADP. Cf. fiche pratique DUC.

des administrateurs fonctionnels en région ou au niveau national. Chaque utilisateur habilité dispose ensuite d'un profil spécifique qui permet de restreindre les accès et possibilités d'actions aux seules données autorisées.

L'application NPP est uniquement accessible via le réseau privé de communication informatique du ministère de la justice (RPVJ). Les données enregistrées dans NPP sont hébergées en local sur des serveurs sur sites placés sous la responsabilité des directions de l'information et des télécommunications (DIT) et sécurisés par des pare-feu. L'ensemble des mesures de sécurité locales mises en place pour l'application NPP est décrite dans l'analyse d'impact relative à la protection des données (PIA) « Traitement des dossiers pénaux numériques ». Des audits d'homologation des serveurs et lieux de stockage concernés par la mise en œuvre du programme PPN seront progressivement réalisés par le service du haut fonctionnaire de défense et de sécurité (HFDS) du ministère de la justice. Au niveau national, pour pallier les risques de pertes d'informations, une réplication des données sur un serveur de stockage pénal sécurisé (SPS), propre au ministère de la justice, est en cours de réalisation pour permettre la conservation, dans un premier temps, des documents nativement numériques, puis des documents numérisés.

Le versement des pièces en archivage se fait par la plateforme d'échange (PFE) ministérielle.

Concernant le SAEH Axone, seuls les agents du ministère disposant d'une identité au sein du LDAP (protocole d'accès aux annuaires léger) du ministère peuvent accéder à la solution. En fonction de son profil LDAP, un agent a des accès dédiés aux seules données autorisées et à certaines fonctionnalités de la solution (consultation, versement d'archives, téléchargement, etc.). Le cycle de vie des dossiers et documents issus des procédures pénales conservés dans Axone est géré automatiquement par le système. En fonction des DUA définies dans la circulaire DGP/SIAF/2019/004 du 25 septembre 2019<sup>6</sup>, le système détermine les durées de conservation intermédiaire de chaque type de dossier/document versé dans la solution et propose, à leur terme, un sort final spécifique (élimination, versement dans un service d'archives définitives, etc.).

Le SAEH Axone est hébergé sur des serveurs nationaux.

---

<sup>6</sup> Circulaire Préconisations de sélection relatives aux impacts de la réforme de la prescription en matière pénale.

#### **IV. AUTORISATION ET PROCEDURE D'ELIMINATION DES DOCUMENTS ET DONNEES**

En application des articles L212-3 et R212-14 du code du patrimoine, et du fait :

- du caractère centralisé du système de procédure pénale numérique,
- de la qualité des processus de numérisation et de gestion du cycle de vie des données respectant le cadre réglementaire et normatif et le socle technique prévu par le ministère de la justice
- de la traçabilité et de la transparence des éliminations,

Le service interministériel des archives de France donne au ministère de la justice, par la signature du présent protocole, une autorisation « a priori » pour l'élimination des éléments listés dans le § II. 1 :

- pour la destruction anticipée des archives papier numérisées dans le cadre du programme PPN,
- pour la destruction à l'issue de leur durée d'utilisation administrative des données et documents numériques, conservés dans NPP et dont la destruction est prévue dans le texte de préconisation de sélection DGP/SIAF/2019/003 du 25 septembre 2019 relatif aux impacts de la réforme de la prescription en matière pénale sur les archives des juridictions de l'ordre judiciaire.

La signature de ce protocole par l'administration des archives de France vaut autorisation de destruction de ces documents. Cette autorisation est valable pour une durée d'un an, dans l'attente de la mise en production du SAEH Axone.

Les éliminations sont ensuite mises en œuvre de la manière suivante au sein du ministère de la Justice.

Du fait du caractère centralisé du système de procédure pénale numérique, l'élimination des dossiers conservés pour archivage intermédiaire dans Axone est soumise à l'approbation du chef du DADP. Lorsque la durée d'utilité administrative (DUA) des dossiers arrive à échéance, le système identifie les documents à éliminer et génère une proposition d'élimination. A partir de cette proposition, un bordereau d'élimination est créé qui doit être validé par le chef du DADP. Une fois le bordereau validé, les archives ainsi que les notices descriptives de ces archives sont éliminées.

## **V. MISE EN ŒUVRE ET SUIVI DU PROTOCOLE**

L'exécution du présent protocole est suivie par un comité composé des services centraux du ministère de la justice en charge du suivi du programme PPN (Directeur de programme PPN, chef du DADP) et d'un représentant du SIAF. Les membres du comité de suivi se tiennent mutuellement informés, sans délai, de toute difficulté rencontrée à l'occasion de l'application du présent protocole.

Le comité est particulièrement attentif à la bonne mise en œuvre des règles de numérisation dans les juridictions. Les membres du comité de suivi peuvent être amenés à réaliser des audits de contrôle sur le processus de numérisation des pièces de procédure pénale dans les juridictions, ceci afin de vérifier la conformité des mesures mises en œuvre aux règles énoncées dans le présent protocole. Ces audits peuvent également être menés par les services d'archives départementales, à la demande du comité ou à leur propre initiative pour vérifier la réalité de l'application locale des mesures énoncées dans le § 2. du présent protocole. Ces audits font l'objet de rapports transmis à l'ensemble des membres du comité.

En sus de ces audits, pour des besoins de capitalisation des retours d'expériences, des remontées sont effectuées auprès des services centraux du ministère de la justice et auprès des directions des archives départementales (DAD) sur les anomalies bloquantes et/ou récurrentes constatées au cours du processus de numérisation via le support technique NPP. En outre, des rapports relatifs aux contrôles exercés en interne dans les juridictions sont également adressés aux services centraux du ministère de la justice. Ces rapports sont partagés avec les membres du comité de suivi.

L'autorisation d'élimination sera reconductible chaque année sous les conditions suivantes :

- Réalisation d'un bilan annuel recensant l'évolution du déploiement de PPN, les problèmes détectés, les audits éventuels à mener dans l'année suivante et les modifications apportées au socle technique et aux processus (numérisation, conservation, archivage), l'activité des outils NPP et SAEH, anomalies éventuelles rencontrées en terme d'archivage.
- Information du responsable du contrôle scientifique et technique du ministère de la justice et du SIAF de tout changement dans la procédure de numérisation validée ainsi que de tout incident survenu dans l'application du présent protocole.

- Information par chaque juridiction du directeur des archives départementales en cas d'incident ou de problème majeur survenu localement et affectant le processus de numérisation.

Le non-respect de l'un de ces points ou la découverte lors d'une inspection d'un problème grave peut entraîner l'annulation immédiate de l'autorisation d'élimination accordée. Cette annulation ne sera levée qu'après constatation par un représentant de l'administration des archives de France et membre du comité de suivi, de la mise en œuvre de mesures correctives.

Le présent protocole entre en vigueur le jour de son adoption. Il est révisé à la demande de l'une des parties contractantes ou à chaque modification majeure des principes et mesures décrites ci-dessus. Il est accessible sur le site Intranet du ministère de la justice :

<http://intranet.justice.gouv.fr/site/dsj/dematerialisation-16004/>

<http://intranet.justice.gouv.fr/site/archives/>

Et sur le portail France Archives :

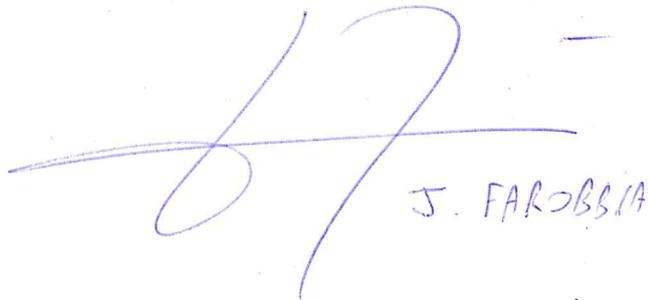
<https://francearchives.fr/fr/card/tableau-circulaires-fr.>

Fait à Paris, le

## SIGNATAIRES

**Le directeur du programme procédure pénale numérique (MJ/SG/DP PPN)**  
Haffide BOULAKRAS

*A/o le directeur et joint*



J. FAROBBIA

**La cheffe du Service interministériel des archives de France (SIAF)**  
Françoise BANAT-BERGER



