Commission nationale de l'informatique et des libertés

Délibération n° 2011-316 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de procédure d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel

NOR : *CNIA1100014X*

La Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment ses articles 11, (3°, *c*) et 13 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération n° 2011-249 du 8 septembre 2011 portant modification de l'article 69 du règlement intérieur de la Commission nationale de l'informatique et des libertés et insérant un chapitre IV *bis* intitulé « Procédure de labellisation » ;

Après avoir entendu M. Jean-François Carrez, commissaire, en son rapport et Mme Elisabeth Rolin, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

L'article 11, (3°, *c*) de la loi du 6 janvier 1978 modifiée dispose qu'*« à la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements, [...la CNIL] délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la [loi du 6 janvier 1978 modifiée] »*.

La commission a estimé que les demandes faites par des organisations professionnelles ou institutions regroupant principalement des responsables de traitements correspondent à un besoin des professionnels de ce secteur.

C'est la raison pour laquelle la commission accepte de délivrer des labels en matière d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel.

L'article 53-3 du règlement intérieur de la commission précise que *« l'examen d'une demande de label est effectué sur la base d'un référentiel établi par la commission. Ce référentiel définit les caractéristiques que doit présenter un produit ou une procédure afin que celui-ci soit reconnu conforme aux dispositions de la loi du 6 janvier 1978 modifiée. Il précise les modalités d'appréciation de cette conformité et, le cas échéant, les particularités relatives aux vérifications subséquentes à la délivrance du label »*.

Par conséquent, la présente délibération fixe le référentiel d'évaluation des procédures d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel.

Décide que le référentiel permettant l'évaluation des demandes de labels relatifs à des procédures d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel figure en annexe de la présente délibération, qui est publiée au *Journal officiel* de la République française.

Pour la présidente :
Le vice-président délégué,
E. DE GIVRY

ANNEXE

RÉFÉRENTIEL AUX FINS DE LABELLISATION DES PROCÉDURES D'AUDIT DE CONFORMITÉ DE TRAITEMENTS

Introduction

Un audit « Informatique et libertés » est un audit dont les critères permettent de juger de la conformité de traitements de données à caractère personnel à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

Le champ d'un tel audit concerne les traitements de données à caractère personnel mis en œuvre dans un périmètre délimité, non seulement en termes de lieux, d'unités organisationnelles, d'activités, de processus ou de période de temps couverte, mais aussi en termes de types de traitements ou de traitements particuliers.

La procédure d'audit décrit le déroulement, la gestion et le contenu des audits, tel qu'ils sont mis en œuvre par le requérant. La terminologie complète est présentée dans les pages suivantes.

A cet effet, le présent référentiel définit les critères d'évaluation :

– portant sur la manière de conduire un audit (exigences sur la méthode, notées « EMxx » dans le chapitre Ier) ;
– portant sur les éléments à contrôler concernant les traitements de données à caractère personnel pendant l'audit (exigences sur le contenu, notées « ECxx » dans le chapitre II).

Une partie de ce référentiel (chapitre Ier) a été élaborée par la commission à partir des exigences de la norme NF ISO 19011 (Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental, 2002) et en les adaptant au contexte spécifique des audits « Informatique et libertés ». Seul le texte original et complet de la norme NF ISO 19011, telle que diffusée par AFNOR et accessible via le site internet www.afnor.org, a valeur normative en tant que norme industrielle.

Pour être valable, la démonstration de l'organisme sollicitant le label de la CNIL ne devra pas se contenter de reprendre le contenu des exigences pour indiquer que la procédure d'audit soumise à l'évaluation est conforme à celles-ci. Elle devra décrire la manière dont sa procédure d'audit y répond de manière spécifique, en fournissant des explications et des éléments de preuve tels que :

– un extrait pertinent du référentiel interne d'audit ;
– des exemples de questionnaires ou de scénarios d'entretiens utilisés ;
– un descriptif d'une méthode ou d'une procédure ;
– un descriptif de logiciel d'aide à la décision ou de tout autre système expert informatisé ;
– des copies d'écran illustrant des contrôles informatiques ou organisationnels ;
– tout autre élément documenté à disposition des auditeurs appliquant la procédure d'audit.

Terminologie

Audit	Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits (d'après NF ISO 19011). Note. – Lorsque deux ou plusieurs organismes d'audit coopèrent pour auditer un seul audité, on parle d'audit conjoint.
Audité	Organisme qui est audité (NF ISO 19011).
Auditeur	Personne possédant la compétence nécessaire pour réaliser un audit (NF ISO 19011).
Champ d'audit	Etendue et limites d'un audit (NF ISO 19011). Note. – Le champ décrit généralement les lieux, les unités organisationnelles, les activités et les processus ainsi que la période de temps couverte.
Commanditaire de l'audit	Organisme ou personne demandant un audit (NF ISO 19011). Note. – Le commanditaire peut être l'audité ou tout autre organisme qui a le droit réglementaire ou contractuel de demander un audit.
Compétence	Qualités personnelles et capacité démontrées à appliquer des connaissances et des aptitudes (NF ISO 19011).
Conclusions d'audit	Résultat d'un audit fourni par l'équipe d'audit après avoir pris en considération les objectifs de l'audit et tous les constats d'audit (NF ISO 19011).
Constats d'audit	Résultats de l'évaluation des preuves d'audit recueillies, par rapport aux critères d'audit (NF ISO 19011). Note. – Les constats d'audit peuvent indiquer la conformité ou la non-conformité aux critères d'audit ou des opportunités d'amélioration.
Critères d'audit	Ensemble de politiques, procédures ou exigences déterminées (NF ISO 19011). Note 1. – Les critères d'audit sont la référence vis-à-vis de laquelle les preuves d'audit sont comparées. Note 2. – En français, les critères d'audit sont couramment appelés référentiel d'audit.
Equipe d'audit	Un ou plusieurs auditeurs réalisant un audit, assistés, si nécessaire, par des experts techniques (NF ISO 19011). Note 1. – Un auditeur de l'équipe d'audit est nommé responsable de l'équipe d'audit. Note 2. – L'équipe d'audit peut comprendre des auditeurs en formation.
Expert technique	Personne apportant à l'équipe d'audit des connaissances ou une expertise spécifiques (NF ISO 19011). Note 1. – Ces connaissances ou cette expertise spécifiques sont relatives à l'organisme, au processus ou à l'activité à auditer, ou elles consistent en une assistance linguistique ou culturelle. Note 2. – Au sein de l'équipe d'audit, un expert technique n'agit pas en tant qu'auditeur.

Plan d'audit	Description des activités et des dispositions nécessaires pour réaliser un audit (NF ISO 19011).
Preuves d'audit	Enregistrements, énoncés de faits ou autres informations, qui se rapportent aux critères d'audit et sont vérifiables. (NF ISO 19011). Note. – Les preuves d'audit peuvent être qualitatives ou quantitatives.
Procédure d'audit	Description de l'ensemble du processus de gestion des audits mise en œuvre par le requérant.
Programme d'audit	Ensemble d'un ou plusieurs audits planifiés dans un laps de temps et dans un but déterminés. (NF ISO 19011). Note. – Un programme d'audit comprend toutes les activités nécessaires pour la planification, l'organisation et la réalisation des audits.
Rapport d'audit	Document réalisé par l'équipe d'audit et remis à l'audité, qui fournit un enregistrement complet, concis, précis et clair de l'audit.

1. **Référentiel d'évaluation de la méthode des audits de conformité de traitements**

1.1. *Exigences relatives aux principes à respecter*

EM01. Le requérant a mis en place une démarche visant à s'assurer de la conformité à la loi Informatique et libertés de l'ensemble des traitements qu'il met en œuvre pour l'ensemble de ses activités, dont l'audit.

EM02. La procédure d'audit comprend l'engagement que les auditeurs respectent les principes de déontologie, de présentation impartiale des résultats, de conscience professionnelle, d'indépendance et d'approche systématique.

1.2. *Exigences relatives à tous les auditeurs*

EM03. La procédure d'audit permet d'assurer que les auditeurs ont une expérience professionnelle de cinq ans au minimum.

EM04. La procédure d'audit permet d'assurer que les auditeurs ont suivi une formation à la méthodologie d'audit (principes, procédures et techniques d'audit, documents relatifs à l'audit, lois, réglementations et autres exigences applicables pertinentes pour la discipline...) de vingt heures au minimum.

EM05. La procédure d'audit permet d'assurer que les auditeurs ont participé à deux audits au minimum, depuis leur déclenchement jusqu'à leur clôture, dans les deux dernières années.

EM06. La procédure d'audit permet d'assurer que les auditeurs ont vingt jours d'expérience d'audit au minimum.

EM07. La procédure d'audit permet d'assurer que les auditeurs continuent à se perfectionner professionnellement.

EM08. La procédure d'audit permet d'assurer que les auditeurs sont évalués selon des critères et des méthodes définies dans le cadre de chaque audit et que les auditeurs qui ne satisfont pas à ces critères complètent leur formation ou leur expérience.

1.3. *Exigences relatives aux responsables d'équipe d'audit*

EM09. La procédure d'audit permet d'assurer que les responsables d'équipe d'audit ont participé à trois audits au minimum, depuis leur déclenchement jusqu'à leur clôture, dans les deux dernières années.

EM10. La procédure d'audit permet d'assurer que les responsables d'équipe d'audit ont quinze jours d'expérience d'audit au minimum en tant que responsable d'équipe d'audit.

1.4. *Exigences relatives aux auditeurs « juridiques »*

EM11. La procédure d'audit permet d'assurer que les auditeurs « juridiques » ont obtenu un diplôme de master 1 ou équivalent dans le secteur du droit au minimum.

EM12. La procédure d'audit permet d'assurer que les auditeurs « juridiques » ont une expérience de deux ans au minimum dans le domaine Informatique et libertés (exemple : conseil, contentieux, accomplissement de formalités préalables...).

1.5. *Exigences relatives aux auditeurs « techniques »*

EM13. La procédure d'audit permet d'assurer que les auditeurs « techniques » ont obtenu un diplôme de master 1 ou équivalent dans le domaine de l'informatique ou des systèmes d'information au minimum.

EM14. La procédure d'audit permet d'assurer que les auditeurs « techniques » ont suivi une formation sur les référentiels utiles au management de la sécurité des systèmes d'information (réglementation, normes, méthodes, bonnes pratiques, gestion des risques...) de deux jours au minimum.

EM15. La procédure d'audit permet de s'assurer que les auditeurs « techniques » ont suivi une formation dans le domaine Informatique et libertés.

EM16. La procédure d'audit permet d'assurer que les auditeurs « techniques » ont suivi une formation d'audit de sécurité technique (intrusion, investigation, détection de vulnérabilités techniques...) de deux jours au minimum.

EM17. La procédure d'audit permet d'assurer que les auditeurs « techniques » ont une expérience de trois ans au minimum dans le domaine de la sécurité des systèmes d'information.

1.6. *Exigences relatives à la préparation des audits*

EM18. La procédure d'audit permet d'assurer que les responsabilités de chacun, les objectifs, le champ, les critères et le déroulement de l'audit sont définis avec le commanditaire en tenant compte des éventuels audits préalablement réalisés.

EM19. La procédure d'audit permet d'assurer que la faisabilité de l'audit est étudiée et que les actions nécessaires sont prises en fonction de cette étude.

EM20. La procédure d'audit permet d'assurer que l'équipe d'audit est constituée en fonction des compétences « juridiques » et « techniques » nécessaires pour atteindre les objectifs de l'audit et dans le respect des principes relatifs aux auditeurs.

EM21. La procédure d'audit prévoit l'insertion d'une clause particulière dans le contrat établi entre le prestataire et le commanditaire de l'audit, afin de garantir la confidentialité des données à caractère personnel qui pourraient, le cas échéant, être portées à la connaissance du prestataire dans le cadre de l'audit.

EM22. La procédure d'audit permet d'assurer que la documentation examinée par l'auditeur est consultée dans les locaux de l'audité ou est anonymisée si elle est consultée hors des locaux de l'audité. Ce principe est inscrit dans la clause de confidentialité établie entre le prestataire et le commanditaire de l'audit.

EM23. La procédure d'audit permet d'assurer que la documentation examinée par l'auditeur est adéquate pour réaliser l'audit et que le commanditaire de l'audit en est informé si ce n'est pas le cas. Pour qu'elle soit adéquate, elle comprend notamment les critères et les conclusions des éventuels audits préalablement réalisés, ainsi que les politiques internes relatives à la protection des données à caractère personnel, dans le champ de l'audit.

EM24. La procédure d'audit permet d'assurer que les instruments de recueil d'informations qui seront employés par l'équipe d'audit (questionnaires, guides d'entretien, logiciel d'analyse...) sont pertinents au regard des vérifications prévues et qu'ils sont éprouvés (des tests préliminaires ont été réalisés, des utilisations antérieures ont démontré leur justesse...).

EM25. La procédure d'audit permet d'assurer que les échantillonnages réalisés (personnes interrogées, vérifications effectuées, données contrôlées...) sont suffisamment représentatifs.

EM26. La procédure d'audit permet d'assurer que le plan d'audit, la manière dont les actions d'audit seront menées et les circuits de communication sont validés avec les responsables des activités du champ de l'audit et leurs questions traitées.

EM27. La procédure d'audit permet d'assurer que le responsable de l'équipe d'audit élabore un plan d'audit validé par le commanditaire de l'audit. Ce plan d'audit contient notamment les objectifs de l'audit, les critères d'audit, les documents de référence, le champ d'audit, les dates, lieux, horaires et durée d'audit sur site, les rôles et responsabilités ainsi que la mise à disposition des ressources appropriées et, éventuellement, les objections de l'audité. Les critères d'audit tiennent compte des audits préalablement réalisés et des politiques internes relatives à la protection des données à caractère personnel.

1.7. *Exigences relatives à la réalisation des audits*

EM28. La procédure d'audit permet d'assurer que l'accès et l'utilisation de données à caractère personnel nécessitant une habilitation particulière sont réservés aux personnes dûment habilitées à le faire, et ce dans le respect de la loi et de la réglementation. Ce principe est inscrit dans le contrat établi entre le prestataire et le commanditaire de l'audit.

EM29. La procédure d'audit permet de vérifier que seules les personnes disposant d'une habilitation particulière ont effectivement accès aux données et peuvent les utiliser.

EM30. La procédure d'audit permet d'assurer que l'audité, et, si nécessaire, le commanditaire de l'audit, est informé de l'avancement et de toute difficulté rencontrée de manière régulière.

EM31. La procédure d'audit permet d'assurer que les preuves d'audit sont constituées à partir d'une vérification « juridique » et « technique » des informations recueillies et consignées.

EM32. La procédure d'audit permet d'assurer que les données à caractère personnel collectées en tant que preuve sont soit anonymisées, soit uniquement consultables au sein des locaux de l'audité, tout en étant conservées de manière à assurer leur confidentialité. Ce principe est inscrit dans la clause de confidentialité établie entre le prestataire et le commanditaire de l'audit.

EM33. La procédure d'audit permet d'assurer que les constats d'audit sont élaborés en évaluant la conformité des preuves d'audit par rapport aux critères d'audit.

EM34. La procédure d'audit permet d'assurer que l'équipe d'audit prépare les conclusions d'audit sur la base des constats d'audit.

EM35. La procédure d'audit permet d'assurer que les preuves, les constats et les conclusions d'audit sont présentés à l'audité afin de vérifier sa compréhension et de faire reconnaître les preuves comme exactes et que toute divergence d'opinion subsistant à l'issue de la discussion est consignée.

1.8. *Exigences relatives à la finalisation des audits*

EM36. La procédure d'audit permet d'assurer que le rapport d'audit fournit un enregistrement complet, concis, précis et clair de l'audit (contenant au minimum : date du rapport d'audit, objectifs de l'audit, champ d'audit, commanditaire de l'audit, équipe d'audit, dates et lieux des activités d'audit sur site, critères d'audit, constats d'audit et conclusions d'audit), est émis dans les délais convenus à moins qu'une nouvelle date d'émission ne soit fixée, est approuvé selon la procédure retenue et est diffusé aux destinataires identifiés par le commanditaire de l'audit.

EM37. La procédure d'audit permet d'assurer que les documents relatifs à l'audit (documentation fournie, plan d'audit, preuves d'audit, rapport d'audit...) sont conservés de manière à préserver leur confidentialité ou détruits de manière définitive et sécurisée s'ils ne sont plus utiles à l'issue de l'audit.

2. **Référentiel d'évaluation du contenu des audits de conformité de traitements**

2.1. *Exigences relatives aux bases de connaissances utilisées*

EC01. La procédure d'audit s'appuie sur une base de connaissances en conformité avec les réglementations françaises et communautaires. Les recommandations d'interprétation au niveau français et européen peuvent également être prises en compte.

EC02. La procédure d'audit s'appuie sur une base de connaissances reflétant l'état de l'art en matière de sécurité des systèmes d'information et dispose d'une méthode permettant de la mettre à jour régulièrement.

2.2. *Exigences relatives à l'organisme audité*

EC03. La procédure d'audit dispose d'une méthode permettant d'identifier la structure organisationnelle de l'organisme audité, les systèmes d'information, les flux d'information concernés et les normes juridiques spécifiques dans le champ de l'audit.

EC04. La procédure d'audit permet d'apprécier l'existence et l'efficacité de l'organisation et de la documentation pour gérer les traitements de données à caractère personnel dans le champ de l'audit.

EC05. La procédure d'audit permet d'apprécier, dans le cas où l'audité dispose d'un correspondant Informatique et libertés (CIL), les moyens qui lui sont accordés pour réaliser sa mission et le bilan de celle-ci.

2.3. *Exigences relatives à l'identification des traitements*

EC06. La procédure d'audit décrit un processus méthodologique d'énumération de tous les traitements identifiés à l'intérieur du champ de l'audit.

EC07. La procédure d'audit contient un processus de détection des traitements éventuellement non identifiés par le responsable de traitement au sein du champ de l'audit.

EC08. La procédure d'audit permet d'identifier les recours éventuels à des prestataires extérieurs.

EC09. La procédure d'audit permet d'identifier et de catégoriser l'ensemble des données à caractère personnel utilisées dans les traitements inclus dans le champ de l'audit.

EC10. La procédure d'audit permet de caractériser la responsabilité de l'organisme audité au regard des traitements au sein du champ de l'audit, en déterminant notamment si l'organisme est responsable de traitement ou sous-traitant au sens de la loi Informatique et libertés.

EC11. La procédure d'audit permet de déterminer la loi nationale de protection des données applicable à chaque traitement se trouvant dans le champ de l'audit.

EC12. La procédure d'audit contient une approche méthodologique pour réaliser un bilan des formalités préalables ou des éléments portés dans le registre du CIL, le cas échéant permettant de vérifier leur exhaustivité et leur exactitude.

2.4. *Exigences relatives à l'appréciation de la licéité des traitements*

EC13. La procédure d'audit permet d'obtenir une description exacte des finalités des traitements inclus dans le champ de l'audit.

EC14. La procédure d'audit permet d'apprécier le fondement légal de chaque traitement inclus dans le champ de l'audit.

EC15. La procédure d'audit comprend une démarche particulière pour déterminer si les données à caractère personnel des traitements inclus dans le champ de l'audit sont pertinentes, adéquates et non excessive au regard des finalités identifiées.

EC16. La procédure d'audit permet d'évaluer si les données à caractère personnel utilisées sont toutes nécessaires au regard de la finalité recherchée et si certaines d'entres elles pourraient être partiellement ou totalement anonymisées tout en permettant d'atteindre la finalité désirée.

EC17. La procédure d'audit permet d'évaluer la qualité de la méthode de recueil des données à caractère personnel auprès de personnes concernées, notamment pour apprécier son caractère loyal et licite.

EC18. La procédure d'audit permet de s'assurer que les traitements confiés à des prestataires font l'objet d'un contrat de prestation de service.

EC19. La procédure d'audit permet de s'assurer que les contrats de prestation de services contiennent des dispositions relatives aux mesures de sécurité et des instructions claires données par le responsable de traitement à son prestataire.

EC20. La procédure d'audit dispose d'une méthode d'identification des flux de données hors de l'Union européenne.

EC21. La procédure d'audit permet de vérifier l'existence et la conformité des instruments juridiques permettant d'encadrer les transferts hors de l'Union européenne.

2.5. *Exigences relatives à l'étude des personnes accédant aux données*

EC22. La procédure d'audit dispose d'une méthode permettant de recenser et de catégoriser l'ensemble des personnes qui, en raison de leurs fonctions, sont chargées de traiter les données à caractère personnel qui sont inclues dans le champ de l'audit.

EC23. La procédure d'audit permet d'évaluer la politique d'habilitation appliquée à chaque personne ayant un accès légitime aux données identifiées, au regard du principe de limitation des accès au besoin d'en connaître.

2.6. *Exigences relatives à l'analyse des durées de conservation*

EC24. La procédure d'audit comprend une démarche particulière pour recenser les durées de conservation des données à caractère personnel utilisées.

EC25. La procédure d'audit comprend une démarche particulière pour déterminer si les durées de conservation sont adéquates.

EC26. La procédure d'audit prévoit des contrôles pertinents sur les systèmes d'information par des auditeurs « techniques » afin de vérifier si les durées de conservation appliquées sont conformes aux durées prévues.

EC27. La procédure d'audit prévoit des contrôles afin de vérifier que les données font l'objet d'une suppression effective à l'expiration de leur durée de conservation.

EC28. La procédure d'audit examine également la politique d'archivage des données à caractère personnel, le cas échéant, au regard des recommandations de la CNIL en la matière.

2.7. *Exigences relatives à l'étude de la sécurité*

EC29. La procédure d'audit permet d'analyser et d'évaluer la démarche mise en œuvre par les responsables de traitement pour assurer la confidentialité, l'intégrité et la disponibilité des données à caractère personnel entrant dans le champ de l'audit.

EC30. La procédure d'audit comprend une démarche particulière pour identifier les principaux risques que les traitements dans le champ de l'audit font peser sur les libertés et la vie privée des personnes concernées en cas d'atteinte à la sécurité des données à caractère personnel, en tenant compte des éventuels sous-traitants. Cette démarche permet notamment d'estimer ces risques en termes de gravité et de vraisemblance.

EC31. La procédure d'audit comprend une démarche particulière pour identifier les mesures de sécurité mises en œuvre et pour évaluer leur pertinence vis-à-vis des risques identifiés et estimés, notamment pour gérer les incidents de sécurité liés aux données à caractère personnel.

EC32. La procédure d'audit permet de déterminer si les mesures de sécurité identifiées sont correctement mises en œuvre et s'appuie sur des vérifications adéquates effectuées sur les systèmes d'information, réalisées par des auditeurs « techniques ».

2.8. *Exigences relatives à l'étude du respect des droits des personnes*

EC33. La procédure d'audit permet de vérifier que les personnes concernées disposent d'un droit d'accès, de rectification et, le cas échéant, d'un droit d'opposition.

EC34. La procédure d'audit permet de contrôler que les droits des personnes peuvent être exercés de manière effective et dans des délais raisonnables.

EC35. La procédure d'audit permet de vérifier que les personnes disposent d'une information correcte, accessible et claire sur leurs droits, ainsi que sur les autres éléments d'information prévus par la loi.

2.9. *Exigences relatives à l'étude des traitements particuliers*

EC36. La procédure d'audit permet de déterminer le régime juridique dont relèvent les traitements au sein du champ de l'audit et d'étudier la conformité aux dispositions particulières afférentes en matière de protection des données à caractère personnel, notamment :

– l'utilisation de données sensibles ;

– les traitements portant sur des données génétiques, les traitements portant sur des infractions, les traitements d'exclusion, les interconnexions, les traitements utilisant le NIR, les traitements portant une appréciation sur les difficultés sociales des personnes, les traitements biométriques ;

– les traitements du monde de la santé (recherche et évaluation des pratiques) ;

– les traitements aux fins de journalisme et d'expression littéraire et artistique ;

– les traitements mettant en œuvre un processus d'anonymisation ;

– les traitements mis en œuvre par l'Etat.