PROTECTION SOCIALE

SÉCURITÉ SOCIALE : ORGANISATION, FINANCEMENT

MINISTÈRE DU TRAVAIL,
DE L'EMPLOI ET DE LA SANTÉ

MINISTÈRE DU BUDGET,
DES COMPTES PUBLICS,
DE LA FONCTION PUBLIQUE
ET DE LA RÉFORME DE L'ÉTAT

MINISTÈRE DES SOLIDARITÉS
ET DE LA COHÉSION SOCIALE

Direction de la sécurité sociale

Circulaire DSS-4C n° 2011-273 du 7 juillet 2011 relative aux règles communes d'organisation des échanges électroniques dans le cadre de l'activité des organismes de protection sociale

NOR : *ETSS1118996C*

Date d'application : immédiate.

Résumé : règles d'organisation des échanges électroniques entre organismes de sécurité sociale et avec les assurés ainsi que procédures de contrôles mises en œuvre pour garantir leur qualité.

Mots clés : dématérialisation – sécurité – interopérabilité – validité des données – téléservice – audit – contrôle.

Références :

Loi n° 78-17 du 6 janvier 1978 ;

Ordonnance n° 2005-1516 du 8 décembre 2005.

Le ministre du travail, de l'emploi et de la santé à Monsieur le directeur de la Caisse nationale de l'assurance maladie des travailleurs salariés ; Monsieur le directeur de la Caisse nationale d'allocations familiales ; Monsieur le directeur de la Caisse nationale d'assurance vieillesse des travailleurs salariés ; Monsieur le directeur de l'Agence centrale des organismes de sécurité sociale ; Monsieur le directeur de la Mutualité sociale agricole ; Monsieur le directeur du régime social des indépendants ; Monsieur le directeur de Pôle emploi (pour attribution).

Dans le cadre de leurs activités et de leurs missions, les organismes de protection sociale ont besoin de partager des informations, d'accéder aux systèmes d'information de leurs partenaires et d'interagir avec les usagers qui effectuent en ligne des démarches administratives.

Ces objectifs s'inscrivent dans une démarche commune visant à :

– améliorer le service rendu à l'usager par la simplification des démarches administratives ;
– sécuriser les échanges dématérialisés afin de les rendre le plus fiable possible ;
– faciliter le contrôle et la lutte contre la fraude ;
– répondre aux attentes en matière de développement durable.

Ces échanges sont effectués dans le respect des dispositions 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 et ses textes d'application, ainsi que dans le respect des dispositions de la loi du 6 janvier 1978 modifiée, dite informatique et libertés.

L'ordonnance n° 2005-1516 du 8 décembre 2005 pose le cadre juridique général de ces échanges, qui correspond à :

– la réaffirmation de la valeur juridique du courrier électronique pour une demande d'information (art. 2) et de la régularité d'une demande adressée à une administration par voie électronique (art. 3) ;
– la possibilité d'échanger des informations personnelles avec l'accord exprès de la personne concernée (art. 6) ;
– la création d'un espace personnel de stockage (art. 7) ;

– la reconnaissance d'une signature électronique spécifique pour les actes administratifs des autorités administratives (art. 8) ;
– la mise en place de deux référentiels : l'un concernant la sécurité (RGS – art. 9) et l'autre concernant l'interopérabilité (RGI – art. 11).

Dans ce cadre, la présente circulaire a vocation à :
– s'appliquer à l'ensemble des organismes de protection sociale ;
– décrire les règles applicables à la dématérialisation des données et documents reçus et échangés dans le cadre des activités de ces organismes, la dématérialisation étant entendue comme la gestion des données et documents sous forme électronique.

Ces données et documents dématérialisés transitent notamment :
– au sein des administrations et organismes de protection sociale ;
– entre ces derniers et leurs usagers ;
– à l'occasion d'échanges entre administrations et organismes de protection sociale.

En outre, la mise en œuvre de la dématérialisation implique pour une majorité d'opérations le traitement de données à caractère personnel. À ce titre, afin d'assurer la confidentialité et la protection desdites données, les traitements concernés devront satisfaire aux formalités prévues par la loi n° 78-17 du 6 janvier 1978 modifiée.

La présente circulaire a pour objet de fixer les conditions de mise en œuvre des échanges dématérialisés entre les organismes de protection sociale, d'une part, (1) et des échanges dématérialisés entre les usagers et les organismes de protection sociale, d'autre part (2).

Elle prévoit également les modalités propres aux garanties de la fiabilité des données échangées et au contrôle (audit et contrôle interne) mis en place afin de maîtriser les risques inhérents aux échanges (3).

Les échanges d'informations dématérialisées portent en priorité sur des données. Néanmoins, pour les cas où seules des images de documents pourraient être transmises, et notamment dans une phase de transition, les conditions dans lesquelles les organismes peuvent valablement échanger des documents numérisés sont également précisées dans cette circulaire.

1. **Les conditions de mise en œuvre des échanges dématérialisés entre les organismes de protection sociale**

Concernant la mise en œuvre des échanges dématérialisés entre les organismes de protection sociale, la présente circulaire s'applique :
– aux échanges dématérialisés entre les organismes de la sphère sociale par voie de fichiers électroniques (dits « échanges de fichiers » ou « batch ») ;
– aux échanges dématérialisés entre les organismes de protection sociale dans le cadre des webservices, en utilisant un standard d'interopérabilité (Interops).

1.1. *Les échanges de fichiers*

1.1.1. Sécurité des échanges

Les organismes qui procèdent à des échanges de fichiers par voie électronique doivent respecter des procédures et mesures de sécurité leur permettant de mettre en œuvre et de maintenir l'environnement technique opérationnel approprié à la sécurité de ces échanges, conformément au référentiel général de sécurité (RGS, approuvé par arrêté du 6 mai 2010 publié le 18 mai 2010) et aux politiques de sécurité des systèmes d'information (PSSI) définies par chaque organisme, afin d'assurer, notamment, la protection des données transmises ou consultées, contre les risques d'accès non autorisés, de modification, de destruction ou de perte des données y figurant.

Dans ce cadre, des exigences minimales communes de sécurité sont établies de façon mutualisée entre les organismes ayant des besoins communs.

L'utilisation du chiffrement est gérée en fonction :
– de la sensibilité des données (données de santé, numéro de sécurité sociale...) conformément à l'état de l'art ;
– de la qualité du réseau utilisé.

Ces procédures et mesures de sécurité (y compris la gestion des habilitations) devront être également respectées lorsqu'un agent d'un organisme est amené à alimenter le système d'information d'un autre organisme en intégrant des données, notamment par le biais d'un portail.

1.1.2. Traçabilité des échanges

L'organisme qui reçoit le fichier est tenu de ne le conserver que le temps nécessaire à son exploitation complète.

Il appartient à l'organisme émetteur de conserver les données contenues dans ledit fichier, notamment aux fins éventuelles de preuve, selon les textes qui lui sont applicables.

Toutes les traces des échanges doivent être conservées par les deux organismes concernés afin de répondre aux exigences de sécurité nécessaires à leur mise en œuvre.

Les conditions de conservation des traces s'appliqueront aux domaines suivants :

Les traces liées à la gestion de l'échange du fichier

Une trace de la gestion de l'échange réalisé avec un organisme doit être conservée dans un référentiel d'historique et de suivi des échanges de fichiers. Cela concerne les éléments de traces de prise en compte du fichier (notamment traces de réception, d'exploitation, de notification d'exploitation du fichier adressées à l'autre organisme). Les actions menées sur le fichier sont historisées par l'organisme qui a reçu le fichier.

Les traces liées à la gestion de l'échange du fichier sont historisées sur une durée qui sera définie contractuellement entre les deux organismes qui échangent. Ce délai de conservation est fixé dans le respect des dispositions de la loi nº 78-17 du 6 janvier 1978.

Cas particulier : les traces liées à l'alimentation (saisie de données) via *le portail d'un organisme*

Toute activité réalisée par l'agent d'un organisme sur un portail doit être techniquement et fonctionnellement tracée dans un système adapté.

1.1.3. La gestion des dates dans le cadre des échanges de fichiers

La date de réception du fichier par l'organisme ou l'administration récepteur est tracée dans l'historique des échanges.

1.2. *Les échanges par webservices*

Un webservice correspond à une technologie permettant à des applications de dialoguer/de communiquer à distance, en s'appuyant sur un ensemble de protocoles d'échanges standards (notamment XML, http).

Pour communiquer par le biais de webservices et répondre de façon pérenne aux préoccupations énoncées au présent préambule, les organismes de protection sociale utilisent le standard d'interopérabilité, appelé standard Interops, qui a été défini par lesdits organismes de protection sociale.

Ce standard Interops a vocation à être utilisé par tous les organismes de protection sociale pour échanger en temps réel des informations de manière sécurisée.

Les principes suivants sont retenus pour la mise en place de ce standard :

– la création d'un cercle de confiance entre les organismes ;
– l'authentification de l'utilisateur réalisée par l'organisme client ;
– l'attribution de l'habilitation par l'organisme client à ses agents selon les règles établies avec l'organisme fournisseur au moyen d'une convention propre à chaque échange ;
– la transmission de l'habilitation, de manière sécurisée, à l'organisme fournisseur par un vecteur d'identification ;
– toute création d'un vecteur d'identification est tracée afin d'en permettre le contrôle *a posteriori*.

Les conditions de sécurité et de traçabilité mises en place et fixées entre les organismes dans le cadre du standard Interops sont les suivantes :

1.2.1. Sécurité

Concernant les aspects relatifs à la sécurité physique

Les organismes qui utilisent le standard Interops doivent :

– mettre en œuvre et maintenir respectivement des procédures et des mesures de sécurité afin d'assurer la protection de leurs matériels, de leurs locaux, et de leurs services ;
– respectivement mettre en œuvre et maintenir des procédures et des mesures de sécurité afin d'assurer la protection des accès aux services proposés contre les risques d'accès non autorisés, de modification, de destruction de perte de données y figurant.

Les modalités d'interconnexion des réseaux utilisés se conforment aux règles définies lors de la contractualisation entre les organismes.

Concernant les aspects relatifs à la sécurité logique

1. La gestion des habilitations

Les agents ou applications habilités à accéder aux services et applications sont désignés par l'organisme client dans des conditions prévues contractuellement qui détaillent notamment les modalités procédurales techniques et de sécurité d'utilisation.

L'organisme client transmet au fournisseur l'habilitation de l'agent ou de l'application devant accéder au service, au moyen du vecteur d'identification (notamment clé d'accès) défini dans le cadre des travaux sur le standard Interops.

Il appartient à l'organisme client de s'assurer :

– que les services offerts par l'organisme fournisseur dans le cadre du standard Interops ne soient accessibles à ses agents et/ou à ses applications clientes qu'après vérification formelle de leur identité et de leur habilitation ;

– que ses agents ou ses applications n'utilisent les services offerts que conformément à l'habilitation qui leur a été donnée et à leurs missions.

2. La gestion des certificats dans le cadre du standard Interops

Les organismes utilisent des certificats générés par une infrastructure de gestion de clés validée par eux.

1.2.2. La traçabilité des échanges

Les traces concernées sont les traces de connexion et les traces de constitution du vecteur d'identification telles que définies dans les spécifications détaillées propres au standard Interops.

Les organismes qui échangent définiront et préciseront le contenu des traces souhaité.

Toute interruption du service de trace du côté de l'organisme fournisseur induit l'arrêt des services concernés. L'organisme client ne devra pas accéder aux services concernés en cas d'interruption de son service de trace.

Le standard Interops exige le respect des conditions de conservation des traces définies ci-après :

– l'accès aux traces doit être limité à des personnes spécifiquement habilitées à consulter ce type d'informations ;
– les dispositifs physiques et méthodes logiques doivent garantir leur intégrité, y compris lors d'un changement de support ;
– pendant le délai de conservation défini par les organismes, le mode de conservation des traces doit garantir leur communication en moins de quinze jours calendaires selon le format d'échange pivot d'Interops.

Les traces sont conservées pendant un délai défini par les organismes. Si pendant la durée du délai défini un incident était identifié, les traces propres à cet incident devront être conservées le temps nécessaire à l'investigation en vue d'éventuelles poursuites pénales ou civiles avec la même disponibilité.

1.3. *Validité des données échangées par fichiers ou webservices*

Dès lors que les conditions énoncées aux points 1.1, 1.2 et 3 sont respectées par les organismes, les données transmises sont réputées valides au jour de leur transmission pour les traitements propres à leur activité et à l'intégration éventuelle dans leur système d'information.

1.4. *Formalisation des échanges par voie contractuelle*

Tout échange de données doit donner lieu à une procédure de contractualisation entre les administrations et organismes de protection sociale concernés.

Les documents contractuels (convention et annexes associées) prévoiront au minimum les clauses suivantes :

– l'objet de la convention ;
– les données échangées ou transférées (notamment la nature et le format des données, les états et dates d'état des données) ;
– les modalités de l'échange ou du transfert : le support échangé ou transféré, l'engagement des parties en termes de sécurité, la gestion des traces, les aspects techniques (notamment les moyens et règles d'échange ou de transfert des fichiers, interlocuteurs, plage d'ouverture, procédure de secours, périodicité des échanges ou transferts, sécurité, traçabilité, traitement des incidents) ;
– les garanties et contrôles, prévus au point 3 de la présente circulaire, mis en œuvre entre les partenaires pour maîtriser les risques inhérents aux échanges des données, l'utilisation des données, la confidentialité et la protection des données échangées ;
– le suivi et à la gestion de la convention.

1.5. *Échange de documents numérisés*

Dans les cas où seules des images de documents pourraient être transmis, et notamment dans une phase de transition, des échanges de documents numérisés peuvent être opérés entre organismes et avec les usagers, dans le respect des conditions prévues par l'article 1316-1 du code civil pour établir l'équivalence des supports papier et électronique. L'écrit sur support électronique a la même valeur que l'écrit sur support papier à deux conditions :

– que la personne dont il émane soit dûment identifiée ;
– que le document soit établi, transmis et conservé dans des conditions de nature à en garantir l'intégrité.

En outre, conformément à l'article 1334 du code civil, une copie sur support électronique pourra être acceptée par les organismes, à la condition que l'original puisse être présenté sur demande.

Toutefois, en application de l'article 1348 du code civil, dans le cas où le document original n'aurait pas été conservé, la copie (papier ou électronique) pourra servir de preuve à la place de l'original, à la double condition qu'elle en soit la reproduction fidèle et durable.

Les règles prévues aux 1 et 2 de la présente circulaire sont également applicables aux échanges de documents numérisés. Ainsi, à l'instar des échanges portant sur les données, ces échanges de documents entre organismes peuvent s'opérer sous la forme de fichiers ou de webservices, dans le respect des conditions décrites au 1 de la présente circulaire.

Les organismes sont invités, dès lors que des documents porteurs de données qui émanent de l'un des organismes sont échangés entre eux, à prévoir le passage de l'échange de documents numérisés vers un échange de données, dans les conditions prévues par l'ordonnance n° 2005-1516 du 8 décembre 2005.

2. **Les conditions de mise en œuvre des échanges dématérialisés entre les usagers et les organismes de protection sociale**

2.1. *La valeur juridique des échanges dématérialisés entre l'usager et l'organisme de protection sociale*

2.1.1. Les principes

Conformément à l'article 3 de l'ordonnance visée au présent préambule, les demandes ou informations transmises par voie électronique à une administration ou un organisme de protection sociale, dès lors qu'il en a été accusé réception, doivent être prises en compte par l'organisme qui les reçoit, sans qu'il soit nécessaire pour l'usager de confirmer ou répéter son envoi sous une autre forme.

Une administration ou un organisme de protection sociale peut répondre par voie électronique à toute demande d'information qui lui a été adressée par cette voie par un usager.

Pour pouvoir répondre aux obligations issues de cette ordonnance ainsi qu'aux exigences fixées par la loi n° 78-17 du 6 janvier 1978, et pouvoir s'assurer de la valeur juridique de ces échanges, les organismes visés par la présente circulaire doivent respecter les principes visés au 2.2.

Dans tous les cas, l'acceptation de données dématérialisées est soumise à la capacité du processus mis en œuvre à garantir l'identité de l'émetteur et l'intégrité du contenu informationnel, depuis sa date de création et tout au long de son cycle de vie, incluant sa conservation et son archivage.

2.1.2. Le cas des messages électroniques

Dès lors que les échanges dématérialisés ont pour objet d'échanger des données à caractère personnel (notamment demandes susceptibles de générer un droit, demande de consultation de documents contenant des données à caractère personnel) et/ou des documents comportant des données à caractère personnel, les échanges entre les usagers et les organismes de protection sociale concernés doivent être sécurisés proportionnellement à la sensibilité des données traitées.

Par ailleurs, les messages électroniques n'offrent pas toujours la sécurité nécessaire pour protéger les données à caractère personnel traitées et ne permettent pas de structurer les échanges avec les assurés.

Par conséquent, ces questions devront être évaluées lors de l'analyse de risque réalisée par l'organisme de protection sociale dans le cadre de la dématérialisation de la démarche. La mise en place d'un téléservice ou d'une messagerie sécurisée peut être nécessaire pour garantir la sécurité des données échangées.

Les messages électroniques reçus par une administration ou un organisme de protection sociale, qu'ils contiennent ou non des pièces jointes, devront être conservés dans les conditions prévues au point 3.1.2 de la présente circulaire.

Conformément à l'article 4 de l'ordonnance n° 2005-1516 du 8 décembre 2005, les autorités administratives qui créent un téléservice rendront accessibles les modalités d'utilisation de ce téléservice (notamment les modes de communication possibles qui incluent éventuellement la messagerie électronique sécurisée mise en place). Ces modalités, propres à l'utilisation de ce téléservice, s'imposent alors aux usagers.

2.1.3. Les pièces jointes transmises par messageries sécurisées ou par téléservice

Les conditions prévues au 1.5 de la présente circulaire sont applicables à ce cas d'échange de documents numériques.

Cas des pièces d'état civil faites en pays étranger

En ce qui concerne les pièces d'état civil, l'article 47 du code civil établit que « tout acte de l'état civil des Français et des étrangers fait en pays étranger et rédigé dans les formes usitées dans ce pays fait foi ».

Dans ce cadre-là, la communication d'une copie dématérialisée de l'acte d'état civil devra nécessairement répondre aux conditions de sécurité susvisées.

Toutefois, conformément à l'article 3 du décret n° 2000-1277 du 26 décembre 2000, l'original pourra être exigé par les administrations s'il existe un doute sur la validité de la photocopie produite ou envoyée, les procédures engagées au sein desdites administrations étant suspendues jusqu'à la production des pièces originales.

2.2. *Le niveau de sécurité requis pour l'accès aux téléservices mis à disposition des usagers*

2.2.1. Principes

Il est indispensable de fixer *a minima* des règles communes afin de permettre aux organismes d'assurer un certain niveau de sécurité d'accès aux téléservices qu'ils mettent en ligne.

Ainsi, les démarches effectuées par le biais d'un téléservice seront considérées par les organismes comme valables, dès lors que les modalités d'utilisation du téléservice intégreront les règles suivantes :

– un accès sécurisé (conformément aux modalités fixées au 2.2.2) ;
– la mise en place d'un système de case à cocher pour valider la demande, associée à une mention obligatoire précisant que l'usager a effectivement décidé de faire la démarche et qu'il s'engage sur les éléments déclarés ;
– une mention obligatoire avertissant l'usager que, dès lors qu'il utilise un des services sécurisés mis à sa disposition pour transmettre une demande ou une information, il s'engage, le cas échéant, à conserver les originaux de ses justificatifs, sauf si une administration est dépositaire desdits originaux, et à les mettre à la disposition des organismes qui lui en demanderaient la production ;
– la conservation, dans le système d'information, des informations permettant à tout moment d'identifier le demandeur, la date et la nature de la démarche.

2.2.2. Niveau minimum de sécurité

Afin de pouvoir s'assurer de l'identité de l'usager qui utilise un téléservice, les procédures d'authentification mises en place par les organismes de protection sociale doivent respecter un niveau de sécurité minimum.

Ce niveau commun de sécurité doit aboutir à l'authentification certaine de l'usager. Cependant, il semble nécessaire de ne pas complexifier outre mesure les méthodes d'authentification afin d'éviter que l'accès au téléservice devienne une source de contrainte plus importante pour l'usager que le besoin qu'il en a.

Le niveau minimum de sécurité impose :

– la mise en place d'une liaison sécurisée (https) entre l'usager et le service ;
– pour certaines démarches, le téléservice ne sera ouvert qu'aux personnes déjà connues de l'organisme. Dans ces cas-là, une affiliation certaine est nécessaire : le fait que l'usager soit, ou ait été, inscrit dans les bases de l'organisme auquel il s'adresse pour avoir accès au téléservice est une condition préalable qui, si elle n'est pas remplie, doit conduire au refus de l'inscription au téléservice ;
– un identifiant commun qui pourra être le numéro de sécurité sociale (NIR) et le nom, le n° SIRET ou, le cas échéant, un numéro interne. Il est recommandé de confronter cet identifiant avec des informations personnelles concernant l'usager lorsqu'elles sont inscrites dans le système d'information de l'organisme (contrôle de cohérence sur adresse, datation du NIR...) ;
– une désynchronisation lors de la transmission des clés d'accès qui conduira à ne jamais associer dans le même support identifiant et code secret. La recommandation est d'utiliser l'envoi par courrier postal mais de ne pas proscrire l'envoi par courriel compte tenu du besoin d'instantanéité que peut avoir l'usager lors de l'échange dématérialisé ;
– un avertissement sur l'engagement de la responsabilité de l'usager en cas de diffusion de ses clés d'accès à un tiers qui doit être clairement délivré par les organismes (mention sur le portail de l'organisme, sur le courrier ou dans le courriel de transmission des clés d'accès) ;
– une modification obligatoire du code secret qui a été délivré initialement par l'organisme lors de la première connexion de l'usager. Le code secret devra comporter un nombre minimum de caractères alphanumériques de la même façon que le mot de passe qui sera choisi par l'usager. Le mot de passe choisi par l'usager pourra avoir une durée de vie illimitée contrairement au code secret transmis par l'organisme dont le temps de validité dépendra du mode par lequel il a été transmis (courrier, courriel). Il est également recommandé aux organismes d'offrir la possibilité aux usagers d'avoir une visibilité sur la robustesse du mot de passe qu'ils choisissent (jauge indiquant le niveau de sécurité) ;
– un blocage de l'accès aux données ou une suspension de la session en cas de répétition de mots de passe erronés. L'usager devra alors soit patienter un certain délai, soit se réinscrire. En cas de perte du mot de passe ou de verrouillage, un code secret provisoire sera renvoyé à l'assuré, soit au terme d'une nouvelle procédure d'inscription identique, soit après que l'usager est entré en contact avec une hotline chargée de l'identifier, soit lorsqu'une réponse correcte à la question secrète aura été donnée.

Les organismes doivent prévoir des procédures (papier ou électronique) permettant de garantir le respect du secret professionnel auquel ils sont tenus et la protection des données à caractère personnel.

2.3. *La signature*

L'ordonnance n° 2005-1516 du 8 décembre 2005 ne fait pas obligation à l'usager d'apposer sa signature électronique lorsqu'il adresse par voie électronique une demande ou une information, dans la mesure où cela s'inscrit dans le cadre d'un téléservice.

Par conséquent, dès lors que la demande est régulièrement effectuée par le biais d'un téléservice, conformément aux règles d'identification et d'acceptabilité des demandes saisies en ligne, telles que décrites ci-dessus, on considère que la démarche a été régulièrement effectuée.

Les procédures mises en place dans le cadre des téléservices ou de messageries électroniques devront permettre :
– d'identifier/authentifier la personne dont émane l'écrit électronique ou qui procède à des démarches en ligne ;
– de garantir le lien entre cette personne et son écrit électronique ou sa démarche en ligne ;
– de garantir l'intégrité de son écrit électronique ou des données transmises dans le cadre de sa démarche en ligne.

2.4. *Les accusés de réception et d'enregistrement électroniques*

Conformément à l'ordonnance n° 2005-1516 du 8 décembre 2005, deux procédés attestent qu'une demande, déclaration ou production de documents adressée par l'usager par voie électronique a bien été prise en compte :
– l'accusé de réception électronique ;
– l'accusé d'enregistrement électronique, lorsque l'accusé de réception électronique n'est pas instantané.

Ces deux procédés doivent être conformes aux règles fixées par le référentiel général de sécurité et aux dispositions fixées par décret en Conseil d'État (non paru à ce jour).

Le principe

Toute demande, déclaration ou production de documents adressée par un usager à une autorité administrative par voie électronique ainsi que tout paiement opéré dans le cadre d'un téléservice fait l'objet d'un accusé de réception électronique et, lorsque celui-ci n'est pas instantané, d'un accusé d'enregistrement électronique.

Les conditions et délais d'émission de l'accusé de réception et de l'accusé d'enregistrement ainsi que les indications devant y figurer seront fixées par décret en Conseil d'État.

Les conséquences

Lorsqu'un usager a transmis à un organisme de protection sociale une demande, déclaration ou production de document dans le cadre d'un téléservice et qu'il en a été accusé réception, celui-ci est régulièrement saisi et traite la demande ou l'information sans demander à l'usager la confirmation ou la répétition de son envoi sous une autre forme.

L'accusé d'enregistrement informe l'internaute que sa démarche a bien été enregistrée et prise en compte par l'organisme concerné.

L'accusé de réception servira de point de départ du délai de traitement de la demande et du délai relatif aux voies de recours.

Forme de l'accusé d'enregistrement et de l'accusé de réception

Les accusés d'enregistrement et accusés de réception électroniques doivent être émis et conservés dans des conditions sécurisées.

L'accusé de réception électronique doit comporter les mentions suivantes :
– les éléments d'identification du demandeur ;
– la date et l'heure de réception de l'envoi électronique effectué par l'usager ;
– la désignation, l'adresse postale et, le cas échéant, électronique, ainsi que le numéro de téléphone du service chargé du dossier.

L'accusé d'enregistrement électronique doit comporter les mentions suivantes :
– les éléments d'identification du demandeur ;
– la date et l'heure d'enregistrement de l'envoi électronique effectué par l'usager.

2.5. *La gestion des dates dans le cadre des échanges dématérialisés avec les usagers*

La date qui fait foi lors d'un échange électronique (concernant toute demande, information ou production de document) entre l'usager et l'administration ou l'organisme de protection sociale est la date figurant sur l'accusé de réception ou, à défaut, sur l'accusé d'enregistrement adressé à l'usager par la même voie, conformément aux dispositions de l'ordonnance n° 2005-1516 du 8 décembre 2005 (art. 5-I).

3. **Les modalités propres aux garanties dues par les organismes et au contrôle (audit et contrôle interne) mis en place**

3.1. *Garanties et charge de la preuve*

L'organisme émetteur doit mettre en œuvre tous moyens propres à garantir la fiabilité et la conformité des données qu'il transmet et être en mesure d'en apporter les preuves. Dès lors que les conditions et contrôles prévus par la présente circulaire sont mis en œuvre, l'organisme qui utilise des données reçues d'un autre organisme, d'une autorité administrative ou d'un assuré, dans le respect du cadre législatif et réglementaire qu'il est chargé d'appliquer, est engagé sur leur fiabilité dans l'utilisation qu'il en fait pour les besoins de sa mission.

3.1.1. Le principe : la garantie propre à l'émetteur

Garantie de la fiabilité des données

Dès lors que les conditions et contrôles prévus par la présente circulaire sont mis en œuvre, l'organisme émetteur à l'origine de données :

– qu'il a lui-même établies, ou

– qu'il a reçues d'un autre organisme ou d'un assuré et qu'il utilise dans le cadre de ses missions,

est garant vis-à-vis de l'organisme récepteur à qui il les transmet ou dont il alimente le système d'information, de la fiabilité de ces données au regard du cadre législatif et réglementaire qu'il est chargé d'appliquer. À cette fin, il lui appartient de définir et mettre en œuvre un dispositif de contrôle interne garantissant un niveau acceptable de maîtrise des risques pouvant affecter la fiabilité des données.

Ce principe s'applique également lorsque l'organisme qui émet les données a procédé à leur enrichissement avec des données reçues d'un autre organisme ou autorité administrative.

Garantie de la conformité des données

Dès lors que les conditions et contrôles prévus par la présente circulaire sont mis en œuvre, l'organisme qui transmet ou retransmet des données à un autre organisme est garant vis-à-vis de ce dernier de la conformité de ces données à celles dont il est à l'origine ou à celles qu'il a reçues d'un autre organisme, d'une autorité administrative ou d'un assuré.

3.1.2. Modalités de conservation

Pendant toute la durée légale de conservation applicable à chaque organisme de protection sociale, l'émetteur conserve les données qu'il a transmises par voie électronique.

La conservation de ces données devra être réalisée dans des conditions permettant d'en garantir l'imputabilité, l'intégrité, la fidélité, la durabilité/pérennité, ainsi que l'accessibilité.

3.1.3. Principes de communication des données

Dans le cadre d'un litige ultérieur, l'organisme de protection sociale qui a reçu les données peut demander à l'administration ou organisme émetteur une copie du document ou un état restituant la donnée source stockée dans son système d'information, ainsi que les éléments de traçabilité associés.

L'organisme émetteur doit être en mesure de répondre à cette demande pendant toute la durée de conservation définie pour son propre système d'information ou par voie contractuelle (notamment en matière d'échanges fichiers).

Dès lors que l'usager dispose de données ou documents originaux, il doit pouvoir en fournir un exemplaire à l'organisme de protection sociale ou l'administration qui lui en fait la demande.

Conformément à l'article 1348 alinéa 2 du code civil, si le document original n'a pas été conservé par l'usager ou l'organisme émetteur, une copie pourra être présentée, à condition qu'elle en soit la reproduction fidèle et durable.

Toute demande de communication des traces à l'administration ou l'organisme émetteur devra respecter le circuit propre à l'organisme qui reçoit cette demande.

Dans le cadre des échanges dématérialisés entre organismes de protection sociale une annexe au contrat ou à la convention précise les durées et les modalités de conservation des données par l'organisme émetteur ainsi que les modalités d'accès ou de communication à l'organisme récepteur.

3.2. *Le contrôle interne des échanges*

3.2.1. Principes

Les organismes ou administrations parties à un échange sont tenus de définir et de mettre en œuvre un dispositif de contrôle interne permettant de maîtriser les risques inhérents aux échanges et au contenu des données échangées.

Ces dispositifs de contrôle interne ont pour objectif d'assurer le respect des exigences prévues dans la présente circulaire et de garantir pour les organismes de protection sociale un niveau acceptable de maîtrise des risques inhérents ayant notamment trait :

– à l'exhaustivité, la qualité et la validité des données échangées au regard des règles de droit applicables à l'émetteur et de l'utilisation des données par l'organisme récepteur ;

– à la sécurité, la confidentialité et la traçabilité des échanges.

Outre la mise en place d'un dispositif de contrôle interne propre à chaque organisme, les parties à un échange de données doivent prévoir un dispositif coordonné de contrôle interne des échanges qui précise les contrôles mis en place par chaque organisme. Celui-ci peut notamment reposer sur des contrôles permettant de s'assurer de la cohérence et de l'exhaustivité des données échangées tels que :

– l'établissement de revues analytiques ;

– la réalisation et l'analyse de comptes-rendus d'exploitation et de contrôles de gestion permettant de faire des comparaisons entre les données attendues et les données reçues ;
– la mise en œuvre de procédures de circularisation.

Le cas échéant, les organismes s'engagent à adapter si nécessaire leurs outils pour mettre en œuvre ces contrôles.

L'élaboration des plans de contrôle interne des organismes partenaires fait l'objet d'une concertation visant à permettre une homogénéité du dispositif.

En outre, avant tout échange de données par voie électronique, les administrations et organismes de protection sociale devront nécessairement procéder à une phase préalable de qualification (recettage) dont les modalités seront définies en commun.

3.2.2. La surveillance du dispositif

Afin de s'assurer de la mise en œuvre et de l'efficacité des dispositifs de contrôle interne (dispositif propre à chaque organisme et dispositif coordonné) qui s'appliquent aux échanges et à leur contenu, les parties à un échange s'engagent :

– à transmettre à leur partenaire, et sur leur demande, le rapport relatif à la description de leur contrôle interne, précisant les différents processus, les contrôles réalisés et leurs résultats ;
– à autoriser la réalisation d'audits de ces dispositifs de contrôle interne à l'initiative d'un partenaire.

Les modalités et la fréquence de ces actions doivent être précisées dans le contrat ou la convention prévue au paragraphe 1.4 de la présente circulaire.

Les règles prévues au 3 de la présente circulaire s'appliquent également aux documents numérisés dans les cas où seules des images de documents pourraient être transmises, et notamment dans une phase de transition vers un échange de données.

Pour le ministre et par délégation :
Le directeur de la sécurité sociale,
D. Libault