GUIDE PRATIQUE

« tiers autorisés »

Juillet 2020

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

AVANT-PROPOS

Un certain nombre d'autorités ont, en vertu de dispositions législatives et plus rarement réglementaires, **le pouvoir d'exiger la transmission de documents ou de renseignements.** De telles demandes impliquent fréquemment **la transmission de données à caractère personnel par le responsable de traitement sollicité**.

C'est le 9) de l'article 4 du RGPD relatif à la notion de « destinataire » qui mentionne l'existence de cette catégorie d'acteurs susceptibles de recevoir communication de données « *dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre* ». Ces acteurs sont communément appelés « *tiers autorisés* » en raison de leur pouvoir leur permettant de prendre connaissance, et au besoin copie ou saisie, d'informations et de documents détenus par des organismes de toute nature (de mettre en œuvre, en d'autres termes, un droit de communication).

Concrètement, les tiers autorisés sont l'ensemble des autorités et organismes (publics le plus souvent) disposant, en vertu de l'intérêt public qui s'attache à l'accomplissement de leur mission, du pouvoir de solliciter l'obtention de données à caractère personnel issues de fichiers détenus par des personnes ou organismes publics et privés.

Pour cette raison, les « tiers autorisés » sont à distinguer des différents acteurs susceptibles de recevoir communication d'informations **en dehors des missions d'enquête précitées** (par exemple, accès d'un usager aux documents administratifs, échanges légalement prévus entre administrations, droit d'accès d'une personne concernée).

Le pouvoir d'un tiers autorisé s'appuie **systématiquement** sur un cadre juridique prévoyant ses modalités de mise en œuvre : organismes concernés, objet de la demande d'accès ou de la copie, nature des informations et documents concernés.

Prérogative légale et confidentialité

Au regard du RGPD, l'enjeu principal pour un responsable de traitement recevant une telle demande est double : veiller à se conformer aux demandes **prévues par les dispositions légales** et garantir la **sécurité des données à caractère personnel** traitées.

En application des articles 5-1-f et 32 du RGPD, tout responsable de traitement doit en effet assurer la confidentialité des données en veillant à limiter les accès et transmissions aux seuls acteurs habilités ou autorisés (dont font partie les tiers autorisés lorsqu'une disposition législative ou réglementaire le prévoit).
Ces exigences doivent conduire le responsable de traitement interrogé à impérativement suivre trois étapes :

1. Vérification de **l'existence d'un fondement légal** autorisant la demande et la communication de données ;
2. Vérification de la **qualité de l'organisme** à l'origine de la demande et du **périmètre des informations** ciblées ;
3. **Sécurisation** de la communication des données ou des modalités d'accès par le tiers autorisé.

Ce guide a pour objectif de présenter en pratique le respect de ces exigences par tout organisme. Les conséquences d'une communication de données à des personnes non autorisées sont en effet multiples :

- Conséquences sur les droits et libertés des personnes concernées (articles 33 et 34 du RGPD), y compris en matière de droit à réparation (article 82 du RGPD) ;
- Procédure de sanction et mesures correctrices par la CNIL (article 83 et 84 du RGPD) ;
- Engagement de la responsabilité pénale du responsable de traitement (articles 226-13, 226-17 et 226-22 du code pénal).

PARTIE I : Identifier une demande « tiers autorisés »

Les formes que peut prendre une demande de communication de données d'un tiers autorisé sont diverses : il n'existe pas de document ou de formulation type que le responsable de traitement pourrait systématiquement exiger (sauf lorsque le texte le prévoit explicitement).
Lorsqu'un responsable de traitement reçoit une demande exigeant la communication de données à caractère personnel, le premier réflexe à avoir est de s'assurer que la requête se fonde sur une disposition légale en vigueur. Deux scénarios sont possibles :

- Si la demande mentionne une référence légale ou réglementaire précise, alors le responsable de traitement doit vérifier (depuis le site web Légifrance, par exemple) la réalité des dispositions mentionnées[1] ;
- Si la demande ne mentionne aucune disposition particulière, alors le responsable de traitement doit demander à l'organisme s'il agit en application d'un texte et de préciser la référence légale afin que la vérification précitée puisse être menée.

Le responsable de traitement ne peut en effet se satisfaire d'une demande uniquement fondée sur des éléments contextuels (nature de l'organisme émetteur, habitudes relationnelles, tournures de phrases impératives, etc.). Il doit s'assurer que l'organisme agit effectivement, au moment de la demande, en tant que tiers autorisé. Adresser des données à caractère personnel à un organisme sans qu'une telle vérification n'ait été réalisée expose le responsable de traitement à deux risques susceptibles de conduire aux sanctions précitées :

- Transmettre des données à caractère personnel à des personnes non autorisées ;
- Transmettre des données sans respecter le cadre établi par les dispositions légales relative au droit de communication exercé.

1 Cette vérification doit être réalisée en choisissant la version consolidée du texte en vigueur à la date du jour de la vérification.

TESTEZ-VOUS

Ces demandes permettent-elles de vérifier que l'organisme s'adresse au responsable de traitement en tant que tiers autorisé ?

Demandes	Réponses
Bonjour, merci de bien vouloir nous communiquer toute information relative à M. Dupont pour lequel notre service investigation réalise actuellement un contrôle en application des dispositions légales en vigueur. Ne pas répondre à cette demande sous 15 jours à compter de sa réception vous expose à des poursuites judiciaires en vertu des dispositions du code de procédure pénale. Nous vous demandons de déposer les documents réunis sur la plateforme sécurisée accessible en ligne et gérée par les services du ministère (accessible depuis ce lien). Cordialement	Non. Cette demande ne mentionne aucun texte permettant de vérifier si l'organisme agit en tant que tiers autorisé. Le responsable de traitement doit, avant toute éventuelle transmission de données, exiger cette information de l'organisme à l'initiative de la demande.
Bonjour, l'entrée en vigueur de la loi du 16 avril 2077 relative à l'encadrement des implants cybernétiques a prévu une mission de suivi technologique au sein des corporations partenaires. La Direction Prospective et Mise à jour du ministère vous prie de communiquer dans les plus brefs délais l'intégralité du registre des agents (comprenant le nom, le prénom et le matricule) actuellement bénéficiaires de cette technologie. Cordialement	Non. Bien que l'institution précise agir sur le fondement d'un texte effectivement en vigueur, la mention d'un ensemble large de dispositions ne permet pas de considérer que le responsable de traitement est en mesure de répondre en étant assuré de la légalité de la demande. De nombreux textes peuvent en effet prévoir plusieurs modalités d'échange de données, selon différentes conditions et à des fins distinctes. La corporation ciblée est fondée par conséquent à demander quelles dispositions précises de la loi (et le cas échéant des textes réglementaires d'application) sont appliquées dans le cadre de cette demande.
Bonjour, le service investigation du ministère réalise actuellement un contrôle sur pièce de votre entreprise. En application des dispositions des articles L. 32 et R. 32-1 et suivants du code des contrôles, nous vous demandons de bien vouloir nous communiquer, dans un délai de 15 jours, les dossiers des nouveaux clients obtenus durant le mois de janvier de cette année. Cordialement	Oui. L'organisme adresse sa demande en précisant agir sur le fondement de dispositions précises, ce qui permet à l'entreprise de vérifier sa qualité de tiers autorisé à exiger et recevoir communication de ces informations de façon sécurisée.
Bonjour, je mesure pleinement en tant qu'élu national les difficultés des familles impactées par la fermeture des établissements scolaires durant cette crise sanitaire d'ampleur. C'est pour leur apporter un message d'encouragement et les soutenir dans cette épreuve que je vous saurais gré de me remettre les informations de contact des parents d'élèves de vos communes. Cordialement	Non. Malgré la qualité de l'auteur, cette demande ne permet pas de répondre positivement dans la mesure où aucun texte juridique prévoyant une telle transmission n'est cité. Le responsable de traitement doit, avant tout éventuel envoi, exiger cette information.

PARTIE II : Vérifier la source et le périmètre de la demande

La connaissance des dispositions légales prévoyant le droit de communication répond à une seconde exigence relative au contrôle par le responsable de traitement :

- de l'organisme à l'origine de la procédure ;
- du périmètre de la demande (quelles informations demandées, à quel acteur).

Chaque procédure légalement prévue présente en effet des spécificités déterminantes qu'il convient de vérifier avant de réunir et de communiquer les éléments d'information demandés. Une disposition peut prévoir un périmètre très large (par exemple : « toute donnée utile détenue par tout organisme peut être exigée ») ou restreint (« la copie des factures détenues par les organismes mentionnés à l'article 10 peut être exigée »). Certaines dispositions peuvent par ailleurs prévoir des règles supplémentaires, en précisant par exemple qu'une demande doit être émise par une personne détenant une fonction particulière (tel qu'un officier de police judiciaire).

1. La vérification de l'organisme à l'origine d'une demande

Cette vérification est double.

Vérification juridique

Elle consiste à s'assurer que l'acteur émetteur de la demande est effectivement cité dans la disposition légale invoquée comme autorisé à exiger la communication des informations.
Il s'agit ici d'une vérification des termes des dispositions législatives et réglementaires pertinentes.

Vérification pratique

Elle consiste à s'assurer que l'émetteur de la demande de communication reçue par le responsable de traitement provient effectivement de l'autorité ou de l'organisme public mentionné. Il s'agit ici d'entraver les éventuelles tentatives frauduleuses de récupération d'informations par des acteurs malveillants ou non autorisés.

Cette seconde vérification doit conduire le responsable de traitement à adapter sa vigilance et ses contrôles en cas de doute raisonnable ou au regard des enjeux, notamment lorsque :

- les échanges entre le responsable de traitement et l'acteur émetteur de la demande ne sont pas habituels (par exemple : premier échange avec l'organisme, nouvel interlocuteur d'un organisme « connu ») ;
- la demande est transmise par un moyen ne permettant qu'un contrôle limité par le responsable (par téléphone, par courriel, en personne) ;
- la demande concerne des données d'un volume important, de nature inhabituelle ou d'une particulière sensibilité.

Lorsque le responsable de traitement est dans l'un de ces cas ou dans toute autre situation faisant peser un doute raisonnable, il conviendra de prévoir les mesures adaptées pour s'assurer de la réalité de la procédure auprès de l'organe émetteur de la demande.

Modalités de vérification

Il pourra s'agir notamment de procéder aux contrôles suivants :

- Effectuer un contre-appel en utilisant le numéro de contact diffusé par l'administration (sur son site web ou sur l'annuaire public des administrations accessible depuis cette page) – ne pas utiliser le numéro fourni par le demandeur ;
- Vérifier que l'adresse postale communiquée correspond à celle diffusée par le tiers autorisé sur son site web (ou sur l'annuaire précité) ;
- Vérifier que le nom de domaine de l'adresse courriel utilisée ou indiquée (la partie qui suit le signe « @ » dans une adresse de messagerie) correspond à celui diffusé par l'administration sur son site web (vérification à faire lors de la réception du message et lors de la réponse, si une réponse par courriel est attendue) ;
- Recueillir toute information identifiant la personne se présentant dans les locaux aux fins de vérification auprès de son organisme d'appartenance (le cas échéant nom, prénom, fonction, matricule, ou présentation d'une carte professionnelle) ;
- Contacter pour toute vérification utile le délégué à la protection des données (DPD / DPO) de l'organisme à l'origine de la demande (les organismes autorisés à agir en tant que « tiers autorisés » disposent généralement d'un DPO, dont les coordonnées sont accessibles depuis la page « data.gouv.fr » dédiée).

Remarque : Si un responsable de traitement réalise a posteriori que des données à caractère personnel ont été transmises « à tort » (par exemple : acteur malveillant s'étant fait passer pour un tiers autorisé légitime), il devra aussitôt envisager de notifier une violation de données à la CNIL, en application de l'article 33 du RGPD (ainsi que, le cas échéant, aux personnes concernées, en application de l'article 34).

Illustration : les contrôles de la CNIL

Contrôle sur place

À l'occasion des contrôles sur place que réalise la CNIL, il arrive que la délégation de contrôle invite l'organisme à contacter de lui-même la Commission en cas de doute raisonnable quant au cadre légal prévoyant ses actions. Cet appel lui permet d'obtenir la confirmation que les agents agissent effectivement en application d'une décision formelle de la CNIL de procéder à un contrôle de l'organisme.

Contrôle sur pièces

À l'occasion des contrôles sur pièces que réalise la CNIL (par exemple : transmission d'un courrier exigeant de l'organisme qu'il communique certaines informations), l'organisme peut à tout moment contacter la Commission afin de se faire confirmer la réalité de la procédure.

2. La vérification du périmètre des données transmises

Les textes relatifs aux pouvoirs des tiers autorisés prévoient systématiquement un périmètre délimitant les informations ou documents pouvant faire l'objet d'une demande de communication.

Le tiers autorisé est tenu de respecter ce périmètre à l'occasion de sa demande. Néanmoins, cela ne décharge pas le responsable de traitement de la vigilance dont il doit faire preuve afin de veiller à répondre conformément au périmètre d'une part, et précisément à la demande d'autre part.

Il revient ainsi au responsable de traitement de s'assurer :

- Que les informations transmises sont effectivement visées par les dispositions invoquées par le tiers autorisé ;
- Que les informations réunies, avant transmission, ne contiennent pas de données à caractère personnel « en trop », c'est-à-dire non demandées par le tiers autorisé dans sa requête.

Cas des données « en trop »

Lorsque le tiers autorisé requiert la communication des noms et prénoms des agents ou salariés d'un service, le responsable de traitement peut, par commodité, transmettre la copie de l'organigramme correspondant, à condition de masquer les informations « en trop » (photo, adresse de messagerie et numéro de téléphone).

Lorsque la demande n'exige pas, en elle-même, la transmission de données personnelles, le responsable de traitement doit envisager de minimiser sa réponse jusqu'à l'anonymisation des éléments fournis.

Question s'agissant des collectivités : une enquête peut-elle être menée pour répondre à un droit de communication ?

Questions	Réponses	Exemples
S'agissant des collectivités : une enquête peut-elle être menée pour répondre à un droit de communication ?	Une collectivité ne peut, dans le but de satisfaire à une demande de renseignement d'un tiers autorisé, diligenter une enquête auprès d'un autre organisme afin d'obtenir des données qu'elle ne détient pas. Il convient de rappeler qu'aucune disposition législative ne permet en effet aux mairies d'agir ainsi, même à la demande de tiers autorisés.	Les services municipaux ne peuvent pas, afin de répondre à un tiers autorisé, utiliser les fichiers des centres communaux d'action sociale (CCAS) car ce sont des responsables de traitements distincts. Par ailleurs, une collectivité ne peut pas davantage recueillir des données à caractère personnel sans lien avec la finalité d'un fichier, afin de répondre à une demande.

3. Le respect du secret professionnel et l'exercice du droit de communication

L'obligation de respect du secret professionnel résulte de la volonté du législateur de protéger certaines informations en interdisant leur divulgation à des personnes non autorisées par la loi (sous peine de poursuites pénales).

En pratique, le secret professionnel doit être opposé par l'organisme en réponse à une demande provenant d'un tiers autorisé pour lequel aucune disposition ne prévoit la levée d'un ou de plusieurs secrets professionnels. Le responsable doit donc, avant toute invocation du secret professionnel, vérifier si les deux conditions précitées sont effectivement réunies :

- La demande de communication vise-t-elle des informations ou documents protégés par un secret professionnel ?
- Dans l'affirmative, la demande de communication provient-elle d'un organisme bénéficiant d'une disposition législative prévoyant la levée du secret professionnel concerné ?

La bonne connaissance et le suivi de ces règles sont primordiaux dans la mesure où les décisions prises par le responsable sur leur fondement, transmission ou refus de transmission d'une information, peuvent donner lieu aux suites contentieuses précitées : violation du secret professionnel ou, en cas d'opposabilité non fondée du secret professionnel, entrave au contrôle (lorsque les textes le prévoient).

a) La demande vise-t-elle des informations protégées par un secret professionnel ?

L'existence d'un secret professionnel peut être vérifiée dans deux cas de figure, selon qu'il existe ou non des dispositions explicites le prévoyant.

Dans le premier cas, il revient au responsable de traitement d'identifier et d'invoquer l'existence de dispositions expresses protégeant les informations qu'il détient. De telles dispositions pourront viser des informations d'une certaine nature ou détenues et exploitées dans un contexte particulier.

L'absence de disposition explicite ne signifie cependant pas nécessairement que le responsable de traitement n'est pas soumis au secret professionnel.

Un responsable de traitement peut en effet être soumis au respect d'un secret professionnel malgré l'absence de disposition légale explicite le concernant. Les critères d'appréciation en la matière ont trait à « la nature secrète de l'information en cause et, d'autre part, à la fonction ayant permis à l'intéressé d'obtenir ladite information » (arrêt n° 1-2019 du 30 septembre 2019 - Cour de justice de la République).

b) Le secret professionnel est-il opposable au tiers autorisé ?

Les dispositions relatives au droit de communication peuvent être accompagnées de précisions explicites quant aux modalités de respect du secret professionnel. De telles dispositions peuvent prévoir ou exclure les cas d'opposabilité d'un secret professionnel, de manière générale ou dans des conditions spécifiques.

Ici encore, l'absence de dispositions explicites en la matière ne signifie pas nécessairement l'impossibilité pour un tiers autorisé de lever un secret professionnel.

À plusieurs reprises, les juridictions ont en effet estimé que des informations pourtant protégées par un secret professionnel devaient être transmises à un tiers autorisé car leur divulgation était la conséquence nécessaire des dispositions légales applicables à ce tiers (en particulier celles relatives à la mission attribuée au tiers autorisé par le législateur). Autrement dit, outre les cas dans lesquels le secret est expressément rendu inopposable par une disposition législative spécifique, il existe un certain nombre d'hypothèses dans lesquelles un texte doit être interprété comme ayant, implicitement, pour effet de lever le secret à l'égard d'un tiers.

Au regard de la jurisprudence chaque « autorisation » en la matière fait cependant l'objet d'un examen au cas par cas par le juge afin de vérifier que l'application des dispositions légales précitées requiert impérativement la

transmission d'informations couvertes par un secret, ou si l'objectif fixé par les dispositions peut être atteint sans qu'il soit nécessaire de le transgresser (un certain nombre de décisions du Conseil d'Etat ont été prises en ce sens).

Dès lors, la vigilance du responsable de traitement (ainsi que, le cas échéant, les motifs avancés par les tiers autorisés à l'occasion de leurs demandes) devra s'étendre à l'interprétation des textes par les éventuelles décisions juridictionnelles le concernant directement ou par analogie.

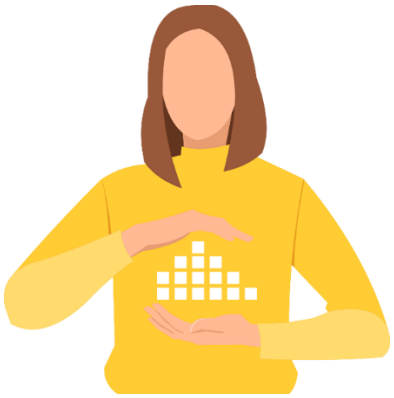
Pour mémoire, un droit de communication exercé irrégulièrement est de nature à vicier la procédure qui en découle, comme l'a rappelé le Conseil constitutionnel (décision n° 2013-679 DC du 4 décembre 2013, § 32 à 34).

TESTEZ-VOUS

Plusieurs questions relatives aux obligations en matière de respect du secret professionnel.

Questions	Réponses
Une disposition légale prévoyant la communication obligatoire par un responsable de « tous documents ou informations utiles » est-elle suffisante à elle seule pour considérer que le secret professionnel ne peut être opposé ?	Non, des formulations de cette nature ne permettent pas de lever un secret professionnel si elles ne sont pas complétées par la présence de l'une des dispositions précitées : une disposition explicite ou ayant pour effet de lever un tel secret.
Une disposition prévoyant qu'un organisme tiers autorisé ne peut demander la communication d'informations couvertes par un secret professionnel spécifique (ex. secret médical) a-t-elle implicitement pour effet de permettre une demande de communication d'informations couvertes par un autre secret professionnel ?	Non, un secret professionnel est opposable à un tiers autorisé quand bien même les dispositions détaillant les limites de son droit de communication n'y fait pas référence, à moins que la formulation ne soit exclusive (par exemple : « Le respect du secret des sources journalistiques est le seul secret professionnel opposable »).
Une disposition prévoyant que les agents de l'organisme tiers autorisé sont soumis au secret professionnel a-t-elle pour effet d'autoriser cet organisme à exiger la communication de données couvertes par un secret professionnel ?	Non, une telle disposition n'a pas pour effet d'étendre le périmètre des informations et documents pouvant faire l'objet d'un droit de communication. Elle vient cependant préciser explicitement que la révélation, par l'organisme ou les agents précités, d'une information à caractère secret est susceptible d'engager leur responsabilité pénale dans les conditions précisées aux articles 226-13 et 226-14 du code pénal.

PARTIE III : Veiller à sécuriser la communication



Les dispositions légales encadrant les pouvoirs des tiers autorisés prévoient différentes modalités d'obtention des informations auprès des responsables de traitement :

- Communication de documents ou d'informations par le responsable de traitement au tiers autorisé ;
- Consultation et / ou copie de documents ou données par le tiers autorisé (lors d'un contrôle sur place, par exemple) ;
- Saisie par le tiers autorisé de documents ou de supports de stockage de données ;
- Audition du responsable de traitement (qui pourra notamment donner lieu à consultation à distance ou échanges oraux sur le contenu de documents ou de données) ;
- Ouverture d'un accès distant à un système d'information par le tiers autorisé.

Il revient à chaque acteur de s'assurer que la modalité de communication utilisée est conforme aux dispositions invoquées. Les développements suivants se pencheront sur le cas de la communication dématérialisée par le responsable de traitement, en raison des enjeux particuliers relatifs à la sécurité des données.

1. La détermination du canal de transmission des informations

Les dispositions en vigueur ne prévoient que rarement les modalités de transmission des informations demandées entre l'organisme détenteur de l'information et l'organisme agissant en tant que tiers autorisé.

Par principe, les acteurs doivent conjointement veiller à respecter l'obligation de sécurité des données, en particulier en termes de confidentialité et d'intégrité des données. Le responsable de traitement doit, à ce titre, privilégier dans la mesure du possible les modalités[2] de communication offrant un niveau de sécurité adapté, le cas échéant en définissant de lui-même des modalités sécurisées de transmission.

Ces modalités peuvent concerner le canal de transmission ou l'information elle-même, au moyen par exemple :

- De l'utilisation de procédés de chiffrement afin de rendre l'information inintelligible à toute personne ne disposant pas de la clef (par exemple : utilisation des outils gratuits et reconnus fiables tels que 7-zip, Veracrypt ou Zed!) ;
- De l'utilisation de procédés de hachage afin de s'assurer, si nécessaire, que les informations n'ont pas subi d'altérations non prévues lors de la transmission (en veillant à n'utiliser que des algorithmes reconnus et sûrs) ;
- De l'utilisation d'une plateforme d'échange en ligne présentant des standards de sécurité conformes à l'état de l'art ;
- De l'utilisation systématique de deux canaux de transmission distincts pour l'envoi d'un document chiffré et de la clef de déchiffrement correspondante (par exemple : courriel puis téléphone).

[2] Voir la fin du guide pour les ressources relatives à la mise en œuvre pratique.

Remarque : Le choix par le tiers autorisé de modalités d'échanges jugées peu sûres par le responsable de traitement ne peut pas en principe l'autoriser à s'opposer à la transmission.
Il est cependant conseillé au responsable de traitement d'adresser cette observation à l'organisme tiers autorisé et de conserver tout échange et élément jugé utile sur ce point.

TESTEZ-VOUS

Ces modalités de transmission de données à caractère personnel vous paraissent-elles satisfaisantes ?

Modalités	Réponses
Transmission des données à caractère personnel par courriel contenant en pièce-jointe les données chiffrées. À la réception des données, le destinataire utilisera le mot de passe renseigné dans le corps du courriel. Ce mot de passe comporte les 8 caractères suivants : « hJrc8p3W ».	Non. Cette transmission n'apparaît pas satisfaisante. D'une part, l'utilisation du même canal (courriel) pour la transmission de la pièce jointe et du mot de passe n'est pas pertinente. Il convient en effet de communiquer séparément le mot de passe et le document chiffré (au moyen du téléphone, du SMS ou du courrier postal, par exemple). D'autre part, lorsque l'accès à un fichier de données personnelles est uniquement protégé par l'utilisation d'un mot de passe, la CNIL recommande que celui-ci présente a minima une complexité de 12 caractères avec une majuscule, minuscule, chiffre et caractère spécial (voir recommandation CNIL sur les mots de passe du 22 juin 2017). Une communication en retour accusant réception des informations devrait par ailleurs être prévue.
Transmission des données à caractère personnel non chiffrées au moyen de la remise en mains propres d'un dispositif de stockage amovible (par exemple clé USB ou CD-ROM) contenant les informations.	Non. Cette méthode peut-être problématique dans la mesure où la perte ou le vol du dispositif de stockage lors du déplacement à l'extérieur de l'organisme du tiers autorisé expose les données personnelles à des accès et réutilisations non prévues. Il convient de prévoir le chiffrement de données avant leur transfert sur le support et de consigner sa remise à l'organisme tiers autorisé (au moyen d'une signature de l'agent, par exemple).
Transmission des données à caractère personnel par pli avec accusé réception contenant un CD-ROM sur lequel sont placées les informations exigées dans un format chiffré. Le mot de passe « Soc13t3X-CNIL20 » est transmis oralement par téléphone.	Oui. Les modalités d'échanges paraissent satisfaisantes pour une transmission ne présentant pas de spécificités particulières. Le mot de passe ne doit cependant pas être prévisible ni réutilisé pour plusieurs échanges de cette nature.

2. Peut-on contester une demande de communication de données d'un tiers autorisé ?

Des voies de recours permettant de contester ou de s'opposer à une demande d'un tiers autorisé existent. Celles-ci devront être rigoureusement identifiées et employées selon les modalités prévues, dans la mesure où :

- un « simple » refus de répondre est susceptible de donner lieu à l'engagement de la responsabilité de l'organisme visé ;
- les conditions d'usage des voies de recours et leurs effets immédiats peuvent sensiblement différer selon les dispositions applicables (par exemple : un recours peut ou non suspendre l'obligation de transmission d'information).

Il est dans tous les cas hautement recommandé de documenter rigoureusement tout élément pertinent se rapportant au contexte et aux échanges, afin de pouvoir justifier cette décision.

3. Peut-on conserver les éléments transmis ?

Des constats fréquents de la CNIL au sein d'organismes de différentes natures font état de pratiques disparates concernant les modalités de traitement des informations par les organismes, une fois celles-ci transmises à un organisme tiers autorisé.
La pluralité des situations possibles ne permet pas d'avancer une réponse générale. Il peut néanmoins être indiqué que la conservation des échanges est envisageable dans la mesure où un tel traitement (inscrit au registre comme tel) :

- pourra être justifié par la poursuite d'une finalité déterminée, explicite et légitime (article 5-1-b du RGPD) ;
- concernera un périmètre de données minimisées au strict nécessaire selon la finalité précitée (conservation de la seule preuve de la transmission ou conservation des données transmises, à justifier rigoureusement dans ce cas) ;
- ne pourra être mis en œuvre au-delà du délai (préalablement fixé) nécessaire à l'accomplissement de cette finalité ;
- bénéficiera de mesures de sécurité adaptées, en particulier s'agissant de l'obligation de confidentialité.

La documentation « tiers autorisés » : un outil interne

Pour certains organismes, l'établissement d'une documentation relative à la gestion des demandes « tiers autorisés » s'avèrera indispensable.

Une telle documentation devra être diffusée aux agents susceptibles d'être destinataires ou en charge de telles demandes (ainsi qu'aux éventuels sous-traitants de l'organisme). Elle devra mentionner les principaux points abordés jusqu'ici :

- Les premiers gestes de tout agent à la réception d'une demande à la forme « impérative » (informations à demander, référent interne à saisir etc.) ;
- La désignation du ou des référents chargés veiller à la prise en compte de la demande (si la validation définitive revient au responsable de traitement, le DPO devra a minima être en mesure de donner son avis au préalable sur la procédure interne et, le cas échéant, sur la réponse au cas particulier) ;
- Informer rigoureusement chaque agent et salarié sur les menaces connues et / ou référencées par les acteurs institutionnels compétents (notamment ANSSI, DGCCRF, CNIL) en matière de tentatives d'extractions malveillantes ;
- Prévoir les outils de chiffrement, modes de communication, politique de mot de passe privilégiés et tout autre standard pour la transmission de données personnelles à un organisme tiers autorisé.

SOURCES JURIDIQUES ET OUTILS

Centralisation des coordonnées des contacts pertinents pour toute vérification utile :

- coordonnées de contact des délégué(e)s à la protection des données (accessibles en OPEN DATA depuis cette page) ;
- coordonnées de contact des administrations (accessibles depuis cette page)

Référencement des pratiques malveillantes et arnaques liées au RGPD ayant notamment pour objet la collecte d'informations (Signalement CNIL accessibles depuis cette page ; Signalements DGCCRF accessibles depuis cette page).

Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (et sa modification)

Recueil des procédures « tiers autorisés » référençant les principaux acteurs et procédures susceptibles de concerner les responsables de traitement de données

Article web CNIL « Comment chiffrer ses documents et ses répertoires ? »

Passeport de conseil aux voyageurs (ANSSI), qui traite notamment des cas de demandes d'accès aux données et équipements par des autorités étrangères à l'occasion de déplacements

Liste des produits de sécurité qualifiés par l'ANSSI

Page web CNIL « Comment se passe un contrôle de la CNIL ? »