

LES ISCG ET LE STOCKAGE DES DONNÉES

QU'EST-CE QUE LE RGPD ?

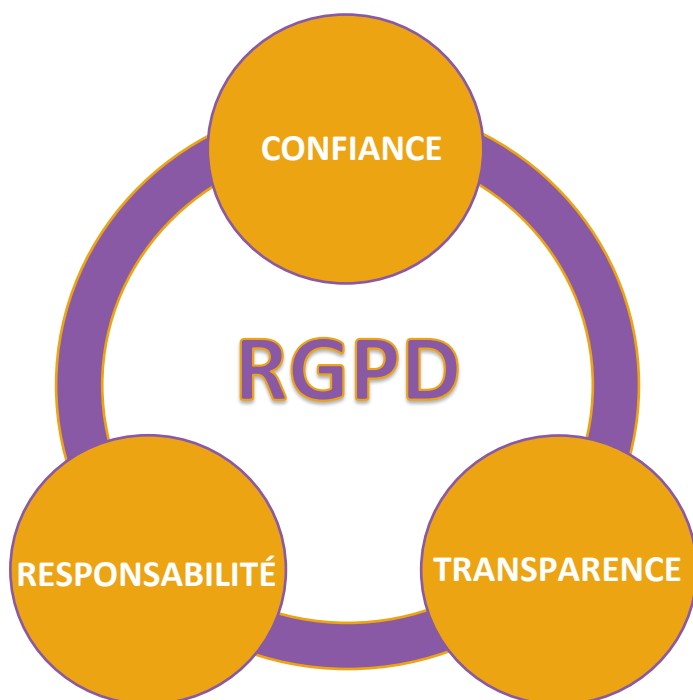
Le RGPD s'impose aux ISCG. Le sigle RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne. Les ISCG sont soumis aux règles RGPD de leur employeur et non à celles de leur autorité fonctionnelle (Police/Gendarmerie)

Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

En 3 points, **l'objectif du RGPD** c'est :

- Une protection des données à caractère personnel **similaire** entre les habitants de l'UE ;
- Un cadre légal sur le traitement de données personnelles **simplifié** et **allégé** ;
- **Une responsabilité accrue** de la part des institutions.



PROTECTION DES DONNÉES : **Les 6 bons réflexes à adopter**

1. Ne collectez que les données vraiment nécessaires pour atteindre votre objectif.
2. Soyez transparent.
3. Organisez et facilitez l'exercice des droits des administrés.
4. Fixez des durées de conservations.
5. Sécurisez les données et identifiez les risques.
6. Inscrivez la mise en conformité dans une démarche continue.

Les 8 principes de la protection des données



Pour résumer :

- **Le principe de finalité** : avoir une raison bien précise, légale et légitime pour chaque traitement
- **Le principe de proportionnalité et de pertinence** : Ai-je bien besoin de cette information ? Ai-je bien limité ma collecte et ma conservation de données au minimum de ce dont j'ai besoin ?
- **Le principe d'une durée de conservation limitée** : Une durée de conservation précise doit toujours être fixée, en rapport avec la sensibilité de l'information, et la finalité définie au départ
- **Le principe de sécurité et de confidentialité** : le responsable du fichier/des données doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
- **Les droits des personnes** : La personne a le droit d'accéder à ses données personnelles, mais pas à celles concernant des tiers, même si elles figurent dans son dossier

Le cycle de vie des données collectées



A chaque étape du cycle de vie d'une donnée (document, notes d'entretien, dossier...) les grands principes des règles RGPD devront s'appliquer.

ISCG ET DOSSIER SOCIAL

Le dossier social ne peut contenir que des documents administratifs (copies) et des documents professionnels finalisés. Ce sont des documents transmissibles et accessibles par la personne accompagnée.

Selon les règles RGPD, le dossier social est à détruire après 2 ans sans contact avec la personne accompagnée. En cas de contentieux, le dossier peut être conservé 5 ans. Néanmoins, il peut être conservé aussi longtemps que le professionnel le juge nécessaire si l'accompagnement se poursuit sur une plus longue période.

Les documents administratifs

Il s'agit de copies de documents (ex : CNI, fiche de paie, avis d'imposition...) confiés par la personne accompagnée dans le cadre d'une aide pour réaliser une démarche judiciaire, sociale, administrative. La règle ici est de conserver ces documents le temps nécessaire à cette aide. Une fois terminé, ces documents sont à détruire.

Les documents finalisés

Il s'agit d'un document rédigé par le professionnel et transmis à un service ou à la personne accompagnée (ex : attestation, note sociale, information préoccupante...). Il existe donc un lieu dans lequel ce document est conservé (selon les règles d'archivage de l'institution destinataire de cet écrit). Aussi, il semble cohérent d'appliquer le droit à l'oubli, ainsi une fois transmis ce document peut être conservé pendant une durée raisonnable puis il convient de le détruire.

Les notes d'entretien

La prise de note personnelle par l'ISCG est non obligatoire et sans conditions de formes particulières (document manuscrit ou tapuscrit). Il s'agit d'un outil de travail pour le professionnel. Ce document est à la seule destination du professionnel et reste sous la responsabilité de l'ISCG, il ne peut être compris que par ce dernier et ne doit pas figurer dans un quelconque dossier social.

Ces notes ne peuvent pas être remises aux personnes accompagnées mais peuvent être saisies par un enquêteur, en cas de procédure judiciaire même si elles sont stockées indépendamment du dossier social.

Accès au dossier social de l'ISCG par le policier/gendarme

Il n'existe qu'une seule possibilité pour un enquêteur d'accéder au dossier social d'une personne : La réquisition judiciaire (Pour davantage d'information, voir la fiche ISCG et Secret Professionnel [ici](#)).

AU DÉPART DE L'ISCG

Quels sont les documents transmissibles ?

Le dossier social (contenant des documents administratifs et documents professionnels finalisés) est transmissible à l'ISCG remplaçant (à condition que l'ISCG qui prend le relais ait le même employeur, c'est la question de la continuité de service). Si le poste risque d'être vacant pendant une période conséquente, l'ANISCG conseille de ne laisser que des écrits produits à la demande des personnes accompagnées (ex : attestation, note sociale, information préoccupante...), il s'agit ici de garantir le droit à l'accès de ces dernières. Ainsi, lors du départ de l'ISCG, l'employeur devient responsable des documents laissés et doit penser le stockage de ces documents.

Les notes d'entretiens, étant des notes personnelles, elles ne sont en aucun cas transmissibles à l'ISCG suivant. Ainsi les conserver sur une durée excessive leur fait perdre de leur utilité et renforce inutilement le risque que d'autres personnes y accèdent et engage la responsabilité de l'ISCG.

LES DOCUMENTS TRANSMIS À L'ISCG

Les documents transmis par Policiers et Gendarmes : En principe, l'ISCG n'a pas vocation à être destinataire de documents établis par les services de police ou de gendarmerie (plainte, main courante, procès-verbal d'audition, PVRJ, etc.). Toutefois, localement, certains de ces documents peuvent lui être transmis lorsque cette possibilité est expressément prévue par une convention, une note de service ou tout autre texte interne encadrant cette pratique. Cette transmission a pour seul objectif de faciliter l'évaluation de la situation et l'accompagnement social des personnes concernées.

À savoir : Si l'ISCG doit se déplacer avec ces documents (ex : en cas d'intervention sur plusieurs commissariats ou unités de gendarmerie ou lors du télétravail), en cas de vol ou perte, si ces documents étaient nécessaires pour sa mission, le professionnel ne peut pas être tenu responsable, il s'agira alors d'une faute du service et non d'une faute professionnelle. Pour lever le doute, l'ISCG pourrait mentionner dans son bilan annuel présenté à l'employeur que des documents sont transportés pour nécessité de service (l'employeur ne pourra alors pas ignorer cette information).

Les documents transmis par les personnes accompagnées : L'ISCG peut également être destinataire de ces documents (plainte et main-courante) qui lui sont remis directement par les personnes accompagnées dans le cadre d'une aide aux démarches sociales et administratives. Dans ce cas, les règles RGPD s'appliquent de la même manière en ce qui concerne le stockage, la conservation et la destruction que pour le dossier social et les documents finalisés.

Cas particulier : les documents confiés à l'ISCG pour être conservés en lieu sûr.

Certaines personnes accompagnées peuvent demander au professionnel de garder des documents sensibles (ex : plainte, certificat médical...) en sécurité pour éviter qu'ils ne soient par exemple détruits par un conjoint violent. Il s'agit ici d'un service rendu à ces personnes, l'ISCG peut au préalable conseiller de mettre en sécurité ces documents dans un lieu sûr (travail, chez un ami...) mais aussi sur des plateformes de stockage sécurisées comme le site *Mémo de Vie*. Si l'ISCG doit conserver ces documents, il s'agit d'un engagement moral entre le professionnel et la personne avec des règles clairement établies entre eux (mode de conservation, limite de temps...) Il pourrait alors être envisagé que ces documents soient conservés dans une enveloppe (indépendamment du dossier social) et garantir le droit d'accès même en cas de changement de professionnel. En ce qui concerne les documents officiels (pièce d'identité, livret de famille, carnet de santé...) il est préférable de proposer de conserver uniquement des copies certifiées conformes si besoin et non les documents originaux.

ARCHIVAGE ET DESTRUCTION

Les règles concernant l'archivage et la destruction des documents appartenant à l'ISCG sont régies par les règles RGPD de l'employeur. Ainsi quand il est nécessaire de détruire un document, l'ISCG peut le faire sur son lieu d'exercice (Commissariat ou Unité de Gendarmerie). Le principe de la destruction est que l'identité et les informations contenues dans le document détruit ne puissent pas aisément être retrouvées (ex : broyeuse). Si aucun moyen de destruction n'est à disposition directe de l'ISCG, le professionnel peut le faire dans les locaux de son employeur.

En ce qui concerne l'archivage, les règles ont été développées dans l'encart sur **le dossier social** avec un rappel important ici sur le fait que les documents appartenant à l'institution Police/Gendarmerie doivent être conservés dans un lieu seulement accessible à l'ISCG, ces documents ne peuvent donc pas être archivés dans les locaux de l'employeur.

Pour toutes informations complémentaires, les ISCG peuvent se renseigner auprès de l'archiviste de leur institution.

Mails, messages, application de discussion...

Les ISCG sont amenés dans leurs pratiques à communiquer par écrit avec les personnes accompagnées, notamment par mails ou messages. Il peut également arriver que des documents soient transmis par ces personnes à l'ISCG via ces outils informatiques ou inversement. Il est alors important de rappeler que **dès lors que l'on produit un écrit qui est diffusé, cela engage la responsabilité du professionnel qui le rédige**. De même, le Secret des correspondances (Art 226-15 et 432-9 du Code Pénal) ne s'applique qu'à un tiers (personne morale ou physique) et non au professionnel et à la personne accompagnée. Ainsi, l'ISCG soumis au SP ne pourra en aucun cas divulguer les informations contenues dans cet échange écrit mais la personne accompagnée pourra elle, si elle le souhaite, diffuser ou partager cet échange. **Il est à noter que dans le cadre d'une enquête judiciaire, sous certaines réserves, les outils informatiques peuvent être saisis ainsi les données contenues dans la messagerie ou le téléphone portable peuvent faire l'objet d'une exploitation.**

En ce qui concerne les documents transmis via ces outils, la bonne pratique est d'enregistrer ces derniers en les sécurisant et de supprimer le message ou mail les contenant. Il est également judicieux de proposer à l'expéditeur d'effacer également ce message pour limiter les risques en cas de piratage. Dans tous les cas il est possible pour l'ISCG de se référer à la charte informatique de son employeur pour préciser les règles en vigueur dans son institution.



* Virtual Private Network : Réseau privé et sécurisé virtuel

Cette fiche regroupe les règles générales du RGPD mais il est important de prendre en considération les règles établies par chaque employeur localement, règles qui diffèrent selon l'institution employeur (ex : association ou collectivité territoriale)

Pour toutes questions ou interrogations, le référent RGPD de l'employeur est le mieux placé pour y répondre, il ne faut donc pas hésiter à le solliciter en cas de besoin.

Une question, un doute, une idée à ajouter à cette fiche? Vous pouvez contacter les chargés de mission ANISCG via le mail contact@aniscg.org ou les référents régionaux via leurs mails.