ESFIN GESTION	**Politique relative à la protection et traitement des données personnelles**	

DATE DE CREATION :	10/02/2022
DATE DE MISE A JOUR :	25/11/2025
VERSION	V2
REDACTEUR :	AGAMA CONSEIL
VALIDATION :	DIRECTOIRE D'ESFIN GESTION
LISTE DE DIFFUSION :	TOUS LES COLLABORATEURS D'ESFIN GESTION

Table des matières

Préambule

Références réglementaires

Règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (dit « RGPD »)

Le RGPD vise à renforcer les droits des personnes physiques à l'égard du traitement de leurs données à caractère personnel. Les entreprises se trouvent soumises à un ensemble d'obligations renforcées voire nouvelles, afin de garantir une légitimité du traitement ; elles devront en effet assurer une protection optimale des données et être en mesure de la démontrer en documentant leur conformité.

La mise en application du RGPD a ainsi pour conséquence de supprimer les formalités préalables exigées auprès de la CNIL. Sauf exception, il n'y a donc plus de déclaration ou d'autorisation préalable à la mise en place d'un traitement de données à caractère personnel. Cette obligation a été substituée par l'obligation pour les entreprises de démontrer sa mise en conformité, notamment par la tenue des registres des traitements effectués (ci-après développé).

La CNIL peut ainsi effectuer des enquêtes de sa propre initiative ou à la suite d'une réclamation d'une personne concernée (un formulaire en ligne est prévu afin de faciliter la démarche).
L'autorité de contrôle dispose du pouvoir d'adopter diverses mesures correctrices, à savoir :

- Prononcer un avertissement ou un rappel à l'ordre sur le fait que les opérations de traitement envisagées sont susceptibles d'une violation du règlement
- Demander une mise en conformité dans un délai déterminé
- Ordonner de satisfaire aux demandes de respect des droits des personnes et de son exercice
- Limiter temporairement ou définitivement un traitement
- Suspendre les flux de données
- Retirer la certification
- **Prononcer des amendes pouvant aller jusqu'à 20 millions d'euros et 4% du chiffre d'affaires annuel monde.**

Par ailleurs, des actions de groupe peuvent être portées devant les tribunaux judiciaires par les personnes concernées de façon à obtenir des dommages et intérêts qui viendraient donc s'ajouter au montant des amendes prononcées par la CNIL.

Définitions

Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable » une personne physique qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Destinataire : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

«**Catégories particulières de données à caractère personnel** » ou « **Données sensible** » est défini comme les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

I. Organisation des ressources pour la protection des données

A. Périmètre d'application

Le *« règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* [1]*»*.

Les données auxquelles ESFIN Gestion a accès dans l'exercice de ses activités sont susceptibles de relever de la vie privée des personnes avec qui elle traite. Cela peut concerner les clients, prospects, fournisseurs, sous-traitants, collaborateurs…

B. Organisation interne

Les sociétés doivent désigner un Délégué à la Prospection des Données (DPO) dans les cas suivants :

- Si la Société appartient au secteur public ;
- Si les activités de base (principales) de la Société l'amène à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- Si ses activités de base (principales) de la Société l'amènent à traiter (toujours à grande échelle) des catégories particulières de données, dites « sensibles », et des données relatives à des condamnations pénales et à des infractions.

[1] article 3 RGPD

Dans les autres cas, la désignation d'un Délégué à la protection des données est encouragée par la CNIL.

ESFIN Gestion apprécie, si en fonction notamment du nombre de personnes concernées par les traitements de données à caractère personnel, du volume des données traitées, de la durée ou de la permanence des activités de traitement, de l'étendue géographique de l'activité de traitement, elle doit nommer un référent RGPD. La nomination d'un référent RGPD peut également se faire de façon volontaire.

Le référent RGPD est chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de s'assurer du respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Au sein de ESFIN Gestion le référent RGPD est Alexis FUZIER, Secrétaire Général.

II. La mise en place d'un traitement

A. La justification du traitement

▪ La licéité du traitement

Le traitement doit être justifié par une base légale qui autorise sa mise en œuvre.

✓ **Le consentement**

Le consentement est défini comme étant « une manifestation libre, spécifique, éclairée et univoque par laquelle une personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fasse l'objet d'un traitement ».

Ainsi, le consentement de la personne n'est pas obligatoire pour recueillir ses données lorsqu'elles découlent d'un intérêt légitime et donc nécessaire à l'exécution d'un contrat (lettre de mission, mandat…).

Le consentement s'accompagne de deux principes importants :

- Droit au retrait : la personne doit avoir la possibilité de retirer son consentement à tout moment, par le biais d'une modalité simple et équivalente à celle utilisée pour recueillir le consentement.

- Preuve du consentement : ESFIN Gestion doit être en mesure de démontrer à tout moment que la personne a bien consenti, dans des conditions valides (bonne information des personnes, caractère positif de l'expression du choix de la personne, …).

✓ **Le contrat**

Afin de pouvoir justifier de cette base légale pour certains traitements, il doit exister une relation contractuelle ou précontractuelle entre ESFIN Gestion et la personne concernée.

Le contrat doit être valide au regard du droit applicable.

Le traitement doit être strictement nécessaire à l'exécution du contrat. Il doit donc permettre uniquement d'exécuter le contrat spécifique avec la personne et n'avoir aucun autre objectif.

- ✓ **L'obligation légale**

Le traitement est imposé par des textes légaux applicables.

- ✓ **L'intérêt légitime**

Afin de répondre à un intérêt légitime dont la liste n'est pas exhaustive, ESFIN Gestion peut mettre en place un traitement sur cette base aux fins de :

- garantir la sécurité du réseau et des informations,
- mettre en œuvre à des fins de prévention de la fraude,
- procéder aux opérations de prospection commerciale auprès de clients d'une société,
- porter sur des clients ou des employés à des fins de gestion administrative interne ;
- […]

L'intérêt légitime doit être justifié par :

- Sa légitimité : licite au regard du droit applicable, déterminé de façon précise et claire, nécessaire pour ESFIN Gestion ;
- L'absence d'atteinte aux intérêts et droits et libertés des personnes, compte tenu de leurs attentes raisonnables ;
- La mise en balance de l'ensemble de ces éléments.

    - **Analyse d'impact**

Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment le traitement à grande échelle de catégories particulières de données, le responsable du traitement doit effectuer, avant toute mise en œuvre, une analyse d'impact.

ESFIN Gestion doit apprécier s'il doit mettre en place une analyse d'impact dans le cadre du traitement des données. Il pourrait avoir à mettre en œuvre une analyse d'impact :

- Si ESFIN Gestion effectue un traitement de données à grande échelle *(considérant 91 : opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernée*) ;
- Quand bien même il ne traiterait pas des données à « grande échelle » si les traitements mis en œuvre répondent à certaines caractéristiques.

En effet, dès lors qu'il répondra à plus de deux des neuf critères déterminés par la CNIL et par le G29 (évaluation/scoring, décision automatique avec effet légal ou similaire ; surveillance systématique ; collecte de données sensibles ; collecte de données à caractère personnel à large échelle ; croisement de données ; personnes vulnérables ; usage innovant ; exclusion du bénéfice d'un droit / contrat), le traitement sera, par principe, soumis à analyse d'impact.

Pour aller plus loin : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

S'il met en place une analyse d'impact, ESFIN Gestion utilise le logiciel open source PIA facilitant la conduite et la formalisation d'analyses d'impact sur la protection des données telles prévues par le RGPD : https://www.cnil.fr/fr/outil-pia-nouvelle-version-beta-du-logiciel

- **En cas de données sensibles**

ESFIN Gestion ne traite pas des informations sensibles relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes, à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, dans le cadre de ces activités .

En effet, l'article 9, al.1, du RGPD prévoit l'interdiction de principe du traitement de telles données et, conformément à l'article 5 du RGPD, ESFIN Gestion ne doit collecter que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

- **Durée de conservation des données**

ESFIN Gestion ne conserve pas indéfiniment les informations figurant dans un fichier. Il établit une durée de conservation en fonction de la finalité de chaque fichier tel que décrit au sein de la procédure relative à l'archivage des données.

B. La communication sur le traitement

- **Le registre**

ESFIN Gestion doit être en mesure de suivre et d'identifier les destinataires des données à caractère personnel qu'il traite.

ESFIN Gestion doit tenir un registre des catégories de traitement de données à caractère personnel mises en œuvre sous sa responsabilité :

- S'il comporte plus de 250 salariés ou ;
- Si le traitement qu'il effectue est susceptible de comporter un risque au regard des droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou ;
- S'il porte notamment sur des données sensibles, ou sur des données se rapportant à des condamnations et des infractions pénales.

Le registre doit comporter les informations suivantes :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- les finalités du traitement ;
- Une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou vers une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale, et les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

A été désigné responsable du traitement des données : Alexis FUZIER, Secrétaire Général.

- **L'information des clients**

✓ **Information générale**

ESFIN Gestion a rédigé sur son site internet une politique de confidentialité comprenant les informations suivantes, afin d'informer les personnes concernées :

- de l'identité et des coordonnées du responsable de traitement ;
- des coordonnées du délégué à la protection des données lorsqu'il y en a un ;
- de l'objectif poursuivi (gestion et suivi des dossiers de ses clients) ;
- de la base juridique du traitement (exécution contractuelle ou précontractuelle à la demande du client) ;
- de l'intérêt légitime s'il s'agit de la base légale du traitement ;
- des destinataires des données (des sous-traitants, des huissiers, etc.) ;
- des flux transfrontières ;
- de la durée de conservation ;
- des droits dont ils disposent ;
- des conditions d'exercice de ces droits ;
- du droit de retirer son consentement s'il s'agit de la base légale du traitement ;
- du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur le caractère réglementaire ou contractuel du traitement lorsqu'il s'agit de la base légale du traitement.

Ces informations peuvent figurer aussi au sein du document d'informations précontractuelles ou des documents contractuels (y compris les contrats des collaborateurs). Elles peuvent également faire l'objet d'une communication par courriel ou par document distinct, notamment pour régulariser la situation auprès des clients qui n'ont pas été correctement informés, ou encore renvoyé sur le site internet.

✓ **Information contractuelle**

ESFIN Gestion communique sous quelque forme que ce soit (document distinct, clauses contractuelles), les informations suivantes lorsque les données sont collectées auprès de la personne concernée :

- les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- les finalités du traitement auquel sont destinées les données à caractère personnel ;
- la base juridique du traitement ;
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque ces intérêts légitimes sont la condition de licéité du traitement ;
- le fait que le responsable de traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ;
- le cas échéant, l'existence ou l'absence d'une décision d'adéquation rendue par la CNIL, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
- lorsque le traitement est fondé sur le consentement de la personne concernée, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

C. Le traitement des données personnelles et les ressources humaines

Dans le cadre du recrutement d'un employé ayant des activités d'intermédiation et de conseil auprès de la clientèle, ou encore de personnel support, ESFIN Gestion est amené à effectuer des traitements de données à caractère personnel, dans le respect des principes du RGPD.

ESFIN Gestion prend connaissance de la Norme simplifiée CNIL NS-046 en matière de gestion du personnel : https://www.cnil.fr/fr/declaration/ns-046-gestion-du-personnel

- **Données recueillies**

✓ **Principe général de respect de la minimisation**

ESFIN Gestion ne doit collecter que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

✓ **Recrutement**

Les données ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé.
Seules des données relatives à la qualification et à l'expérience du collaborateur peuvent être collectées (exemples : diplômes, emplois précédents, etc.)

Il est donc interdit de :
- demander à un candidat son numéro de sécurité sociale ;
- collecter des données sur la famille du candidat ;
- collecter des données sur les opinions politiques ou l'appartenance syndicale du candidat.

✓ **Gestion du personnel**

Dans le cadre de la gestion de son personnel, ESFIN Gestion peut collecter principalement deux types de données :
- des données nécessaires au respect d'une obligation légale.
- des données utiles à la (i) gestion administrative du personnel, (ii) à l'organisation du travail et (iii) à l'action sociale.

L'information relative à la RGPD doit faire l'objet d'un article dans le contrat de travail de tout nouveau collaborateur

✓ **Contrôle de l'activité**

ESFIN Gestion peut mettre en place des outils de contrôle des activités du personnel :
- encadrement des conditions d'utilisation d'internet sur le lieu de travail ;
- dispositif de contrôle des horaires et d'accès du personnel.

ESFIN Gestion prend connaissance de la Norme simplifiée CNIL n°42 portant sur les badges dans les lieux de travail : https://www.cnil.fr/fr/declaration/ns-042-badges-sur-le-lieu-de-travail

- **Dispositif de traitement des données en matière RH**

✓ **Registre de traitement des données**

Le registre des activités de traitement doit contenir une fiche dédiée à la gestion des ressources humaines qui doit comporter les éléments suivants :

- identité et coordonnées du responsable de traitement ;
- finalités ;
- catégories de personnes concernées ;
- catégories de données à caractère personnel ;
- catégories de destinataires ;
- transferts vers un pays tiers ou une organisation internationale ;
- délais prévus pour l'effacement ;
- description générale des mesures de sécurité techniques et organisationnelles.

✓ **Conservation**

ESFIN Gestion conserve ces éléments dans les dossiers courant durant le temps de la période d'emploi de la personne concernée (sauf dispositions législatives ou réglementaires contraires).

Au-delà, ces données peuvent être archivées pendant les durées de prescriptions légales, sur un support informatique distinct et à accès très limité, conformément aux règles applicables en matière d'archives publiques et d'archives privées.

D. Le traitement et les sous-traitants

Le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement ». Il peut s'agir notamment d'un comptable, un éditeur de logiciel, un hébergeur, etc.

- **S'agissant des relations contractuelles préexistantes avec les sous-traitants**

Il convient à ESFIN Gestion de s'assurer que les sous-traitants connaissent leurs nouvelles obligations. Les contrats de sous traitement doivent faire l'objet d'un avenant intégrant les éléments ci-après énumérés.

- **Les mentions d'informations**

Le contrat liant ESFIN Gestion au sous-traitant doit comporter :

- l'objet ;
- la durée ;
- la nature ;
- la finalité ;
- le type de données à caractère personnel ;
- les catégories de personnes concernées ;
- les droits et obligations du responsable de traitement ;

- les mesures de sécurité mises en œuvre concernant le traitement de données à caractère personnel qui sera réalisé.
- la possibilité de ne traiter les données que sur instruction documentée du responsable du traitement, même en ce qui concerne les flux transfrontières ;
- la confidentialité des données ;
- l'exercice des droits des personnes concernées ;
- l'aide qu'il doit fournir au responsable de traitement par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, pour s'acquitter de l'obligation de donner suite aux demandes des personnes concernées ;
- l'aide fournie au responsable de traitement pour garantir le respect de ses obligations compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
- la suppression des données concernées à l'issue du traitement, ou leur renvoi au responsable de traitement ou leur conservation s'il en est tenu par une disposition nationale ou européenne ;
- la mise à disposition du responsable du traitement de toutes les informations nécessaires pour démontrer le respect de ces obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;
- l'éventuel recrutement par le sous-traitant d'un sous-traitant ultérieur, d'un nouveau sous-traitant, et l'obtention de l'autorisation préalable écrite du responsable de traitement relative à ce recrutement qui doit être formalisé par un contrat mentionnant l'ensemble des obligations ci-dessus énumérées.

ESFIN Gestion a l'obligation de ne recourir qu'à « des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée ». Cela comprend notamment l'endroit où se situent les serveurs (UE ou tout lieux respectant la réglementation RGPD).

ESFIN Gestion doit interroger ses sous-traitants sur les garanties qu'ils ont mises en place afin de garantir leur conformité au RGPD. Dans le cas où ESFIN Gestion identifie des lacunes dans les mesures mises en place par le sous-traitant, ils devront conclure un avenant au contrat afin de combler lesdites lacunes.

III. Le dispositif de violation des données personnelles

La violation de données à caractère personnel est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.
En cas de détection par un collaborateur, d'une violation des données au sein ESFIN Gestion, celui-ci procède à la remontée de l'incident auprès du référent RGPD ou le cas échéant auprès de la personne en charge de la protection des données personnelles.

La personne destinataire de la remontée doit procéder à l'évaluation de l'incident afin d'en déterminer le niveau de gravité.

Un comité peut être organisé avec les parties prenantes au sein de l'entité afin de :
- Décider du niveau de gravité de l'incident ;
- Rédiger un post-mortem afin de prendre toutes les mesures nécessaires pour prévenir d'un prochain incident.

Sauf dans les cas où la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, ESFIN Gestion notifie à la CNIL dans les meilleurs délais et au plus tard dans les 72 heures après en avoir pris connaissance.

Un formulaire de notification de violation de données à caractère personnel est à la disposition du responsable de traitement sur le site de la CNIL :
https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

Si ESFIN Gestion a un sous-traitant, celui-ci devra également notifier au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

ESFIN Gestion informera directement la personne concernée de la violation, sauf dans les cas où la violation n'est pas susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

IV. Exercice des droits

A. Réception de la demande

Par ailleurs, toute personne physique justifiant de son identité a le droit d'interroger ESFIN Gestion notamment pour :
- Avoir des informations sur ses données détenues au sein de l'entité ;
- Accéder à ses données détenues au sein de l'entité ;
- Demander la rectification de ses données détenues au sein de l'entité ;
- Demander le droit à l'oubli de ses données détenues au sein de l'entité ;
- S'opposer au traitement de ses données détenues au sein de l'entité ;
- Demander la limitation du traitement de ses données personnelles ;
- Demander la portabilité de ses données personnelles ;
- Demander de ne pas faire l'objet d'une décision exclusivement automatisée.

Le demandeur peut effectuer sa demande via le canal qu'il souhaite (E-mail ; courrier ; de vive voix) auprès d'un collaborateur de ESFIN Gestion.
Ce dernier doit faire remonter la demande sans délai auprès de la personne en charge de la protection des données personnelles : Alexis FUZIER, Secrétaire Général.
Lorsque qu'elle a reçu la demande, elle doit en accuser réception.

Le demandeur doit obtenir une réponse dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande.

Au besoin, ce délai peut être prolongé d'un mois supplémentaire, compte tenu de la complexité et du nombre de demandes, en informant la personne concernée de cette prolongation et de ces motifs.

La personne en charge de la protection des données personnelles a la possibilité de revenir vers le demandeur afin d'obtenir des informations complémentaires. Dans ce cas, le délai d'un mois est suspendu jusqu'à réception des nouveaux éléments.

B. Saisine de la CNIL

Si ESFIN Gestion ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel

V. Transfert des données

A. Vers un pays membre de l'UE ou un pays tiers ayant un niveau de protection adéquat

Les transferts de données vers un pays membre de l'UE (soumis au RGPD) ou vers un pays tiers ayant un niveau de protection adéquat sont garantis par la réglementation applicable au sein de ces Etats.

Les transferts de données personnelles réalisés au sein de ESFIN Gestion doivent tout de même être effectués de manière sécurisée pour maintenir la confidentialité, l'intégrité et la disponibilité des données (mots de passe dans les fichiers, E-mail avec certificats de chiffrement…).

B. Vers un pays tiers ne disposant pas d'un niveau de protection adéquat

En cas de transfert de données par ESFIN Gestion vers un pays tiers ne disposant pas d'un niveau de protection adéquat, des mesures juridiques d'encadrement doivent être mises en place.

Les mesures d'encadrement de ces transferts ne nécessitant pas une approbation préalable de la CNIL sont :

- Une décision d'adéquation de la Commission européenne pour certains pays tiers ;
- Les règles internes d'entreprises (Binding Corporate Rules) pour des transferts intra-groupes ;
- Les clauses contractuelles types (approuvées par la Commission Européenne) ;
- Un code de conduite approuvé rédigé par le destinataire afin d'appliquer les garanties appropriées
- Une certification approuvée permettant au destinataire de démontrer les mesures prises pour garantir le niveau de protection

Les mesures d'encadrement de transferts devant être approuvées préalablement par la CNIL sont les clauses contractuelles types ad'hoc.

C. En interne

Les transferts ou utilisations de données personnelles réalisés au sein de ESFIN Gestion doivent être effectués de manière sécurisée pour maintenir la confidentialité, l'intégrité et la disponibilité des données (mots de passe dans les fichiers, e-mail avec certificats de chiffrement…).

L'accès aux locaux dans lesquels sont stockés les dossiers est suffisamment sécurisé (bureaux fermés à clefs, accès par badge, etc.), ainsi que la sécurité du système d'information sur lequel sont stockés les dossiers sous format numérique (pare- feu, mots de passe, habilitations, etc.).

ESFIN Gestion met en place des mesures de sécurité informatiques des données personnelles :

- authentifier les utilisateurs (mot de passe de minimum 8 caractères contenant une majuscule, une minuscule, un chiffre et un caractère spécial)
- déterminer les personnes qui sont habilitées à accéder aux données à caractère personnel ; supprimer les permissions d'accès obsolètes ;
- sécuriser l'informatique mobile ;
- mettre en place des sauvegardes régulières, stocker les supports de sauvegarde dans un endroit sûr, etc.