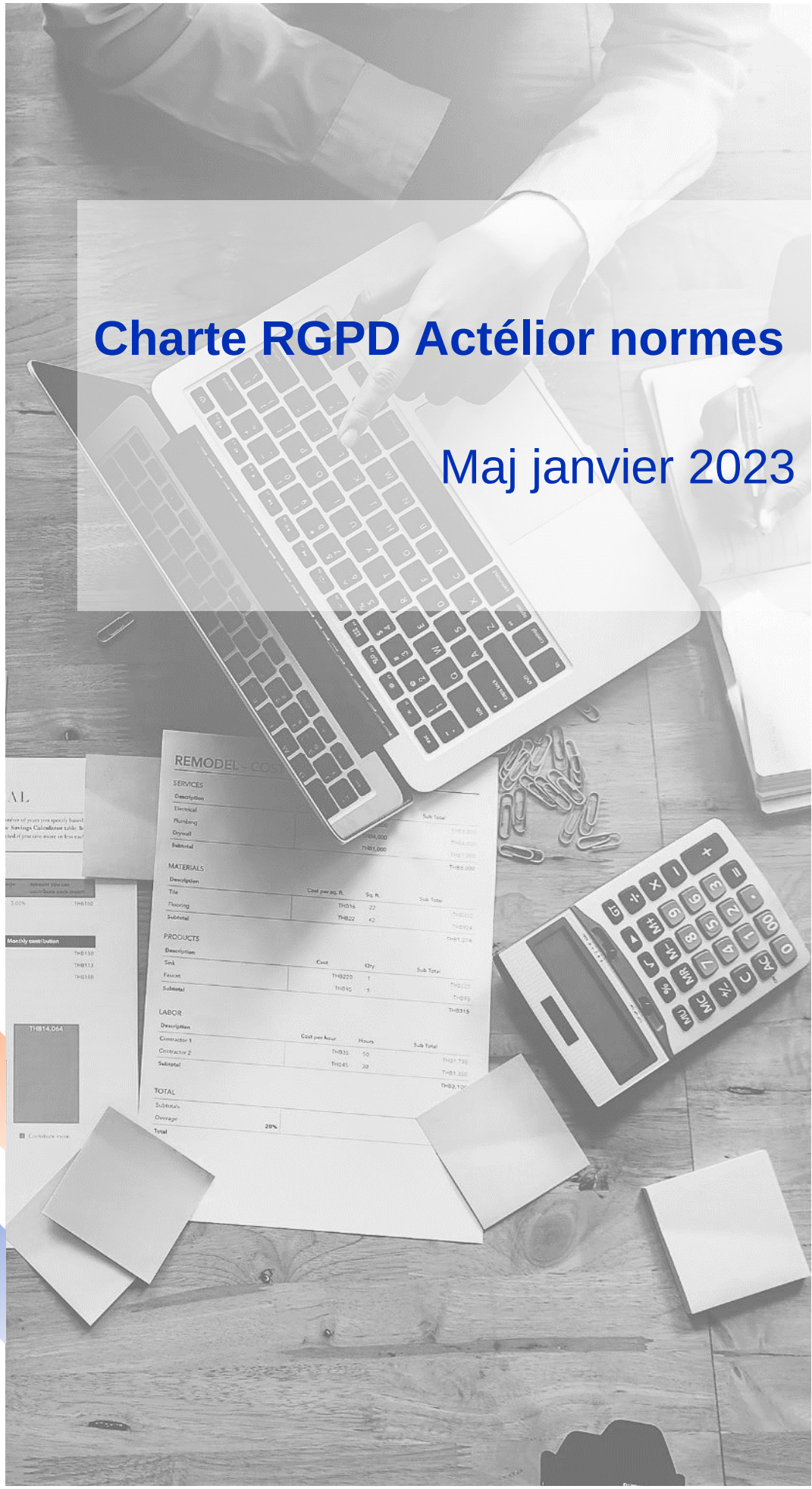
Actélior
Le partenaire catalyseur de toutes vos ambitions



Charte RGPD Actélior normes

Maj janvier 2023

7bis rue des Aulnes - 69410 CHAMPAGNE AU MONT D'OR
12 rue Beccaria – 75012 PARIS
Tél. : 04 78 66 30 00 – e-mail : actelior@actelior.com
RCS LYON 428 658 736

SOMMAIRE

I. Préambule

Actélior accorde une importance toute particulière à la protection des données personnelles. Cette charte a pour objectif de définir un cadre d'application du Règlement Général sur la Protection des Données (RGPD), n° 2016/679 du 27 avril 2016 au sein d'Actélior.

Le Règlement Général sur la Protection des Données poursuit trois objectifs :

- ✓ *Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;*
- ✓ *Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;*
- ✓ *Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.*

L'activité principale d'Actélior n'est pas de collecter ou de traiter1 des données personnelles2 et les données nécessaires à l'exécution des missions n'incluent que ce type de données. Cependant, les données transmises par nos clients peuvent parfois être qualifiées de données personnelles.

Cette charte définit les rôles et responsabilités de chacun et présente le mode opératoire à suivre lors de la réception de données en provenance de clients.

Le respect de cette charte par le collaborateur est matérialisé par la signature d'un engagement, en annexe de ce document.

II. Traitement des données reçues

II.1. Finalité des données

Les données nécessaires à l'exécution de la mission sont définies au préalable par Actélior et communiquées au client. Elles sont limitées aux données strictement nécessaires à l'exécution de la mission d'Actélior et proportionnées aux besoins. Les données de type données personnelles sont évitées autant que possible.

Seules les données nécessaires et pertinentes au regard des finalités définies dans le cadre de la mission d'Actélior sont conservées. Dans le cas de réception de données personnelles ne rentrant pas dans ce cadre, les fichiers réceptionnés concernés sont supprimés et un nouvel envoi en conformité avec le principe ci-dessus est demandé au client. De façon dérogatoire, la suppression des données personnelles non nécessaires et/ou pertinentes pourra être exécuté directement par Actélior après information et accord du client.

[1] Définition de « données personnelles » en Annexes
[2] Définition de « traitements de données » en Annexes

II.2. Traitements des données

Les traitements sont limités aux seules opérations nécessaires à l'exécution de la mission d'Actélior ou aux demandes explicites du client. Tout autre traitement est à proscrire et ne pourra être exécuté qu'après approbation explicite et documentée du client.

II.3. Devoir d'alerte

Si les traitements nécessaires à l'exécution de la mission, ou demandés explicitement par le client, contreviennent au RGPD, ils sont suspendus et le client ainsi que le manager d'Actélior sont alertés. Les traitements ne peuvent être repris qu'après validation de leur licéité.

III. Registre des traitements

Si le traitement de données personnelles s'avère indispensable à la bonne exécution de la mission, ces traitements seront consignés dans le registre de traitement des données Actélior.

Le registre des données sera créé lors de la première occurrence.

IV. Sécurité des données

Les données personnelles étant confidentielles, elles ne doivent être consultées et utilisées que dans le cadre de la mission attribuée à Actélior.

Les données individuelles sont disponibles uniquement sur le réseau sécurisé Actélior. Aucune copie ne doit être effectuée sur un support amovible (clé USB, disque dur externe) ou en local sur un ordinateur portable.

Les données personnelles recueillies par Actélior ne sont en aucun cas cédées, louées ou échangées à des tiers.

Toutes les personnes ayant accès aux données personnelles sont liées par un devoir de confidentialité et s'exposent à des mesures disciplinaires et/ou autres sanctions si elles ne respectent pas ces obligations.

V. Durée de conservation des données

Les données sont stockées et conservées pour une durée conforme aux instructions du client.

VI. Violation des données

Une violation de données est un incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

Si un tel évènement se produit, le manager et le Directeur Général d'Actélior doivent être immédiatement informés. Les mesures nécessaires seront alors prises, notamment concernant la communication au client et, si nécessaire, à la CNIL.

VII. Guide pratique concernant les données personnelles

VII.1. Principe de base

Eviter autant que possible les fichiers avec des données personnelles : nom, prénom, adresse exacte (liste non exhaustive) ainsi que les données non nécessaires à l'exécution de la mission. Par exemple pour la date de naissance, ne pas conserver le jour, voire le mois de naissance. De même, si la situation géographique est nécessaire ne conserver que le code postal voire le département.

Le numéro de Sécurité sociale est à proscrire dans tous les cas.

Dans le cas où un fichier comprend des données personnelles, se poser les questions suivantes :

- ✓ Les données personnelles sont-elles nécessaires à l'exécution de la mission Actélior ?
- ✓ Existe-t-il un autre identifiant ?
- ✓ Une pseudonymisation[3] en concertation avec le client est-elle possible ?

L'utilisation de données personnelles doit être justifiée par des impératifs liés à la mission d'Actélior :

- ✓ Bonne exécution des calculs ;
- ✓ Liens des données avec d'autres sources de données nécessaires au calcul ;
- ✓ Comparaison avec les données des exercices antérieur, à fin de validation ou de consolidation quand ces opérations font partie intégrante de la mission confiée à Actélior.

VII.2. Si les données personnelles ne sont pas indispensables

Idéalement, et après accord du client, supprimer les fichiers reçus et demander de nouveaux fichiers sans données personnelles au client.

A défaut, effectuer les traitements d'anonymisation sur les fichiers reçus (suppression des données personnelles), supprimer les fichiers sources et renvoyer au client les fichiers sources et les fichiers modifiés accompagnés d'une description des traitements effectués.

[3] *La pseudonymisation est une technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme. Cette technique permet la ré-identification ou l'étude de corrélations en cas de besoin particulier. Contrairement à l'anonymisation elle n'est pas irréversible. Une définition se trouve également en annexes.*

VII.3. Si les données personnelles sont indispensables mais une pseudonymisation est possible

Les données seront pseudonymisées en concertation avec le client :

- ✓ Ne pas intégrer Nom, Prénom (ni N° de Sécurité sociale) ;
- ✓ Prendre pour identifiant une codification interne au client (par ex. matricule) et non recoupable par Actélior : attention à l'unicité de l'identifiant et à sa pertinence dans le temps. Le même identifiant doit pouvoir être communiqué pour chaque personne pour chaque transmission de fichier, par exemple lors d'un nouvel envoi suite à une correction ou encore d'une année sur l'autre ;
- ✓ La procédure de pseudonymisation doit s'accompagner d'une limitation des données permettant une identification au stricte nécessaire (limitation de la date de naissance à l'année, limitation de l'adresse au département …).

A défaut, pseudonymisation par Actélior :

- ✓ Génération d'un code aléatoire pour l'identifiant ;
- ✓ Envoi de la correspondance Identifiant Actélior / Identifiant Client au client et suppression du tableau de correspondance chez Actélior ;
- ✓ Conservation du tableau de correspondance par le client.

Attention, la procédure de pseudonymisation par Actélior n'est pertinente que s'il n'y a pas lieu de comparer différents jeux de données entre eux, notamment celui d'une année par rapport à celui de l'année précédente. Du fait du caractère aléatoire de la génération de l'identifiant Actélior, il n'est en effet a priori pas possible de réattribuer le même identifiant Actélior à la même personne lors de deux générations différentes.

VII.4. Si les données personnelles sont indispensables et une pseudonymisation n'est pas possible

Valider avec le client qu'une anonymisation ou une pseudonymisation n'est pas possible. Formaliser autant que possible la demande du client de traitements de données personnelles par Actélior.

Le fichier de données doit être protégé par un mot de passe défini par le client. Ce mot de passe est communiqué à Actélior de façon distincte de l'envoi du fichier.

Le registre des traitements doit également être renseigné.

VIII. Documentation

Le site de la CNIL est également une source d'information importante avec des mises à jour régulières : https://www.cnil.fr/professionnel

Annexe 1 : engagement

Je soussigné(e) …… ……...
Exerçant la fonction de ……... au sein de la société Actélior et étant à ce titre amené(e) à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ✓ *Respecter la Charte Actélior RGPD ;*
- ✓ *Ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;*
- ✓ *Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;*
- ✓ *Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;*
- ✓ *Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;*
- ✓ *Prendre toutes précautions conformes à l'usage et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;*
- ✓ *M'assurer, dans la limite de mes attributions, que seuls les moyens de communication sécurisés seront utilisés pour transférer ces données ;*
- ✓ *En cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données ;*
- ✓ *Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel ;*
- ✓ *J'ai été informé(e) que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales, conformément à la règlementation en vigueur, notamment au regard des articles 226-16 et 226-24 du code pénal ;*

Fait à ……, le ……..

Signature

Annexe 2 : Définitions

« Données à caractère personnel » : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; 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 ;

« Données concernant la santé » : les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

« 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 ;

« Pseudonymisation » : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Actélior Paris

12 rue Beccaria
75012 Paris
Tél. 01 43 40 47 34

Actélior Lyon

7 bis rue des Aulnes
69410 Champagne au Mont d'Or
Tél. 04 78 66 30 00

actelior@actelior.com
www.actelior.com