ADHOC-GTI

adhoc-gti
S.A.S. au capital de 70900 €
RCS Strasbourg
Siret : 448 641 043 00030
Code APE : 5829C / TVA : FR29448641043

Règlement général sur la protection des données (RGPD)

Préambule

Le Règlement général sur la protection des données (RGPD) (en anglais : « General Data Protection Regulation », GDPR) s'applique dans l'ensemble des 28 États membres de l'Union Européenne **à compter du 25 mai 2018**. Il constitue le nouveau texte de référence européen en matière de protection des données à caractère personnel.

Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne mais implique plus de responsabilités pour ceux qui collectent, conservent ou échangent des **données personnelles**.

Dans le présent document, nous ne rentrerons pas dans l'exhaustivité de cette réglementation. Nous aborderons, de façon plus spécifique, **les points mis en œuvre par adhoc-gti sur nos produits** pour vous aider au respect du RGPD. Le lecteur trouvera sur internet ou dans les librairies de nombreux documents qui répondront à ses interrogations sur la mise en oeuvre plus générale du RGPD au sein de sa structure. On citera en particulier le site de la CNIL https://www.cnil.fr/fr/se-preparer-au-reglement-europeen, référence en la matière.

Données à caractère personnel

RGPD, article 4, 1) « Aux fins du présent règlement, on entend par «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 ».

On citera comme exemples de données personnelles : n° de sécurité sociale, adresse postale, adresse mail, n° de contrat, n° de quittance, n° de sinistre, adresse IP, coordonnées de géolocalisation, coordonnées bancaires, ...

Traitements

RGPD, article 4, 2) « Aux fins du présent règlement, on entend par «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 ».

Principes relatifs au traitement des données à caractère personnel

RGPD, article 5, 1) « Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; (...) (limitation des finalités)

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

Le détail des principes et leur application est décrit dans le RGPD.

Nos produits

Concrètement des fonctionnalités vont être déployées sur nos produits :

a) Licéité, loyauté, transparence
Prévenir l'utilisateur et l'acteur (client) de ce qui est collecté

- Consentement
  i. Concernant les utilisateurs d'adhoc : le logiciel adhoc conserve la trace de certaines opérations (date, utilisateur adhoc, action). La liste des opérations faisant l'objet d'une historisation sera accessible depuis adhoc et tous les utilisateurs en seront informés lors de leur connexion. Concernant la gestion de vos clients sous adhoc : adhoc intègrera la gestion de l'acceptation explicite d'email commerciaux (de vous ou de vos partenaires) afin que vous puissiez filtrer vos emailing.
  ii. Concernant les utilisateurs du CEL : il vous faudra informer les utilisateurs à qui vous proposez des accès au courtier en ligne de ce qui est collecté (logs). Nous vous fournirons une liste des informations collectées. C'est vous qui gèrerez la durée d'historisation.
- Liste des champs prévus pour la saisie de données à caractère personnel.
  i. Concernant adhoc : nous vous fournirons la liste des champs prévus pour la collecte de données à caractère personnel. Mais il se peut que vous n'en utilisiez qu'une partie dans votre gestion ou que vous utilisiez des champs différents ou dynamiques pour collecter d'autres informations personnelles. Il vous revient de préciser à vos clients les données personnelles concrètement collectées.
  ii. Concernant CEL : nous vous fournirons la liste des champs prévus pour la collecte de données à caractère personnel dans nos développements standards. Pour les développements spécifiques, vous devrez inventorier et qualifier les données. Il vous revient d'informer vos clients.
- Droit à la portabilité : extraire l'ensemble des données d'une personne à sa demande
  i. Comme expéditeur, concernant adhoc : un moniteur RGPD sera à votre disposition pour couvrir le besoin d'extraction dans un fichier formaté et interopérable.
  ii. Comme destinataire, concernant adhoc : des outils existent déjà pour importer des fichiers comprenant les principales informations personnelles gérées sous adhoc.
  iii. Concernant CEL : toutes les données personnelles sous CEL proviennent ou sont transférées vers adhoc qui assumera donc les fonctionnalités proposées.

b) Limitation des finalités
Prévenir l'utilisateur de ce qui va être fait avec ses données

- Registre des traitements de données personnelles implantés dans adhoc
  i. Concernant adhoc : nous vous fournirons la liste des principaux traitements prévus de base pour le traitement de données à caractère personnel. Il se peut que vous n'en utilisiez qu'une partie dans votre gestion. Par ailleurs, vous utilisez adhoc pour des traitements que nous ne maîtrisons pas (publipostage commerciale, exports, transmissions à des tiers, etc.). Il vous revient donc de recenser et de préciser à vos clients les traitements de données personnelles que vous réalisez concrètement.
  ii. Concernant CEL : nous vous fournirons la liste des traitements de données à caractère personnel intégrés dans nos développements standards. Pour les développements spécifiques, il vous revient d'inventorier et qualifier les traitements. Il vous appartient d'informer vos clients.

c) Minimisation des données
Ne collecter que le nécessaire

- Des alertes dans les textes libres rappellent aux membres du cabinet qu'il ne faut collecter que le strict nécessaire pour le traitement, aucune information dont vous n'avez pas explicitement besoin et dont le client n'aurait pas été informé au point a).
  i. Concernant adhoc : une information « RGPD » rappellera aux utilisateurs leurs obligations de respect des réglementations
  ii. Concernant CEL : non concerné sur les développements standards.

d) Exactitude
Ne conserver que des informations exactes et utiles

- Seul l'historique utile doit être conservé
  i. Concernant adhoc : nous vous fournirons la liste des informations historisées lors des modifications de données personnelles.
  ii. Concernant CEL : non concerné sur les développements standards.

- Droit de rectification
    i. Concernant adhoc : dans le cadre du droit à la portabilité, il sera possible d'extraire les données via le moniteur RGPD sous format structuré afin que le propriétaire puisse les vérifier et proposer leur correction.
    ii. Concernant CEL : non concerné sur les développements standards.

e) Limitation de la conservation
Ne conserver des données que sur une durée légale
- Droit à l'effacement, tout en respectant les règles de conservation réglementaires
    i. Concernant adhoc : le moniteur RGPD permettra d'identifier les données personnelles d'un individu donné et de procéder à un traitement permettant de respecter le « droit à l'oubli ». Il appartiendra à l'utilisateur de juger de l'application du droit en fonction du cadre réglementaire.
    ii. Concernant CEL : les données proviennent d'adhoc.
- Durée de conservation et archivage des données
    i. Concernant adhoc : le moniteur RGPD permettra d'identifier les données personnelles répondant à des critères de conservation/archivage définis par l'utilisateur et de procéder à un traitement permettant d'ôter les données à caractère personnel vers un format interopérable que l'utilisateur pourra archiver selon ses propres procédures.
    ii. Concernant CEL : les données sont gérées sous adhoc

f) Intégrité et confidentialité
Garantir la sécurité des données
- Sécurisation de la base de données : chiffrage, sécurisation de la base de données,
    i. Concernant adhoc : outre la sécurisation de vos serveurs qui appartient à vos SSI et prestataires d'hébergement, nous mettrons en place des solutions de sécurisation sur la base de données.
    ii. Concernant CEL : outre le contrôle de l'engagement au respect de cette garantie par notre sous-traitant qui héberge les CEL, nous mettrons en place des solutions de sécurisation sur les bases de données.
- Communications chiffrées entre adhoc et le CEL
    i. Les informations transmises entre nos deux produits transitent sur internet et sont sécurisées en conséquence.
    ii. La sécurisation des communications entre adhoc et vos potentiels extranets indépendants dépend de votre fournisseur d'extranet
- Politique d'authentification et monitoring de l'historique des connexions.
    i. Concernant adhoc : un gestionnaire des authentifications permettra de gérer les comptes et de définir votre politique d'authentification sous adhoc (mot de passe, historique, droits, sécurisation, …).
    ii. Concernant CEL : la gestion des authentifications sur le CEL sera revue pour mieux répondre à la réglementation (politique et sécurisation des mots de passe, historique, …).
- GED
    i. Concernant la GED adhoc : un gestionnaire des authentifications permettra de gérer les comptes et de définir votre politique d'authentification sous adhoc (mot de passe, historique, droits, sécurisation, …).
    ii. Concernant la GED évoluée : la GED évoluée est encadrée par des droits d'accès. La sécurisation de la machine virtuelle est gérée par votre SSI ou prestataire.
    iii. Concernant CEL : la gestion des authentifications sur le CEL sera revue pour mieux répondre à la réglementation (politique et sécurisation des mots de passe, historique, …).

Les fonctionnalités seront décrites et documentées sur notre documentation en ligne.

Adhoc-gti en tant que sous-traitant

RGPD, article 4, 8) « Aux fins du présent règlement, on entend par « 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 ».

Dans la cadre de son activité principale d'éditeur, adhoc-gti ne traite pas directement les données à caractère personnel de vos clients et n'est donc pas au sens RGPD un « sous-traitant ». Néanmoins, nous fournissons des outils pour le faire. C'est pourquoi, nous mettons en place des fonctionnalités complémentaires qui vous aident à être en conformité avec le contenu du RGPD (cf. supra).

Dans les situations où adhoc-gti est amené à traiter des informations à caractère personnel, nous nous comporterons comme un sous-traitant au sens du RGPD.

- Dans le cadre de son activité de responsable de l'hébergement de la solution « Courtier en Ligne – CEL », adhoc-gti est un sous-traitant au sens RGPD. C'est pourquoi, nous veillerons au respect du RGPD par notre hébergeur CEL.
- Dans le cadre des reprises/fusions/migrations pour nos clients, nous encadrerons nos traitements.
- Le RGPD aura également un impact dans vos relations avec nos services. En effet, par exemple, lorsque vous soulevez auprès du support un besoin d'aide sur un cas spécifique, vous êtes amenés à nous communiquer des données à caractère personnel sur les clients concernés. Ces pratiques devront être revues.

Des garanties techniques et organisationnelles seront prévues et aménagées dans le contrat qui nous lie. Elles couvriront également le traitement des données personnelles vous concernant en tant que clients d'adhoc-gti.

Par ailleurs, dans nos développements, nous veillerons à alerter nos clients sur la conformité des traitements dès le moment le moment de leur conception (privacy by design).

Cadre général et bonnes pratiques

Adhoc-gti a prévu diverses fonctionnalités pour vous aider au respect du RGPD. Mais, la mise en œuvre effective de celles-ci appartient aux utilisateurs.

Par ailleurs, tous les volets de la RGPD ne concernent pas ou ne se limitent pas au cadre de nos logiciels. Nous attirons votre attention sur quelques exemples :

Minimisation des données :

- Il convient, tout d'abord, de rappeler à vos utilisateurs les bonnes pratiques tel que **le respect du principe de proportionnalité**. *Pour couvrir les besoins de tous nos clients, nos logiciels sont riches en matière de champs de saisie et de traitements mais* ***seules les données nécessaires à la finalité de VOS traitements doivent être saisies.***

Intégrité et confidentialité

- Nous vous rappelons qu'adhoc-gti n'héberge pas vos données du logiciel adhoc. Les sauvegardes des données, leur sécurisation, la gestion des accès aux serveurs, la protection et le stockage des sauvegardes et des archives, … sont de votre responsabilité ou du(des) sous-traitant(s) en charge de cette partie.
- Les impressions, les extractions, les imports-exports EDI, les emailings, … manipulent des fichiers dématérialisés ou papier qui font partie du cadre du RGPD. Le respect des règles du RGPD sur ce type de sujet est du ressort des bonnes pratiques de l'utilisateur (registres, application des règles, …).

Au final, quel que soit les solutions techniques mises en œuvre, la protection des données à caractère personnel doit être partagée par tous pour être efficace. Il convient donc d'initier vos salariés aux nouvelles obligations introduites par le RGPD et rappeler qu'un simple fichier Excel **(ou son impression papier)** contenant des contacts constitue un traitement de données personnelles.