Envoyé en préfecture le 14/02/2024
Reçu en préfecture le 14/02/2024
Publié le 15/02/2024
ID : 034-213400880-20240209-D2024_07-DE

Syndicat mixte pour le traitement de l'information et les nouvelles technologies

Conditions de sous-traitance au sens du RGPD pour les adhérents

PREAMBULE

COGITIS, Syndicat mixte pour le traitement de l'information et les nouvelles technologies, dispose statutairement d'une série de compétences transférées par les adhérents du Syndicat.

Dans le cadre de la mise en œuvre de ces compétences, COGITIS traite de l'information sous forme de données, de sons ou d'images, ainsi que les études d'organisation correspondantes.

Dans le cadre de l'exécution des compétences transférées, COGITIS, en qualité de « Sous-traitant » au sens du RGPD, traite des données à caractère personnel appartenant à l'adhérent.

Les données à caractère personnel sont notamment soumises aux dispositions de la loi Informatique et Libertés du 6 janvier 1978 modifiée, et, depuis le 25 mai 2018, date d'entrée en vigueur, le Règlement européen (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD).

Ces textes consacrent une logique de responsabilisation de tous les acteurs impliqués dans le traitement de données à caractère personnel.

C'est dans ce contexte que COGITIS s'engage à respecter les présentes conditions de sous-traitance au sens du RGPD au titre des compétences transférées par ses adhérents.

Les présentes conditions ont été adoptées par délibération n° 2021D816 en date du 20 mai 2021 du Comité Syndical et notifiées à tous les Adhérents.

DEFINITIONS

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.

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.

Responsable de traitement (RT) : 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 ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

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 (RT).

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles COGITIS s'engage à effectuer pour le compte de l'Adhérent, responsable de traitement, les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 ci-après, « ***le* règlement européen sur la protection des données** » **ou RGPD**.

II. Description du traitement faisant l'objet de la sous-traitance

Au sens du RGPD, COGITIS est « sous-traitant ».

COGITIS exploite les données sur les serveurs de l'Adhérent ou sur des serveurs appartenant et gérés par COGITIS. Ces serveurs sont localisés dans des locaux dédiés.

Les serveurs de l'Adhérent se trouvent physiquement soit dans ses locaux soit chez un hébergeur tiers.

COGITIS est autorisé à traiter en fonction des moyens techniques alloués, pour le compte du responsable de traitement, les données à caractère personnel dans le cadre des compétences transférées par l'Adhérent :

- La veille technologique et réglementaire liées aux évolutions dans le domaine des technologies de l'information et de la communication.
- Les études amont, préalables à la réalisation de projets informatiques et de télécommunications.
- Le conseil aux maîtres d'ouvrages, collectivités dans le choix de solutions faisant appel aux technologies de l'information et de la communication, et la maîtrise d'œuvre d'opérations techniques.
- L'installation de ces solutions et leur intégration à l'architecture informatique existante ainsi que la formation correspondante des agents.
- Le développement et/ou la maintenance de solutions logicielles, en l'absence de produits du marché adaptés aux besoins et contraintes des adhérents.
- La gestion opérationnelle des infrastructures techniques (administration des réseaux et des bases de données, gestion des sécurités, gestion technique du parc matériel).
- L'assistance et/ou l'exploitation des solutions mises en œuvre.
- La formation à l'utilisation de logiciels.
- La gestion technique de la téléphonie et de la visiophonie.
- La délivrance de services d'administration électronique, au travers une plate-forme mutualisée ouverte et évolutive et l'accompagnement des collectivités publiques dans l'utilisation des services numériques retenus.

COGITIS réalise au titre des compétences transférées tout ou partie des activités figurant ci-dessous qui impactent les données.

- **Le Maintien en condition opérationnel (MCO)** : exploitation, rapport, statistiques, supervision, gestion du stockage et droits d'accès aux applications, aux données et aux infrastructures, sauvegarde des données des bases et restaurations, interfaces inter applicatifs FTP, dépôt de fichiers sur des serveurs tiers, gestion de la messagerie, des annuaires, gestion des environnements, gestion des applications métiers, gestion des vidéos surveillance, maintenance des développements de scripts ou autres applicatifs.
- **L'hébergement de données** : collecte de données professionnelles dans le cadre de l'utilisation des services numériques (gestion des convocations, site Internet…) ou pour assurer les fonctions du Centre d'Appel Mutualisé**.**
- **L'Intégration** : pilotage de projets, paramétrage, recette, reprise de données, développements de scripts d'interfaces d'automatisation ou autres applicatifs, rapports liés aux données pour lesquelles il existe des infocentres, middleware et socles techniques.
- **L'Assistance et le dépannage** : sur toutes les infrastructures, postes de travail et périphériques associés, et sur les applications métiers.
- **L'Assistance à maîtrise d'ouvrage** : étude du besoin, rédaction de cahiers des charges, dépouillement et analyse des offres.

De manière générale toutes les données personnelles sont collectées et produites par l'Adhérent dans le cadre de l'exercice de ses compétences.

Les données à caractère personnel traitées sont toutes les données nécessaires à l'exercice des compétences de l'Adhérent telles que l'état-civil, identité, données d'identification, de santé, images, données de la vie personnelle et professionnelle, information d'ordre économique et financier, données de connexion, données de localisation, données Internet, numéro de dossier, etc. Les données de santé et de mineurs sont des données sensibles au sens de la réglementation des données à caractère personnel.

Les catégories de personnes concernées par les données personnelles collectées et produites par l'Adhérent sont :

1. Personnel de l'Adhérent
    a. Agents de l'Administration / stagiaires
    b. Elus
2. Bénéficiaires et usagers de l'Adhérent
3. Tiers prestataires et partenaires de l'Adhérent

Pour l'exécution des compétences transférées à COGITIS, le responsable de traitement met à la disposition de COGITIS les informations nécessaires, et notamment toutes les politiques de confidentialité et de sécurité, toutes les règles mises en œuvre par l'Adhérent relatives à la protection des données à caractère personnel.

COGITIS est responsable des opérations de traitement sous son contrôle exclusif sous réserve des instructions délivrées.
Il est précisé que COGITIS en tant que sous-traitant agit uniquement sur instruction claire et documentée du Responsable de traitement.

III. Durée des conditions de sous-traitance

Les présentes conditions sont liées au transfert de ses compétences par l'Adhérent à COGITS.

Elles prennent fin automatiquement au terme du transfert.

IV. Obligations de COGITIS vis-à-vis de l'Adhérent

COGITIS s'engage à :

1. Traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de l'exercice des compétences transférées.
2. Traiter les données **uniquement et conformément aux instructions écrites et documentées** communiqués par l'Adhérent. Si COGITIS considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en **informe immédiatement** l'Adhérent. En outre, si COGITIS est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer l'Adhérent du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
3. **Garantir la confidentialité** des données à caractère personnel traitées dans le cadre des compétences transférées.
4. Veiller à ce que les **personnes de COGITIS autorisées à traiter les données à caractère personnel :**
    - s'engagent individuellement à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
    - reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut.**
6. **Informer d'une Sous-traitance ultérieure** pour mener des activités de traitement spécifiques. Dans ce cas, il en informe l'Adhérent. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance.

    Le « sous-traitant ultérieur » sera contractuellement tenu de respecter les présentes obligations.

    Il appartient à COGITIS de s'assurer que le « sous-traitant ultérieur » présente les mêmes 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 règlement européen sur la protection des données. Si le « sous-traitant ultérieur » ne remplit pas ses obligations en matière de protection des données,

COGITIS, demeure pleinement responsable devant l'Adhérent de l'exécution par le « sous-traitant ultérieur » de ses obligations.

7. **Aider l'Adhérent dans son obligation d'information des personnes concernées** par des opérations de traitement au moment de la collecte des données.
8. Aider l'Adhérent à s'acquitter de son obligation de donner suite **aux demandes d'exercice des droits des personnes :** droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

   Lorsque les personnes concernées exercent auprès de COGITIS des demandes d'exercice de leurs droits ; COGITIS doit adresser ces demandes dès réception par courrier électronique au contact qui aura été communiqué par l'Adhérent à COGITIS.
9. Informer l'Adhérent de tout **incident informatique pouvant relever de l'atteinte à des données à caractère personnel.** COGITIS notifie à l'Adhérent tout incident informatique impactant des données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Il sera notifié par courriel et suivi d'un accusé de réception de la part de l'Adhérent.

   Cette notification est accompagnée de toute documentation utile afin de permettre à l'Adhérent, si nécessaire, de qualifier l'acte de violation de données à caractère personnel à l'autorité de contrôle compétente.
10. Aider l'Adhérent dans le cadre du **respect de ses obligations de traitement** pour la réalisation :

    - d'analyses d'impact relatives à la protection des données.
    - de consultation préalable de l'autorité de contrôle.

    COGITIS fournit les informations utiles en sa possession sur demande expresse de l'Adhérent.
11. Mettre en œuvre **la politique de sécurité** de l'Adhérent avec les moyens qui sont mis à la disposition de COGITIS (PSSI, instructions, règles…).
12. **Se conformer aux instructions écrites de l'Adhérent quant au sort des données.**

    A l'issu de chaque traitement, COGITIS s'engage à détruire toutes les données à caractère personnel dans un délai de 15 jours sauf instruction contraire de l'Adhérent.
13. Communiquer le nom et les coordonnées de son **délégué à la protection des données**.
14. Tenir par écrit un **registre des catégories d'activités de traitement** effectuées pour le compte de l'Adhérent comprenant :
    - le nom et les coordonnées de l'Adhérent pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
    - les catégories de traitements effectués pour le compte du responsable du traitement ;
    - le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
  - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
  - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
  - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. Mettre à disposition de l'Adhérent la **documentation nécessaire pour démontrer le respect de toutes ses 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.

V. Obligations de l'Adhérent vis-à-vis de COGITIS

L'Adhérent s'engage à :

1. Documenter par écrit toute instruction concernant le traitement des données par COGITIS ;
2. Communiquer la liste des personnes habilitées à donner des instructions à COGITIS ;
3. Veiller au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données.