



Annexe 1 au cahier des clauses particulières valant conditions particulières :

Protection et utilisation des données à caractère personnel

LOT 2 Responsabilité civile et risques annexes

La présente annexe a pour objet de définir les conditions dans lesquelles le titulaire du contrat, ci-après dénommé « **le sous-traitant** » s'engage à effectuer pour le compte du Syctom, ci-après dénommé « **le 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 (ci-après, « **le règlement européen sur la protection des données** »).

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

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) faisant l'objet du présent contrat.

La nature des opérations réalisées sur les données, les finalités du traitement, l'identification des données à caractère personnel et les catégories de personnes concernées sont définies au présent article et, le cas échéant, précisées par les pièces particulières du contrat.

La nature des opérations réalisées sur les données est :

- ☒ Collecte de données
- ☒ Enregistrement de données
- ☒ Organisation de données
- ☒ Structuration de données
- ☒ Conservation de données
- ☒ Adaptation ou modification de données
- ☒ Extraction de données
- ☒ Consultation de données
- ☒ Utilisation de données
- ☒ Communication de données (transmission ou toute autre forme de mise à disposition)
- ☒ Rapprochement de données
- ☒ Interconnexion de données
- ☒ Limitation de données
- ☒ Effacement de données
- ☒ Destruction de données

Les finalités du traitement sont :

- **gestion des sinistres et réclamations ;**
- **gestion contractuelle du marché d'assurance ;**
- **instruction, expertise et indemnisation des sinistres ;**
- **gestion des recours et contentieux ;**
- **production des reportings de sinistralité ;**
- **suivi administratif et financier du contrat.**

Les données à caractère personnel traitées sont :

Données courantes

☒ **Etat civil, identité, données d'identification, images**

☒ **Données de connexion (logs, adresse IP, etc.)**

☐ Vie personnelle (habitudes de vie, situation familiale, diplômes, niveau d'études, etc.)

☐ Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, RIB, etc.)

☐ Données de localisation (déplacements, données GPS, données GSM, etc.)

☒ **Autres, préciser :**

- **Données d'identification des interlocuteurs du Syctom ;**
- **Coordonnées professionnelles ;**
- **Informations relatives aux sinistres déclarés ;**
- **Informations relatives aux experts, prestataires et intervenants ;**
- **Données nécessaires à la gestion des indemnisations.**
- **Informations relatives aux tiers impliqués dans un sinistre ;**
- **Informations relatives aux procédures amiables ou contentieuses ;**
- **Informations nécessaires à l'exercice des recours.**

Données sensibles ou à caractère hautement personnel

☐ Données relevant de la prétendue origine raciale ou ethnique

☐ Données révélant des opinions politiques

☐ Données révélant des convictions religieuses ou philosophiques

☐ Données révélant l'appartenance syndicale

☐ Données génétiques

☐ Données biométriques aux fins d'identifier de manière unique une personne

☐ Données concernant la santé

☐ Données concernant l'orientation sexuelle ou la vie sexuelle

☐ Données relatives aux condamnations pénales ou aux infractions

☐ Numéro d'identification dans un registre national unique (NIR)

Il n'est pas attendu du titulaire qu'il collecte ou traite des données sensibles au sens de l'article 9 du RGPD en dehors des situations strictement nécessaires à l'instruction ou à la gestion d'un sinistre.

Lorsqu'un sinistre implique des données relatives à la santé ou d'autres catégories particulières de données, le titulaire ne peut les traiter que dans la mesure strictement nécessaire à l'exécution du marché et met en œuvre des mesures de protection renforcées.

Les catégories de personnes concernées sont :

☒ **Agents publics**

☐ Mineurs

☐ Particuliers

☒ **Autres, préciser :**

Personnes impliquées dans la gestion, l'instruction ou le règlement des sinistres ; Agents habilités à déclarer ou suivre les sinistres ; Représentants du Syctom ; Experts ; Intervenants externes concernés par un sinistre ; Tiers impliqués dans la gestion d'un sinistre ; Tiers victimes ou réclamants

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivant un ordre de service adressé au titulaire.

II. Obligations du sous-traitant vis-à-vis du responsable de traitement

II.1 Généralités

Le sous-traitant s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/ont l'objet de la sous-traitance ;
2. traiter les données **conformément aux instructions documentées** du responsable de traitement. Si le sous-traitant 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** le responsable de traitement. En outre, si le sous-traitant 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 le responsable 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 du présent contrat ;
4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :
 - s'engagent 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**.

II.2 Sous-traitance

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « **le sous-traitant ultérieur** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. 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 responsable de traitement dispose d'un délai de 15 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

III.3 Droit d'information des personnes concernées

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

III.4 Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : 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).

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

III.5 Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

III.6 Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

III.7 Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- la pseudonymisation et le chiffrement des données à caractère personnel

- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- les 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.

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par le responsable du traitement.

III.8 Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à renvoyer toutes les données à caractère personnel au responsable de traitement.

Les dossiers sinistres, historiques de sinistralité, rapports d'expertise, éléments de recours, fichiers de suivi, reportings et documents relatifs à l'exécution du marché sont remis au pouvoir adjudicateur à son terme ou détruits selon ses instructions.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

III.9 Délégué à la protection des données

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

III.10 Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement y compris :

- le nom et les coordonnées du responsable de traitement 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 :
 - la pseudonymisation et le chiffrement des données à caractère personnel ;
 - 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.

III.11 Documentation

Le sous-traitant met à la disposition du responsable de traitement 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.

III. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. fournir au sous-traitant les données visées au I des présentes clauses ;
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
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 de la part du sous-traitant ;
4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

IV. Sanctions pour violation du régime de protection des données à caractère personnel

En cas de violation par le sous-traitant (au sens de la présente annexe) de ses obligations, ce dernier encourt :

- soit en cas de violation ne présentant pas une gravité suffisante, une pénalité forfaitaire de **500 €HT par manquement** et quel que soit le manquement, sur simple constat et sans qu'il soit besoin de mettre en demeure le sous-traitant préalablement ;
- soit en cas de violation suffisamment grave ou répétée, la résiliation du contrat pour faute. Cette mesure est précédée d'une mise en demeure préalable notifiée par accusé de réception, assortie d'un délai de correction mentionné au sein du courrier de mise en demeure.