
**PROCEDURE P2546-AOO-DU – ENQUETES DE SATISFACTION
AUPRES DES USAGERS**

ANNEXE 3 DU CCAP

Sécurité Informatique

Orientations Générales

EXIGENCES DE SECURITE

TABLE DES MATIERES

1	INTRODUCTION	1
1.1	Champ d'application	1
1.2	Objectif du document	1
2	EXIGENCES	1
2.1	Plan d'Assurance Sécurité	1
2.2	Politique, organisation, gouvernance	1
2.3	Conformité à l'état de l'art du SI du Titulaire	1
2.4	Ressources humaines	2
2.5	Gestion des biens	2
2.6	Obligation de confidentialité	2
2.7	Traitement des incidents	2
2.8	Continuité d'activité	3
2.9	Lieu d'exécution	3
2.10	Utilisation de ressources basées sur l'intelligence artificielle	3
2.11	Audit de sécurité	4
2.12	Délégation d'usage d'un sous-domaine dédié à l'envoi de mails	4

1 INTRODUCTION

1.1 CHAMP D'APPLICATION

Tout contrat avec un prestataire traitant des données sensibles et induisant des risques sur la sécurité de l'information.

1.2 OBJECTIF DU DOCUMENT

L'objectif de ce document est de lister les exigences de sécurité à intégrer ou à annexer à un contrat afin que le prestataire soit en mesure d'apporter un niveau de sécurité satisfaisant face aux attentes de l'ACOSS et aux risques auxquels l'ACOSS est exposé.

2 EXIGENCES

2.1 PLAN D'ASSURANCE SÉCURITÉ

EX-SEC-PAS-01 : Le Titulaire est responsable de l'élaboration, de la mise en œuvre, du maintien à jour et du respect par ses éventuels sous-traitants d'un Plan d'Assurance Sécurité (PAS) conforme aux exigences de sécurité et aux besoins de l'ACOSS pendant toute la durée des prestations. Le PAS initial est formalisé dans le cadre de la réponse technique.

2.2 POLITIQUE, ORGANISATION, GOUVERNANCE

EX-SEC-GOUV-01 : Dès la notification de la commande, le Titulaire nomme un responsable du contrat, lequel sera l'interlocuteur privilégié du pouvoir adjudicateur pour le suivi et l'exécution du contrat.

Le Titulaire désigne aussi :

- Le responsable de la sécurité du système d'information habilité à le représenter auprès de l'ACOSS pour traiter tout problème de sécurité durant toute la durée du contrat.
- Le délégué à la protection des données.

EX-SEC-GOUV-02 : Le Titulaire doit disposer d'une PSSI complète, documentée et approuvée formellement par sa direction.

EX-SEC-GOUV-03 : Le Titulaire doit être conforme à sa PSSI durant toute la durée de la prestation pour l'ACOSS.

EX-SEC-GOUV-04 : Le Titulaire doit disposer d'un référent sécurité en charge de l'application et du maintien de la PSSI.

EX-SEC-GOUV-05 : La PSSI du Titulaire doit définir et attribuer les fonctions et responsabilités liées à la sécurité de l'information selon ses besoins.

EX-SEC-GOUV-06 : Le Titulaire doit corriger dans les délais définis ci-après tout problème de sécurité identifié, en fonction de sa criticité :

- Criticité élevée : Problème pouvant entraîner une violation de la sécurité avec un impact significatif sur la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes de l'ACOSS. Délai de correction : 24 heures.
- Criticité moyenne : Problème pouvant entraîner une violation de la sécurité avec un impact limité sur la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes de l'ACOSS. Délai de correction : 72 heures.
- Criticité faible : Problème ayant un impact mineur sur la sécurité de l'information. Délai de correction : 1 mois.

La criticité des problèmes de sécurité est évaluée conjointement par le Titulaire et l'ACOSS.

En cas de désaccord, l'évaluation de l'ACOSS prévaut.

SO-SEC-GOUV-01 : Il est souhaité que le Titulaire définisse et mette en œuvre les processus de sécurité fondamentaux suivants :

- Analyse et gestion des risques liés à l'information
- Gestion et réponse aux incidents de sécurité
- Sensibilisation et formation à la sécurité
- Gestion des correctifs de sécurité
- Surveillance et gestion des vulnérabilités
- Gestion de la sécurité des fournisseurs et sous-traitants
- Gestion de la continuité d'activité
- La gestion des actifs et leur classification

2.3 CONFORMITÉ À L'ÉTAT DE L'ART DU SI DU TITULAIRE

EX-SEC-EA-01 : Le titulaire et ses sous-traitants éventuels s'engagent à maintenir en permanence un niveau de sécurité de leur système d'information et des services fournis à l'ACOSS conforme à l'état de l'art, aux bonnes pratiques de sécurité (ex : guides de l'ANSSI) et à la législation en vigueur, notamment en matière de protection des données à caractère personnel (RGPD). Ils doivent mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour assurer la confidentialité, l'intégrité, la

disponibilité et la traçabilité des données et des systèmes. Sur demande de l'ACOSS, le titulaire et ses sous-traitants éventuels doivent fournir les preuves de cette conformité.

2.4 RESSOURCES HUMAINES

EX-SEC-RH-01 : Le Titulaire s'engage à ce que chaque acteur du projet ait connaissance de sa « charte utilisateurs du SI » et de sa politique de sécurité.

EX-SEC-RH-02 : Le Titulaire doit former tout nouveau personnel aux règles de sécurité de l'information avant leur prise de fonction et avant tout accès aux systèmes ou aux données de l'ACOSS. Cette formation doit couvrir les principes de base de la sécurité, la protection des données sensibles et la conduite à tenir en cas d'incident de sécurité. Des modules spécifiques doivent être prévus pour les rôles sensibles, tels que les administrateurs système, les développeurs et les chefs de projet. Le Titulaire doit conserver une trace de ces formations et la mettre à disposition de l'ACOSS sur demande.

EX-SEC-RH-03 : Le Titulaire doit mettre en place des actions de sensibilisation régulières et variées pour maintenir un haut niveau de vigilance de son personnel face aux menaces de sécurité. Ces actions doivent inclure des campagnes d'information sur les menaces émergentes et les nouvelles techniques d'attaque, ainsi que des exercices pratiques tels que des simulations d'hameçonnage (phishing) ou d'ingénierie sociale.

2.5 GESTION DES BIENS

EX-SEC-GB-01 : Les données de l'ACOSS, y compris les données à caractère personnel, doivent être formellement identifiées, classifiées selon leur niveau de sensibilité. Elles doivent être isolées de manière logique et/ou physique des données d'autres clients ou tiers traitées par le Titulaire. Seul le personnel du Titulaire dûment habilité et autorisé à intervenir sur les projets ou services de l'ACOSS peut accéder à ces données, dans le strict respect du principe du besoin d'en connaître.

EX-SEC-GB-02 : Le Titulaire doit mettre en place des mesures techniques et organisationnelles pour tracer les accès aux données de l'ACOSS et détecter tout accès suspect.

EX-SEC-GB-03 : Le Titulaire doit mettre en oeuvre des procédures et dispositifs de sécurité pour se protéger contre le traitement non autorisé ou illégal, tout transfert non autorisé à un tiers, toute perte, destruction, altération ou divulgation accidentelle d'informations appartenant à l'ACOSS.

EX-SEC-GB-04 : Au terme de l'exécution du marché ou en cas de résiliation, le Titulaire restitue sans délai à l'acheteur une copie de l'intégralité des données confiées par lui dans le cadre de la prestation. Une fois la restitution effectuée, le Titulaire détruit de manière sécurisée et irréversible, dans un délai d'un mois, les éventuelles copies de données détenues dans son système d'information, y compris les données ayant fait l'objet de sauvegardes ou d'un archivage. La restitution et la destruction des données sont constatées par un procès-verbal daté et signé par le Titulaire. Les procédés de destruction sont conformes aux réglementations et aux normes en vigueur (par exemple NIST SP 800-88) et garantissent l'impossibilité de récupérer les données.

2.6 OBLIGATION DE CONFIDENTIALITÉ

EX-SEC-CONF-01 : Une information confidentielle désigne toute information de quelque nature (y inclus la méthodologie, la documentation, les informations ou le savoir-faire), sous quelque forme que ce soit (y inclus sous forme orale, écrite, magnétique ou électronique), sur tout support dont l'acheteur est propriétaire ou Titulaire, et qui est communiquée au Titulaire, ou obtenue de toute autre façon par ce dernier dans le cadre de ses relations avec l'acheteur. Le Titulaire et son personnel, et le cas échéant ses sous-traitants, ne peut l'utiliser que pour l'accomplissement des prestations prévues au marché.

Toutefois, n'est pas considérée confidentielle toute information :

- Qui était dans le domaine public au moment de sa divulgation ou que l'acheteur aurait lui-même rendue publique pendant l'exécution du marché ;
- Signalée comme présentant un caractère non confidentiel et relative aux prestations du marché ;
- Qui a été communiquée au Titulaire du marché par un tiers ayant légalement le droit de diffuser cette information, comme le prouvent des documents existant antérieurement à sa divulgation par l'acheteur.

2.7 TRAITEMENT DES INCIDENTS

EX-SEC-INC-01 : Les équipes de sécurité de l'ACOSS doivent être informées dans un délai maximum de 12h de tout incident de sécurité pouvant compromettre la sécurité et la confidentialité des données en rapport à tout projet de l'ACOSS. Cette alerte doit être réalisée par mail via à l'adresse de contact cos@acoss.fr. En cas d'urgence ou de de risque imminent pour la sécurité du SI de l'Acoss, l'alerte doit être immédiatement faite par téléphone au numéro 0986000951 puis doublée d'un mail à l'adresse cos@acoss.fr. De plus, la Déléguée à la Protection des Données de l'ACOSS doit être alertée si des données à caractère personnel fournies par l'ACOSS sont compromises dans les conditions indiquées à l'annexe RGPD fournie dans le cadre du marché via l'adresse de contact informatiqueetlibertes.acoss@acoss.fr.

EX-SEC-INC-02 : Le Titulaire doit documenter les procédures de réponse aux incidents et conserver une trace de tous les incidents traités en lien avec le présent marché, y compris les mesures correctives appliquées.

EX-SEC-INC-03 : Le Titulaire doit disposer d'un plan de gestion de crise informatique, intégrant la gestion des incidents de sécurité majeurs susceptibles d'affecter les données, les systèmes ou les services de l'ACOSS. Ce plan doit définir les rôles et responsabilités, les procédures d'escalade et de communication, les moyens de communication de crise, les scénarios de crise envisagés et les procédures associées pour la continuité et la reprise d'activité. Le plan de gestion de crise doit être testé au moins une fois par an.

2.8 CONTINUITÉ D'ACTIVITÉ

SO-SEC-CA-01 : Il est souhaité que le Titulaire dispose d'un Plan de Continuité d'Activité (PCA) et d'un Plan de Reprise d'Activité (PRA) documentés, à jour et adaptés aux services fournis à l'ACOSS. Le PCA doit décrire les dispositions prises pour assurer le maintien des activités essentielles réalisées pour le compte de l'ACOSS en cas de sinistre majeur. Le PRA doit décrire les procédures et les moyens techniques mis en œuvre pour la reconstruction des systèmes et la reprise des services après un sinistre, dans le respect des objectifs de temps de reprise (RTO) de 24h et de perte de données maximale admissible (RPO) de 24h définis dans le présent contrat.

2.9 LIEU D'EXÉCUTION

EX-SEC-LOC-01 : Le Titulaire doit faire connaître à l'ACOSS, sur sa demande, le lieu d'exécution des prestations. L'acheteur peut en suivre sur place le déroulement. L'accès aux lieux d'exécution est réservé aux seuls représentants de l'acheteur.

Les personnes qu'il désigne à cet effet ont libre accès aux seules zones concernées par l'exécution des prestations prévues par le marché, dans le respect des consignes de sécurité prévues pour le site. Elles sont tenues aux obligations de confidentialité prévues au chapitre « Obligation de confidentialité ».

EX-SEC-LOC-02 : Lorsque le Titulaire envisage la réalisation d'une prestation objet du présent accord-cadre depuis un autre pays que la France, il en informe sans délai l'ACOSS. En effet, compte tenu des risques importants de sécurité qu'une telle situation est susceptible de favoriser, l'ACOSS doit pouvoir s'assurer au préalable que le Titulaire est en mesure de garantir une protection optimale du système d'information de l'ACOSS, des données et traitements qui lui sont confiés.

A cet effet, le Titulaire communique à l'ACOSS tous les éléments de nature à l'éclairer sur les conditions de mise en œuvre de cette prestation depuis l'étranger, prenant la forme d'un PAS spécifique répondant aux exigences particulières demandées par l'ACOSS pour apporter toutes les garanties associées à ce type de prestation. De plus, si la prestation implique le traitement de données à caractère personnel, le Titulaire réalise une analyse d'impact relative à la protection des données (AIPD) et la fournit à l'acheteur.

En fonction des réponses fournies dans le PAS spécifique à la prestation réalisée dans un pays étranger, et au regard de la sensibilité de la prestation confiée, l'ACOSS apprécie si le niveau de garantie mis en œuvre est suffisant.

En cas d'acceptation, le PAS spécifique devient une pièce contractuelle, annexée au contrat et les deux parties concluent les clauses contractuelles types de la commission européenne en matière de transfert de données personnelles hors de l'UE.

Il est interdit au Titulaire de réaliser une prestation relevant de l'exécution du présent accord-cadre depuis un pays autre que la France, dès lors que le Titulaire ne s'est pas vu notifié par l'ACOSS une décision expresse favorable et que le PAS spécifique n'a pas été signé par les deux parties.

L'ACOSS se réserve par ailleurs le droit de résilier le présent accord-cadre en cas de manquement du Titulaire à l'une des obligations définies ci-dessus, ce manquement constituant une faute particulièrement grave.

2.10 UTILISATION DE RESSOURCES BASÉES SUR L'INTELLIGENCE ARTIFICIELLE

EX-SEC-IA-01 : Le Titulaire s'engage à ne pas utiliser d'outils, de logiciels ou de services basés sur l'intelligence artificielle (IA) pour l'accomplissement des prestations définies dans le cadre du présent marché, sauf autorisation écrite expresse et préalable de l'ACOSS.

Cette interdiction concerne notamment, mais sans s'y limiter :

- La création, la modification, le traitement ou l'analyse de documents, de données ou d'informations appartenant à l'ACOSS
- L'automatisation de tâches techniques, organisationnelles ou décisionnelles relevant du périmètre contractuel
- Toute autre activité pouvant affecter la sécurité, la confidentialité ou l'intégrité des informations traitées dans le cadre du marché

Si nécessaire, une demande d'autorisation d'utilisation expresse, devra être formulée par le Titulaire à l'ACOSS en y intégrant une description détaillée de l'outil d'IA envisagé et en incluant une évaluation des risques menée par le Titulaire qui sera validée par l'ACOSS. Cette évaluation devra notamment porter sur :

- La finalité d'utilisation
- Ses fonctionnalités principales
- Les données traitées par l'IA

- Les garanties offertes en termes de sécurité, confidentialité et protection des données, notamment en ce qui concerne l'entraînement des modèles et le stockage des données
- Les risques potentiels identifiés et les mesures d'atténuation associées

De plus, si la prestation implique le traitement de données à caractère personnel, le Titulaire réalise une analyse d'impact relative à la protection des données (AIPD) et la communique à l'acheteur.

La mise en œuvre d'un outil intégrant de l'intelligence Artificielle doit se faire conformément aux dispositions du règlement 2024/1689 du 13 juin 2024 (communément appelé IA Act).

L'ACOSS se réserve par ailleurs le droit de résilier le présent accord-cadre en cas de manquement du Titulaire à l'une des obligations définies ci-dessus, ce manquement constituant une faute particulièrement grave.

2.11 AUDIT DE SÉCURITÉ

EX-SEC-AUDIT-01 : L'ACOSS doit pouvoir, à tout moment, contrôler que les exigences de sécurité décrites au sein du PAS, sont satisfaites par le Titulaire pour exécuter les prestations objet du présent accord-cadre.

Les audits pourront être réalisés par l'ACOSS à tout moment, ou délégués à un tiers expert présentant les compétences requises pour réaliser les opérations de vérification.

Le cas échéant, le contrôle s'effectuera selon les modalités décrites au sein du PAS.

Nonobstant les alinéas précédents, dans le cas où l'ACOSS souhaite procéder à des contrôles au sein des locaux du Titulaire, l'ACOSS ou son délégataire procédera à cet audit après information du Titulaire, avec le respect d'un délai de préavis minimum de quinze (15) jours. En cas d'urgence, du fait par exemple de la survenance d'un incident grave de sécurité, l'ACOSS pourra réaliser l'audit de sécurité sur site sans délai de préavis.

En cas de pratique de tests intrusifs, une charte commune sera signée entre le Titulaire, l'exécutant de l'audit et l'ACOSS et sera annexée au PAS.

Si des vulnérabilités sont identifiées à l'issue de la conduite de l'audit, le Titulaire s'engage, sans surcoût, à mettre en œuvre un plan d'actions visant à éliminer ces vulnérabilités. Il s'engage à traiter en priorité les vulnérabilités engendrant les risques les plus élevés et à tenir informée quotidiennement l'ACOSS de l'avancée des travaux. Le Titulaire s'engage par ailleurs à prendre en charge les frais d'audit si celui-ci révèle des manquements avérés à ses obligations en matière de sécurité.

2.12 DÉLÉGATION D'USAGE D'UN SOUS-DOMAINÉ DÉDIÉ À L'ENVOI DE MAILS

Durant la durée du contrat, l'ACOSS donne délégation au Titulaire d'effectuer auprès de ses usagers l'envoi de mails destinés à aux enquêtes nationales de satisfaction annuelles utilisant une adresse mail et un sous domaine créés spécifiquement à cet effet par l'ACOSS se terminant par « @enquête.urssaf.fr ».

Le Titulaire s'engage formellement à mettre en œuvre tous les moyens nécessaires pour garantir à l'ACOSS qu'aucun autre usage ne sera fait par le Titulaire à d'autres fins que celles précisées ci-dessus.

Cette délégation prend fin en cas de résiliation par l'une ou l'autres des parties du contrat, ou à son expiration.

L'adresse mail créée ainsi que le nom de domaine utilisé pour répondre au besoin fonctionnel exprimé ci-dessus sont et reste la propriété de l'URSSAF

Les données personnelles relatives aux destinataires et utilisateurs de la solution font l'objet de mesures de protection prévues dans les articles du contrat et d'une annexe RGPD jointe.