

Annexe « Protection des données à caractère personnel »

(Version du 07 mars 2025)

La présente Annexe fait partie intégrante du Contrat (le « Contrat ») conclu entre le Prestataire et le Client, conjointement désignés les « Parties ».

La présente Annexe et le Contrat sont complémentaires et s'expliquent mutuellement.

ARTICLE 1^{ER} – OBJET

La présente Annexe vient compléter les Conditions générales de vente du Prestataire, qui fixent les relations entre le Client et le Prestataire, afin de tenir compte des dispositions applicables aux traitements de données à caractère personnel (ci-après désigné « traitement »).

Le Prestataire propose des prestations adaptées aux secteurs d'activité et aux exigences de ses clients, afin de leur permettre d'atteindre leurs objectifs opérationnels. Dans ce cadre, le Prestataire peut être amené à traiter des données à caractère personnel pour le compte de son Client.

Les présentes clauses ont pour objet de définir les conditions de mise en œuvre des opérations de traitement de données à caractère personnel nécessaires à l'exécution du Contrat par les Parties.

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter la réglementation en vigueur applicable aux traitements de données à caractère personnel et, à prendre en considération, si applicables, les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 (ci-après, « le Règlement Général sur la Protection des Données » ou RGPD) et lorsqu'applicable la Loi monégasque n°1.565 du 3 décembre 2024 relative à la protection des données personnelles.

ARTICLE 2 – DEFINITIONS

Aux fins de la présente, on entend par :

- « *Donnée 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* » : 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 ;
- « *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.

ARTICLE 3 - DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DES PRESTATIONS

Le Prestataire effectue les prestations décrites dans le contrat pour le compte du Client et selon ses instructions.

Le Client définit les moyens et les finalités du ou des traitements que le Prestataire effectue pour le compte du Client. Le Client est, à ce titre, « Responsable de traitement » au sens de la réglementation relative à la protection des données à caractère personnel.

Le Prestataire est autorisé à effectuer des opérations sur les données à caractère personnel pour le compte du Client nécessaires afin de fournir le ou les service(s) décrits dans les Contrats. Il est à ce titre « Sous-traitant », au sens du RGPD.

Le Client s'engage à identifier et à communiquer les données personnelles nécessaires à l'exécution des Prestations ou à permettre l'accès de manière sécurisée.

ARTICLE 4 - DUREE DE L'ANNEXE

La présente annexe entre en vigueur à compter de la signature du Contrat pour la durée du ou des contrats concernés et de leur renouvellement, le cas échéant.

Les documents établis par le Prestataire sont conservés cinq (5) ans après la fin de la relation d'affaire, pour permettre un accompagnement du client dans le temps.

Toutefois ces documents peuvent être supprimés à la demande du client, dès lors que les délais de recours s'appliquant à la prestation concernée sont prescrits.

ARTICLE 5 - OBLIGATIONS DU PRESTATAIRE VIS-A-VIS DU CLIENT

Le Prestataire s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) nécessaire(s) à l'exécution des prestations objets du ou des Contrat(s) ;
- Traiter les données conformément aux instructions, documentées, du Client.
Si le Prestataire considère qu'une instruction constitue une violation de la réglementation nationale, en matière de protection des données il en informe immédiatement le Client.
En outre, si le Prestataire est tenu de procéder à un transfert de données vers un pays tiers ou à une

organisation internationale, en vertu de la réglementation qui lui est applicable, 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 ;

- Veiller à la sécurité des données du Client ;
- Garantir la confidentialité des données à caractère personnel traitées dans le cadre du Contrat ;
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du Contrat :
 - o S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
 - o Reçoivent ou disposent de la formation nécessaire en matière de protection des données à caractère personnel ;
- 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.

ARTICLE 6 - RECOURS A UN SOUS-TRAITANT

Lorsque le Prestataire recrute un sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques dans le cadre des Contrats, les mêmes obligations en matière de protection des données que celles fixées dans la présente Annexe entre le Client et le Prestataire s'imposent au sous-traitant ultérieur par contrat ou au moyen d'un acte juridique conforme au droit applicable au Contrat.

Le sous-traitant ultérieur est, notamment, tenu de respecter les obligations de la présente Annexe pour le compte et selon les instructions du Client. Il appartient au Prestataire de s'assurer que le sous-traitant ultérieur présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées afin que le traitement ou les traitements de données à caractère personnel répondent aux exigences de la réglementation applicable en matière de protection des données personnelles.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant le Client de l'exécution par le sous-traitant ultérieur de ses obligations.

Préalablement au recrutement d'un sous-traitant ultérieur, le Prestataire informe par écrit le Client de l'ajout ou le remplacement d'un ou de plusieurs 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 Client dispose d'un délai de 7 jours francs à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Client n'a pas émis d'objection pendant le délai précité.

ARTICLE 7 - DROIT D'INFORMATION DES PERSONNES CONCERNEES

Il appartient au Client de fournir l'information aux personnes concernées par les opérations de traitement réalisées par le Prestataire.

ARTICLE 8 - EXERCICE DES DROITS DES PERSONNES

Dans la mesure du possible et selon les informations dont il dispose, le Prestataire s'engage à aider le Client à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées, tels que définis par la réglementation en vigueur, notamment les droits d'accès, de rectification, d'effacement et d'opposition, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du Prestataire des demandes d'exercice de leurs droits, le Prestataire les informe que ces demandes sont à déposer directement auprès du Client.

Le Prestataire informe également le Client de la demande qui lui est parvenue dans les meilleurs délais.

ARTICLE 9 - INFORMATION SUR LES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

Lorsque le Client est établi au sein de l'Union européenne, ou à défaut s'il en fait la demande, le Prestataire l'informe de toute violation de données à caractère personnel dans les meilleurs délais, après en avoir pris connaissance, et par mail.

Cette information est accompagnée de tout élément et documentation utile afin de permettre au Client d'agir comme il se doit, notamment :

- 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 ;
- Si possible, la description des conséquences probables de la violation de données à caractère personnel ;
- La description des mesures prises ou que le Prestataire 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.

Le cas échéant, il appartient au Client, en tenant compte de la réglementation qui lui est applicable, de procéder à la notification de la violation de données à caractère personnel auprès de l'autorité de protection des données compétente.

ARTICLE 10 - AIDE DU PRESTATAIRE AU RESPECT PAR LE CLIENT DE SES OBLIGATIONS

Lorsqu'un traitement exploité par le Client a été identifié par lui comme présentant un « risque élevé » pour les droits et libertés des personnes physiques concernées tel qu'entendu par le RGPD, le Prestataire aide le Client pour la réalisation d'analyses d'impact relative à la protection des données en répondant à ses questions, compte tenu de la nature du ou des traitements dont il est lui-même responsable et des informations à sa disposition.

Lorsqu'en application dudit règlement, le Client doit consulter l'autorité de contrôle compétente considérant le risque élevé que représenterait le traitement si des mesures n'étaient pas prises pour atténuer ce risque, le Prestataire aide le Client pour la réalisation de la consultation préalable en lui fournissant les éléments qu'il demande et dont le Prestataire a connaissance dans le cadre des Contrats.

Compte tenu de la portée des demandes précitées, du temps et des ressources nécessaires pour répondre aux besoins du Client, afin que cette aide ne porte pas préjudice à la bonne exécution des contrats et prestations visés à l'article 1^{er}, les Parties détermineront d'un commun accord les modalités et les conditions de l'aide précitée.

ARTICLE 11 - MESURES DE SECURITE

Compte tenu de la nature du traitement et des informations à sa disposition et des prestations souscrites par le Client, le Prestataire s'engage à informer le Client des mesures de sécurité qui devraient être appliquées aux traitements des données à caractère personnel impactés par les Contrats afin de garantir un niveau de sécurité adapté au risque identifié par le Client, et communiqué au Prestataire, comme :

- Les moyens permettant de garantir la sécurité, la confidentialité et l'intégrité des données du Client ;
- Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services supports des traitements ;
- Les moyens permettant de rétablir la disponibilité des données 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.

Compte tenu de la nature, de la portée et des coûts que pourraient engendrer les obligations précédentes, le Client informe le Prestataire des suites qu'il entend donner aux préconisations précitées.

Le Prestataire s'engage à mettre en place les mesures validées par le Client dans les meilleurs délais et dans le respect, le cas échéant, de contrats subséquents.

Le Prestataire s'engage à mettre en place des mesures de veille technologique et juridique en matière de protection des données à caractère personnel.

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques identifiés et des coûts engendrés, le Prestataire s'engage à appliquer les préconisations des autorités de protection des données ou, selon le cas, à conseiller le Client sur lesdites préconisations afin que le Client puisse prendre les mesures qu'il estime opportunes en la matière.

ARTICLE 12 - SORT DES DONNEES

Au terme de la prestation et à la demande du Client, le Prestataire s'engage à restituer l'ensemble des données, objet de la prestation, au Client et/ou à les supprimer.

A défaut de dispositions particulières dans les documents contractuels tels que définis aux Conditions Générales de Vente, le Prestataire supprime les documents et données au plus tard cinq (5) ans après la fin de la relation d'affaire.

ARTICLE 13 – CONTACT OU DELEGUE A LA PROTECTION DES DONNEES

Le Prestataire communique au Client les coordonnées du point de contact auprès duquel le Client peut obtenir des informations relatives au traitement des données par le Prestataire :

- 1) Dans le cas où Monaco Cyber Sécurité est Prestataire : dpo@monacocyber.mc
- 2) Dans le cas où Avangarde Cyber Sécurité est Prestataire : dpo@avangardecyber.fr

Le Client communique au Prestataire le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à la réglementation en matière de protection des données personnelles applicable à ses activités, ou d'un autre point de contact auprès duquel le Prestataire peut obtenir des informations relatives au traitement des données.

ARTICLE 14 - REGISTRE DES CATEGORIES D'ACTIVITES DE TRAITEMENT

Le Prestataire tient un registre des catégories d'activités de traitement effectuées sur l'environnement relevant de son autorité dans le cadre du Contrat. Ce registre est établi dans le respect de l'article 30 2. du RGPD.

Le Client s'engage à disposer d'un registre des activités de traitements, conforme à l'article 30 1. du RGPD, réalisés sous son autorité.

ARTICLE 15 – DOCUMENTATION

Lorsqu'il dispose des éléments permettant au Client de démontrer le respect de ses obligations à la réglementation en matière de protection des données, le Prestataire les communique au Client à sa demande.

Sauf clause spécifique dans le contrat de prestation, le Client peut réaliser, ou faire réaliser par une personne mandatée à cet effet, des audits et des inspections sur les activités du Prestataire, au titre du ou des traitements de données à

caractère personnel exploités par le Prestataire dans le cadre des Contrats qui le lient au Client, au maximum une (1) fois par an, sur site, pour une durée de deux (2) jours maximum.

Le Client informera par écrit le Prestataire de sa visite au moins un (1) mois avant la date effective de l'audit, en lui indiquant notamment : l'objet de l'audit, la durée de l'audit, la prestation concernée, la liste des éléments à mettre à disposition et l'identité de la société ou des personnes qui effectueront l'audit. Chaque audit sera effectué aux frais du Client.

Le périmètre de l'audit est strictement limité à un contrat identifié encadrant les prestations réalisées pour le compte du Client.

La personne mandatée choisie par le Client s'engage à signer un accord de confidentialité avec le Prestataire préalablement au démarrage de la mission d'audit. Le Prestataire se réserve le droit de refuser le mandat si ce dernier est un concurrent ou agit pour le compte d'une entreprise concurrente du Prestataire.

ARTICLE 16 - OBLIGATIONS DU CLIENT VIS-A-VIS DU PRESTATAIRE

Le Client définit les moyens et les finalités du ou des traitements que le Prestataire mettra en œuvre pour le compte du Client dans le cadre du Contrat. Ce ou ces traitements sont précisés en Appendice 1.

Le type de Données à caractère personnel et les catégories de personnes concernées sont déterminés et contrôlés par le Client, à sa seule discrétion.

En tant que « responsable de traitement », le Client s'engage à :

1. Fournir au Prestataire les données visées à l'article 3 des présentes clauses ;
2. Communiquer au Prestataire les politiques, procédures, instructions et documents portant sur la gouvernance des données à caractère personnel qui doivent être respectés au sein de l'organisation du Client, responsable de traitement ;
3. Documenter par écrit toute instruction concernant le traitement des données par le Prestataire ;
4. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par la réglementation en matière de protection des données qui lui est applicable ;
5. Collaborer avec le Prestataire afin de permettre à chacun de disposer des informations nécessaires au respect de la réglementation en matière de protection des données.

Le Client s'engage à respecter les obligations qui sont les siennes à ce titre, notamment à effectuer les formalités préalables ou à mettre en place les documents obligatoires lorsque nécessaire.

ARTICLE 17 – TRANSFERTS DE DONNEES A CARACTERE PERSONNEL VERS MONACO

Par ailleurs, si les filiales du Prestataire localisées en Principauté de Monaco sont soumises à des obligations légales en matière de protection des données à caractère personnel équivalentes

à celles imposées en Europe, l'Union européenne n'a pas encore accordé à la Principauté une reconnaissance du caractère « adéquat » de ces règles.

Dans le cas où Monaco Cyber Sécurité est Prestataire et que le Client est localisé au sein de l'Union européenne : en application de l'article 46 du RGPD, un Accord de transfert de données à caractère personnel à partir d'un pays membre de l'Union européenne (ex. la France) vers un pays tiers, la Principauté de Monaco, devrait être signé. Cet accord est établi sur le fondement des clauses contractuelles types (transferts de responsable du traitement à sous-traitant) de l'Union européenne. Le Prestataire tient à disposition des Clients concernés des clauses contractuelles répondant auxdites obligations.

Dans le cas où Avangarde Cyber Sécurité est Prestataire et que le Client est localisé au sein de l'Union Européenne mais que les opérations précitées impliquent un transfert de données du Prestataire vers ces filiales en Principauté de Monaco : un Accord de transfert de données à caractère personnel a été mis en place. Les transferts sont encadrés par des garanties appropriées, conformes à la législation applicable.

ARTICLE 18 – IDENTIFICATION DU REPRESENTANT DU PRESTATAIRE SUR LE TERRITOIRE DE L'UNION EUROPEENNE

Monaco Cyber Sécurité étant localisée en dehors de l'Union européenne et réalisant une offre de biens ou de services à des personnes concernées sur le territoire de l'Union, un représentant a été désigné sur le territoire français conformément à l'article 27 du RGPD par :

AVANGARDE CYBER SECURITE
Situé 618, avenue Roumanille
06410 BIOT

Toute question sur le sujet peut être adressée à :
dpo@monacocyber.mc

APPENDICE 1 - IDENTIFICATION DES TRAITEMENTS CONCERNES

Selon la prestation exécutée, le Prestataire effectue, pour le compte du Client les traitements listés ci-après qui intègrent les traitements mis en œuvre par le Client auxquels le Prestataire peut avoir ou est susceptible d'avoir accès, et/ou sur lesquels le Prestataire peut ou est susceptible d'intervenir dans le cadre des prestations précitées.

Lorsque le Client estime que les traitements listés ci-après ne sont pas adaptés aux opérations exécutées par le Prestataire sur les données à caractère personnel, la présente annexe devra être complétée par le Client et validée par le Prestataire.

Les terminologies utilisées ci-dessous répondent aux définitions suivantes :

- Nature du traitement : le type d'opérations effectuées sur les données prévu à l'article 4 alinéa 1 chiffre 2 du RGPD 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 » ;
- Finalité du traitement : l'objectif principal de l'utilisation de données personnelles. Exemples de finalité : gestion des recrutements, gestion des paies, gestion des clients, surveillance des locaux etc. (<https://www.cnil.fr/fr/definition/finalite-dun-traitement>) ;
- Personnes concernées : les catégories de personnes susceptibles de faire l'objet du traitement de données ;
- Catégories de données concernées : les types de données concernées par le traitement.

Nature du traitement	Finalité du traitement effectué pour le compte du Client selon les prestations souscrites	Personnes concernées	Catégories de données concernées
Accès technique, collecte, collecte de contacts professionnels, consultation, structuration, utilisation	Gestion des audits des systèmes d'information (PASSI, 27001...)	Collaborateurs du prestataire Collaborateurs des clients Utilisateurs du SI du client Sous-traitants du prestataire Contacts professionnels auprès du client	Identité, coordonnées, vie professionnelle, traçabilité des actions, données techniques des équipements du client, données techniques du prestataire
Collecte, collecte de contacts professionnels, utilisation	Gestion de l'assistance technique chez le client	Collaborateurs du prestataire Collaborateurs des clients Utilisateurs du SI du client Contacts professionnels auprès du client	Identité, coordonnées, vie professionnelle
Collecte, collecte de contacts professionnels, utilisation	Organisation des formations / sensibilisations sécurité	Collaborateurs du prestataire Collaborateurs des clients Utilisateurs du SI du client Contacts professionnels auprès du client	Identité, coordonnées, vie professionnelle
Accès technique, collecte, collecte de contacts professionnels, consultation, structuration, utilisation	Organisation de la mission de conseil en cybersécurité	Collaborateurs du prestataire Collaborateurs des clients Utilisateurs du SI du client Sous-traitants du prestataire Contacts professionnels auprès du client	Identité, coordonnées, traçabilité des actions, données techniques des équipements du client, données techniques du prestataire
Accès technique, utilisation, collecte de contacts professionnels, consultation, hébergement	Organisation de tests d'intrusion	Collaborateurs du prestataire Collaborateurs des clients Utilisateurs du SI du client Contacts professionnels auprès du client Sous-traitants du prestataire	Identité, coordonnées, vie professionnelle, traçabilité des actions, données techniques des équipements du client, données métiers du client
Collecte, collecte de contacts professionnels, utilisation	Organisation des campagnes de phishing	Collaborateurs du prestataire Collaborateurs des clients Contacts professionnels auprès du client	Identité, coordonnées, données techniques des équipements
Accès technique, collecte, collecte de contacts professionnels, consultation, hébergement, structuration, utilisation	Gestion et analyse d'événements de sécurité (SOC)	Collaborateurs du prestataire Collaborateurs des clients Sous-traitants du prestataire Contacts professionnels auprès du client	Identité, coordonnées, traçabilité des actions, données techniques des équipements
Accès technique, collecte, collecte de contacts professionnels, consultation, hébergement, structuration, utilisation	Gestion de la réponse à incidents (CERT)	Collaborateurs du prestataire Collaborateurs des clients Sous-traitants du prestataire Contacts professionnels auprès du client	Identité, coordonnées, traçabilité des actions, données techniques des équipements