POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL DE MONACO DIGITAL ET SES FILIALES

Préambule :

Monaco Digital et ses filiales (Monaco Cyber Sécurité et Fab Digital) sont liées par une dynamique commune autour de leurs activités et de leurs métiers.

La politique de protection des données à caractère personnel commune participe à l'engagement de ces entreprises (ci-après « les Sociétés » ou « Monaco Digital et ses filiales » ou « Société » lorsqu'elles sont concernées individuellement) pour un développement du numérique éthique et respectueux des personnes.

Monaco Digital et ses filiales s'intéressent aux data et à leurs écosystèmes (système d'information, infrastructures, applications, cybersécurité, accompagnement dans la maîtrise des ressources informatiques…).

Parmi ces data, les données à caractère personnel (ci-après « données personnelles ») présentent une caractéristique particulière qui nous est chère : elle traite des personnes physiques, de l'humain. Elles sont des indications sur les hommes et les femmes avec lesquelles nous travaillons au quotidien, ou pour lesquels nous travaillons souvent sans les connaître ou les rencontrer car utilisateurs des systèmes sur lesquels nous intervenons.

Ces données à caractère personnel font l'objet d'une attention particulière de l'ensemble des entités du groupe et de l'ensemble de ses collaborateurs.

Monaco Digital et ses filiales ont engagées une démarche afin de veiller à ce que les opérations effectuées sur ces données dans le cadre de leurs activités respectent les réglementations relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel applicables.

Cette démarche vise, notamment, à prendre en compte les 7 principes relatifs au traitement des données à caractère personnel fixés par la réglementation : (1) licéité, loyauté, transparence ; (2) limitation des finalités ; (3) minimisation des données ; (4) exactitude des données ; (5) limitation de la conservation ; (6) intégrité et confidentialité ; (7) responsabilité.

[1] Au sens du Règlement (UE) 2016/679 du 27 avril 2016, soit du Règlement Général européen sur la Protection des Données, appelé RGPD

Sur cette base, la présente politique expose les engagements pris par les Sociétés. Elle est complétée, lorsqu'opportun, par des politiques ou informations spécifiques (ex. sites internet, notices d'information sur les traitements des données des collaborateurs).

1. Être acteur de la protection des données

Selon que les Sociétés effectuent des opérations sur des données personnelles pour leur compte ou pour le compte de leurs clients, leur rôle dans la chaîne du traitement de ces données n'est pas identique :

- Chaque Société est « responsables de traitement »[1] pour les opérations réalisées dans le cadre de la gestion de l'entreprise et des activités qu'elle effectue pour son compte (ex. gestion des ressources humaines, sécurisation de ses locaux, sécurisation de son système d'information, gestion des opérations commerciales…).

- Chaque Société peut être « sous-traitante »[2] pour les opérations réalisées sur les données personnelles pour le compte de ses clients dans le cadre des prestations exécutées pour le client à la suite d'une demande formalisée par une proposition commerciale validée, un bon de commande, un contrat, des instructions particulières documentées de ses clients…

2. Identifier les données traitées et leur cadre

En tant que « Responsables de traitement », les Sociétés se doivent :

- D'identifier les données personnelles qu'elles exploitent ;

- De mettre en évidence les raisons pour lesquelles elles ont besoin de ces données ;

- De ne pas collecter et de ne pas conserver des données personnelles non nécessaires « au cas où » …

Ainsi, selon les situations, chaque Société traite des données personnelles sur la base des justifications suivantes :

- L'exécution de mesures précontractuelles prises à la demande de cette personne ;

- L'exécution d'un contrat avec la personne sur laquelle les données sont traitées[1] ;
- Le respect d'une obligation légale à laquelle la Société est soumise ;
- Des intérêts légitimes poursuivis par la Société ou par un tiers ;
- Le consentement de la personne concernée, soit de la personne physique sur laquelle des données sont traitées.

De manière générale, les données personnelles concernent :

- Ses collaborateurs et assimilés (ex. un sous-traitant agissant sous sa responsabilité chez un client, un stagiaire, le membre de la famille du collaborateur) ;
- Les contacts auprès de ses clients et prospects ;
- Les contacts auprès des fournisseurs, partenaires, prestataires ;
- Les contacts auprès des autorités administratives et assimilées ;
- Les utilisateurs des systèmes d'information de ses clients ;
- Les personnes rencontrées à l'occasion des activités de l'entreprise comme ses prestations de conseil, d'audit, de développement d'applicatifs, d'accompagnement dans le cadre de la transition numérique…
- Les invités et participants aux manifestations et évènements professionnels ;
- Les participants aux activités du Campus pour Monaco Digital ;
- Les internautes / mobinautes visiteurs de son site internet.

Il importe de préciser que les données exploitées s'inscrivent dans un contexte professionnel, d'une relation BtoB, de l'exécution des actions professionnelles des personnes sur lesquelles les données sont traitées.

[1] Soit, selon le RGPD « l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures »

Lorsque les Sociétés collectent des données sur les personnes précédentes, elles visent à répondre aux objectifs suivants :

2.1 S'agissant des collaborateurs et assimilés

- Gestion des ressources humaines (ex. recrutement, dossier du personnel, formation, paie, élections des délégués du personnel…) ;
- Gestion des outils de communication électronique (ex. messagerie, téléphone) ;
- Suivi de l'activité des collaborateurs (ex. affectation sur les missions, établissement et suivi des plannings, suivi des prestations chez les clients, support aux clients) ;
- Sécurisation des activités (ex. sécurisation du système d'information, sécurisation physique des sites, sécurisation des documents, sécurisation des impressions) ;
- Tenue des outils de gestion et méthodes (ex. établissement et suivi des procédures).

Les traitements associés sont détaillés dans une notice d'information communiquée aux collaborateurs et diffusée sur les outils internes de l'entreprise.

2.2 S'agissant des clients et prospects

- Gestion de la relation clientèle (CRM) ;
- Gestion du fichier client ;
- Gestion comptable et financière ;
- Gestion du support aux clients ;
- Organisation et suivi des prestations délivrées par les Sociétés (général ou spécifique selon les prestations – ex. phishing, e-formation, coaching individuel ou collectif, gestion des homologations…) ;
- Gestion du Campus ;
- Emargement dématérialisé (aux évènements / activités au sein du Campus) ;
- Etablissement et suivi d'analyse de risques.

Les catégories de données traitées sur les collaborateurs des clients qui peuvent être des contacts commerciaux, les utilisateurs du SI du Client, les personnes rencontrées lors d'entretiens à l'occasion de prestation de conseil, d'audit, d'accompagnement, les participants aux sessions du Campus.

Selon le cas, les données traitées seront :

- L'identité, les coordonnées, la fonction ;
- Les informations relatives à la relation commerciale (demandes, identification des besoins, dates des rendez-vous, réclamations) ;
- Les informations relatives aux activités sur le SI du Client (données d'identification électronique, log de connexion, ressources utilisées, demande et détail de l'intervention) notamment pour certaines prestations supports, infrastructure, audits, pentest… ;
- Les informations relatives aux sessions du Campus (éléments de suivi de la formation).

Les données proviennent de la personne elle-même, d'un contact au sein d'une entreprise cliente ou d'un tiers, ou du système d'information infogéré.

Il importe dans ce contexte que chaque Client informe ses collaborateurs ou toute personne qu'il met en contact avec les Sociétés à l'occasion de l'exécution des prestations commandées, de la communication de leurs données à Monaco Digital, Monaco Cyber Sécurité ou Fab Digital, ou plus généralement aux prestataires agissant pour le compte du Client.

En cas de droit d'accès, selon les circonstances de la collecte des données, les Sociétés précisent aux personnes qui les saisissent que leurs droits doivent s'exercer en première intention auprès du Client pour le compte duquel les données ont été traitées.

2.3 S'agissant des fournisseurs

- Gestion des fichiers fournisseurs ;
- Gestion de la relation fournisseur ;
- Gestion comptable et financière.

Les catégories de données traitées sont l'identité, les coordonnées, la fonction, les informations relatives à la relation commerciale.

Les données proviennent de la personne elle-même, d'un contact au sein de l'entreprise cliente ou d'un tiers (ex. un autre client, un annuaire professionnel, un partenaire).

Il importe dans ce contexte que chaque Client informe ses collaborateurs ou toute personne qu'il met en contact avec les Sociétés à l'occasion de l'exécution des prestations commandées, de la communication de leurs données à Monaco Digital, Monaco Cyber Sécurité ou Fab Digital.

2.4 S'agissant des partenaires

- Gestion de la relation partenaire

Les catégories de données traitées sont l'identité, les coordonnées, la fonction.

Les données proviennent de la personne elle-même, d'un contact au sein de l'entreprise cliente ou d'un tiers.

2.5 S'agissant des internautes

Enfin, une catégorie particulière de personnes sur lesquelles les Sociétés peuvent disposer de données personnelles : les internautes qui surfent sur leurs sites Internet respectifs.

Le traitement associé de « Gestion du site internet » collecte en effet des données indirectement nominatives : les logs de connexion, et peut permettre la collecte de données directement nominatives si la personne utilise la rubrique contact ou recrutement. Une information sur la protection des informations nominatives et, si nécessaire, une information sur les Cookies et traceurs accessibles sur les sites le décrivent.

Par ailleurs, ces personnes (collaborateurs et assimilés, prospects, clients et collaborateurs du clients, fournisseurs, partenaires…) peuvent être mentionnées dans les traitements du quotidien des Sociétés :

- Gestion de la messagerie (identité, coordonnées, fonction, signature) ;
- Identification des visiteurs du site internet (identité, coordonnées, fonction, horodatage) ;
- Gestion des évènements et manifestations professionnelles (identité, coordonnées, participation aux évènements, opposition à invitation future) ;
- Gestion du Wifi public (identité, ressource d'accès, données de connexion) ;
- Gestion du registre des demandes de droit d'accès (identité, coordonnées, type de droit, suivi de la demande) ;
- Gestion des violations de données à caractère personnel (identité, coordonnées, fonction, éléments de suivi de la violation).

L'ensemble de ces traitements est décrit dans les registres des activités de traitement respectifs des Sociétés.

En tant que « Sous-traitantes », les Sociétés agissent sur instruction(s) de leurs clients. Lorsque les prestations commandées concernent, impactent ou nécessitent l'exécution d'opérations sur des traitements de données à caractère personnel, il appartient au client, Responsable de traitement, de :

- Définir la ou les finalités du ou des traitements, le type de données à caractère personnel et les catégories de personnes concernées ;
- Déterminer les mesures de sécurité à respecter afin de protéger les données et leur(s) traitement(s) dompte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les droits et libertés des personnes physiques identifiés par le Client.

Ces éléments sont décrits, selon le cas, dans les documents contractuels entre les Sociétés et le Client, et/ou les procédures et documentations du Client (ex. PSSI, Charte informatique, registre des activités de traitement…).

3. Identifier les durées de conservation des données

Sujet délicat et compliqué de la protection des données à caractère personnel : la conservation des données et le respect du principe de limitation de la conservation des données.

De manière générale, les données personnelles sont conservées pendant une durée proportionnelle aux finalités (précitées) pour lesquelles elles ont été collectées, dans le respect, notamment, des instructions des Clients ou des dispositions légales ou réglementaires.

Pour les collaborateurs, la durée de conservation des données varie de quelques mois (ex. 12 mois pour les logs de connexion) à plusieurs années (ex. données traitées par les ressources humaines pendant la durée du contrat de travail suivi des délais de prescription des recours).

La durée de conservation de ces données est mentionnée dans la notice d'information évoquée précédemment.

Au cas particulier des informations collectées à l'occasion des relations commerciales, les durées de conservation varient selon la nature de la relation :

- S'agissant d'un prospect : la durée de conservation est de 3 ans à compter du dernier contact ;
- S'agissant d'un Client actif, avec lequel les Sociétés ont une relation de nature contractuelle en cours (un Client actif), les données sont conservées pendant 10 années après la fin de la relation d'affaire, hors les cas où les Sociétés se sont engagées à supprimer les informations à l'issue de la prestation (ex. audit PASSI) ou lorsque le client demande la suppression des données (à l'exception des informations de nature comptable et financière ou de toute donnée que les Sociétés doivent conserver en application de la réglementation en vigueur) ;
- S'agissant d'un Client non actif, une relation contractuelle non renouvelée, les données sont conservées pendant 10 années après la fin du dernier contrat ;
- S'agissant des fournisseurs, les données sont conservées 10 ans, après règlement. Cependant, selon les éléments objet des factures, ce délai sera étendu à la période de garantie ou à la qualité de propriété du bien.

Les données des contacts professionnels auprès de nos prospects, clients, fournisseurs, partenaires, sont conservées tant que la personne est en fonction et mises à jour ou supprimées lorsque les Sociétés sont informées des changements.

4. Identifier les destinataires des informations

Les données (personnelles ou non) qui nous sont confiées sont destinées aux collaborateurs qui ont besoin d'en connaître. L'accès à ces données se fait sur la base d'autorisations d'accès individuelles, limitées et encadrées selon le principe du moindre privilège.

Les collaborateurs des Sociétés sont liés par une clause de confidentialité incluse dans leur contrat de travail, rappelée dans divers documents des Sociétés comme le règlement intérieur ou la charte informatique. Ils sont par ailleurs sensibilisés aux sujets de la protection des données à caractère personnel et de la sécurité des systèmes d'information.

La communication des données de nos collaborateurs, en général, liés à des obligations légales ou contractuelles des Sociétés, est précisée dans la notice d'information précitée.

S'agissant de nos Clients, des données strictement nécessaires à l'exécution des prestations souscrites peuvent être communiquées à nos sous-traitants, aux fournisseurs d'équipements de logiciels, matériels, services ou prestations souscrites dans le respect des contrats, commandes, demandes de nos Clients.

S'agissant de nos fournisseurs et partenaires, des informations concernant les personnes à contacter peuvent être communiquées à nos Clients ou prospects selon leurs attentes.

5. Veiller à la sécurité des données personnelles

Les Sociétés mettent en place des mesures techniques et organisationnelles destinées à veiller à la sécurité des données personnelles tenant compte de l'état de l'art, des coûts de mise en œuvre, de l'évolution des technologies et des risques pesant sur les systèmes d'information et les réseaux.

Les Sociétés ont ainsi mis en place une Gouvernance de la sécurité du SI qui repose sur :

- Des ressources humaines : un responsable de la sécurité des systèmes d'Information désigné par la Direction, des collaborateurs sensibilisés au sujet de la sécurité du SI, des collaborateurs suivant des formations spécifiques certifiantes (ex. CISSP, ISO 27001 LA, ISO 27001 LI, ISO 27005 Risk Manager, CEH, OSCP, OSCE, CISA, PMP et ITIL), des réunions régulières d'un comité de Sécurité (COSEC) ;

- Une formalisation de process avec, par exemple, une politique de sécurité des systèmes d'information, une charte utilisateur, un règlement intérieur, des politiques thématiques comme une politique de sauvegarde, une politique de maintien en condition de sécurité, une politique de gestion des accès logiques, une politique de gestion des alarmes, une politique de mise au rebut, et des procédures comme une procédure de gestion des arrivées/mutations/départs, une procédure de gestion d'alertes de l'Agence Monégasque de Sécurité Numérique (AMSN) pour les Sociétés localisées en Principauté de Monaco, une procédure de gestion des alarmes, une procédure de gestion des contrôles d'accès…

- Des mesures techniques effectives destinées à protéger les systèmes d'information, l'ensemble de leurs ressources et données, s'intéressant

- La protection logique du SI comme des pare-feu dernière génération, le cloisonnement des réseaux, des connexions à distance via VPN, des équipements protégés par des antispam et des antivirus, le chiffrement des ordinateurs, des outils de gouvernance (gestion des tickets, gestion des incidents …), des solutions d'accès à distance pour l'assistance des clients, des sauvegardes en ligne et hors ligne, la mise à jour des correctifs de sécurité, des scanner de vulnérabilité ;

- La protection physique des locaux et des équipements avec des locaux placés sous vidéosurveillance, un contrôle d'accès physique aux heures de bureau, des locaux sous alarme et protection incendie, des locaux dédiés aux ressources selon leur sensibilité, des zones réservées aux seules personnes habilitées, des locaux avec accès par badge nominatif.

6. Identifier les transferts de données personnelles hors « protection adéquate »

L'activité de Monaco Digital et de Monaco Cyber Sécurité est réalisée à partir de Monaco.

Elles sont soumises à des obligations légales équivalentes à celles imposées au sein de l'Union européenne par le biais d'une réglementation issue de la loi n° 1.165 du 23 décembre 1993 relative à protection des informations nominatives. Toutefois, l'Union européenne n'a pas encore accordé à la Principauté une reconnaissance du caractère « adéquat » de ces règles avec celles fixées en Europe.

En conséquence, en application de l'article 46 du RGPD, les deux entreprises proposent une annexe à leurs contrats ou un avenant (selon l'antériorité du contrat) établi en tenant compte des clauses contractuelles types de protection des données établies par l'Union européenne s'agissant du transfert de données à caractère personnel entre un responsable de traitement (le Client) et son sous-traitant au sens du RGPD (Monaco Digital ou Monaco Cyber Sécurité), lorsque les prestations s'y prêtent.

Nous conservons les données (personnelles ou non) en Principauté ou au sein de l'Union Européenne. Toutefois, si nous devions transférer des données à des sous-traitants ou partenaires commerciaux hors de l'Union, nous nous assurerions que le traitement soit encadré par des garanties respectueuses des attentes de la réglementation monégasque, de la réglementation européenne et de nos clients.

Dans le cadre de leurs engagements en matière de protection des données à caractère personnel, Monaco Digital et Monaco Cyber Sécurité ont désigné un représentant sur le territoire européen :

FAB DIGITAL
618 Avenue Roumanille - 06410 Biot

7. Permettre aux personnes physiques d'exercer leurs droits

Conformément à la réglementation protégeant les traitements des données à caractère personnel, toute personne dispose de droits s'agissant du traitement de SES données personnelles.

Plus précisément, il s'agit :

- Du droit de savoir si des données la concernant sont exploitées par un responsable de traitement ;
- D'un droit d'accès à ses données ;
- D'un droit de rectification, lorsque les données sont inexactes ; d'un droit d'effacement, dans les cas prévus par les textes ;
- D'un droit de limitation du traitement de ses données, dans les cas prévus par les textes ; - D'un droit à la portabilité de ses données, dans les cas prévus par les textes, soit du droit de recevoir les données personnelles que la personne nous a fournies dans un format structuré, couramment utilisé et du droit de demander que ces données soient transmises à un autre responsable de traitement ; - D'un droit d'opposition à ce que ses données personnelles fassent l'objet d'un traitement, dans les cas prévus par les textes pour des raisons tenant à sa situation particulière;
- D'un droit d'opposition à ce que ses données soient utilisées à des fins de prospection notamment commerciale ;
- Lorsque les activités de traitement sont soumises à la réglementation française relative à la protection des données à caractère personnel, d'un droit de définir des directives relatives au sort de ses données personnelles après son décès (à cet égard, en cas de décès qui serait porté à notre connaissance, les données sont supprimées, sauf nécessité de conservation pendant une durée déterminée pour des motifs tenant aux finalités de traitement, aux obligations légales et réglementaires et/ou aux délais légaux de prescription, et après le cas échéant avoir été communiquées à un tiers éventuellement désigné par ses soins).

Toute personne peut ainsi exercer ses droits par courrier postal en s'adressant selon le cas à
Monaco Digital ou Monaco Cyber Sécurité
Protection des Données Personnelles
9, avenue Albert II – Le Copori

Des informations complémentaires peuvent également être demandées à

- Pour Monaco Digital, pdcp@monacodigial.mc
- Pour Monaco Cyber Sécurité, dpo@monacocyber.mc

Dans un souci de confidentialité et de protection de la personne et de leurs données, les Sociétés doivent veiller à pouvoir identifier le demandeur avant de répondre.

Selon, les Sociétés pourront demander à l'intéressé de justifier de son identité. Si la demande est effectuée par un mandataire, elle devra être accompagnée du mandat désignant nommément le mandataire et d'une copie d'un titre d'identité du mandant et du mandataire.

Les Sociétés se réservent la possibilité de demander des compléments d'information afin de garantir l'identité du demandeur.

En cas de réponse insatisfaisante, le requérant pourra introduire une réclamation auprès de l'autorité de protection des données compétente, par exemple la Commission de Contrôle des Informations Nominatives (CCIN) pour Monaco (www.ccin.mc) ou la Commission nationale de l'informatique et des libertés (CNIL) pour la France (www.cnil.fr).

Version 3
Fait à Monaco, le 1ier août 2024