

Obligation de protection des données et de confidentialité

Type de document	Obligation
Propriétaire	Chef de division HFC
Classification	Externe
Version	13 décembre 2021

1. Objet de la présente obligation

Diartis propose aux entreprises des secteurs public et privé des solutions logicielles complexes. Celles-ci servent en règle générale à traiter des données personnelles.

La présente obligation de protection des données et de confidentialité régit les obligations du collaborateur dans le cadre du travail qu'il effectue pour Diartis, notamment pour les projets clients. Les freelances, les consultants externes ou les rapports de service similaires sont assimilés aux collaborateurs pour cette obligation, raison pour laquelle nous appelons ces groupes "personne signataire" dans le texte suivant.

La personne signataire note que le contenu du présent accord de protection des données et de confidentialité est communiqué au client.

2. Classification des données

La loi relative à la protection des données distingue en principe les catégories de données suivantes :

2.1. Données personnelles

Il s'agit des données concernant une personne identifiée ou identifiable.

2.2. Données personnelles particulièrement sensibles

Il s'agit des données relatives

- aux opinions ou activités religieuses, idéologiques, politiques ou syndicales,
- à la santé, à la sphère intime ou à l'appartenance raciale,
- génétique,
- biométrie, qui identifient une personne physique de manière univoque,
- à des mesures d'aide sociale,
- à des poursuites et des sanctions administratives ou pénales.

2.3. Profils de personnalité

Le profilage est toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou le déplacement de cette personne physique.

3. Les grands principes de la protection des données

3.1. Objectif ou Pourquoi traiter des données ?

Le traitement de données doit servir un objectif. Cet objectif résulte d'une base légale ou d'un consentement exprès de la personne concernée. Dans le cas des projets clients, l'objectif du traitement est défini par le client, qui fait appel à Diartis dans le cadre de cet objectif.

La personne signataire est tenu de traiter les données uniquement dans le cadre de cet objectif contractuel.

3.2. Proportionnalité ou Dans quelle mesure les données sont-elles traitées ?

Le traitement de données n'est autorisé que dans la mesure où il est impérativement nécessaire pour atteindre l'objectif légal ou celui convenu par contrat. Il faut donc s'assurer que les données ne sont traitées que dans la mesure où cela est absolument nécessaire et que n'ont pas accès aux données plus de personnes que strictement nécessaires.

Dans son travail, la personne signataire doit donc veiller à observer le principe de la proportionnalité et à ce qu'à cet égard, les dispositions contractuelles du client soient respectées.

3.3. Droit d'accès ou Qui traite les données ?

Toute personne peut demander au maître d'un fichier de données s'il traite des données la concernant. Dans le cadre de projets clients, Diartis n'est pas maître du fichier de données, c'est la personne signataire doivent toujours transmettre les éventuelles demandes aux responsables internes de la protection des données.

4. Garantie de la protection des données

La personne signataire garantit

- de traiter les données de manière appropriée et proportionnée, conformément aux instructions précises du client.
- de ne traiter les données que dans la mesure où l'objectif convenu contractuellement avec le client l'exige.
- de respecter, lors de l'acquittement de ses obligations contractuelles, les lois spécifiques applicables au client que ce dernier lui a communiquées.
- de transmettre immédiatement aux responsables internes de la protection des données pour traitement toute demande de renseignements, de quelque nature qu'ils soient, qui lui a été faite par un tiers.
- d'informer sans délai les responsables internes de la protection des données en cas de problèmes ou de risques liés à la protection des données.

- de traiter de manière strictement confidentielle toutes les informations révélées dans le cadre de l'exécution du contrat.
- de respecter les mesures de protection des données spéciales voulues par le client.

5. Garantie de la sécurité des données

La personne signataire garantit

- dans le cadre de son travail, d'empêcher l'accès des personnes non autorisées par des mesures techniques et organisationnelles appropriées.
- de ne se connecter à Internet ou à d'autres systèmes que dans la mesure où cela a été convenu ou est strictement nécessaire¹.
- d'empêcher l'introduction de logiciels non autorisés ou malveillants.
- de ne transférer aucune donnée sur des supports de données privés.
- d'informer immédiatement le client des défauts ou dysfonctionnements des systèmes dont la personne signataire prend connaissance dans le cadre de son travail.
- de respecter les mesures de sécurité spéciales convenues par contrat avec le client.

6. Confidentialité concernant les clients

La personne signataire garantit

- la confidentialité absolue de l'organisation et de l'infrastructure techniques du client.
- à la fin du contrat, restituer tous les documents physiques au client ou à l'autorité compétente. Si cela n'est pas possible, les documents doivent être restitués à Diartis.
- les dossiers électroniques doivent être effacés sur des supports de données dans les 3 mois suivant la fin du mandat et le client doit être informé à l'avance de l'effacement.
- ne pas fournir de renseignements sur le contenu et l'existence d'accords avec des clients à une personne qui n'a pas besoin de ces informations dans l'exercice de ses fonctions au sein de Diartis.
- le maintien du secret même après la fin du contrat conclu avec le client.

7. Confidentialité concernant Diartis

Dans le cadre de son travail chez Diartis, la personne signataire a accès à des informations confidentielles. Par "informations confidentielles", on entend des informations ou des sujets qui ont une valeur commerciale pour l'entreprise et qui ne sont pas généralement connus ou facilement accessibles dans le secteur. Il s'agit par exemple d'informations techniques sur les produits et services de l'entreprise, y compris le savoir-faire en matière de produits, les formules, les plans, les appareils, les diagrammes, le code logiciel, les résultats de tests, les processus, les inventions, les projets de recherche et le développement de produits et la correspondance, ainsi que toute autre information qui n'est pas généralement connue du public et dont on peut s'attendre à ce qu'elle ait un effet négatif sur les activités de l'entreprise en cas d'abus ou de divulgation.

La personne signataire est tenue de traiter les informations confidentielles de l'entreprise, qu'elles aient été créées ou développées par la personne signataire, de manière strictement confidentielle. Ces informations ne doivent pas être divulguées à des tiers sans l'accord écrit préalable de l'entreprise.

¹ cf. à ce sujet la directive de Diartis SA concernant l'accès VPN.

8. Responsabilité

La personne signataire est responsable vis-à-vis de Diartis et de ses clients de tous les dommages résultant du non-respect du présent accord.

9. Autres conséquences juridiques

La personne signataire note que, si elle contrevient à la présente obligation de protection des données et de confidentialité, elle s'expose personnellement à des sanctions pénales et que cette obligation de protection des données et de confidentialité s'applique au-delà de la relation de travail ou de la relation contractuelle.

.....
Lieu/date

.....
Prénom, nom (en majuscules)

.....
Signature