PROTECTION DES DONNÉES CLIENTS & RGPD

SECURISATION DES DONNEES SENSIBLES RGPD OU NON

SECURISATION DES LOCAUX		REMARQUES
Bureaux situés chez le Dirigeant	☐	
Bureaux de type agence sur rue	☐	
Bureaux en rdc	☒	
Bureaux en étages	☐	
Bureaux avec interphone	☒	Avec visiophone
Bureaux avec accueil immeuble	☐	
Bureaux avec Vigiles	☐	
Bureaux avec blindages (portes/fenêtres)	☐	
Bureaux avec alarme	☐	
Bureaux avec serrure 3 points	☐	
Autre (préciser)	☒	Caméra vidéo dans hall d'entrée

SECURISATION DES DONNEES PAPIER		REMARQUES
Meuble fermant à clef (minimum)	☒	
Meuble/coffre-fort ignifugé fermant à clef	☐	
Pièce archivage dossier fermant à clef	☐	
Copie systématique et conservation copie éloignée	☐	
Scanne toutes pièces puis destruction ou éloignement de la sauvegarde	☒	
Destructeur de documents papier	☒	
Autre (préciser)	☐	

SECURISATION DES DONNEES NUMERIQUES		REMARQUES
Sur Ordinateur du conseiller avec mot de passe pour accès à la partie professionnelle (minimum)	☒	
Sur ordinateur du conseiller avec mot de passe pour accès à la partie professionnelle et cryptage des données	☒	
Sur serveur centrale sur site avec accès réservé/VPN sécurisé	☐	
Sur disque dur externe ou Clef USB qui sont mis sous clef (minimum)	☐	
Sur disque dur externe ou clef cryptés mis sous clef	☐	
Sur disque dur externe ou clef cryptés et éloignés	☒	Au domicile d'un des dirigeants
Sur Ordinateur sécurisé plus Cloud sécurisé et RGPD compatible	☒	Serveur Nas crypté avec sauvegarde RAID et cloud Synologie. www.synology.com/fr-fr/privacy
FireWall et autre systèmes antivirus et d'analyse des systèmes et entrants/sortants	☒	Antivirus Kaspersky Total Sécurité et Avast Premium
Autre (préciser)	☐	

I. REGISTRE DES ACTIVITÉS DE TRAITEMENT DE PAGNOT-TRILLAUD ET ASSOCIES

Coordonnées du responsable de l'organisme <i>(Responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)</i>	Nom : PAGNOT Prénom : PHILIPPE Adresse : 17 RUE DUGUESCLIN CP : 69006 Ville : LYON Téléphone : 0472695190 Adresse de messagerie : philippe.pagnot@traces-patrimoine.fr
Nom et coordonnées du délégué à la protection des données <i>(Si vous avez désigné un DPO)</i>	Nom : _____ Prénom : _____ Société (si DPO externe) : _____ Adresse : _____ CP : _____ Ville : _____ Téléphone : _____ Adresse de messagerie : _____

Activités de l'organisme impliquant le traitement de données personnelles
Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	gestion des prospects
Activité 2	gestion des clients
Activité 3	gestion des fournisseurs
Activité 4	
Activité 1	
Activité 6	
Activité 7	
Activité 8	

FICHE DE REGISTRE DE L'ACTIVITÉ
Nom de l'activité : GESTION DES PROSPECTS
(Créer cette fiche pour chaque activité listée)

Date de création de la fiche	Entrer une date. 16/05/2017
Date de dernière mise à jour de la fiche	Entrer une date. 15/07/2022
Nom du responsable conjoint du traitement (Dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)	
Nom du logiciel ou de l'application (Si pertinent)	

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

Permettre la prise de renseignements à des fins de découverte du prospect en vue de délivrer un conseil et une étude.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. PROSPECT	2. DIRIGEANT D'ENTREPRISE
3. SALARIE	4. RETRAITE

Catégories de données collectées (Cochez et listez les différentes données traitées)

État-civil, identité, données d'identification, images

nom, prénom, adresse, date et lieu de naissance, pièce d'identité

Vie personnelle

situation familiale, régime matrimonial, enfants.

Vie professionnelle

situation professionnelle, statut.

Informations d'ordre économique et financier

revenus, situation financière, données bancaires, données fiscales, statuts personnes morales

Données de connexion

Données de localisation

Internet

adresse mail, site internet

Autres catégories de données (précisez) :

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

Oui Non

Si oui, lesquelles ? :

[Redacted area]

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

[Redacted] Jours, [Redacted] Mois, [Redacted] Ans, Autre durée : [Redacted]

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

[Redacted] 5 ans après la fin de la relation d'affaires

Remarque ANACOFI : La durée de conservation légale pour prestations AMF/ACPR est de 5 ans après la fin de la relation d'affaires.

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

- 1. DIRIGEANTS
- 2. CONSEILLERS
- 3. [Redacted]
- 4. [Redacted]

Organismes externes

(Exemples : filiales, partenaires, etc.)

- 1. PARTENAIRES
- 2. FOURNISSEURS
- 3. [Redacted]
- 4. [Redacted]

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

- 1. PRESTATAIRE INFORMATIQUE
- 2. [Redacted]
- 3. [Redacted]
- 4. [Redacted]

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

Oui Non

Si oui, vers quel(s) pays :

[Redacted area]

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et 47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

Contrôle d'accès des utilisateurs

Tous les accès au logiciels et applications sont protégés par identifiant et mot de passe

Mesures de traçabilité

Précisez la nature des traces (exemple : journalisation des accès des utilisateurs), les données enregistrées (exemple : identifiant, date et heure de connexion, etc.) et leur durée de conservation :

Les connexions sont enregistrées de façon journalière pour chaque conseiller (O2S)

Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Les logiciels de protection sont mis à jour quotidiennement

Sauvegarde des données

Les données sont sauvegardées dans la GED (O2S) et également par une sauvegarde RAID. Une sauvegarde sur disque externe conservée en dehors des locaux est faite de manière hebdomadaire.

Chiffrement des données

Les données sur le serveur NAS sont cryptées ainsi que dans le cloud Sinology.

Contrôle des sous-traitants

Validation et agrément par les organismes professionnels pour l'utilisation des outils informatiques. Echanges régulier avec le sous traitant.

Autres mesures :

ACTIONS QUI DECOULENT DE CETTE ANALYSE :

Suite à cette première analyse, mise à jour régulièrement, notre entreprise réalise une autre analyse en vue d'identifier les risques portant sur les données obtenues et les moyens de :

- ✓ Ne recueillir que des données dont la finalité est celle annoncée
- ✓ Ne recueillir que des données utiles ou imposées par les textes pour ce type de mission

Date d'analyse	Risques identifiés	Mesures prises
15/07/2022	Aucun	Aucune

INFORMATION DU PROSPECT OU CLIENT QUANT A NOTRE PROCEDURE, L'USAGE DES DONNEES ET LE DROIT DU CLIENT A UN ACCÈS, CORRECTIONS OU DEMANDES DE RECUPERATION/DESTRUCTION :

L'information est assurée par des mentions expresses ajoutées sur :

- ✓ La Fiche d'Information Légale ou le Document d'Entrée en Relation
- ✓ Un document spécifique (l'insérer dans la fiche)
- ✓ La synthèse client (ou KYC) visée par lui
- ✓ La Lettre de Mission ou le Mandat
- ✓ Site Internet

L'acceptation expresse du client est recueillie :

- ✓ Par signature des documents précédemment cités
- ✓ Par signature d'un document spécifique
- ✓ Par renvoi de sa part d'un message validant l'acceptation
- ✓ Par validation par système digital
- ✓

EN CAS D'ARRET DE LA RELATION ET DE DEMANDE DU CLIENT DE RECUPERATION DE SES DONNEES, ELLES SONT RECUPERABLES

Envoi Automatique	☐	Sur demande	☒
Accès libre sur site en ligne	☐	Durée	1 mois
Mode d'information du moyen de récupération			
Format papier	☒	Format pdf	☒
Format digital	☐	Lequel	
Remarque	Le client est informé de notre obligation de conserver copie de certaines données pendant une durée qui dépend de la mission.		

Souscription Assurance	OUI	NON	Assureur/contrat
	☒	☐	

Suivi formation dédiée (intitulé)	Quand	Quel personnel	Description rapide