REGISTRE DES ACTIVITÉS DE TRAITEMENT DE ACANTHES EXPERTISES

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Nom : MÉNARD Prénom : Sandrine Adresse : 8 rue Castelviel CP : 31180. Ville : Rouffiac Tolosan Tél : 05.61.14.27.89 Adresse de messagerie : sandrine.menard@acanth.fr
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	Nom : MÉNARD Prénom : Sandrine Société (si DPO externe) : Cliquez ici. Adresse : 32 rue de l'Eden CP : 31180 Ville : Rouffiac Tolosan Tél: 05.61.14.27.89. Adresse de messagerie : sandrine.menard@acanth.fr

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	Expertise Comptable
Activité 2	Conseil en gestion et secrétariat juridique
Activité 3	
Activité 4	
Activité 5	
Activité 6	
Activité 7	
Activité 8	

FICHE DE REGISTRE DE L'ACTIVITÉ

Expertise Comptable

Date de création de la fiche	19 décembre 2018
Date de dernière mise à jour de la fiche	19 décembre 2018
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	N/A
Nom du logiciel ou de l'application *(si pertinent)*	

Objectifs poursuivis

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

Suivi des situations fiscales et sociales du dirigeant et des associés éventuels des entreprises clientes du cabinet.
Traitement des informations de l'Entreprise pour l'établissement des déclarations fiscales, sociales et juridiques.
Traitement des données personnelles des salariées du cabinet.

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. Salariés
2. Prospects
3. Clients
4.

Catégories de données collectées

Cochez et listez les différentes données traitées

☒ État-civil, identité, données d'identification, images : *nom, prénom, adresse, photographie, date et lieu de naissance, copie de cni et passeport…*

☒ Vie personnelle *: habitudes de vie, situation familiale, etc.*

☒ Vie professionnelle : *situation professionnelle…*
Cliquez ici.

☒ Informations d'ordre économique et financier *: revenus, situation financière, données bancaires, etc.*
Cliquez ici.

☒ Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
Cliquez ici.

☐ Données de localisation

☒ Internet : *cookies, données de navigation,*

☐ 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 ? :

NIR uniquement (Numéro de sécurité sociale)

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Les données permanentes (Identités…) sont conservées 5 ans à compter de la date de fin de relation contractuelle.
Les données de chaque année d'exercice sont conservées 5 ans

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. Salariés
2. Collaborateurs

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. Impôts
2. Tiers (à la demande expresse du client
3. Organismes Sociaux, Fiscaux, Administrations
4. Banques.

Sous-traitants

1. Bureautique : CSC CANON
2. Logiciel Métier : AGIRIS – EIC - RCA
3. Informatique générale : ICLUB INFORMATIQUE
4. Sauvegarde : SYNOLOGY INC
5. Paye : PAC SOCIALE
6. Dossiers Agricoles : FORDERER

Transferts des données hors UE

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

☐ Oui ☒ Non

Si oui, vers quel(s) pays :

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 et47 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

Décrivez les mesures :

Contrôle des accès utilisateurs et gestion des droits d'accès par ensemble d'identifiant / mot de passe personnel.
Règles de définition de mot de passe complexe (anti-forçage).
Validité de mot de passe fixée à 30 jours.
Blocage automatique des accès après 5 tentatives de connexion infructueuse sur 60 secondes avec capture de l'adresse IP sur serveur de sauvegarde
Blocage automatique des accès après 10 tentatives de connexion infructueuse sans timing avec capture de l'adresse IP sur serveur de sauvegarde.

☒ 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 :

Traçage des accès et des tentatives d'accès utilisateurs (Identifiant, date et heure de connexion, protocole utilisé, adresse IP). Données conservées 90 jours.
Traçage et gestion de la vie des données par utilisateur (ajout / modification / suppression)

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

Décrivez les mesures :

Mise à jour de sécurité automatique sur Serveur principal et sur Serveur de Sauvegarde et postes clients lourds (pc portables, Ordinateur Sandrine Ménard), Protection Antivirale active en temps réel sur Serveur principale et Serveur de Sauvegarde + planification d'une analyse quotidienne complète de l'intégrité de l'ensemble des données sur le serveur de sauvegarde.
Tests réguliers de restauration de données distantes.

☒ Sauvegarde des données

Sauvegarde incrémentale en temps réel sur ensemble de disque en RAID1 et sur site distant (en HTTPS avec clé de cryptage SSL unique. Versionnage intelligent. Protection contre la suppression volontaire ou involontaire de données. Accès unique par administrateur.

☒ Chiffrement des données

Protection des dossiers sauvegardés par cryptage AES 256 bits. Verrouillage automatique des dossiers en cas de tentative d'intrusion. Déverrouillage par clé de cryptage.

Cryptage des disques durs des Ordinateur Portables du cabinet.

Utilisation de HTTPS avec certificat SSL pour connexion distante au serveur de sauvegarde et lien de sauvegarde.

Chiffrement des données du disque dur de l'imprimante multifonctions de l'agence (AES256) et procédure d'effacement des données de ce disque sécurisé (10 passes d'écriture à 0)

☐ Contrôle des sous-traitants

Décrivez les modalités :

☒ Autres mesures :

Accès au Bureau Distant (Sessions TSE sur Server Acanthes) à travers un réseau VPN Sécurisé et crypté

FICHE DE REGISTRE DE L'ACTIVITÉ

Conseil en gestion et secrétariat juridique

Date de création de la fiche	19 décembre 2018
Date de dernière mise à jour de la fiche	19 décembre 2018
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	N/A
Nom du logiciel ou de l'application *(si pertinent)*	

Objectifs poursuivis

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

Suivi des situations fiscales et sociales du dirigeant et des associés éventuels des entreprises clientes du cabinet.
Traitement des informations de l'Entreprise pour l'établissement des déclarations fiscales, sociales et juridiques.
Traitement des données personnelles des salariées du cabinet.

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. Salariés
2. Prospects
3. Clients
4.

Catégories de données collectées

Cochez et listez les différentes données traitées

☒ État-civil, identité, données d'identification, images : *nom, prénom, adresse, photographie, date et lieu de naissance, copie de cni et passeport…*

☒ Vie personnelle *: habitudes de vie, situation familiale, etc.*

☒ Vie professionnelle : *situation professionnelle…*
Cliquez ici.

☒ Informations d'ordre économique et financier *: revenus, situation financière, données bancaires, etc.*
Cliquez ici.

☒ Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
Cliquez ici.

☐ Données de localisation

☒ Internet : *cookies, données de navigation,*

☐ 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 ? :

NIR uniquement (Numéro de sécurité sociale)

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Les données permanentes (Identités…) sont conservées 5 ans à compter de la date de fin de relation contractuelle.
Les données de chaque année d'exercice sont conservées 5 ans

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. Salariés
2. Collaborateurs

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. Impôts
2. Tiers (à la demande expresse du client
3. Organismes Sociaux, Fiscaux, Administrations
4. Banques.

Sous-traitants

1. Bureautique : CSC CANON
2. Logiciel Métier : AGIRIS – EIC - RCA
3. Informatique générale : ICLUB INFORMATIQUE
4. Sauvegarde : SYNOLOGY INC
5. Paye : PAC SOCIALE
6. Dossiers Agricoles : FORDERER

Transferts des données hors UE

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

☐ Oui ☒ Non

Si oui, vers quel(s) pays :

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 et47 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

Décrivez les mesures :

Contrôle des accès utilisateurs et gestion des droits d'accès par ensemble d'identifiant / mot de passe personnel.
Règles de définition de mot de passe complexe (anti-forçage).
Validité de mot de passe fixée à 30 jours.
Blocage automatique des accès après 5 tentatives de connexion infructueuse sur 60 secondes avec capture de l'adresse IP sur serveur de sauvegarde
Blocage automatique des accès après 10 tentatives de connexion infructueuse sans timing avec capture de l'adresse IP sur serveur de sauvegarde.

☒ 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 :

Traçage des accès et des tentatives d'accès utilisateurs (Identifiant, date et heure de connexion, protocole utilisé, adresse IP). Données conservées 90 jours.
Traçage et gestion de la vie des données par utilisateur (ajout / modification / suppression)

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

Décrivez les mesures :

Mise à jour de sécurité automatique sur Serveur principal et sur Serveur de Sauvegarde et postes clients lourds (pc portables, Ordinateur Sandrine Ménard), Protection Antivirale active en temps réel sur Serveur principale et Serveur de Sauvegarde + planification d'une analyse quotidienne complète de l'intégrité de l'ensemble des données sur le serveur de sauvegarde.
Tests réguliers de restauration de données distantes.

☒ Sauvegarde des données

Sauvegarde incrémentale en temps réel sur ensemble de disque en RAID1 et sur site distant (en HTTPS avec clé de cryptage SSL unique. Versionnage intelligent. Protection contre la suppression volontaire ou involontaire de données. Accès unique par administrateur.

☒ Chiffrement des données

Protection des dossiers sauvegardés par cryptage AES 256 bits. Verrouillage automatique des dossiers en cas de tentative d'intrusion. Déverrouillage par clé de cryptage.

Cryptage des disques durs des Ordinateur Portables du cabinet.

Utilisation de HTTPS avec certificat SSL pour connexion distante au serveur de sauvegarde et lien de sauvegarde.

Chiffrement des données du disque dur de l'imprimante multifonctions de l'agence (AES256) et procédure d'effacement des données de ce disque sécurisé (10 passes d'écriture à 0)

☐ Contrôle des sous-traitants

Décrivez les modalités :

☒ Autres mesures :

Accès au Bureau Distant (Sessions TSE sur Server Acanthes) à travers un réseau VPN Sécurisé et crypté