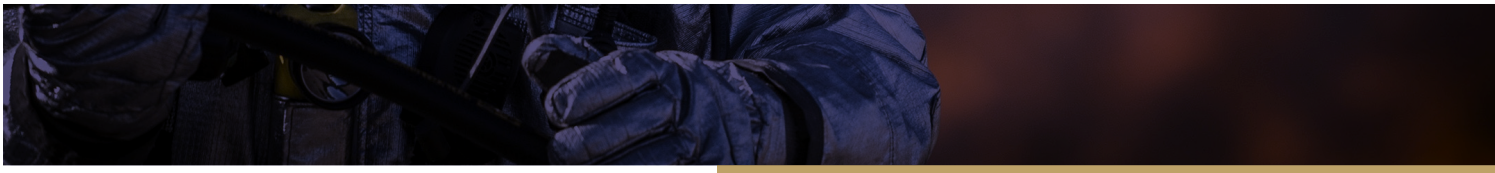
RÉGLEMENTATION PUPA TRACFIN LIVRE BLANC

WATERLOT & ASSOCIÉS

TABLE DES MATIÈRES

PLAN D'URGENCE DE POURSUITE DE L'ACTIVITÉ



INTRODUCTION

PUPA

Entre les catastrophes naturelles, les défaillances techniques et les erreurs humaines, la fréquence et le coût des crises ont tendance à augmenter, entraînant des perturbations impactant fortement le fonctionnement des entreprises par l'imbrication de leurs activités.

Le plan d'urgence de poursuite de l'activité est un acte d'engagement sur la planification de la réaction à un incident technique ou sinistre grave. Son objet est de minimiser les impacts sur l'activité de notre entreprise afin de ne pas affecter celle de nos partenaires, les garantissant de notre anticipation dans l'analyse du risque et de notre préparation.

En échange de cette confiance dont vous faites preuve en externalisant une partie de vos activités vers notre entreprise, nous vous devons cette garantie d'exigence dans notre rôle de prestataire de services essentiels externalisés (PSEE).

C'est pour répondre à cette exigence que nous avons construit ce plan PUPA depuis plusieurs années, qui se veut révélateur de nos bonnes pratiques en parallèle à notre livre blanc sur les règles de bonne conduite en matière de protection des données.

C'est un plan évolutif, régulièrement mis à jour et dont les fonctions font l'objet de contrôles et de tests inopinés.

Il est construit sur :

- L'anticipation : analyse du risque par l'identification de celui-ci, adaptation de mesures de prévention ;
- Le traitement : détermination du mode de gestion du risque, plan de réaction ;
- La solution : restauration intégrale ou en mode dégradé provisoire ;
- La protection : analyse du dommage a posteriori, retour d'expérience sur le traitement, mise en place d'une protection renforcée si nécessaire.

DESCRIPTIF ET SYSTÈMES DE SÉCURITÉ DU **SYSTÈME D'INFORMATION**

RÉSEAU LOCAL INTERNET

- Sonicwall TZ400 ;
- 1 fibre optique Absystech Telecom 100 Mbps - GTR 4H ;
- 1 ADSL Orange (opérationnelle le jour de la MEP du sonicwall. Down aujourd'hui) ;
- Les différents sites de la SAS Waterlot sont interconnectés en MPLS via des liens à haut-débit (Fibre sinon VDSL lorsque la fibre n'est pas disponible).

CONNEXIONS DISTANTES

Les personnes en nomadisme ou télétravail se connectent sur le réseau de la SAS Waterlot via un client VPN Fortinet :

- Chiffrement par matériel : Prévention des piratages et sécurité des données en transit.
- Sécurité évolutive : Sécurité évolutive intégrée en toute transparence au routage.
- Sécurité totale des communications de données : Protège les communications d'application à application, d'utilisateur à utilisateur, d'utilisateur à machine et de machine à machine.

PROJETS TECHNIQUES EN COURS

- Développements d'applications mobiles.
- Développement d'une version web pour la gestion de nos dossiers.

SERVEUR

- 1 serveur physique ESXI principal simulant 5 machines virtuelles :
  - Serveur TSE
  - Serveur étude
  - Serveur Base de données
  - Serveur Réseau
  - Serveur Active Directory ;
- Double alimentation et onduleurs ;
- Le serveur est situé dans un local ventilé nécessitant un code pour entrer ;
- Chaque machine virtuelle est répliquée (J-1) sur un serveur physique ESXI de secours ;
- Antivirus Files Security (ESET).

LOGICIEL

- Logiciel INTHUISS 7 développé par la société APTITUDE LOGICIELS, agréé par la Chambre Nationale des Huissiers de Justice, sur rapport de conformité d'un commissaire aux comptes agréé, en application de l'article 10 de l'arrêté du 31 mai 2011 ;
- EDI (Adec et propriétaire) flux entrants et sortants, gestion des flux financiers ;
- Gestion complète des dossiers : GED, intégration des mails et scans, gestion des sms ;
- Gestion des données personnelles compatible au RGPD.

DESCRIPTIF ET SYSTÈMES DE SÉCURITÉ DU SYSTÈME D'INFORMATION

TÉLÉPHONIE

- ABSYSTECH Telecom ;
- Appliance EASY2CALL 100, modèle hybride T2/IP, disques durs en Raid 1. Communications en Full IP sur le site ;
- 2 switchs HP Procures E2530-24-PoE+ ;
- 10 postes Aastra 6755i dont deux avec module d'extension LCD ;
- 33 postes Aastra 6731i ;
- 37 postes Aastra 6737i ;
- 1 poste Mitel 6867i ;
- 2 Cisco SPA122 (fax) ;
- 1 Konftel (conférencier) ;

- Centre d'appels CTI administrés par ABSYSTECH Telecom ;
- Service Hotline. Portail disponible 24h/24, 7j/7 ;
- Prise en charge dans les 4 heures ouvrées.

AUTOMATE D'APPELS

- L'automate d'appels, est basé sur une solution de type Asterisk, dimensionnée pour prendre en charge un très grand nombre d'appels en simultané.
- Les messages passent directement par nos serveurs, via notre installation interne.
- La solution apporte souplesse et efficacité à notre plateau téléphonique, tout en proposant une série de données statistiques permettant de vérifier la pertinence de nos campagnes d'appels.

IMPRIMANTES

- 5 SHARP MX-M565N Impression, copie, scan, fax.
- Haute protection des données et contrôle d'accès optimisé.
- Fonction «impression suivie» permettant une libération d'impression sécurisée au moment et à l'endroit souhaités après authentification sur le matériel.
- Les significateurs et huissiers sont équipés d'une imprimante nomade (en wifi) pour les interventions urgentes.

SITE INTERNET DE PAIEMENT

- Hébergement chez OVH SAS ;
- Sauvegarde quotidienne assurée par l'hébergeur ;
- Système de paiement SPPLUS (Natixis Intégration automatique ;
- Portail d'accès à notre cloud sécurisé DropAct (RGPD).

POSTES DE TRAVAIL

- 70 postes physiques ;
- 30 postes mobiles (ordinateurs portables équipés d'un bureau distant et d'un softphone) ;
- Garantie constructeur J+1 ;
- Administration par console de l'ensemble du parc informatique avec ENDPOINT antivirus (ESET) et pour les mobiles Encryption (ESET).

DESCRIPTIF ET SYSTÈMES DE SÉCURITÉ DU SYSTÈME D'INFORMATION

SÉCURITÉ

L'intégralité du réseau est protégé derrière un firewall FortiGate 3000D :

- Firewall « Sateful » : Règles de firewall par session multi-critères pour améliorer les performances.
- Proxy
- NAT
- Accès distant IPSEC et SSL : Connexions sécurisées pour les nomades et les sites distants.
- Anti-intrusion : Protection contre les attaques criminelles en analysant le trafic, et blocage des menaces avant qu'elles n'atteignent les ressources sensibles. Fonctionnalités activables à la demande et facilement configurables telles que la détection d'anomalies protocolaires, la gestion de sondes IPS et la démarche préventive DDOS.
- Filtrage d'URL & filtrage protocole : Contrôle du contenu que l'internaute est autorisé à consulter: Maitrise de la productivité des collaborateurs, limitation des risques de congestion du réseau, prévention des fuite d'informations confidentielles, diminution des risques d'exposition aux menaces, protection de la responsabilité légale de notre entreprise.
- Contrôle applicatif : Analyse en temps réel du trafic et la mise en correspondance avec une base de données de signatures embarquées sur l'équipement et référençant plus de 3500 applications réparties en grandes familles pour simplifier et optimiser notre politique de sécurité.
- Antivirus : Double détection reposant à la fois sur une base de signatures et via un algorithme d'analyse du comportement supposé d'un programme. Élimination d'un large spectre d'attaques et d'activités malicieuses (virus, les chevaux de Troie, spywares, botnets, adwares...).

SAUVEGARDE ET RÉPLICATION

Deux serveurs NAS sont déployés dans l'étude lilloise pour les sauvegardes ; réplication vers un 3ème serveur NAS déployé sur le site de Valenciennes.

Un export des données les plus sensibles (à savoir les bases de données Inthuiss) est réalisé chaque jour grâce au système de sauvegarde Oodrive (Adbackup). Oodrive garantie la sauvegarde des données et permet de prévenir les pires scénarios.

Chaque jour, différentes sauvegardes sont réalisées :

- Une copie de chaque machine virtuelle à un instant T (sur 7 jours).
- Une copie des données Partage & GED est sauvegardée sur 2 NAS différents, et une réplication sur un NAS à Valenciennes.
- Une réplication miroir de la base de données, des données Partage & GED est synchronisé sur le serveur ESXI de secours pour permettre une reprise rapide.

IMMOBILIER

Locaux sous alarme volumétrique, connexion à un central d'intervention.

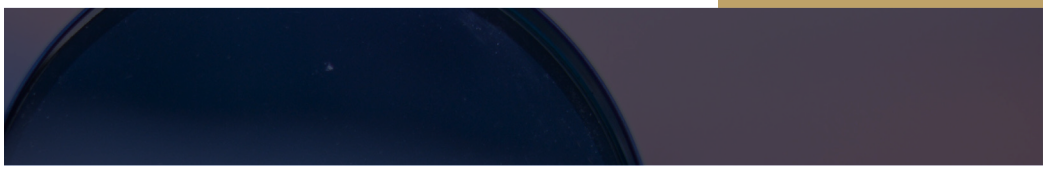
En cas de sinistre rendant inexploitables les locaux de l'Étude, un plan de relogement a été conçu avec une entreprise spécialiste de l'immobilier de l'entreprise, leader sur le marché et partenaire historique de l'Étude, afin de réinstaller les bureaux sous un délai de huit jours avec bail précaire. La ville de Lille bénéficie d'un parc immobilier d'entreprise particulièrement dynamique et développé.

VALIDITÉ DU PUPA

Une fois par an WATERLOT & ASSOCIÉS organise une réunion avec l'ensemble de ses partenaires dans le but de réviser et optimiser ce plan d'urgence.

ACTIVITÉS CRITIQUES ET MISE EN PLACE DU **PUPA**

ACTIVITÉ	SERVICE	SERVICE MINIMUM	SOLUTIONS
ACCÈS À LA BASE DE DONNÉES INFORMATIQUE	Information et travail sur l'évolution des dossiers en cours de gestion à l'Étude.	Information interne puis externe sur impossibilité temporaire de communiquer.	Matériel sous garantie constructeur, sauvegardes disponibles immédiatement.
REVERSEMENT DES FONDS	Reverser par voie dématérialisée les disponibles de gestion aux clients de l'Étude.	Les reversements pourront s'effectuer par édition de lettres chèques	Redémarrage des services ADSL et du SI.
ÉDITION / GESTION DES ACTES	Édition et passage au répertoire des actes signifiés par l'Étude.	Information interne puis externe sur l'impossibilité de produire et de répertorier les Actes.	Redémarrage du SI.
ÉDITION DES COURRIERS	Support d'information sur l'évolution et le suivi des dossiers en cours.	Externalisation (impression, mise sous plis et affranchissement) des éditions par l'outil DSO-Print.	Redémarrage du SI ; Contrat d'intervention sur site des copieurs connectés.
APPELS ENTRANTS	Informations relatives à l'évolution des dossiers en gestion.	Mise en place d'un message d'accueil informant l'incapacité technique de l'Étude à communiquer.	Redémarrage sous contrat de maintenance.
APPELS SORTANTS	Relance des clients.	Relance téléphonique manuelle des clients.	Redémarrage du CTI sous contrat.
ENCAISSEMENT DES CHÈQUES, MANDATS, ESPÈCES	Assurer les paiements faits à l'Étude ou reçus par courrier.	Placement des règlements reçu dans le coffre de l'Étude.	Redémarrage du SI.
ENCAISSEMENTS PAR CB	Assurer le paiement des clients se présentant ou appelant l'Étude.	Utilisation d'un TPE physique à l'Étude et par téléphone.	Redéploiement du site internet de paiement de l'Étude.



PROCESS ENCAISSEMENT ESPÈCES / **TRACFIN**

1. REMISE DES ESPÈCES À L'ACCUEIL

VÉRIFICATION DU MONTANT < 1000€

VÉRIFICATION ÉTAT DES ENCAISSEMENTS ANTÉRIEURS

- *Montant*
- *Périodicité*

ESTIMATION DE L'ABSENCE DE DOUTE SUR L'ORIGINE DES FONDS

2. ENREGISTREMENT INFORMATIQUE ENCAISSEMENT

SI OK

Enregistrement automatique sur logiciel agréé Chambre Nationale des Commissaires de Justice (CNCJ).

SI DOUTES SUR ORIGINE DES FONDS OU MONTANT PROPOSÉ À L'ENCAISSEMENT SUPÉRIEUR OU ÉGAL À 1000€ :

Information référent RGPD / TRACFIN : Me Julien VANVEUREN

Déclaration de soupçons si doutes à TRACFIN via plateforme ERMES

Opération à partir de 1000€ COSI

3. DÉLIVRANCE D'UN REÇU INFORMATIQUE

4. MISE SOUS PLI DES FONDS DANS UNE URNE SÉCURISÉE

5. RELEVÉ JOURNALIER DE L'URNE

6. ÉDITION BORDEREAU DE REMISE INFORMATIQUE

7. DÉPOT BANQUE

LIVRE BLANC
CODE DE BONNE CONDUITE

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES.

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016.

Relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (publiée au Journal Officiel de la République Française du 21 Juin 2018).

- *RGPD : règlement général sur la protection des données.*
- *DPO : délégué à la protection des données (data protection officer).*

INTRODUCTION

Livre Blanc

Responsable de traitement : Maître Julien VANVEUREN, Huissier de Justice associé, 36 rue de l'Hôpital Militaire à LILLE (Nord).

Délégué à la protection des données (DPO) : le délégué à la protection des données mutualisées de la profession des huissiers de justice (Chambre Nationale des Huissiers de Justice), 44 rue de Douai à PARIS.

Le responsable de traitement sous le contrôle et les recommandations du délégué à la protection des données est en charge de :

- La mise en place du règlement général à la protection des données au sein de l'entreprise ;
- La tenue à jour des méthodes par le suivi des dispositions légales et leur évolution ;
- Il a le rôle de conseil interne/externe - sensibilisation ;
- Il procède aux contrôles du respect des règles de fonctionnement, inventaire des traitements ;
- Il est responsable de la conception et des améliorations ;
- Il est le point de contact CNIL et de coopération avec les autorités de contrôle.

Il est en charge de la tenue des registres de traitement.

Le présent livre blanc est un compte rendu descriptif des moyens développés pour la mise en œuvre du Règlement Général sur la Protection des Données au sein de l'entreprise, tant au niveau de la mise en conformité, du contrôle et du suivi.

Le respect de la protection des données se décompose en plusieurs parties :

- Interne : méthodologie au sein de l'entreprise imposée aux associés et salariés ;
- Externe : traitement des données dans le cadre des relations avec les donneurs d'ordre et les clients ;
- Partenaires privilégiés : informatique, téléphonie, traducteurs, serruriers, dépanneurs, témoins, et de façon générale toute entreprise intervenant dans les locaux ;
- Procédure d'alerte ;
- Mesures de contrôle.

INTERNE

- Le personnel : Formation, information, engagement de confidentialité, collecte et traitement des données ;
- Ordinateur : contenu des fichiers ;
- Boîte mail : contenu des fichiers ;
- Téléphones professionnels : antivirus, verrouillage et non conservation de données sensibles et personnelles ;
- Ordinateurs portables : antivirus, verrouillage et non conservation de données sensibles et personnelles ;
- Tablettes : antivirus, verrouillage et non conservation de données sensibles et personnelles ;
- Mots de passe de confidentialité sur l'ensemble des postes informatiques fixes : pertinents et périodiquement changés ;
- Antivirus et contrôle périodique des mises à jour ;
- Effacement des données (y inclus les mails) :
  mode de conservation
  délai de conservation
  effacement ;
- Fichier du personnel (ressources humaines) - clause de confidentialité - effacement ;
- Tenue d'un registre des traitements relatant les mesures et contrôles ;
- Conservation des minutes et pièces de procédure en format papier et dématérialisé (coffre-fort sécurisé) ;
- Règles de sécurité sur les sauvegardes en support physique et virtuel ;
- Protection des locaux.

PROCÉDURE D'ALERTE

Organisation d'une procédure de traitement sur les cas détectés de violation supposée ou avérée :

- Procédure d'urgence ;
- Procédure de traitement ;
- Notification à la CNIL ;
- Notification aux donneurs d'ordre.

MESURES DE CONTRÔLE

- Organisation d'une procédure de contrôle (rythme, moyens, méthodologie...) ;
- Registre des traitements ;
- Compte rendu de contrôle à diffusion externe (donneurs d'ordre) pour les informer de la bonne réalisation des mesures ;
- Possibilité d'audit sur site.

EXTERNE

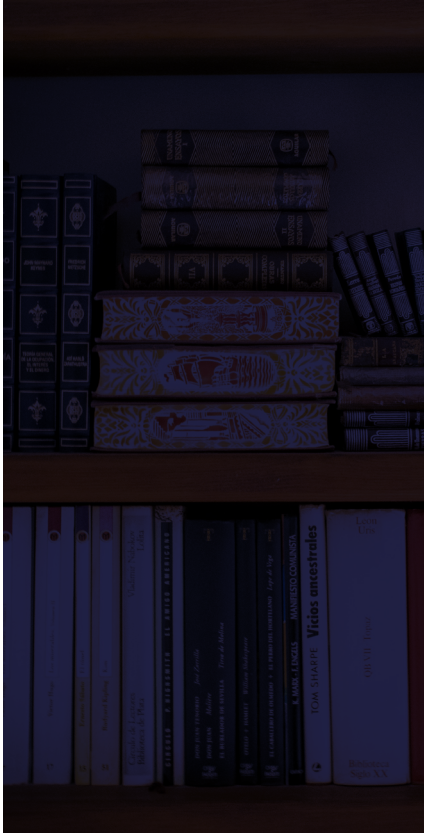
- Dématérialisation et transmission des données : cryptage / codage / mot de passe (en entrée et sortie) ;
- Engagement de confidentialité des sous-traitants (confrères, avocats, etc.) ;
- Nos engagements vis-à-vis des pièces (ged, coffre-fort sécurisé) ;
- Procédures dématérialisées (ADEC & banques & préfectures).

PRESTATAIRES PRIVILÉGIÉS OU ÉPISODIQUES

- Partenaire informatique : APTITUDE LOGICIELS ;
- Partenaire téléphonie : ABSYSTECH ;
- Clauses réciproques de confidentialité ;
- Clause de non conservation des données ;
- Clause de non diffusion des données ;

- Partenaire de sauvegarde informatique : OODRIVE ;
- Partenaires divers : Traducteurs, serruriers, dépanneurs, témoins, entreprises de nettoyage, entreprise de destruction papier.

INTRODUCTION



Sauf indication contraire, les articles visés se rapportent au règlement (UE) 2016/679 du 27 avril 2016.

Le présent Livre Blanc se rapporte au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier (selon art. 2).

Il se rapporte à leur réception, leur conservation, leur transmission, leur destruction. ◆

DÉFINITIONS SELON LES DISPOSITIONS DE L'ARTICLE 4 (EXTRAIT) :

1. "Données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable; 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.
2. "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;
3. "Limitation du traitement", le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur;
4. "Profilage", toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;
5. "Fichier", tout ensemble structuré de données à caractère à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;
6. "Responsable du 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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;
7. "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;
8. "Destinataire", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. [...];
9. "Tiers", une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;
10. "Consentement" de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée, et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fasse l'objet d'un traitement;
11. "Violation de données à caractère personnel", une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. ◆

INTERNE

1-1. GESTION INTERNE

Il est précisé en préambule que :
Toute référence aux données s'entend à la fois pour les documents papier et les documents dématérialisés.
Par données à caractère personnel ou données nominatives, il faut entendre tout élément d'identification : nom, prénoms, dates et lieux de naissance, adresses, téléphones, mails, immatriculations, employeurs, etc.

Une formation est assurée à l'ensemble des personnes travaillant au sein de l'entreprise, cette date figurant dans le registre des traitements. Des fiches reprenant les règles impératives au respect du Règlement sur la Protection des Données sont diffusées, et actualisées afin d'entretenir la formation.

Lors de la formation initiale, un exemplaire papier du livre blanc et des fiches de mise en œuvre du RGPD sont remis à chacun des salariés comme récépissé, afin de s'assurer d'une parfaite connaissance des règles applicables et de leur respect.

Cette formation sera renouvelée au rythme mentionné au même registre, et actée dans celui-ci.

Elle est immédiatement assurée à chaque nouvel arrivant.

Celle formation porte sur les obligations et le respect des règles, avec un focus sur :
La finalité et la conservation des données : les données nominatives collectées doivent être nécessaires à la finalité de leur traitement et conservées dans la durée limitée à leur utilité, sauf délai de conservation eu égard aux règles de l'archivage, et dans le respect dur droit à l'effacement "droit à l'oubli".
L'archivage est de la responsabilité des huissiers qui s'assurent de la bonne conservation et de la destruction.

La sécurité des données : interdiction de transmission de données, sauf utilisation d'un cryptage out mot de passe dont la transmission est assurée de façon distincte du document, et dans la limite de leur pertinence.

Les règles de conservation et de destruction se rapportent aux documents papier, aux documents enregistrés sur ordinateur, aux mails. Les renseignements nominatifs une fois intégrés ne doivent pas être conservés dans les mails qui feront l'objet d'une destruction immédiate.

La destruction s'entend aussi des "corbeilles" de stockage des éléments détruits (ordinateurs, mails).

Les mails et fichiers peuvent se retrouver sur les matériels portables : ordinateurs portables, téléphones, tablettes. Le traitement de conservation et de destruction est appliqué de la même façon.

Rappel est fait aux équipes de l'utilisation de termes appropriés dans la tenue des notes, dans le respect de la personne. Il est rappelé à ce titre que ces notes doivent être pertinentes avec le dossier, et sont soumises aux mêmes règles de conservation et de destruction.
L'ensemble du matériel est protégé par un antivirus.
Chacun est responsable de sa mise à jour et des contrôles périodiques. Des vérifications sont effectuées.

Rappel est fait sur l'utilisation obligatoire des mots de passe, dont la pertinence et le rythme est établi selon le registre des traitements.

Les postes de travail sont paramétrés avec écran de veille et de fermeture automatique selon un tempo établi. Des postes sont plus spécialement contrôlés à ce titre dès lors qu'ils peuvent être accessibles au regard des personnes extérieure : accueil, espaces de réception. Les postes installés dans les bureaux non accessibles au public sont soumis à la même règle eu égard au personnel d'entretien ou réalisant des travaux. Pour rappel, les documents papier doivent être également tenus à l'abri des regards extérieurs.

Les données nominatives et les éléments personnels ne sont pas communiqués hors des règles légales.

Une partie des personnes liées à l'entreprise utilise des véhicules de fonction. Leur vigilance porte sur la non visibilité de l'extérieur de documents nominatifs et l'absence de conservation d'éléments inutiles à leur mission quotidienne.

1-2. SOCIAL - RESSOURCES HUMAINES

Pour les personnes présentes antérieurement à l'application du RGPD, il est réalisé un avenant au contrat de travail reprenant l'obligation de confidentialité et le respect des règles de traitement, faisant référence à ce règlement.

Les nouveaux arrivants seront tenus à cette même clause, figurant à leur contrat de travail.

Outre ces clauses, le personnel est déjà tenu par les règles inhérentes au secret professionnel.

Les données à caractère personnel des employés sont conservées dans la pertinence de leur utilité, et dans la limite des délais suffisants à compter de leur date de départ de l'entreprise (actuellement cinq ans eu égard aux règles du droit social). ◆

1-3. CONSERVATION DES MINUTES ET DES PIÈCES DE PROCÉDURE

La conservation des minutes (originaux des actes de procédure) et des pièces de procédure répondent à un délai légal de conservation des archives.

Leur destruction est assurée sous le contrôle et la responsabilité des huissiers de justice.

Ils en assurent la destruction par les moyens appropriés au respect de la confidentialité conformément aux règles de conservation légale.

La destruction concerne à la fois les documents dématérialisés sur les documents papier. ◆

1-4. SAUVEGARDES

Plusieurs types de sauvegarde sont en application afin d'assurer une parfaite sécurité dans la continuité des activités. Les sauvegardes sont réalisées quotidiennement.

Sauvegarde dématérialisée : société OODRIVE
Sauvegarde dématérialisée : société APTITUDE LOGICIELS
Sauvegarde physique des fichiers sur disque dur externe

Les sauvegardes dématérialisées sont soumises aux règles de sécurité et de confidentialité reprises dans le chapitre des intervenants extérieurs.

Les sauvegardes physiques ne sortent pas des locaux. Elles sont préservées dans un coffre ignifugé. ◆

1 - 5. PROTECTION DES LOCAUX

Les locaux sont sous alarme volumétrique, vérifiée et contrôlée selon cahier des charges.

Le déclenchement de l'alarme provoque une écoute par les services de la société de surveillance qui prévient les personnes déterminées dans le cahier des charges, avec un appel immédiat des services de secours et de police selon le type de détection. ◆

EXTERNE

Par externe, il faut entendre tous les intervants extérieurs selon les catégories suivantes : Donneurs d'ordre, clients, intervenants / sous-traitants, entreprises de service.

2-1. DONNEURS D'ORDRE

Les mesures d'échange avec les donneurs d'ordre respectent les règles de déontologie.

Les données relatives aux donneurs d'ordre leur donne un droit d'accès et de rectification.

La transmission des données personnelles et nominatives, qu'elles soient relatives au donneur d'ordre ou au client, ne porte que sur les éléments répondant à la finalité de la mission et aux procédures applicables.

Ces données, en cas de dématérialisation et de transmission électronique, sont communiquées sur des boîtes mail protégées.

Elles ne sont conservées que le temps de la création du dossier, puis détruites immédiatement (corbeille incluse), sauf cas particulier pouvant prévoir un mode de restitution.

Ces données électroniques n'ont pas vocation à sortir de l'Étude durant leur temps de traitement.

Selon la nature du document, l'Étude peut procéder à la mise à disposition de celui-ci sur son coffre-fort "Dropact" accessible au moyen d'un identifiant et d'un mot de passe transmis de façon séparée, et non accessible aux robots.

L'Étude ne transmet pas d'éléments en retour dont elle a pu avoir connaissance durant le temps de traitement du dossier, en dehors de ceux nécessaires aux règles légales de procédure. ◆

2-2. CLIENTS

Les données relatives aux clients sont soumises au droit d'accès et de rectification.

Ne sont conservées que les données utiles et pertinentes pour la mission.

Toute donnée qui n'est pas en rapport avec la mission confiée ne peut figurer dans le dossier physique et/ou informatique.

Seules les données à caractère objectif doivent être traitées, les données subjectives étant immédiatement exclues.

Un défendeur incarcéré pour quelque cause que ce soit peut être repris en domiciliation dans un centre de détention ou maison d'arrêt, s'agissant d'une réalité dans le cadre de la signification des actes et des procédures d'exécution. La durée peut être une notion pertinente dans le cadre des mesures à engager. La cause de son incarcération ne peut figurer dans les informations car sans rapport avec la mission.

Toute considération idéologique, religieuse ou orientation politique est sans pertinence.

La finalité de la mission est le critère exclusif à retenir pour décider de l'enregistrement ou du rejet de l'information.

à l'issue de la mission, les données sont détruites sauf délai de conservation imposé par les règles régissant l'archivage. ◆

2-3. SOUS-TRAITANTS

Sont sous-traitants : les confrères, avocats, notaires et autres professionnels dont l'intervention est rendue nécessaire dans l'accomplissement de la mission.

Les pièces et données sont couvertes par le secret professionnel inhérent à ces professions.

Le mode de transmission des échanges est protégé en cas de transfert dématérialisé, par l'application des règles de confidentialité.

En cas de transfert dématérialisé l'utilisation du coffre-fort électronique "DROPACT" est privilégié, sauf autre mode de transmission sécurisé en cours dans les échanges avec le sous-traitant.

Il est demandé aux sous-traitants, une réciprocité d'échange dans les règles de la sécurisation, et la garantie de la mise en œuvre du RGPD dans leur structure.

Des sous-traitants d'un type particulier sont à considérer dans les échanges dématérialisés : l'ADEC (Applications Dématérialisées Et Cloud), les banques, les préfectures.

Dans la signification des actes dématérialisés et l'interrogation des fichiers des administrations selon les règles de procédure, l'ADEC est l'intermédiaire en sa qualité d'émanation de la Chambre Nationale des Huissiers de Justice. Le site n'est accessible que par code et signature électronique par clef, rendant les transmissions sécurisées et cryptées.

2-4. PRESTATAIRES PRIVILÉGIÉS OU ÉPISODIQUES

Ces prestataires sont des partenaires de l'Étude à titre privilégié ou épisodique.

Les prestataires privilégiés sont les sociétés suivantes :

APTITUDE LOGICIELS :
Société à responsabilité limitée immatriculée au registre du commerce et des sociétés de Nantes sous n° 417 645 009, dont le siège social est à NANTES 44000, 38 boulevard Gabriel Guist'Hau.

ABSYSTECH :
Société à responsabilité limitée immatriculée au registre du commerde et des sociétés de Lille Métropole sous le n° 444 804 066, dont le siège social est à ROUBAIX 59100, 139 rue des Arts.

OODRIVE :
Société par actions simplifiée, au capital de 309 126 euros, immatriculée au registre du commerce et des sociétés de Paris, sous le n° 432 735 082, dont le siège social est à PARIS 75010, 26 rue du Faubourg Poissonnière.

Ces partenaires développent pour l'Étude :
APTITUDE LOGICIELS : le logiciel informatique (agréé par la Chambre Nationale des Huissiers de Justice) ;
ABSYSTECH : le logiciel téléphonique ;
OODRIVE : la conservation des données sauvegardées.

Des règles de confidentialité existent avec ces sociétés. Toutefois et en application des dispositions du RGPD, un engagement a été contractualisé avec celles-ci dans la mesure où elles traitent des données sensibles. Cet engagement est relatif à la confidentialité des données, à leur non-conservation, à leur non-diffusion.

Les prestataires épisodiques sont les intervenants requis lors d'opérations bien spécifiques en matière de constats et mesures d'exécution :

- Serruriers
- Témoins
- Dépanneurs
- Déménageurs
- Traducteurs
- Etc.

Les éléments dont ils peuvent avoir connaissance lors des opérations revêtent un caractère de confidentialité et leur donnent parfois accès à des données personnelles. Un engagement est requis de leur part afin qu'ils n'enfreignent pas les règles de cette confidentialité.

D'autres intervenants peuvent avoir accès aux locaux, ce qui les amèneraient à voir ou entendre des informations personnelle : les services d'entretien, de nettoyage, de réparation, de destruction des documents papier, etc. L'attention est attirée auprès de la direction de ces entreprises sur le caractère confidentiel, et un engagement de leur part est requis.

PROCÉDURE **D'ALERTE**

Un registre de notification des violations des données est tenu par le DPO.

Prévenir - Alerter - Secourir.

Une procédure d'urgence est mise en place, se déroulant en trois temps.

3-1. PRÉVENIR

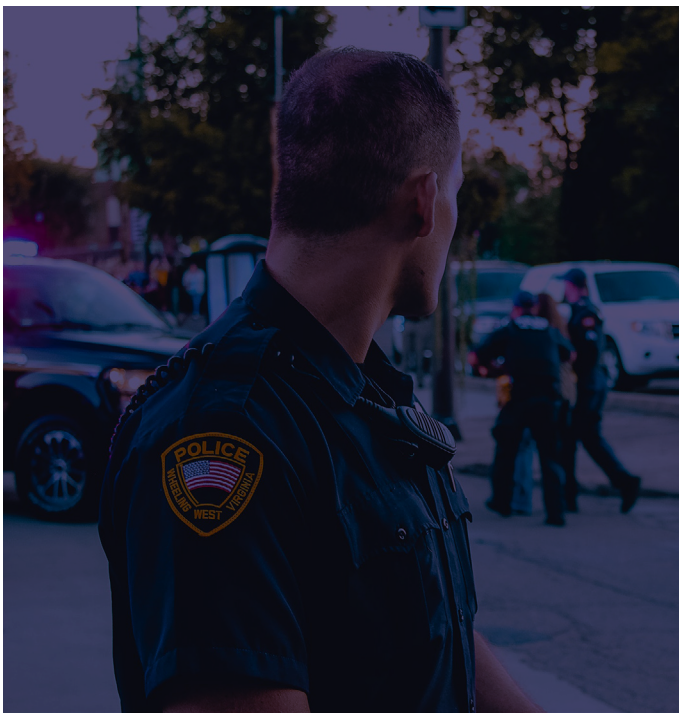
C'est empêcher le mal de s'étendre. Il consiste par exemple à interrompre l'extension du sinistre par la déconnexion d'un poste infecté avant contamination de l'ensemble du réseau, en cas de piratage. C'est la première réaction : éviter une propagation.

3-2. ALERTER

C'est une procédure d'alerte des partenaires avec notification à la CNIL, afin que chacun puisse prendre les mesures propres à son mode de fonctionnement et à ses règles de sécurité.

3-3. SECOURIR

C'est solutionner le problème par le traitement adéquat, en concours avec nos partenaires informatiques.



MESURES DE **CONTRÔLE**

Les mesures de contrôle sont de la responsabilité du délégué à la protection des données (DPO).

Il en est l'organisateur et en assume la responsabilité.

Pour rappel, deux types de données sont concernées :
- Les données papier
- Les données dématérialisées.

Les données papier sont représentées par les dossiers physiques contenant les pièces de procédure et la conservation des minutes (originaux des actes de procédure).

La protection de ces données est assurée par :
Un stockage sécurisé dans les locaux de l'étude ;
Une destruction en fonction des délais de conservation légale des archives.

La destruction des archives papier est réalisée une fois par an, conformément aux règles de la prescription. Elle est effectuée sous contrôle par une entreprise spécialisée dans la destruction de données sensibles et après engagement de confidentialité.

Chaque destruction est actée dans le registre des traitements.

La destruction des données informatiques est également réalisée une fois par an, sous le contrôle d'un Huissier de Justice, au rythme des délais de prescription.

Chaque destruction est actée dans le registre des traitements. ◆

REGISTRE DES TRAITEMENTS

Deux registres son tenus par le délégué à la protection des données (DPO).

- *Le registre des traitements ;*
- *Le registre des notifications de violations des données à caractère personnel.*

Le premier recense tous les évènements de formation, de contrôle, de mise à niveau. Il relate toutes les actions entreprises au titre des méthodes de réception des données, de leur conservation, de leur destruction.

Le second recense toutes les violations détectées, et qui donnent lieu à une notification à la CNIL.

Outre les incidents, il précise la nature des traitements entrepris :
- Prévention
- Alerte
- Sécurisation. ◆

COMPTE RENDU DE CONTRÔLE À DIFFUSION EXTERNE (DONNEURS D'ORDRE)

Dans un souci de transparence, le DPO tient informés les donneurs d'ordre de :
- La mise en place des méthodes (le présent livre blanc) ;
- L'actualisation de celles-ci ;
- Au mois une fois par an, il adresse un bilan des formations et contrôles ;
- Un audit sur site peut être réalisé à leur convenance. ◆

CHARTE DES BONNES PRATIQUES EN **TÉLÉTRAVAIL**

Le télétravail conduit à transposer les règles applicables en matière de sécurité informatique et de protection des données personnelles en vigueur dans l'entreprise à son domicile.

1. LES RÈGLES IMPÉRATIVES DU TÉLÉTRAVAIL

- Appliquer rigoureusement les règles en vigueur dans l'entreprise ;
- Ne pas faire en télétravail ce qui ne se fait pas au bureau ;
- Avoir une utilisation responsable et vigilante des équipements et accès professionnels, notamment concernant la navigation web, en veillant à bien séparer les usages professionnels des usages personnels ;
- Respecter impérativement les horaires de travail, en se connectant uniquement lors de ceux-ci et mettant un terme à la connexion à la fin de la journée de travail ;
- Être vigilant dans la gestion des contacts pour éviter toute tentative de piratage ou d'hameçonnage ;
- Informer immédiatement l'employeur en cas de violation des données à caractère personnel.

2. SÉCURISATION DE LA CONNEXION INTERNET

- Assurer le bon paramétrage de la box Internet. Vérifier le mot de passe d'accès administrateur et le changer s'il est faible ;
- En cas d'utilisation du Wi-Fi, activer l'option WPA2 ou WPA3 avec un mot de passe long et complexe. Désactiver le Wi-Fi invité.

3. UTILISATION DES ÉQUIPEMENTS FOURNIS ET CONTRÔLÉS PAR L'ENTREPRISE

- Utiliser autant que possible le VPN mis à disposition par l'entreprise ;
- Privilégier les échanges de données à travers les stockages disponibles depuis le VPN plutôt que par la messagerie électronique ;
- Se connecter au moins une fois par jour au VPN pour appliquer les mises à jour ;
- Désactiver le VPN lors de l'utilisation de services consommateurs de bande passante, comme le streaming vidéo, qui ne nécessitent pas de passer par le réseau de l'entreprise.

4. SÉCURISATION DE L'ORDINATEUR UTILISÉ

- L'ordinateur utilisé doit être équipé d'un anti-virus et d'un pare-feu ;
- Utiliser un compte personnel avec des droits limités protégé par un mot de passe fort et non partagé avec d'autres personnes (par exemple avec d'autres membres de la famille et sur lequel les applications se limitent au strict nécessaire pour l'activité professionnelle des mises à jour régulières du système d'exploitation et des logiciels utilisés doivent être effectuées ;
- Réaliser des sauvegardes journalières du travail sur l'infrastructure de l'entreprise, si possible en activant une solution de sauvegarde automatique.

Pictures made by freepik,
itim2101, ultimatearm from
www.flaticon.com

LILLE
03 20 12 84 30
etude@huissier-waterlot-lille.com
www.huissier-waterlot-lille.com
36 rue de l'Hôpital Militaire
59044 LILLE CEDEX

PARIS
01 42 33 12 35
etude@huissier-waterlot-paris.com
www.huissier-waterlot-paris.com
6 rue d'Astorg
75008 PARIS

@wahuissiers

SAINT-OMER
03 59 61 60 67
etude@ huissier-waterlot-saintomer.com
www.huissier-waterlot-saintomer.com
4 rue des Epéers
62500 SAINT-OMER

VALENCIENNES
03 59 61 42 90
etude@huissier-waterlot-valenciennes.com
www.huissier-waterlot-valenciennes.com
47 rue de Paris
59300 VALENCIENNES