Cybersécurité et conformité RGPD

EDITION JANVIER 2021

PRORISK **CYBER** est la marque de **GROUPE** PRORISK dédiée à ses activités de conformité avec le Règlement Général pour la Protection des données

SAS GROUPE PRORISK
Capital social : 400 000€ - SIREN 799 322 169
RCS BREST
7, rue du commandant Malbert
29200 Brest – France

PRESENTATION

GROUPE PRORISK est spécialisé depuis 14 ans dans la maitrise des risques et accompagne les entreprises soumises à des obligations réglementaires de prévention contre les actes malveillants.

Depuis 2015, pour s'adapter à la forte recrudescence des cyberattaques, GROUPE PRORISK a renforcé ses compétences en matière de sécurité des systèmes d'informations.

Parallèlement, le règlement européen 2016/679 sur la protection des données personnelles (RGPD) a été promulgué en avril 2016 pour être appliqué au 25 mai 2018. La conformité avec ce règlement repose sur le principe que l'on peut manipuler les données d'une personne si l'on maîtrise le risque pour sa vie privée.

Le RGPD impose donc la prise de mesures organisationnelles et techniques pour garantir la sécurité des données, donc des systèmes d'information qui les contienne.

L'obligation de conformité avec le RGPD et le besoin de résilience des sociétés face aux agressions cybercriminelles convergent vers les mêmes solutions. Elles nécessitent un triptyque de compétences :

- Analyse des risques ;
- Sécurité des systèmes d'information ;
- Conformité juridique.

GROUPE PRORISK déploie ces compétences au profit de ses clients.

L'offre PRORISK CYBER, détaillée dans ce catalogue de services, s'adresse particulièrement aux TPE et aux PME.

Dans une approche globale des besoins, elle s'articule autour des trois métiers de GROUPE PRORISK :

- L'ingénierie-conseil ;
- La formation ;
- L'assistance opérationnelle.

Elle comprend des interventions ponctuelles (audit, élaboration et suivi de plans d'actions) mais également un accompagnement de longue durée à travers l'exercice, au profit de nos clients, des fonctions de :

- Délégué à la Protection des Données externe (Data Protection Officer ou DPO) ;
- Responsable de la Sécurité des Systèmes d'Information Externalisé.

GROUPE PRORISK est certifié QUALIOPI ce qui ouvre la voie à des financements par les Opérateurs de Compétences (OPCO) pour toutes les actions de formations voire de mentoring.

SOMMAIRE

PRINCIPES

La démarche de GROUPE PRORISK s'articule autour des principes suivants :

- **Complétude** du traitement des difficultés et de la rédaction des livrables pour limiter le travail des correspondants « clients » à des arbitrages ou des relectures ;
- **Disponibilité** par un tuilage permanent des membres de l'équipe de projet permettant une réponse rapide aux événements ;
- **Prévention** des cyberattaques par la formation des collaborateurs ainsi que la veille technique et réglementaire ;
- **Indépendance** par le respect des règles déontologiques liées à l'activité de Délégué à la Protection des Données

Les prestations sont adaptées à la taille des entreprises. En particulier, GROUPE PRORISK propose des formules condensées en conformité RGPD et en cybersécurité spécialement adaptées aux TPE (moins de 20 collaborateurs). Elles sont accessibles sous certaines conditions.

GROUPE PRORISK octroie à chaque client un **accès permanent sécurisé** à ses documents réglementaires sur un serveur de Gestion Electronique de Documents (GED) hébergé en France. Les livrables sont disponibles sous des formats bureautiques standard : PDF, Excel, Word, ...

GROUPE PRORISK bâtit sa prestation sur le rapport humain et rencontre ses interlocuteurs aux moments clés des projets. Hors des déplacements sur site, GROUPE PRORISK réalise du travail collaboratif par l'application de visioconférence.

GROUPE PRORISK s'engage sur les délais suivants pour apporter son conseil ou réagir à des situations imprévues :

- 1 jour ouvré pour réagir à une suspicion de violation de données, de cyberattaque, d'escroquerie numérique ou d'attaque sur les réseaux sociaux ;
- 2 jours ouvrés à compter de la réception du mail de demande pour toutes questions d'ordre général ;
- 5 jours (ouvrés) maximum à compter de la réception du mail de demande pour :
    - Un avis technique ou organisationnel en matière de cybersécurité
    - La mise en œuvre de nouveaux traitements ;
    - Les demandes d'expression de droits.

NOS CLIENTS

Collectivités territoriales

Communauté de Communes Parthenay-Gâtine

Isigny Omaha INTERCOM

Parapublic

brestaim
Gestion d'équipements publics

Comité d'entreprise

COMITÉ D'ENTREPRISE EURO DISNEY

Groupement d'Intérêt Public

Santé Social Services en logistique
DU GOLFE DU MORBIHAN

Santé et médico-social

FONDATION ilovs SANTÉ SOLIDARITÉ BRETAGNE

HOPPEN
TIME TO CARE

Groupe Scolaire Privé

La Croix Rouge
La Salle - Brest

Acteur social

clarpa56

Santé et médico-social

theotokos
pour fonder un foyer chrétien

Groupes privés

DistriCenter
DÉCLENCHEUR DE BONNE HUMEUR

DAMEN
DAMEN SHIPREPAIR BREST S.A.S.

GROUPE COFIBEL

TANGUY
MATERIAUX DISTRIBUTION

GLOSSAIRE

GROUPE PRORISK utilise les sigles suivants dans la suite du document :

Terme	Définition
DPD	Délégué à la Protection des Données, mission instaurée par le RGPD
RGPD	Règlement Général sur la Protection des Données
SI	Système d'Information
SSI	Sécurité du Système d'Information
DCP	Données à Caractère Personnel, objet du RGPD
PIA	Privacy Impact Assessment, analyse d'impact sur la vie privée requise pour les traitements à risques
PSSI	Politique de Sécurité des Systèmes d'Informations

PRESTATIONS RGPD

PACK DE MISE EN CONFORMITE TPE

1. OBJECTIF

Le **projet de conseil** consiste à réaliser la mise en conformité avec le Règlement Général pour la Protection des Données pour vérifier le respect des principes fondamentaux du RGPD :

- Poursuivre des objectifs déclarés et légitimes ;
- Manipuler les données de manière légale et transparente ;
- N'utiliser des données que si l'on peut en justifier le besoin ;
- Ne les conserver que pour la durée nécessaire ;
- S'assurer que les données restent exactes ;
- En garantir la sécurité vis-à-vis des dangers naturels et des actes de malveillance ;
- Prouver par des documents réglementaires que l'on respecte ces principes et que l'on maîtrise les risques sur les données.

La prestation comprend une enquête documentaire, l'élaboration de projets de documents de suivi, une intervention personnalisée sur place ou par visioconférence, la réalisation des analyses de risques obligatoires, la finalisation des livrables, et la formation de deux collaborateurs, selon l'échéancier ci-dessous.

2. CRITERES DE SIMPLICITE

L'application de ce pack n'est possible que si le volume d'opérations sur les données personnelles et nombre d'analyse de risques à réaliser peuvent être traités dans les durées imparties pour le projet.

Ainsi, les critères de simplicités de cette prestation sont :

- Pas plus de 20 opérations de traitement présentes dans le catalogue ;
- Pas plus de 2 opérations nécessitant la rédaction d'une analyse de risque particulière (Privacy Impact Assesment ou PIA).

GROUPE PRORISK propose de réaliser cette mise en conformité RGPD du client sur une période de 2 mois.

L'intervention personnalisé sur place n'est pas possible au-delà de 150 kms d'une agence GROUPE PRORISK.

3. INTERVENANT

Un CHEF DE PROJET

4. DEROULEMENT

GROUPE PRORISK | **TPE CLIENTE**

A la signature du contrat — **Accord sur date d'intervention**

1. APPROPRIATION DU CONTEXTE

Envoi d'un questionnaire de recensement des activités soumises aux RGPD

1 MOIS avant intervention

→ Renseignement questionnaire

2 SEMAINES avant intervention

2. ELABORATION PROJETS DOCUMENTS

Rédaction des projets de :
- Registre traitement des données
- Mentions légales
- Exigences sous-traitance
- Charte informatique

← Retour

1 SEMAINE avant intervention

→ Accusé de réception

3. INTERVENTION PERSONNALISEE : 3 heures

Revue des activités manipulant des données personnelles (2 heures) pour :
- Vérifier le respect des principes du RGPD
- Finaliser le registre
- Diffuser les mentions légales
- Identifier les actions vers les sous-traitants.

Renforcement des mesures de cybersécurité (1 heure) par l'examen du contenu de la charte informatique

Ouverture formation en ligne (3H) pour 2 collaborateurs

Suivi formation selon rythme collaborateurs

4. CONSOLIDATION

Correction des documents suite intervention
Rédaction analyses réglementaires de risques sur la vie privée
Elaboration des procédures expressions des droits et incident de sécurité

3 SEMAINES Après intervention

→ Accusé de réception

Clôture formation en ligne

1 MOIS après intervention

FIN DU PROJET – RECEPISSE DES LIVRABLES

5. LIVRABLES

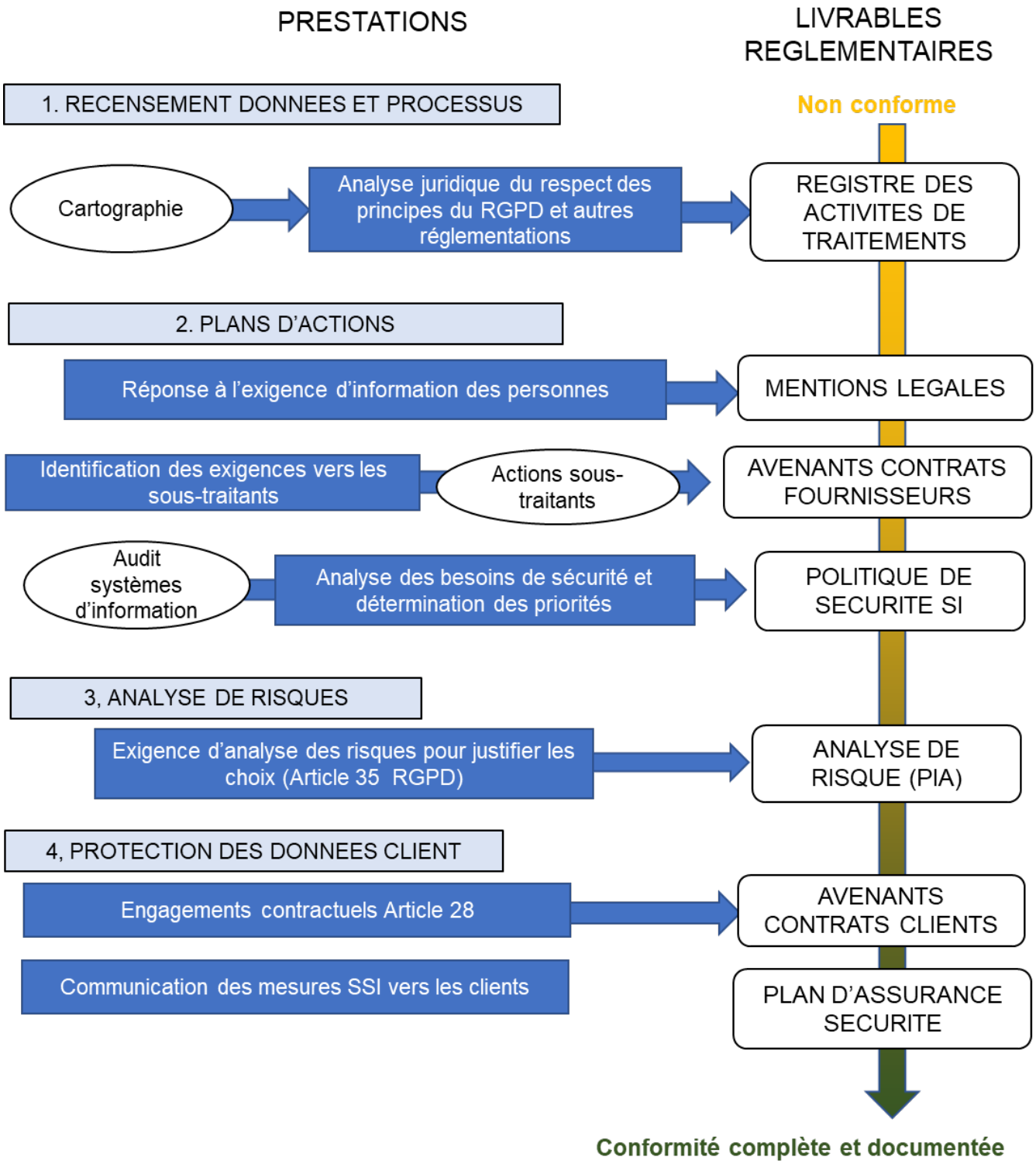
- Registre de traitement des données sous format PDF
- Mentions légales sous format Word
- Modèle d'avenant au contrat sous format Word
- Charte Informatique sous format Word
- Analyses de risque (PIA) sous format PDF
- Recueil de procédures particulières sous format Word
- Journal d'Exercice des droits sous format Word
- Compte-Rendu à renseigner en cas de violation de donnée sous format Word
- Attestation de formations sous format PDF

PRESTATIONS RGPD

PACK DE MISE EN CONFORMITE PME

1. OBJECTIF

Le **projet de conseil** consiste à réaliser la mise en conformité avec le Règlement Général pour la Protection des Données selon l'enchaînement de prestations décrites ci-dessous ;



2. DUREE

Le projet s'étale sur une période de 4 à 6 mois selon la taille et la disponibilité des interlocuteurs de l'organisme client.

3. INTERVENANTS

CHEF DE PROJET, DPD certifié BUREAU VERITAS.

EXPERT SSI

AVOCATS

4. DEROULEMENT

Le projet s'articule autour de 3 réunions clés : LANCEMENT, ARBITRAGE et CLOTURE.

Une première intervention sur site permet de réaliser la réunion de LANCEMENT immédiatement suivie de la cartographie des Données à Caractère Personnel (DCP).

La cartographie est réalisée à partir d'entretiens avec les services manipulant des DCP permettant d'auditer la conformité des pratiques.

La première intervention permet également de conduire l'audit de sécurité des systèmes d'information selon le plan de la norme ISO 27001.

L'analyse à froid de ces deux audits donne lieu à la rédaction d'un plan des actions correctrices et du registre de traitements des donnés. Les recommandations sont mises en œuvre rapidement si elles ne posent pas de difficulté particulière. Dans le cas contraire, elles sont présentées en réunion d'ARBITRAGE qui se tient sur site ou en visioconférence. A cette occasion, la direction statue sur certains points juridiques ou de sécurité que GROUPE PRORISK juge nécessaire de trancher.

Lorsque les arbitrages sont obtenus, GROUPE PRORISK conduit et déploie les actions de conformité en lien avec les services. Cette phase s'achève par une réunion de CLOTURE sur site pour rendre compte du projet et passer éventuellement sur une prestation de DPD externe.

Une réunion de CLOTURE, concomitante avec la formation des collaborateurs impliqués dans le traitement des DCP.

5. LIVRABLES

- Le registre des activités de traitement sous format PDF (ou Word).
- Un plan d'action JUR /ORG, onglet du classeur Excel de pilotage ;
- Mentions d'informations légales sous format PDF (ou Word).
- Un plan d'action SOUS-TRAITANTS, onglet du classeur Excel de pilotage ;
- Contrats relus et commentés sous format Word ;
- Notes de demande vers un sous-traitants sous format Word ;
- Un plan d'action SSI, onglet du classeur Excel de pilotage ;
- Politique de Sécurité des Systèmes d'Information PSSI sous format Word ;
- Charte d'usage de l'informatique sous format Word.
- Analyses de risques (PIA) sous format PDF
- Feuille d'émargement sous format PDF pour tracer l'action de formation ;
- CR de session sous format PDF par synthèse des questionnaires de satisfaction ;
- Des attestations individuelles pour chaque agent.

PRESTATIONS RGPD

AUDIT DE CONFORMITE

1. OBJECTIF

L'intervention consiste à évaluer la conformité avec le Règlement Général pour la Protection des Données (RGPD)

Elle comprend :

- L'évaluation de la cartographie des données ;
- L'examen des conditions juridiques de traitement des DCP ;
- L'analyse des documents de conformité (mentions, contrats, ...) ;
- L'audit de sécurité des SI.

2. DUREE

Cette **prestation de conseil** cette prestation s'étale sur une période entre 2 semaines et 1 mois selon la taille et la disponibilité des interlocuteurs de l'organisme client.

3. INTERVENANT

CHEF DE PROJET, DPD certifié BUREAU VERITAS.

EXPERT SSI

4. DEROULEMENT

Une première intervention sur site permet de contrôler la cartographie des traitements la cartographie, analyser les conditions juridiques et les documents de conformité manquants ou existants à partir d'entretiens avec les services manipulant des DCP.

La première intervention permet également de conduire l'audit de sécurité des systèmes d'information selon le plan de la norme ISO 27001.

L'analyse à froid de ces deux audits donne lieu à la rédaction d'un registre de traitement corrigé et d'un plan des actions correctrices. Les recommandations sont mises en œuvre rapidement si elles ne posent pas de difficulté particulière.

Une seconde intervention sur site est consacrée à la RESTITUTION devant la direction.

5. LIVRABLES

- Le registre des activités de traitement sous format PDF (ou Word).
- Restitution des 2 audits sous format Powerpoint et PDF ;
- Un plan d'actions sous Excel de pilotage.

PRESTATIONS RGPD

MENTORING DU DELEGUE A LA PROTECTION DES DONNEES

1. OBJECTIF

La formation intra-client consiste à accompagner le Délégué à la Protection des Données désigné et ses référents pour qu'ils garantissent la conformité avec le Règlement Général pour la Protection des Données (RGPD) ;

Les compétences visées sont :

- Comprendre et mettre en œuvre les principes généraux du RGPD ;
- Rédiger une fiche de traitement ;
- Rédiger et déployer les mentions légales ;
- Connaître les spécificités de certains traitements ;
- Communiquer avec les sous-traitants ;
- Définir les exigences de sécurité ;
- Evaluer les risques.

2. DUREE

Cette formation de 2 à 4 jours à la carte s'étale sur plusieurs semaines selon la taille et la nature des activités de l'organisme.

3. PRE-REQUIS

Être désigné comme Délégué à la Protection des Données ou référent dans son organisme.

Connaître le fonctionnement de son organisme et de son système d'information.

4. INTERVENANT

CHEF DE PROJET-FORMATEUR, DPD certifié BUREAU VERITAS.

5. CAPACITE

Parcours pour 1 à 4 personnes

6. DEROULEMENT

Le parcours de mentoring comprend :

- Un diagnostic des compétences ;
- Une période d'accompagnement pour la maîtrise des actions de mise en conformité ;
- Un atelier Analyse des Risques.

En début de prestation, le diagnostic de compétences permet d'évaluer le niveau de compréhension des principes fondamentaux par les stagiaires à partir des travaux de mise en conformité avec le RGPD réalisé ou à conduire. Les stagiaires mécanisent l'enchainement méthodologique par traitement de DCP pendant une journée et construisent leur plan d'action.

La période d'accompagnement se fait par visioconférence d'une heure par mois pour échanger sur les difficultés de mise en œuvre du plan d'action et le déploiement des mesures de sécurité.

Les organismes mettant en place des traitements particuliers de DCP

Le parcours de mentoring s'achève par un atelier d'analyse des risques sur les DCP et de rédaction de PIA conformément aux modèles fournis par la CNIL.

7. LIVRABLES

- Feuille d'émargement
- Attestation de formation
- Questionnaires de satisfaction
- Livret de cours
- Modèles de documents à élaborer

PRESTATIONS RGPD

SENSIBILISATION DES COLLABORATEURS

1. OBJECTIF

Cette formation intra-client consiste à sensibiliser les membres impliqués dans les opérations manipulant les données à caractère personnel.

La sensibilisation des membres vise l'acquisition des compétences suivantes :

- Connaitre les enjeux de sécurité des SI et, en particulier, la mise en œuvre du RGPD pour la sécurité des données personnelles ;
- Répondre aux questions des personnes sur leur droits et la sécurité numérique ;
- Connaître les méthodes employées par les acteurs malveillants et les cyber-attaquants (informatique, actions physiques, manipulation des membres) ;
- Appliquer les règles d'hygiène informatique ;
- Appliquer les procédures internes ;
- Réagir en cas d'urgence.

2. DUREE

Cette formation dure 1 demi-journée

3. PRE-REQUIS

Aucun.

4. INTERVENANT

FORMATEUR, DPD certifié BUREAU VERITAS.

5. CAPACITE

Pas de seuil minimal

Capacité maximale de 20 personnes

6. LIVRABLES

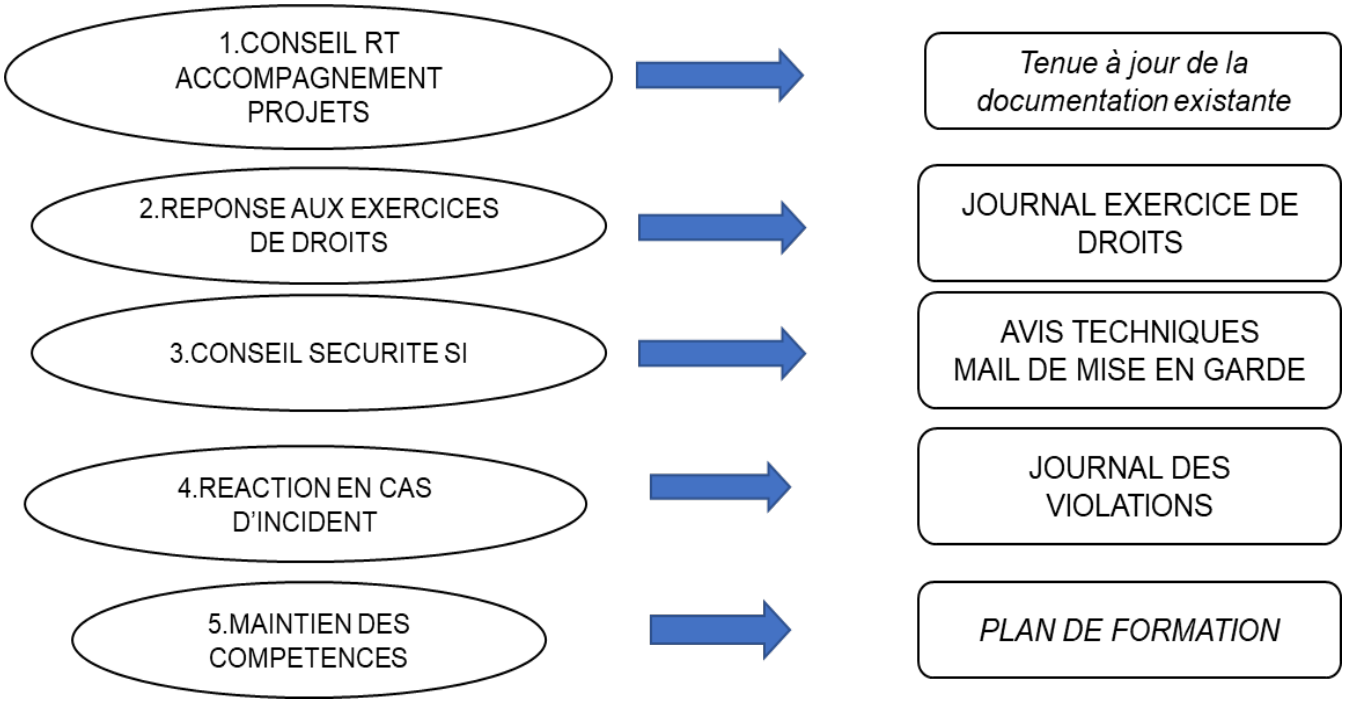
- Feuille d'émargement
- Attestation de formation
- Questionnaires de satisfaction
- Livret de cours

PRESTATIONS RGPD

DELEGUE A LA PROTECTION DES DONNEES EXTERNE (DATA PROTECTION OFFICER)

1. OBJECTIF

La mission de Délégué à la Protection des Données comprend 5 volets selon le schéma suivant :



Elle est conduite conformément aux dispositions des articles 37 à 39 du RGPD.

La désignation d'un DPD est obligatoire pour :

- Les organismes publics ;
- Les organismes manipulant de manière systématique des DCP à grande échelle (Terme à apprécier ne correspondant à aucun plancher réglementaire) ;
- Les organismes manipulant des données sensibles : santé, médico-social, social, données sur des mineurs, situation judiciaires, opinions religieuses, ...

2. DUREE

La mission d'assistance opérationnelle est permanente pendant la période de contractualisation.

3. PRE-REQUIS

Conformité effectuée ou en cours de réalisation par GROUPE PRORISK

4. INTERVENANTS

CHEF DE PROJET, DPD certifié BUREAU VERITAS.

EXPERT SSI

AVOCATS

5. DEROULEMENT

5.1. Activation

La fonction est formellement activée par une déclaration à la CNIL de GROUPE PRORISK en tant que DPD de l'organisme. Les déclarations sont envoyées par mail. Cette désignation officielle entérine le positionnement de GROUPE PRORISK comme point de contact auprès de la CNIL.

Cette activation peut intervenir dès que les traitements sont cartographiés.

5.2. Conseil aux responsables de traitement

Ce volet traite le maintien en conformité des traitements et le respect de l'exigence *Privacy By Design*.

Les méthodologies sont identiques à celles décrites au chapitre 2.

GROUPE PRORISK s'appuie sur le réseau des interlocuteurs de l'organisme. GROUPE PRORISK répond directement à l'ensemble de leurs questions et prend les mesures adéquates pour assurer la conformité de traitements nouveaux : organisation d'événement nécessitant un traitement éphémère, mise en place d'un fichier, ….

Le CHEF DE PROJET s'accorde avec le représentant de l'organisme sur la fréquence des points de situation et le plan de leur réalisation.

La fréquence minimale est mensuelle par courrier électronique (envoi d'un point de situation) et annuelle sur le site de l'organisme pour la rédaction du bilan mensuel. Cette fréquence s'accélère selon la taille de l'organisme.

Le CHEF DE PROJET peut rédiger sur demande une fiche d'activité de traitement, ou une note d'éléments de langage ou se met en contact avec le partenaire ou sous-traitant extérieur.

Les documents sont soumis à la relecture de l'AVOCAT lorsque cela est nécessaire.

Les opérations effectuées sont tracées par écrit dans le classeur Excel de pilotage et recensées lors de l'entretien mensuel.

Pour ce volet, GROUPE PRORISK assure les relations courantes avec la CNIL qui concernent :

- La demande de préconisations pour des traitements atypiques ;
- L'impossibilité d'atténuer le risque pour un traitement malgré la mise en place des mesures de protection de la vie privée et, donc, la demande de mise en œuvre ;
- L'exportation de données hors de l'UE dans un pays non adéquat.

GROUPE PRORISK rédige le bilan annuel recommandé par la CNIL.

5.3. Réponse aux exercices de droit

Pour fluidifier l'exercice des droits et, donc limiter la charge des membres, l'organisme redirige l'adresse mail qu'elle a créée pour la fonction DPD du type dpd@domaine_organisme.fr vers l'adresse fonctionnelle dpoexterne@groupe-prorisk.com (alerte DPD externe chez GROUPE PRORISK).

En cas de demande, GROUPE PRORISK l'évalue et la prend automatiquement en charge la demande en lien avec les interlocuteurs de l'organisme traitant les données de la personne concernée.

GROUPE PRORISK garantit le délai réglementaire d'un mois (article 12 du RGPD) et tient à jour le journal réglementaire d'exercice des droits par application des délais de la partie 1 – paragraphe 2.2. (5 jours pour expression des droits).

En cas de réclamation formulée contre le client par une personne auprès de la CNIL, GROUPE PRORISK diagnostique la situation, prépare les éléments de langage et propose une stratégie de réponse.

En cas de contrôle de la CNIL, le client mandate GROUPE PRORISK qui dépêche selon les délais, un conseiller auprès de lui.

GROUPE PRORISK tient à jour le **journal** réglementaire **d'exercice des droits**.

5.4. Conseil en sécurité SI

GROUPE PRORISK veille, pour l'ensemble de ses clients, le site officiel des alertes en cybersécurité https://www.cert.ssi.gouv.fr/ de l'Agence Nationale pour la Sécurité des Systèmes d'Information.

Elle diffuse des messages d'alerte triés avec des consignes à suivre.

Sur demande, elle fournit des avis techniques quant à la sécurité de choix techniques sur ses systèmes d'information.

5.5. Réaction en cas d'incident

En cas d'incident sur les DCP, nécessitant un arbitrage quant à l'obligation de notifier vers la CNIL et les personnes concernées : GROUPE PRORISK débute

automatiquement les opérations prévues dans cette situation dès lors qu'il en a connaissance sur l'adresse dpoexterne@groupe-prorisk.com.

GROUPE PRORISK coordonne les mesures urgentes pour limiter les effets d'une éventuelle cyberattaque avec le client ou les prestataires d'INFOGERANCE.

Si le premier diagnostic laisse penser à un incident grave au regard des PIA rédigés, GROUPE PRORISK dépêche un consultant sur place pour piloter un processus de gestion de crise.

GROUPE PRORISK recueille les éléments pour remplir le formulaire de notification de violation de la CNIL.

Si l'incident ne justifie pas une déclaration de violation, le formulaire de notification est conservé pour justifier la décision prise.

En cas d'incident grave, GROUPE PRORISK intervient par avenant au contrat et peut mettre à disposition une intervention d'investigation numérique assurée par une société labellisée par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) pour ce type d'opérations.

Cette investigation peut être nécessaire pour la constitution des preuves matérielles d'une agression numérique pouvant conduire à une plainte par le client.

GROUPE PRORISK tient à jour le **journal** réglementaire **de violation de données**.

5.6. Maintien des compétences

GROUPE PRORISK propose l'organisation chaque année des sensibilisations définie dans le plan de formation RGPD.

6. LIVRABLES

Classeur Excel de pilotage

Ensemble de la documentation de conformité tenue à jour

Journal d'expression des droits au format Word

Journal de violation des données au format Word

Documents liés à la réalisation des formations.

PRESTATIONS CYBERSECURITE

PROPOSITION TECHNIQUE - CYBERSÉCURITÉ TPE

1. OBJECTIF

Le **projet de conseil** consiste à accroître la résilience de l'entreprise face aux agressions numériques :

- Attaque par rançongiciel ;
- Sabotage de process techniques ;
- Modification de données dans des fichiers ;
- Vol de documents ou de savoir-faire confidentiels ;
- Arnaque au « Président » ;
- Diffamation sur les réseaux sociaux.

La prestation comprend une enquête préliminaire auprès du dirigeant pour bien cerner son activité, l'architecture utilisée et ses priorités en matière de cybersécurité.

Une intervention personnalisée permet d'évaluer les vulnérabilités de l'entreprise et d'en déduire les mesures d'atténuation des risques au regard des priorités identifiées.

Le parcours comprend la formation de deux collaborateurs

2. CRITERES DE SIMPLICITE

L'application de cette prestation n'est possible que si la TPE ne manipule pas de données ou d'information soumises à des réglementations particulières :

- Entreprises offrant des services financiers ;
- Activité centrée sur une plate-forme numérique (vente en ligne, réseau social) ;
- Fournisseur de services numériques (Infogérance, réseaux, éditeur sites web) ;
- Données de santé ou considérées sensibles au regard du RGPD.

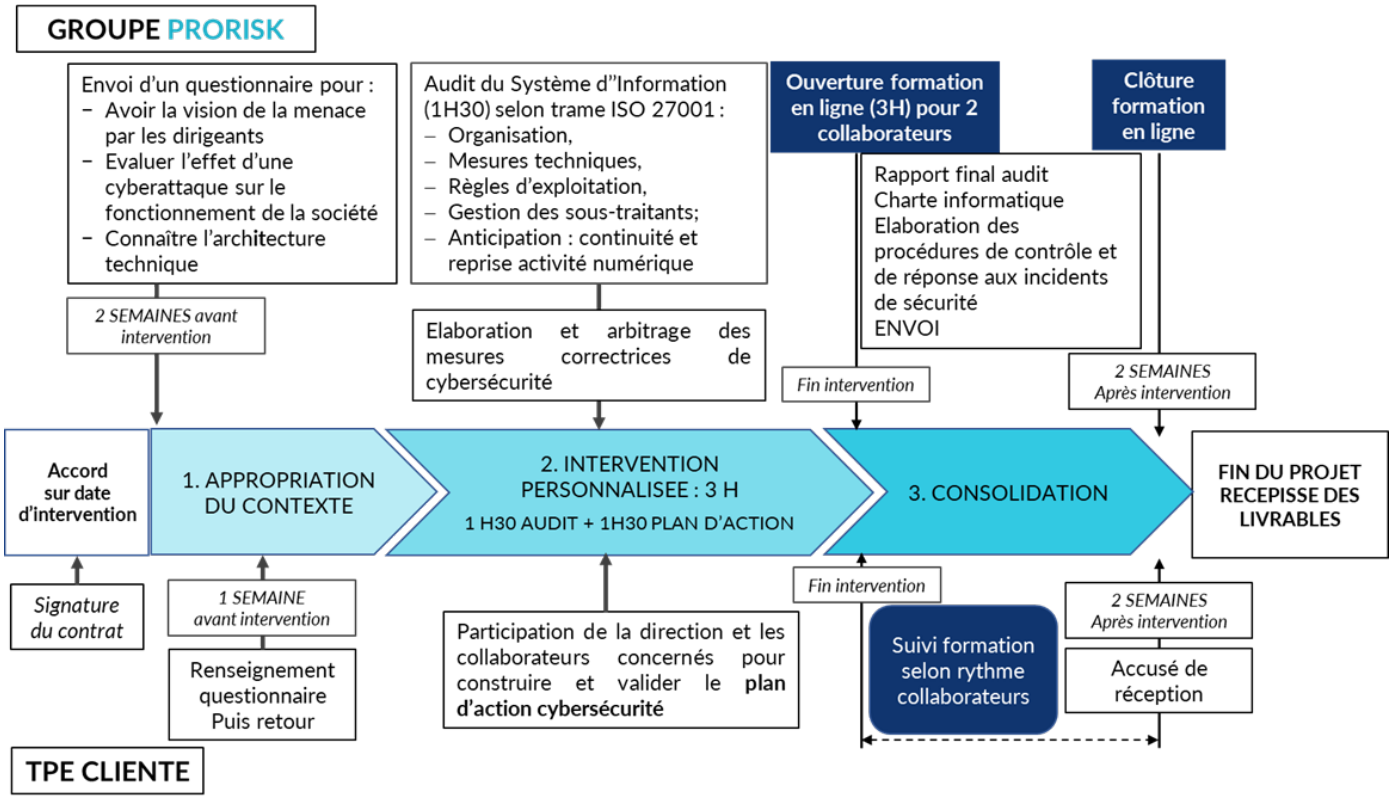
GROUPE PRORISK propose de réaliser cette mission Cybersécurité du client sur une période d'un mois.

L'intervention personnalisé sur place n'est pas possible au-delà de 150 kms d'une agence GROUPE PRORISK.

3. INTERVENANT

Un EXPERT SSI

4. DEROULEMENT



En option, GROUPE PRORISK propose une revue du plan d'action à une échéance fixée par le client.
Cette revue est réalisée par visioconférence et peut durer jusqu'à 2 heures.
Le client envoie la liste éventuelle des points particuliers qu'il souhaite aborder une semaine avant la visioconférence de revue.

5. LIVRABLES

Ensemble des livrables fournis – mentionnés au récépissé

- Rapport d'audit sous format Word ou Open Document
- Charte Informatique sous format Word ou Open Document
- Recueil de procédures sous format Word ou Open Document
- Attestation de formations sous format PDF.

PRESTATIONS CYBERSECURITE - PME

AUDIT DE SECURITE DES SYSTEMES D'INFORMATION

1. OBJECTIF

Les objectifs de l'audit de Sécurité des Systèmes d'Information (SSI) sont de :

- Identifier les vulnérabilités du système d'information ;
- En déduire une cartographie des risques sur la disponibilité, l'intégrité et la confidentialité des fonctions du système d'information ;
- Emettre des recommandations pour réduire ses risques et accroitre la résilience du client.

L'audit SSI est inclus dans le pack de mise en conformité RGPD. Il peut être conduit hors de ce contexte dans le cadre d'autres norme ou réglementations.

2. DUREE

Cette **prestation de conseil** s'étale sur une période entre 2 semaines et 2 mois selon la taille et la disponibilité des interlocuteurs de l'organisme client.

3. PREREQUIS

Transmission des architectures techniques du SI.

4. INTERVENANTS

CHEF DE PROJET

EXPERT SSI

5. DEROULEMENT

5.1. Préparation

Le client communique les documents techniques et les éventuels documents fournis par son prestataire informatique avant l'audit.

5.2. Audit

L'**audit de sécurité du SI** est conduit dans les locaux du client en suivant la norme ISO 27001 qui traite :

- De l'identification des objectifs de sécurité basée sur une analyse des risques ;
- De l'organisation ;
- Des ressources humaines ;
- De la gestion des actifs ;
- Des contrôles d'accès ;
- Des mesures cryptographiques ;
- De la sécurité physique ;
- De la sécurité à l'exploitation et de la traçabilité des opérations ;

- De la sécurité des transferts ;
- De la sécurisation des sites internet et extranet ;
- Du maintien en condition du système ;
- Des relations avec les fournisseurs du SI ;
- De la continuité des activités ;
- De l'audit et la revue périodique de sécurité.

La documentation de l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI), en particulier le guide d'hygiène informatique version 2017, sert de référence de cotation des pratiques.

GROUPE PRORISK émets des recommandations classées selon la gravité et la vraisemblance d'une atteinte aux systèmes d'informations du client.

GROUPE PRORISK propose des options de mise en œuvre des recommandations.

6. LIVRABLES

Un rapport d'audit sous format PowerPoint

Un plan d'action SSI sous format Excel.

PRESTATIONS CYBERSECURITE – PME

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION

1. OBJECTIF

Le déploiement de la Politique de Sécurité des Systèmes d'Informations permet la mise en œuvre des recommandations de sécurité élaborées dans la continuité de l'audit SSI.

2. DUREE

Cette **prestation de conseil** s'étale sur une période entre 2 semaines et 2 mois selon la taille et la disponibilité des interlocuteurs de l'organisme client.

3. PREREQUIS

Compte-rendu d'audit SSI et plan d'action SSI.

4. INTERVENANTS

CHEF DE PROJET

EXPERT SSI

5. METHODOLOGIE

Le client arbitre l'exécution des recommandations inscrites dans le « plan d'action SI » ainsi que les échéances de déploiement.

GROUPE PRORISK suit le déploiement des mesures en liaison avec les responsables de l'informatique au sein de l'organisme client.

GROUPE PRORISK rédige un projet charte de l'usage de l'informatique et le soumet à l'approbation du client.

Une fois la charte approuvée, GROUPE PRORISK rédige une Politique de Sécurité des Systèmes d'Information (**PSSI)** qui inclut les procédures de réaction d'urgence

GROUPE PRORISK conduit sur site une réunion de CLOTURE à l'issue de la prestation.

6. LIVRABLES

Un plan d'action SSI sous format Excel.

Une Charte de l'usage de 'informatique sous format Word

Une Politique de Sécurité des Systèmes d'Information sous format Word

PRESTATIONS CYBERSECURITE - PME

RESPONSABLE DE SECURITE DES SYSTEMES D'INFORMATION EXTERNE

RSSI EXTERNE

1. OBJECTIF

La mission de RSSI garantit la permanence de la Sécurité des Systèmes d'Informations par des mesures de prévention, de contrôle, de relation avec les acteurs extérieurs, d'assistance en cas de cyberattaque et de tenue à jour de la cartographie des risques.

2. DUREE

La mission d'assistance opérationnelle est permanente pendant la période de contractualisation.

3. PREREQUIS

Compte-rendu d'audit SSI et plan d'action SSI.

4. METHODOLOGIE

4.1. Points communs et différences avec mission de DPD

La mission de RSSI externe prend en compte l'ensemble des scénarios de cyberattaques à la différence de celle de DPD qui n'intègre que la sécurité des données personnelles.

Elle intègre la tenue à jour d'une cartographie des risques en cybersécurité.

Elle ne comprend pas les volets spécifiques RGPD : analyse juridique de traitement, réponse à exercices de droits, notification de violation.

4.2. Conseil en Sécurité des SI

GROUPE PRORISK anime l'exécution des mesures préconisées par le plan d'action SSI.

GROUPE PRORISK conseille la direction et les responsables informatiques quant à leur choix organisationnels et techniques pour garantir la résilience face à d'éventuelles cyberattaques ou campagnes de dénigrement.

GROUPE PRORISK veille, pour l'ensemble de ses clients, le site officiel des alertes en cybersécurité https://www.cert.ssi.gouv.fr/ de l'Agence Nationale pour la Sécurité des Systèmes d'Information.

Le CHEF DE PROJET fait au minimum un point mensuel par e-mail et annuel sur site pour réévaluation de la cartographie des risques.

4.3. Réaction en cas d'incident

En cas d'incident, GROUPE PRORISK coordonne les mesures urgentes pour limiter les effets d'une éventuelle cyberattaque avec le client ou les prestataires d'INFOGERANCE.

Si le premier diagnostic laisse penser à un incident grave au regard de la cartographie des risques, GROUPE PRORISK dépêche un consultant sur place pour piloter un processus de gestion de crise.

En cas d'incident grave, GROUPE PRORISK intervient par avenant au contrat et peut mettre à disposition une intervention d'investigation numérique assurée par une société labellisée par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) pour ce type d'opérations.

Cette investigation peut être nécessaire pour la constitution des preuves matérielles d'une agression numérique pouvant conduire à une plainte par le client mais également pour assurer la continuité de l'activité.

GROUPE PRORISK tient à jour un historique des incidents.

4.4. Plan de Continuité/Plan de reprise

GROUPE PRORISK appuie la rédaction ou l'examen du plan de continuité et de reprise.

A la demande du client, il peut coordonner l'organisation, l'animation et l'évaluation d'un exercice annuel de plan de continuité des fonctions numérique.

4.5. Maintien des compétences

GROUPE PRORISK propose l'organisation chaque année des sensibilisations définie dans le plan de formation RGPD.

5. INTERVENANTS

CHEF DE PROJET

EXPERT SSI pour analyse incident SSI

6. LIVRABLES

Classeur Excel de pilotage

Ensemble de la documentation de conformité tenue à jour

Journal des incidents au format Word

Documents liés à la réalisation des formations.

PRESTATIONS CYBERSECURITE - PME

SENSIBILISATION CYBERSECURITE

1. OBJECTIF

Cette formation intra-client consiste à sensibiliser les usagers des systèmes d'information.

La sensibilisation des membres vise l'acquisition des compétences suivantes :

- Connaitre les enjeux de sécurité des SI ;
- Comprendre la logique de risque en cybersécurité ;
- Connaître les méthodes employées par les acteurs malveillants et les cyberattaquants (informatique, actions physiques, manipulation des membres) ;
- Se tenir informé des menaces ;
- Appliquer les règles d'hygiène informatique ;
- Appliquer les procédures internes ;
- Réagir en cas d'urgence.

2. DUREE

Cette formation dure 1 demi-journée

3. PRE-REQUIS

Aucun.

4. INTERVENANT

EXPERT SSI

5. CAPACITE

Pas de seuil minimal

Capacité maximale de 20 personnes

6. LIVRABLES

- Feuille d'émargement
- Attestation de formation
- Questionnaires de satisfaction
- Livret de cours

COMPETENCES DE GROUPE PRORISK

1. COMPETENCES COLLECTIVES

La mise en conformité RGPD, comme l'exercice de la fonction de DPD, nécessite un triptyque de compétences :

- Analyse des risques ;
- Sécurité des systèmes d'information ;
- Conformité juridique.

GROUPE PRORISK est spécialisé depuis 14 ans dans la maitrise des risques : chacun de ses intervenants possède une expérience forte de cette méthodologie dans différents contextes.

En particulier, dans le domaine de la sûreté, GROUPE PRORISK est régulièrement amené à soumettre les livrables produits à la validation des autorité publiques.

2. REFERENCES

Les références en matière de maîtrise des risques sont consultables sur le site https://www.groupe-prorisk.com/nos-references_1.php.

Depuis 2 ans, GROUPE PRORISK a conduit ou poursuit les projets RGPD suivants :

- Société du GROUPE COFIBEL (négoce et immobilier) ;
- ASSA-CLARPA et CLARPA 56, associations d'aide à domicile ;
- Groupe scolaire LA CROIX ROUGE-LASSALLE à BREST ;
- 3 cabinets d'imagerie médicale ;
- GIP de logistique hospitalière, SILGOM dans le Morbihan ;
- Communauté de communes ISIGNY-OMAHA ;
- Communauté de communes PARTHENAY-GATINE ;
- Site de rencontres entre catholiques THEOTOKOS ;
- Groupe TANGUY, vente de matériaux ;
- Chaîne de magasins DISTRICENTER ;
- Comité Social et Economique d'EURODISNEY ;
- Chantiers de construction navale DAMEN.

3. EQUIPE PROJET

CHEF DE PROJET : Pascal LE CLAIRE :

- DPD **certifié BUREAU VERITAS** selon le référentiel CNIL (https://www.cnil.fr/fr/certification-des-competences-du-DPD-la-cnil-adopte-deux-referentiels)
- 25 ans d'expérience en protection des données et en sécurité des systèmes d'information
- Capitaine de vaisseau de réserve (30 ans de service dans la Marine Nationale) ;
- Titulaire d'un diplôme d'ingénieur et d'un master en « formation pour adultes » ;
- Suit la conformité RGPD sur une quinzaine de projets divers (Commerce, Groupe scolaire, Aide à domicile, Santé, Comité d'Entreprise).

Il assure la coordination de la fonction de DPD et de RSSI, suit les mesures en organisation et les relations avec les sous-traitants ou partenaires.

EXPERT SSI : Olivier STELANDRE :

- DPD en cours de certification ;
- 20 ans d'expérience en administration de réseau et en cybersécurité au sein de la marine nationale et de l'OTAN
- Spécialiste de sécurité des systèmes d'informations agissant sur une quinzaine de projets.

Il assure la prévention en cybersécurité pour les clients de GROUPE PRORISK et la suppléance du CHEF DE PROJET.

AVOCAT : Benoît LE GOAZIOU :

- Avocat au barreau de Paris ;
- 25 ans d'expérience en protection d et contentieux sur la protection des données sensibles.

Il agit en back office pour la validation des mentions d'informations légales et le contrôle des clauses contractuelles RGPD des sous-traitants.

ENGAGEMENTS

1. CONFIDENTIALITE

GROUPE PRORISK et le CLIENT s'engagent à considérer comme “confidentielles”, les informations de toute nature, écrites ou orales, par voie électronique, relatives aux sujets sur lesquels ils échangent, qui ne sont pas dans le domaine public.

GROUPE PRORISK s'engage à ne rien révéler ni oralement ni par écrit, à qui que ce soit, de tout ou partie des informations confidentielles qu’il aura recueillies au cours de sa mission.

GROUPE PRORISK et le CLIENT s'engagent à respecter la présente clause de confidentialité, aussi longtemps que lesdites informations ne seront pas tombées dans le domaine public, ou portées à la connaissance d’un tiers au contrat selon un accord des deux partis.

GROUPE PRORISK adopte une **politique des systèmes d’information** qui préserve la confidentialité des informations collectées dans le cadre de ses travaux.

GROUPE PRORISK proposera un protocole de sécurité au CLIENT visant la disponibilité, l’intégrité, la confidentialité et la traçabilité des opérations réalisées conjointement dans le cadre des opérations de sécurité des systèmes d’information.

2. QUALITE

GROUPE PRORISK s’engage à mettre en œuvre tous les moyens intellectuels et matériels nécessaires pour assurer cette mission. Cet engagement de moyens ne constitue pas un engagement sur les résultats.

Le CLIENT accepte de communiquer à GROUPE PRORISK les informations nécessaires à la réussite de la mission.

Les interventions de GROUPE PRORISK donneront lieu à une enquête de satisfaction.

3. PROPRIETE INTELLECTUELLE

Il est expressément stipulé que les livrables établis par GROUPE PRORISK dans le cadre de sa mission seront la propriété exclusive du CLIENT. GROUPE PRORISK s’engage à détruire les données collectées sur leur demande.

4. PROTECTION DES DONNEES A CARACTERE PERSONNEL

GROUPE PRORISK a établi son propre dossier de conformité et désigné un DPD en interne.

La conservation et la manipulation des coordonnées de contact professionnel sont nécessaires pour communiquer avec vous et donc vous apportez les meilleures prestations.

Les données, collectées et traitées par GROUPE PRORISK, concernent le nom, prénom, téléphone, adresse et e-mail professionnels des contacts au sein du CLIENT avec qui il est amené à travailler.

Elles sont conservées de manière sécurisée au maximum 11 ans après la dernière collaboration.

Elles ne sont pas transmises à d'autres organismes à des fins commerciales.

Pour les prestations de formation, la durée de conservation est de 6 ans.

Sur simple demande et sans avoir à la motiver, chaque personne peut **obtenir une copie des données** qui la concernant.

Elle peut obtenir la **rectification** de ces données personnelles sur demande.

En particulier, chaque STRUCTURE informe GROUPE PRORISK de toute mobilité de vos membres ayant un impact sur notre relation commerciale.

Chaque personne concernée peut obtenir **la suppression** si elle ne contrevient pas aux obligations de GROUPE PRORISK notamment en matière fiscale.

Les demandes sont à formuler auprès du Délégué à la Protection des Données de GROUPE PRORISK par email à l'adresse contact@groupe-prorisk.com ou par voie postale 7 rue du commandant Malbert, 29200 BREST.

Si vous considérez que l'utilisation de ces données est abusive, la personne peut porter réclamation auprès de la CNIL via son site internet (https://www.cnil.fr/fr/plaintes).

5. DEVELOPPEMENT DURABLE

GROUPE PRORISK est engagé dans un plan de maîtrise de la consommation d'énergie au sein de ses locaux et dans le cadre des déplacements de consultants.

GROUPE PRORISK utilise des documents électroniques dans la majorité de ses productions.

GROUPE PRORISK a mis en place une procédure de tri sélectif des déchets et fait appel à un prestataire engagé lui-même dans le développement durable pour la propreté de ses locaux.