

ANNEXE TECHNIQUE

SUR L'INTERVENTION RGPD

Le présent document complète la méthodologie de l'intervention, en expliquant les différentes missions réalisées dans le cadre de l'accompagnement RGPD.

Ce document, à vocation pédagogique, permet de cerner l'étendue des missions réalisées pour le compte du client.

Contour de la mission :

Le projet CARE CONNECT permet d'identifier un patient au cours d'un parcours de soin à l'aide d'un bracelet contenant une puce RFID avec l'identité complète du patient dessus. L'équipe soignante peut disposer d'un lecteur de puce permettant d'identifier avec certitude le patient.

La mission implique de faire une analyse complète des droits des patients, de la collecte du traitement et du stockage des données personnelles à la fois pour le bracelet et pour l'analyse des interactions bracelet / personnel soignant.

Cette analyse s'étend à des patients considérés comme « sensibles », comme les mineurs ou les personnes vulnérables.

Les relations entre la société CARE CONNECT et les établissements de santé devront être analysées et encadrées juridiquement.

D'une manière prospective, il faudrait voir si certaines données considérées comme médicales peuvent être stockées sur le bracelet et vérifier la conformité du dispositif à l'égard de la réglementation sur les dispositifs médicaux.

Nous proposons une méthodologie en 4 phases :

- 1) Analyse de situation et Audit RGPD
- 2) Rédaction des livrables
- 3) Formation, sensibilisation et mise en place des process
- 4) Suivi du projet

Un macro-planning est également fourni qui prévoit :

- Les phases de recherches (1), rédaction (2) et formation (3) avant le lancement ;
- Une phase de suivi du projet (4) après le lancement.

Le planning est établi sur deux mois pour laisser de la flexibilité et du confort dans les échanges nécessaires avec la structure.

Toutefois, ce planning prévisionnel est indicatif et pourra être réduit en fonction des besoins du client.

PHASE N°1 : ANALYSE DE SITUATION ET AUDIT

L'analyse de la situation (1.1) reprend les missions suivantes :

- Une analyse complète des droits des patients (information, consentement, accès et modification) ;
- Une analyse de la collecte des données (notamment biométriques) sur le support physique au regard de la réglementation RGPD ;
- Une analyse de la collecte et de la conservation des données relatives aux interactions bracelet / personnel soignant ;
- Une analyse de la collecte, du traitement et du stockage des données à caractère personnel des personnes considérées comme sensibles, à savoir :
 - Les mineurs ;
 - Les personnes vulnérables comme les patients de gériatrie ou psychiatrie sous tutelle ou curatelle.
- Une analyse de la relation contractuelle entre la société CARE CONNECT et l'établissement hospitalier ;
- Une analyse prospective portant sur la réglementation des dispositifs médicaux et à la réglementation sur le Dossier Patient Informatique ;
- Une analyse prospective sur l'éventualité de stocker des données de santé sur le bracelet (type « côté opéré » ou les allergies).

La cartographie des données personnelles (1.2) permet d'avoir une vision d'ensemble des flux de données personnelles (collecte) et du traitement par les différents acteurs. C'est la première étape du registre de traitement des données personnelles.

On construit cette cartographie en interrogeant le projet sur :

- L'identité des responsables de traitement et des sous-traitants ;
- Les types de données collectées ;
- Les finalités du traitement ;
- Le lieu d'hébergement des données ;
- La durée de conservation des données ;
- Les mesures de protection mises en place.

Enfin, un audit de sécurité des systèmes informatiques et RGPD (1.3) permet de mettre en place les fondamentaux de la protection des SI.

Il faut noter que ce n'est pas un audit technique, comme le propose un prestataire informatique. Nous formulons des préconisations et des standards de protection conforme à la protection des données personnelles.

Nous pouvons conseiller des prestataires techniques qui peuvent intervenir pour la mise en œuvre de certaines préconisations.

PHASE N°2 : RÉDACTION DES LIVRABLES

La rédaction des livrables permet d'obtenir une documentation complète de la gestion des données personnelles par la société CARE CONNECT.

Le RGPD a introduit un principe d'accountability, qui selon la CNIL se définit comme :
« l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données ».

En synthèse, l'accountability implique notamment de :

- déployer les mesures techniques, organisationnelles et contractuelles appropriées ;
- démontrer sa conformité au RGPD à tout moment.

Cette démonstration se base sur la production d'une documentation exhaustive et détaillée, décrivant l'ensemble des procédures et des bonnes pratiques appliquées par l'organisme en matière de données personnelles.

La conclusion de la première phase permettra de définir les livrables nécessaires.

Nous proposons, à travers la rédaction de livrable, de rédiger un ensemble cohérent permettant de créer un « dossier d'accountability » pouvant comprendre notamment :

- **Les fondamentaux de la conformité :**
 - ✓ Code d'éthique sur les principes fondamentaux appliqués ;
 - ✓ Documentation relative à la nomination du DPO ;
 - ✓ Cartographie des traitements et schémas des flux de données ;
 - ✓ Registre des traitements.
- **Transparence et information des personnes :**
 - ✓ Procédure sur la gestion des demandes de droits d'accès ;
 - ✓ Politique de confidentialité interne et externe ;
 - ✓ Politique de confidentialité du site web et gestion des cookies ;
 - ✓ Formulaire de consentement et traçabilité.
- **Sécurité, intégrité et confidentialité:**
 - ✓ Politique de Sécurité des Systèmes d'Informations (PSSI) ;
 - ✓ Procédures internes ;
 - ✓ Charte informatique ;
 - ✓ Règlement intérieur ;

- **Aspects contractuels :**
 - ✓ Politique d'éthique du choix des fournisseurs et partenaires ;
 - ✓ Contrats sous-traitants / avenants RGPD ;
 - ✓ Contrat de travail des salariés traitant les données (clause sur obligation de confidentialité spécifique).

- **Contrôle et audit de l'efficacité des mesures déployées :**
 - ✓ Politique d'audit interne et des sous-traitants ;
 - ✓ Comptes rendus des audits internes et indépendants effectués ;
 - ✓ Traçabilité des modifications et mises à jour apportées au dossier d'accountability.

PHASE N°3 : FORMATION ET MISE EN PLACE DES PROCESS

La méthodologie proposée intègre une grande part à la formation des usagers, à la sensibilisation aux données personnelles et à la mise en place de process de manière concrète.

a) Formation et sensibilisation

La formation est une obligation du RGPD. En effet, l'article 39 du texte détaille les missions du DPO : *« contrôler le respect du présent règlement [...] et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant »*.

La sensibilisation (3.1) permet aux acteurs du projet de connaître les fondements du RGPD et ainsi connaître les fondamentaux.

La formation (3.2) permet aux utilisateurs de disposer des connaissances permettant de mettre en œuvre les process RGPD.

Les attestations de formation et de sensibilisation seront jointes au dossier d'accountability.

b) La mise en place de process

Les process sont élaborés dans la phase n°2 doivent être mis en place au sein de la structure et le personnel préparé à mettre en œuvre chaque process interne (3.3).

PHASE N°4 : MISSION DE DPO - SUIVI DU PROJET

Le suivi du projet est particulièrement important pour vérifier que les process internes sont bien maîtrisés et que des corrections ne sont pas nécessaires.

Dans tous les cas, le DPO suit l'accomplissement du projet et peut être interrogé à tout moment sur des extensions du projet.

Le suivi du projet (4.1) comprend notamment la mise à jour régulière du dossier d'accountability.

L'implantation du projet dans des établissements hospitaliers peut amener à des discussions avec les DPO de ces établissements. Nous pouvons intervenir à la demande en cas de besoin.

Nous assurons une veille juridique et technique régulière qui nous permettent de tenir à jour votre dossier d'accountability.

Nous proposons un audit de fonctionnement au bout du 3^{ème} mois de commercialisation (4.2) pour nous assurer que les premières mesures mises en place sont pratiques et efficaces. Nous entreprenons dès lors les actions correctives nécessaires au bon fonctionnement du traitement des données personnelles.

En fin d'année, nous réalisons un bilan sur l'activité (4.3).

En cas de besoin, nous pouvons réaliser une analyse d'impact sur la protection des données et nous pouvons vous assister dans toutes les phases de discussions avec des autorités de contrôle (4.4).



SELARL CARLINI & ASSOCIES
60 Boulevard des Dames
13002 Marseille

Marseille le 31.03.22

INIZIA
Maison du Parc Technologique
ZI Erbajolo – 20600 Bastia

DEVIS
BORDEREAU DES
PRIX UNITAIRES

POSTE DE PRIX	PRESTATION	PRIX UNITAIRE HT	TAUX DE TVA	PRIX UNITAIRE TTC
1	Analyse et audit	3 562,50 €	20%	4 275,00 €
2	Rédaction des livrables	3 562,50 €	20%	4 275,00 €
3	Formation et mise en place des process	1 125,00 €	20%	1 350,00 €
4	Suivi annuel du projet	1 125,00 €	20%	1 350,00 €
TOTAL		9 375,00 €		11 250,00 €

Bar pour accord.
Le Président

Jean-Nicolas ANTONIOTTI

Philippe CARLINI
Avocat Associé

le 1/04/2022

Incubateur d'entreprises innovantes

inizià

Maison du Parc - ZI Erbajolo - 20600 BASTIA
Siret : 798 482 097 00010