aixial

AN ALTEN COMPANY

PROTECTION DES DONNÉES PERSONNELLES (RGPD / GDPR)

MISE EN OEUVRE DE EU GDPR DANS UNE CRO

Véronique MERIC, Head of Quality Assurance AIXIAL

EU GDPR / RGPD

AIXIAL

Ses obligations en tant que CRO

AIXIAL, CRO du Groupe ALTEN

- **Le RGPD impose des obligations aux entreprises en matière de gouvernance et de protection des données à caractère personnel**

  - **Article 2 du RGPD : « Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ».**

AIXIAL, CRO du Groupe ALTEN

- **Domaines d'activités**

Clinical Operations

Regulatory Submissions

Project Management

Monitoring

Consulting

Platforms

Projects

Vigilance & Medical Affairs

Vigilances

Medical Information

Medical Writing

Biometrics

Data Management

Biostatistics / SAS Programing

CDISC

Quality & Regulatory Affairs

Submissions/ Regulatory Maintenance

CMC

AIXIAL, CRO du Groupe ALTEN

Champs d'application, le RGPD s'applique

- **pour AIXIAL en tant que**
  - « Responsable de Traitement » : **détermine les finalités et les moyens d'un Traitement,**
    - **et/ou**
  - « Sous-traitant » : **traite des Données pour le compte d'un tiers** (Responsable de Traitement).

- **à tous les traitements de données personnelles réalisés en tant que Responsable de Traitement et Sous-traitant**

AIXIAL, Responsable de Traitement

- **Doit organiser le traitement des données personnelles en interne**
  - **Ressources Humaines**
  - **Administration**
  - **Prospection**

- **Responsabilités prises en compte dans le Plan d'Actions de mise en conformité**

AIXIAL, Sous-Traitant

- **Doit organiser le traitement des données personnelles dans le domaine de ses activités opérationnelles**
  - **Données de santé**

- **Responsabilités prises en compte dans le Plan d'Actions de mise en conformité**
  - **Déclinées sur les obligations du sous-traitant**

RGPD – Mise en conformité

Objectifs

- Répondre aux obligations du RGPD
- Surveiller et améliorer en continu
- Informer et former les collaborateurs et les sous traitants

RGPD – Mise en conformité

Démarche

- **S'appuyer sur l'existant**
  - Conformité à la réglementation applicable
  - Equipes sensibilisées et formées
- **Mise en place Plan d'actions de mise en conformité**
  - Répondre aux exigences du RGPD
  - Dès Mai 2018
- **Maintien de la conformité**
  - Surveillance & vigilance
  - Amélioration

RGPD – Mise en conformité

Plan d'actions

- **Répondre aux obligations RGPD**
  - **Recenser tous les traitements de données personnelles**
    - Registre pour cartographie
  - **Réaliser un Audit interne**
    - Analyser les exigences RGPD versus Organisation actuelle
    - Mettre en place un CAPA et suivi
  - **Gérer les risques**
    - Analyse impact si risques élevés identifiés

RGPD – Mise en conformité

Plan d'actions

- **Répondre aux obligations RGPD**
  - **Organiser les processus internes**
    - Mettre en place / à jour les procédures & processus
  - **Mettre à jour les contrats clients/sous-traitants**
  - **S'assurer de la mise en conformité des sous-traitants**
  - **Nommer un DPO**
  - **Désigner des Relais, responsables par Département**
  - **Documenter la conformité**
    - Création, modification formulaires / modèles

RGPD – Mise en conformité

Plan d'actions

- **Surveiller et améliorer**
  - **Réalisation des audits en interne**
  - **Réalisation des audits de sous-traitants focus RGPD**
    - **Procédure de vérification dès le référencement**
      - Responsabilités engagées
  - **Favoriser la remontée d'informations en interne**
  - **Ajouter Indicateurs qualité**
    - **non-conformités, remontées incidents,**
  - **Pistes amélioration pour anticiper les violations de données**

RGPD – Mise en conformité

Plan d'actions

- **Informer et former les collaborateurs et les sous traitants**
  - **Campagne de re-sensibilisation sécurité et protection des données**
  - **Formation des équipes au RGPD**
  - **Relation régulière avec les relais dans l'entreprise**
  - **Communication et actions auprès des Sous-traitants**

EU GDPR / RGPD

AIXIAL – EN TANT QUE SOUS TRAITANT

Vers la mise en conformité avec le RGPD

Données de Santé

En 2017

- **Cadre légal proche du RGPD**
  - **sur le traitement des données de santé**
    - Règlement Européen relatif aux essais cliniques
    - Bonnes Pratiques Cliniques
    - CNIL, Méthodologies de références…
  - **Respect des Obligations**
    - Sécurité et confidentialité des données
    - Protection et droits des Patients
  - **Actions pour assurer**
    - Anonymisation / Pseudonymisation
    - Obtention du consentement
    - Validation des Systèmes Informatisés

Données de Santé

En 2017, MR001 & MR 003

- Méthodologies de références
  - Engagement de conformité
  - Par le Responsable du Traitement ou son Sous Traitant
  - Notion de Responsabilités
  - Analyse des risques pour la vie privée du patient
    - Sécurité et confidentialité des données collectées.
  - Durée de conservation
  - Obligation information écrite du Patient
  - Consentement écrit du Patient pour la MR001
  - Transfert données hors UE

RGPD : Obligations du Sous Traitant

En 2017,

- Conformité avec la réglementation existante
- Equipes formées aux exigences
  - Protection des données personnelles
  - Droit des Patients
- Base solide pour
  - Adaptation au RGPD
- Mais nouveautés à prendre en compte….
  - Changements RGPD

RGPD : Obligations du Sous Traitant

Nomination d'un DPO

- Doit être Vigilant sur la gestion des données en tant que
  - « Responsable de Traitement »
  - « Sous-traitant » => Données de Santé
- Doit s'appuyer sur
  - les Relais Experts
  - La Direction
  - L' Assurance Qualité
- Connaitre le Domaine des Essais Cliniques
- S'aider de la Réglementation existante
  - Sans négliger les nouveaux requis

RGPD : Obligations du Sous Traitant

Obligation de Transparence et Traçabilité

- Mise à jour des contrats avec
  - les clients
  - Les sous-traitants
  - Prise en compte
    - Obligations/responsabilités de chaque partie
    - Obligations article 28 sur la sous-traitance
  - Notion d'assistance auprès du client

RGPD : Obligations du Sous Traitant

Obligation de Transparence et Traçabilité

- **Renforcement des preuves documentées**
  - Instructions sur traitement des données par le client
  - Ajout dans la documentation essentielle du Projet
- **Autorisation préalable et écrite du client**
  - Changement ou ajout de sous-traitant
  - Classé avec les éléments contractuels

RGPD : Obligations du Sous Traitant

Obligation de Transparence et Traçabilité

- **Mise à disposition des informations auprès des clients**
  - **Preuves de conformité GDPR**
  - **Audits clients**
- **Registre de Traitement des Données**
  - **Recensement des clients et description des traitements de données**
  - **Mise à jour régulière**
  - **Mis à disposition des clients et organismes de contrôle**

RGPD : Obligations du Sous Traitant

Prise en compte des principes de protection des données

- **Dès la conception**
- **Par défaut**
  - ***Obligations existantes (CRF ; e-CRF ; Base de données)***
  - **Vérification documentée sur les principes à respecter**
    - Minimisation des données
    - Finalité du traitement / Quantité données collectées
    - Etendue du traitement
    - Durée de conservation
    - Nombre de personnes y ayant accès

RGPD : Obligations du Sous Traitant

Garantir la sécurité des données traitées

- **Obligations de confidentialité**
  - ***Obligations existantes***
  - **Revue des contrats**
  - **Professionnels de santé**
- **Notification de toute violation de données**
  - ***Obligations existantes***
  - **Mise en place formulaire spécifique**

RGPD : Obligations du Sous Traitant

Garantir la sécurité des données traitées

- **Niveau de sécurité adapté aux risques**
  - ***Obligations existantes***
  - **DPIA**
- **Suppression / renvoi / Destruction des données existantes**
  - ***Obligations existantes***
  - **Renforcement**
    - Contrats
    - Procédures

RGPD : Obligations du Sous Traitant

Analyse d'impact - DPIA*

- **Obligatoire lorsque le traitement est susceptible d'entrainer des risques élevés pour les droits et libertés des personnes physiques**

  GDPR – Art 75

  - **le traitement peut donner lieu ….. à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation**
  - **des données personnelles sont traitées qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion …….. et le traitement des données génétiques, les données concernant la santé ou les données concernant la vie sexuelle……**
  - **lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants;**
  - **ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.**

**Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 - Adopté le 04 Avr 2017 et révisé et adopté le 04 Oct 2017*

RGPD : Obligations du Sous Traitant

Analyse d'impact - DPIA

- **Obligatoire sauf si Le traitement a été contrôlé par une Autorité de Contrôle**

- **Process amélioration continue**
  - **Adapté aux exigences du GDPR**
  - **Documentation disponible**

RGPD : Obligations du Sous Traitant

Obligation d'assistance, alerte et conseil

- Violation des règles en matière de protection des données
  - Information immédiate
- Aide lors d'une demande sur droits d'accès, rectification
- Garantie du respect des obligations du GDPR

RGPD : Aide mise en conformité

CNIL

- « Se préparer au règlement »
  - Règlement européen : se préparer en 6 étapes
  - Devenir délégué à la protection des données 23 mai 2017
  - Guide du Sous-Traitant – Septembre 2017
  - Lignes directrices du G29 sur les DPIA – 18 Octobre 2017
  - FAQ
  - Exemples de clauses à insérer dans les contrats

Merci