GHT LOIRE

Groupement Hospitalier de Territoire

« Des femmes et des hommes au service de votre santé »

Règlement Général de Protection des Données

GHT LOIRE
Groupement Hospitalier de Territoire
« Des femmes et des hommes au service de votre santé »

Les grands principes du RGPD

Introduction – les éléments fondateurs

Qu’est ce qu’une donnée à caractère personnel?

constituent des données personnelles, **toute information** se rapportant à une personne physique identifiée ou identifiable. Cela inclut notamment: le nom, un numéro d’identification, une adresse email, des informations génétiques, les adresses IP, etc.

Qu’est ce qu’un traitement?

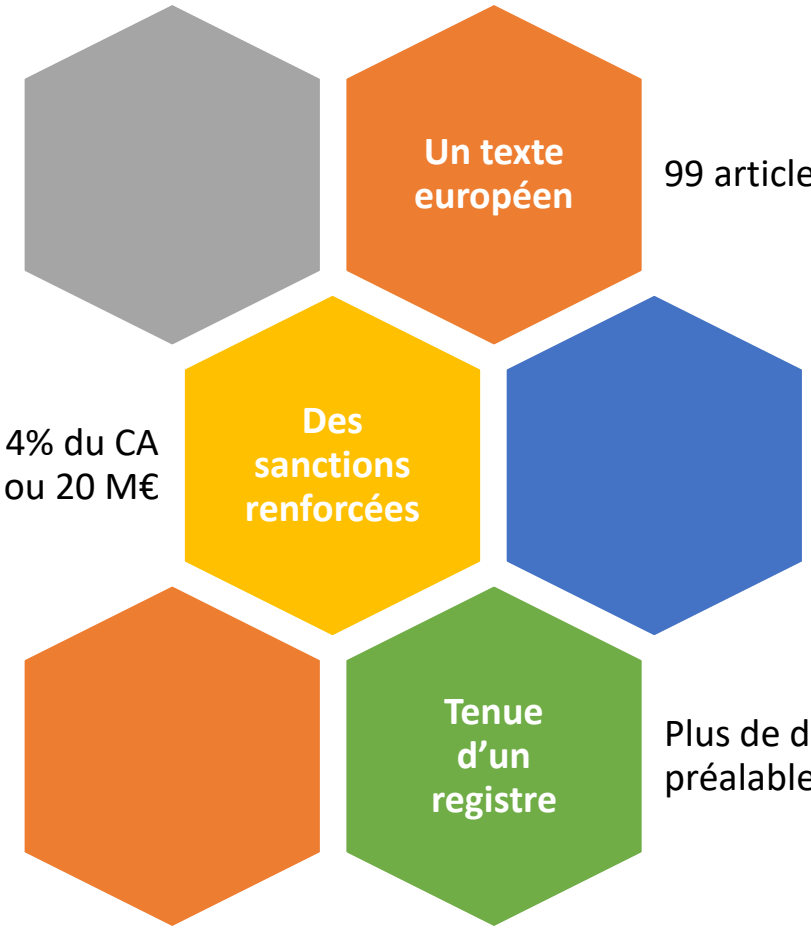
«**toute opération ou tout ensemble d'opérations** effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, 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»

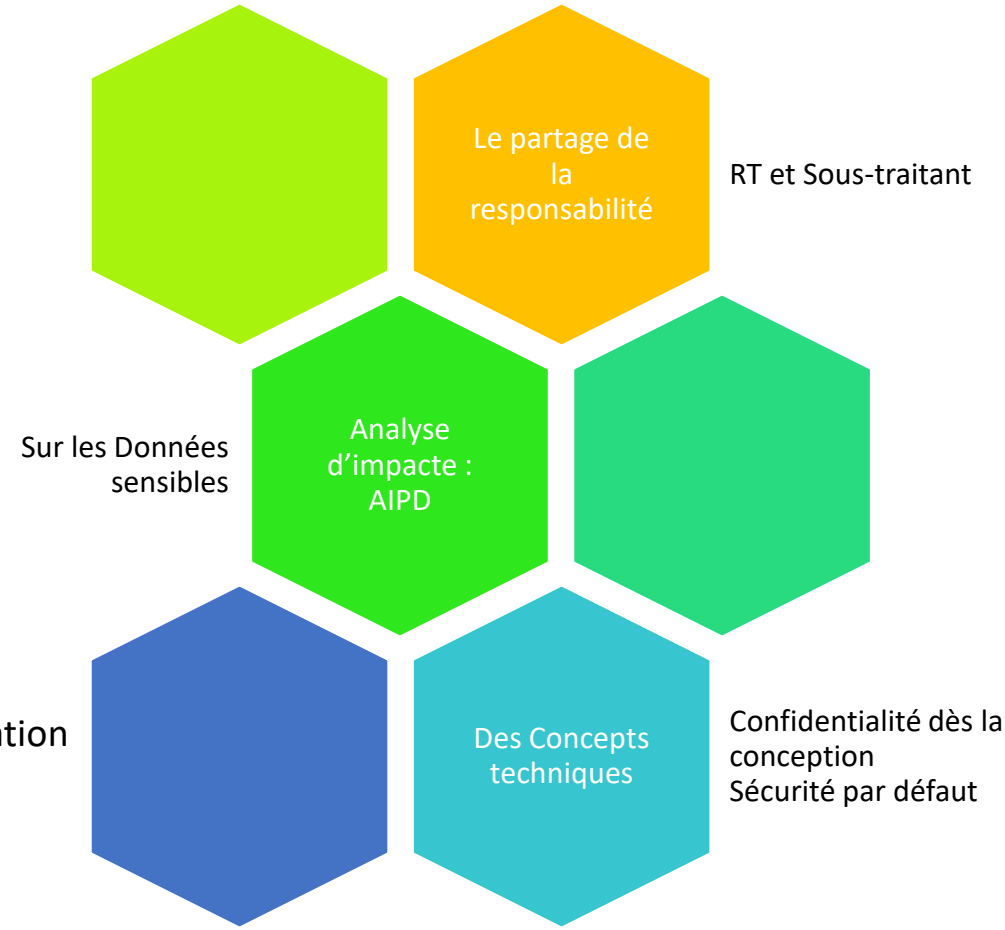
Les acteurs de la protection des données

- ✓ Le **responsable du traitement (RT)** est la personne physique ou morale qui détermine les finalités et les modalités du traitement
- ✓ le **sous-traitant** est celui qui traite des données à caractère personnel pour le compte du responsable de traitement
- ✓ L'autorité de contrôle : en France la CNIL
- ✓ Le Délégué à la protection des données (DPD)

- ✓ **Ne pas confondre avec** :
- ✓ L'exécutant : il s'agit de la personne qui agit directement suivant les consignes du RT
- ✓ Le destinataire : c'est la personne qui va utiliser les données

Les grandes Lignes





* Sauf pour certains cas

Les grandes Lignes

72 H Notification des Violations de données

- Si atteintes possibles sur la vie privée des personnes

Tenir un registre de traitement

- Listing de tous les traitements en place

De nouveaux* droits pour les personnes

- Droit à l'accès
- Droit à la rectification
- Droit à l'oubli ou droit à l'effacement*
- Droit à la portabilité*
- Droit d'opposition

La licéité d'un traitement : Art - 6

Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques; **=> Recueil du Consentement**

le traitement est nécessaire à **l'exécution d'un contrat** auquel la personne concernée est partie prenante ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

le traitement est nécessaire au respect d'une **obligation légale** à laquelle le responsable du traitement est soumis;

le traitement est nécessaire à la **sauvegarde des intérêts vitaux de la personne** concernée ou d'une autre personne physique;

le traitement est nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

le traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le contenu du registre

Un exercice de Formalisation

le nom et les coordonnées du responsable du traitement mis en œuvre

les **finalités** du traitement, l'objectif en vue duquel vous avez collecté ces données

les catégories **de personnes concernées** (patient, entreprise, employé, etc.)

les **catégories** de **données personnelles** (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, etc.)

les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez

les **transferts** de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;

les **délais prévus pour l'effacement** des différentes catégories de données, c'est-à-dire la **durée de conservation**, ou à défaut les critères permettant de la déterminer

dans la mesure du possible, une **description générale des mesures de sécurité** techniques et organisationnelles que vous mettez en œuvre

GHT LOIRE
Groupement Hospitalier de Territoire
« Des femmes et des hommes au service de votre santé »

Les missions du responsable de traitement

Ses Missions

Vos missions

- Fournir les informations aux personnes concernées par les Traitements
- Faciliter aux personnes l'exercice de leur droits : accès, rectification,…
- S'assurer et démontrer que les traitements sont conformes au RGPD
- Mettre en œuvre les politiques et processus nécessaires
- Informer les personnes sur le traitement de leurs demandes : motivation si refus, délais d'obtention, … le tout sous 1 mois maximum
- Mise en œuvre des mesures techniques et organisationnelles pour la sécurité des DCP
- Garantir les objectifs de la finalité tout en ayant à l'esprit les concepts de : minimisation de la quantité, durée de conservation et d'accessibilité.
- Réalise les analyses d'impact si le risque pour les droits et libertés des personnes physiques est élevé

Vos responsabilités

Vos responsabilités	Vous **identifier** auprès du DPD
	Fournir les éléments nécessaires à **l'enregistrement** de vos **traitements** dans le registre
	Vérifier avec les **experts métiers** que les données sont sécurisées
	Mener une **analyse d'impact** lorsque c'est nécessaire
	Répondre aux demandes des **usagers**

GHT LOIRE

Groupement Hospitalier de Territoire

« Des femmes et des hommes au service de votre santé »

Le rôle du délégué à la protection des données

Ses Missions

Informer et conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;

Contrôler le respect du règlement et du droit national en matière de protection des données ;

Conseiller l'organisme sur la réalisation d'une **analyse d'impact** relative à la protection des données et d'en vérifier l'exécution ;

Coopérer avec l'autorité de contrôle et être le point de contact de celle-ci : **la CNIL**

GHT LOIRE
Groupement Hospitalier de Territoire
« Des femmes et des hommes au service de votre santé »

Le transfert de DCP

Attention les échanges de DCP sont très encadrés

- Vous devez informer les personnes au préalable
  - *Exemple : données transmises à un établissement externe au GHT pour un avis complémentaire*

- Tous flux de données sortant de l'UE doit être contractuellement encadré et déclaré au DPD qui doit faire une déclaration auprès de la CNIL.
  - *Exemple : étude de recherche avec un société établie aux Etats-Unis à laquelle vous fournissez des données de patients*

GHT LOIRE
Groupement Hospitalier de Territoire
« Des femmes et des hommes au service de votre santé »

Les outils à votre disposition

Vos outils

Un espace SharePoint documentaire

Fiche type de description de TTT
Vidéo de sensibilisation
Des exemples de mentions d'information
Des procédures standards
Poser vos questions en lignes et FAQ
https://wshp42.chu-st-etienne.fr/sites/ght_loire_rgpd

Un registre de traitement type

À décliner par établissement

Une page d'information et un Formulaire

Sur le Site GHT Loire : http://www.ghtloire.fr/rgpd/

L'outil PIA de la CNIL pour les AIPD

Envoyer au DPD pour validation
Serveur GHT pour la consolidation des AIPD
http://svpia-ex:4200

L’analyse d’impact

Des questions Simples

Quel est le traitement qui fait l'objet de l'étude ?
Quels sont les référentiels applicables ?
Quelles sont les données traitées ?
Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

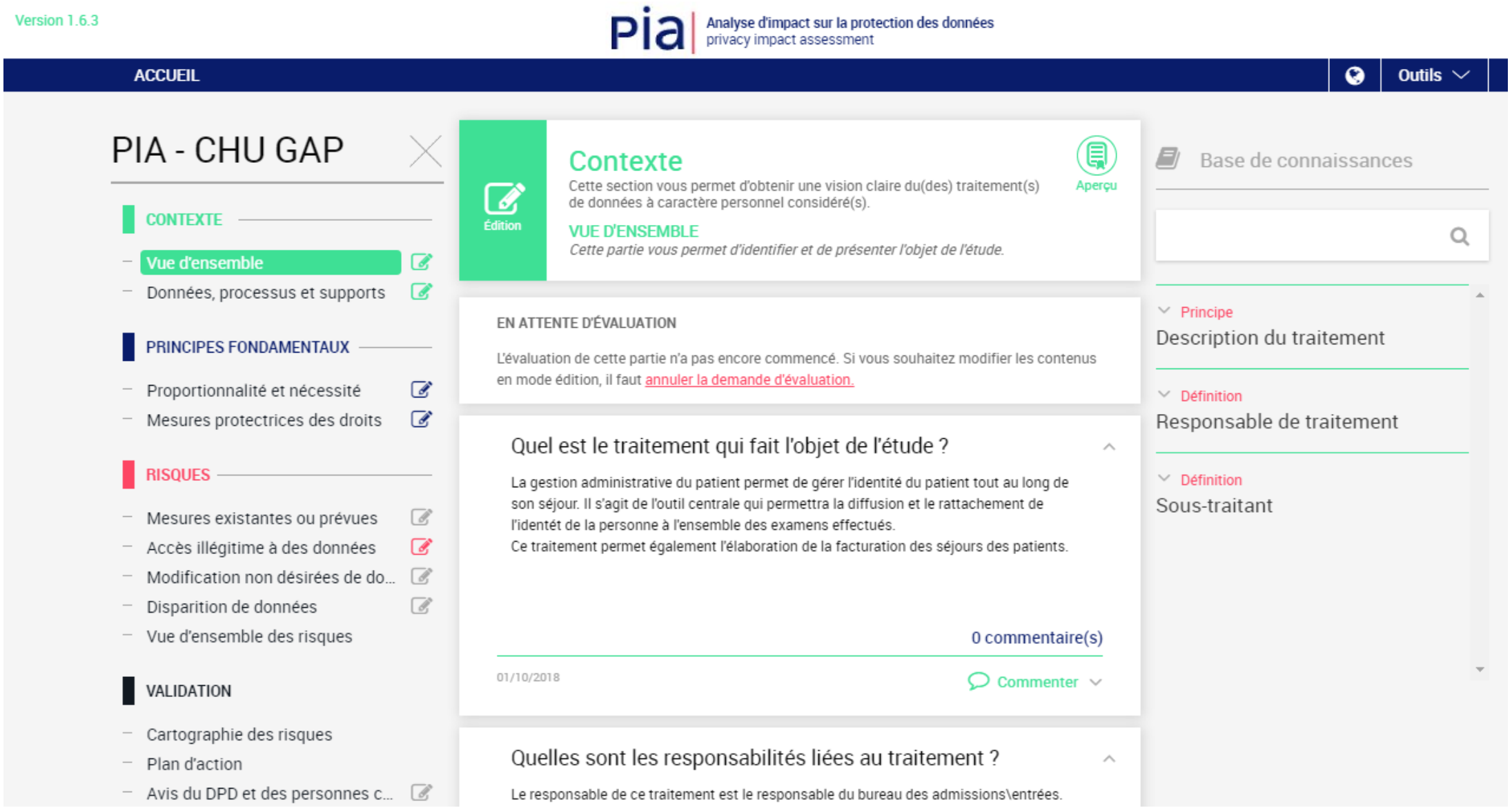
Une description de la conformité

Quel est le fondement qui rend votre traitement licite ?
Respectez vous la minimisation
Quelle est la durée de conservation des données ?

L’analyse de risque

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?
…….

L'analyse d'impact



GHT LOIRE
Groupement Hospitalier de Territoire
« Des femmes et des hommes au service de votre santé »

Le plan d'action

Plan d'action

Identifier les Responsables de Traitement

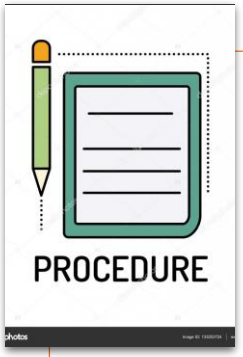
- Accompagnement
- Sensibilisation
- Formation

élaborer les registres

- Un par établissement
- 5 pour la recherche
- Un pour chaque structure indépendante

Réaliser les analyses d'impacts AIPD

- Par les responsables de traitement
- Analysées par le DPD



Mettre en place les procédures

- Déclaration de violation
- Gestion des habilitations
- Exercice des droits des personnes

Sécuriser les Traitements

- Plan de gestion de risques techniques
- Plan d'action sur les pratiques

Et maintenant ….

Identifiez-vous auprès du DPD

En envoyant un mail à rgpd-dpd@ch-st-etienne.fr

Délégué à la protection des données

- Une description courte et simple de votre traitement
- La catégorie des personnes concernées : patients, agents, entreprises
- Combien de personnes sont concernées par ce traitement
- La liste des personnes qui vont les utiliser
- Le type de données collectées : identité, information bancaire, donnée de santé,…
- La durée de conservation des informations
- Les moyens mis en place pour sécuriser les données
- Le logiciel utilisé si il y en a un

Soyez Concis et factuel

Et si vous douter encore….

N’hésitez pas à nous décrire votre activité et votre rôle: rgpd-dpd@ch-st-etienne.fr

GHT LOIRE

Groupement Hospitalier de Territoire

« Des femmes et des hommes au service de votre santé »

Merci de votre participation