Le Règlement Général européen de Protection des Données personnelle

Présentation du RGPD et applications pour le CRJ et les Districts

TOURS, 24 novembre 2018

Rotary | CRJ Centre Rotarien pour la Jeunesse

Réalisée par

Me Hadrien CHOUAMIER

Avocat au Barreau de SAINT MALO DINAN

Le RGPD, c’est quoi ?

Les textes

1. Le 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
2. La loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, modifiant notamment la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Le RGPD, c’est pour qui ?

Article 2 RGPD :

Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Plan

1) Le RGPD, en théorie
    1) Philosophie
    2) Obligations
    3) Sanctions
2) Le RGPD, en pratique
    1) Le recueil du consentement
    2) Le registre des traitements
    3) La sécurisation des données
    4) L'éventuel DPO
3) Le RGPD, appliqué au Youth Exchange Program

Le RGPD, en théorie

1- Le changement de philosophie

- AVANT: logique de déclaration et d'autorisation préalable des traitements auprès de la CNIL
- MAINTENANT : logique de responsabilisation et de contrôles renforcés auprès des responsables de traitement par la CNIL

Le RGPD, en théorie

2- Les obligations

Le traitement de données personnelles doit respecter les grands principes suivants :

- licéité, loyauté, transparence
- limitation des finalités
- minimisation des données
- exactitude
- limitation de la conservation
- intégrité et confidentialité
- responsabilité

Le RGPD, en théorie

D’autres principes s’y ajoutent

- *Privacy by design* : s’assurer dès la conception d’une application de la protection des données personnelles

- *Accountability :* 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.

Le RGPD, en théorie

Quels sont les principaux traitements des entreprises ?

- clientèle
- prospects
- ressources humaines
- archives
- site internet, applications mobiles

Le RGPD, en théorie

Les sous traitants

Il appartient au responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement.

Il faut donc prévoir dans les contrats de sous-traitance des clauses prévoyant l'application du RGPD et de s'assurer auprès de son sous-traitant qu'il met bien en œuvres les préconisations du RGPD.

Le RGPD, en théorie

Comme auparavant pour les Opérateurs d'Importance Vitale, tout responsable de traitement a des obligations de notification en cas de violation des données

- **Article 33.1:** En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance
- **Article 34.1** : Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.
- **Article 34.3.c :** Si cette communication individuelle exige des efforts disproportionnés, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Le RGPD, en théorie

2- Les sanctions

- Jusqu'à **10 millions d'euros** ou, dans le cas d'une entreprise, **2% du chiffre d'affaires annuel mondial** pour des manquements notamment au Privacy By Design, Privacy By Default…
- Jusqu'à **20 millions d'euros** ou, dans le cas d'une entreprise, **4% du chiffres d'affaires annuel mondial** pour manquement notamment aux droits des personnes (droits d'accès, de rectification, d'opposition, de suppression, droit à l'oubli, etc.)

Le RGPD, en théorie

L’obligation de mettre en place un Plan de Continuité d’Activité

Article 32 : […] *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :*

- *le chiffrement des données*
- *la confidentialité, l'intégrité, la disponibilité et la résilience des*
- *systèmes*
- *le rétablissement de la disponibilité des données*
- *le test, l’analyse et l’évaluation régulière de la sécurité*

I. COMMENT RECUEILLIR LE CONSENTEMENT ?

En pratique, le consentement

1- Le consentement des utilisateurs et co-contractants

Article 6 Licéité du traitement

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

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques

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

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

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

e) 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;

f) 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.***

En pratique, le consentement

Il vaut donc mieux obtenir le consentement des utilisateurs, surtout si ceux-ci sont mineurs !!

Or selon l'article 7 RGPD

> *2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples.*

Il faut aussi distinguer si le traitement est nécessaire à la fourniture du service, ou si c'est accessoire

En pratique, le consentement

Le consentement des clients s'accompagne également d'un très large droit à l'information

Les informations suivantes doivent donc être transmises aux clients et au prospects :

- les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- les finalités du traitement auquel sont destinées les données à caractère personnel ;
- la base juridique du traitement ;
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque ces intérêts légitimes sont la condition de licéité du traitement ;
- le fait que le responsable de traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ;
- le cas échéant, l'existence ou l'absence d'une décision d'adéquation rendue par la CNIL, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
- lorsque le traitement est fondé sur le consentement de la personne concernée, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

En pratique, le consentement

Ces mentions doivent donc apparaitre dans les documents contractuels signés par toutes les parties

II. LA TENUE DE REGISTRES

1) Une forte incitation
2) Le contenu des fiches de traitement

En pratique, le registre des traitements

Le RGPD impose la tenue d'un registre regroupant tous les traitements de données personnelles notamment si ces traitements portent sur des données sensibles telles que:

- origine raciale ou ethnique,
- opinions politiques,
- convictions religieuses ou philosophiques
- appartenance syndicale,
- données génétiques,
- des données biométriques
- **des données concernant la santé**
- des données concernant la vie sexuelle ou l'orientation sexuelle
- données relatives à des condamnations pénales

En pratique, le registre des traitements

Si vous n'étiez pas soumis à une telle obligation, la tenue de registre est fortement recommandé dans le cadre d'une démarche pro active permettant de démontrer que l'on respecte le RGPD.

En effet, l'état des lieux des traitements opérés est un préalable nécessaire permettant de connaitre l'étendue des obligations qui s'imposent.

En pratique, le registre des traitements

- **Dans tous les cas, un inventaire des traitements effectués est nécessaires afin de pouvoir demander les autorisations**

Dès lors que l'on liste les traitements, autant avoir une démarche complète et tenir un registre, la différence d'investissement est minime

En pratique, le registre des traitements

Pour chaque traitement de données personnelles, posez vous les questions suivantes :
Qui ?
Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ;
Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme ;
Etablissez la liste des sous-traitants.
Quoi ?
Identifiez les catégories de données traitées
Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé ou les infractions)
Pourquoi ?
Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données (exemple : gestion de la relation commerciale, gestion RH…).
Où ?
Déterminez le lieu où les données sont hébergées.
Indiquez quels pays les données sont éventuellement transférées.
Jusqu'à quand ?
Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.
Comment ?
Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

En pratique, le registre des traitements

Vous devriez donc obtenir une série de fiches avec les informations suivantes:

- Identité et coordonnées du responsable de traitement
- Finalités ;
- Catégories de personnes concernées ;
- Catégories de données à caractère personnel ;
- Catégories de destinataires ;
- Transferts vers un pays tiers ou une organisation internationale;
- Délais prévus pour l'effacement ;
- Description générale des mesures de sécurité techniques et organisationnelles.

En pratique, le registre des traitements

Exemple de registre accessible sur le site de la CNIL

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Nom : Cliquez ici. Prénom : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	Nom : Cliquez ici. Prénom : Cliquez ici. Société (si DPO externe) : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Catégories de données collectées

Cochez et listez les différentes données traitées

☐ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance. etc.)*

En pratique, le registre des traitements

L'Analyse d'Impact

En vertu de l'article 35 du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un **risque élevé pour les droits et libertés des personnes physiques**, notamment le **traitement à grande échelle de catégories particulières de données**, le responsable du traitement doit effectuer, avant toute mise en œuvre, une analyse d'impact.

Cette analyse d'impact se fait au regard de la qualité des personnes dont les données sont traitées, mais aussi en fonction de la sensibilité des données recueillies.

En pratique, le registre des traitements

La CNIL vient de préciser dans une récente délibération du 11 octobre 2018 qu'il fallait comprendre par traitement nécessitant une analyse d'impact tout traitement regroupant au moins deux des catégories de données suivantes:

- Données traitées à grande échelle ;
- Données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, **données génétiques ou de santé**, données biométriques et données concernant la vie ou l'orientation sexuelle) ou données hautement personnelles (données relatives à des communications électroniques, données de localisation, **données financières**, etc.) ;
- Données relatives aux personnes vulnérables (patients, personnes âgées, **enfants**, etc.) ;
- Croisement ou combinaison de données ;
- **Évaluation/scoring (y compris le profilage)** ;
- Prise de décision automatisée avec un effet juridique ou similaire ;
- Surveillance systématique de personnes ;
- **Traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat** ;
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

En pratique, le registre des traitements

Si vous estimez finalement qu'une Analyse d'impact n'est pas nécessaire pour un traitement, il vous faudra justifier et documenter votre choix au regard des risques encouru par les utilisateurs, dans le cadre de la démarche d'*accountability*.

III. LA SECURISATION DES DONNEES

1) Imposer une politique sécuritaire
2) Cloisonner les accès
3) Sécuriser les équipements
4) Sécuriser les données numérique
5) Sécuriser les communications

En pratique, la sécurisation

- Les données personnelles que vous gérer se retrouvent souvent partout, y compris dans votre ordinateur portable ou votre smartphone :
  - Un tiers peut-il les déverrouiller ?
  - Un tiers peut-il accéder aux données ?

En pratique, la sécurisation

L’utilisation de l’outil informatique expose à les données à des risques :

- Virus : destruction des données
- Ransomware : chiffrement des données contre rançon
- Trojan : récupération à distance des données
- Vol de matériel
- Antiterrorisme : surveillance étatique de masse des communications

En pratique, la sécurisation

Article 33.10 RGPD

En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation [...] ***à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.***

Ex : on vous vole votre téléphone ou votre ordinateur portable:

- Il est chiffré et vous l'effacer à distance→ pas de notification
- Il n'est pas chiffré → notification

En pratique, la sécurisation

1- La politique sécuritaire

c’est imposer à son entreprise un ensemble de bonnes pratiques

- Utiliser des comptes utilisateurs sur les postes informatiques (et pas administrateurs)
- Utiliser des logiciels à jour et provenant de sources sûres
- Utiliser un firewall et un antivirus à jour
- Être formé aux risques du *hameçonnage*, de *l’ingénierie sociale…* et donc être suspicieux sur les pièces jointes
- Verrouiller la session dès que l’on quitte son poste de travail
- Utiliser des mots de passe forts
- Faire signer une charte informatique aux salariés et stagiaires rappelant ces bonnes pratiques et leurs obligations

En pratique, la sécurisation

- **Ingénierie sociale :** connaissance de l'environnement social et de l'organisation interne d'une société ou d'un cabinet par l'étude des informations publique (réseaux sociaux notamment)
- **hameçonnage (*fishing*) :** grâce à l'ingénierie sociale, le pirate se fait passer pour un tiers par téléphone, courriel ou sur les réseaux sociaux afin d'obtenir des données, un accès...

En pratique, la sécurisation

- Mots de passe
  - Au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux)
  - 1 service = 1 mot de passe
  - Pas de lien personnel : nom de société, date de naissance, de mariage, prénoms des enfants….
  - Modification systématique et au plus tôt des mots de passe par défaut
  - Renouvellement fréquent : 90 jours pour les données sensibles
  - Ne pas les enregistrer dans sa messagerie, dans un fichier, sur un papier…
  - Configuration logiciels et navigateurs : pas de mémorisation des mots de passe
  - Utiliser dès que possible la double authentification
  - Ne jamais communiquer son mot de passe à un tiers : au besoin lui communiquer un mot de passe temporaire, changé pour l'occasion
  - Si un mot de passe est utilisé sur plusieurs services, le changer partout en cas de risque de compromission

En pratique, la sécurisation

Bref, c’est impossible à réaliser en pratique !

Deux solutions :

- Utiliser un gestionnaire de mots de passe (ex: KeePass)
- Avoir des séries de mots de passe personnels et professionnels à plusieurs niveaux

Il est également fortement recommandé d’activer dès que possible la double authentification limitant les risques de piratage

En pratique, la sécurisation

2- Sécuriser les périphériques

Vos données et courriels professionnels sont accessibles aujourd'hui partout : téléphone, tablette, ordinateur, serveur,…

Il faut donc les sécuriser

- Utiliser un câble antivol (type Kensington)
- Ne pas laisser traîner ses périphériques
- Utiliser un mot de passe, un PIN, un schéma, la biométrie pour le déverrouillage
- Activer systématiquement la localisation et l'effacement à distance
- Limiter les accès physiques à des tiers
- Éviter de traiter de données sensibles dans un lieu public (café, TGV, InOUI)

En pratique, la sécurisation

3) Sécuriser les données

- Activer les outils de chiffrement intégrés de tous vos périphériques
- Utiliser des logiciels chiffrant créant des partitions chiffrées comme VeraCrypt (Windows, MacOs, Linux)
- S’assurer que les logiciels métiers prennent en compte cet impératif de sécurité

En pratique, la sécurisation

4) Sécuriser les communications

- Préférer le câble réseau au wifi
- Si wifi, utiliser le WPA2 (avec précaution) et éviter les réseaux ouverts
- En déplacement, en cas de réseau wifi ouvert (et même si WPA2), utiliser un VPN pour établir un tunnel sécurisée vers son cabinet
- Utiliser sinon la ce partage de connexion du téléphone
- Vérifier l'utilisation du SSL  sur la page de connexion à un service et l'identité du site en cliquant sur 
- Chiffrer vos communication dès que possible (GPG pour les courriels)

En pratique, la sécurisation

4) Limiter les accès aux données

- Cloisonner les accès permet de s'assurer que seules les données nécessaires sont accessibles par une personne donnée
  - Ex : le commercial n'a pas besoin d'avoir accès au numéro de sécurité sociale de la secrétaire, seul les RH en ont besoin
- Identifier chaque acteur par un identifiant unique et journaliser tous les accès
  - Ex : pas d'identifiant partagé entre tous les commerciaux, mais un login par salarié

IV. COMMENT SAUVEGARDER ?

1) Le Plan de Continuité d’Activité
2) Caractéristiques d’une sauvegarde
3) Automatisation des sauvegardes
4) Le cloud est-il une sauvegarde ?
5) La sauvegarde du téléphone

En pratique, la sauvegarde

Le Règlement Général Européen de Protection des Données Personnelles impose la mise en place d'un Plan de Continuité d'Activité qui doit prévoir notamment :

- Article 32 c) : La restauration des données
  - *Rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;*

En pratique, la sauvegarde

1) Le Plan de Continuité d'Activité

Il s'agit d'anticiper afin de garantir la survie du cabinet après un sinistre important touchant le système informatique (on peut y ajouter les données papier)

Objectif : redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

Il faut donc savoir ce qu'il faut faire en cas de virus, d'incendie, d'inondation, d'effraction, de vol…

En pratique, la sauvegarde

2) Caractéristiques d'une bonne sauvegarde

Pour que la sauvegarde soit utile en cas de problème, il faut qu'elle soit :

- Fréquente
- Complète
- Chiffrée
- Externe
- Déconnectée
- Incrémentielle

II. L’EVENTUEL DELEGUE A LA PROTECTION DES DONNEES PERSONNELLES (DPO)

1) Quand est-il nécessaire ?
2) Quel est son rôle ?
3) Qui choisir ?

En pratique, le DPO

1- Quand est-il nécessaire ?

- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées;

- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

En pratique, le DPO

2- Quel est son rôle ?

- Il est le pilote de l'application du RGPD au sein de l'entreprise
- Il tient à jours le registre des traitement et est associé à tout ce qui touche les données personnelles : développements informatiques, modification contractuelles…
- Il ne remplace pas le chef d'entreprise qui reste le responsable des traitements

En pratique, le DPO

3- Qui choisir ?

- Le DPO peut être un salarié ou quelqu'un d'extérieur à la société, y compris un avocat.
- Il doit être en mesure d'exercer son rôle sans interférence, et doit donc être indépendant dans ses fonctions
- Il est soumis à une obligation de confidentialité
- Il peut exercer d'autres fonctions dans la société
- Dans le cas de l'avocat DPO, il ne pourra par contre pas assister la société en tant qu'avocat pour toute procédure juridictionnelle relative aux données personnelles

En pratique, le DPO

Si la désignation d'un DPO n'est pas toujours obligatoire, il est néanmoins important qu'une personne au sein de l'entreprise ou de l'association soit le pilote de la conformité au RGPD, le référent interne.

Qu'il soit ou non DPO, cette personne peut bien entendu faire appel à un conseil extérieur en cas de difficulté ou de question

II. EN PRATIQUE, LES TRAITEMENTS DE DONNEES DANS LE CADRE DU CRJ

1) Les traitements réalisés par le CRJ
2) Les traitements réalisés par les Districts

En pratique, les traitements du CRJ

Le Centre Rotarien pour la Jeunesse permet une mise en commun des moyens des différents Districts dans la participation au programme Youth Exchange du Rotary International

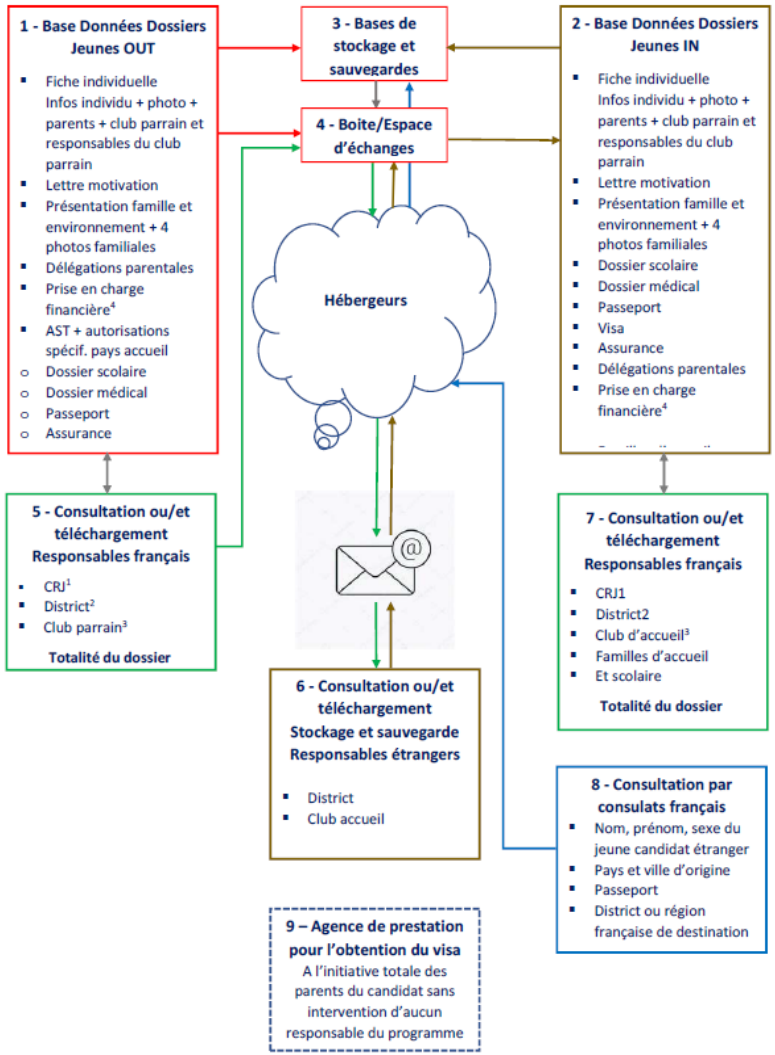
En pratique, les traitements du CRJ

Traitements réalisés par le CRJ

- Les pré-inscriptions par les jeunes français
- Les inscriptions par les jeunes étrangers pour accéder à l'intranet
- Les inscriptions par les districts étrangers souhaitant accéder aux données des jeunes français (non existant à ce jour)

En pratique, les traitements du CRJ

Traitements réalisés par le CRJ



En pratique, les traitements du CRJ

Traitements réalisés par chacun des districts, le CRJ n’étant alors que le sous-traitant

Les dossiers après validation par les districts

En pratique, les traitements du CRJ

Mesures à prendre par le CRJ

- Audit des pratiques (en cours)
- Rédaction du registre des traitements
- Audit des contrats
  - Contrats de travail pour confidentialité
  - Contrat des prestataires techniques
- Modification éventuelle des pratiques
- Modification de la documentation
  - Relation entre le CRJ et les districts
    - Règlement intérieur de l'association
    - Bulletin d'adhésion des districts
  - Relations entre le CRJ et les jeunes français
    - Formulaire d'inscription des jeunes français sur le site du CRJ
  - Relations entre le CRJ et les jeunes étrangers
    - Formulaire d'inscription des jeunes étrangers à l'intranet du CRJ
  - Relations entre le CRJ et les districts étrangers
    - Formulaire d'inscription à l'intranet du CRJ

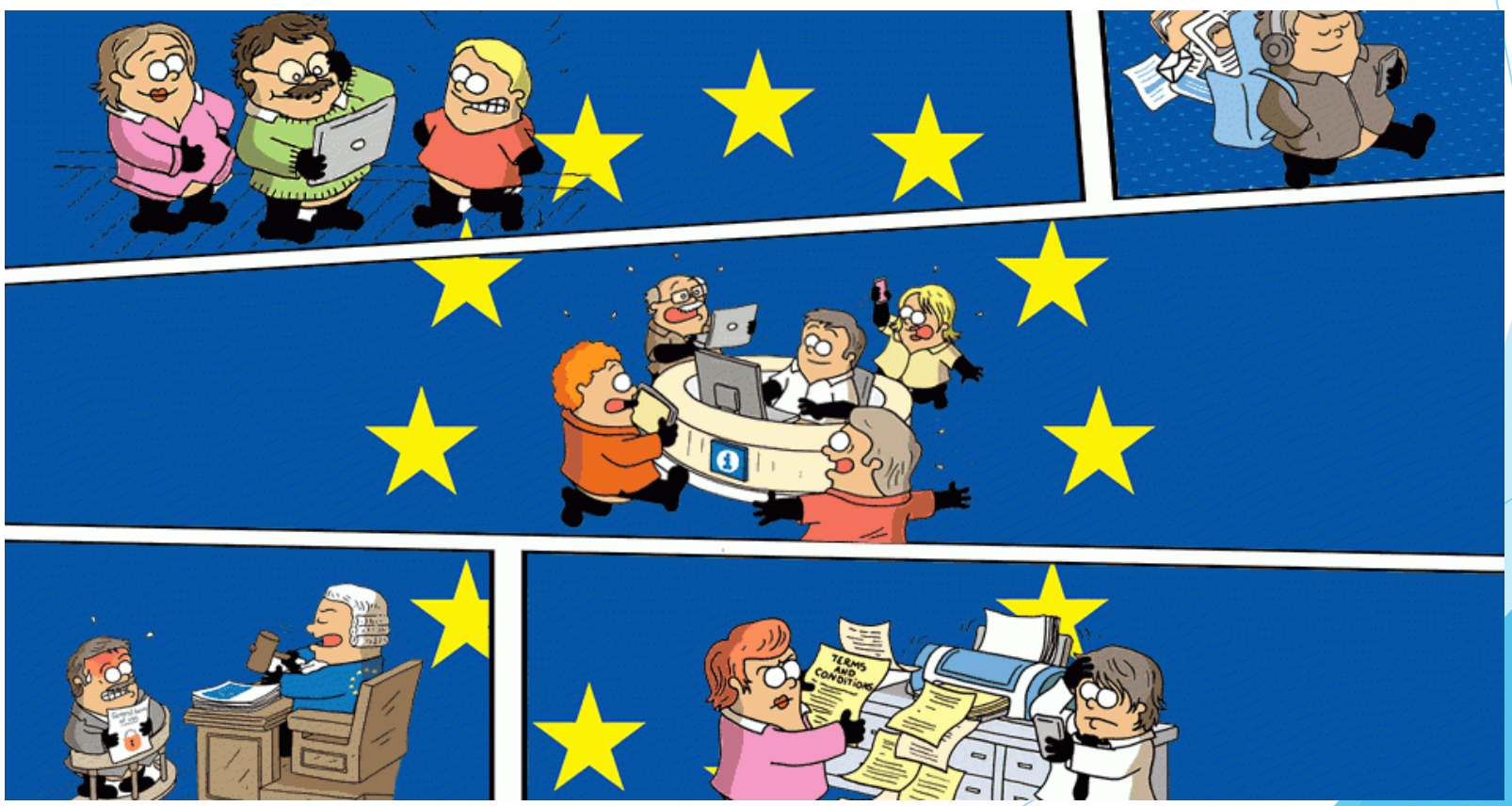
En pratique, les traitements du CRJ

Mesures à prendre par chacun des Districts

- Audit des pratiques locales
- Rédaction du registre des traitements
- Audit des contrats
  - Contrats de travail pour confidentialité
  - Contrat des prestataires techniques (dont le CRJ)
- Modification éventuelle des pratiques
- Modification de la documentation, en collaboration avec le CRJ
  - Formulaire de recueil des données des jeunes

La CNIL

De nombreuses information sont également à retrouver sur le site de la CNIL



MERCI

Je suis bien entendu à votre disposition pour vous accompagner dans la mise en conformité de votre structure avec le RGPD

Hadrien CHOUAMIER

Avocat

24 avenue de Moka – 35400 SAINT MALO

avocat@chouamier.fr

02.57.64.00.55