Le Règlement Général sur la Protection des Données (RGPD)

Quels impacts sur vos activités scientifiques au quotidien ?

1. Cadre général

2. Informer devient obligatoire

3. Mise en conformité

4. Retours d'expériences

17 et 18 Octobre 2023

CC BY NC ND

Chargées de Mission Qualité, Responsables Opérationnelles des Données (RDO), Correspondantes DPO
AUBERT Magali : magali.aubert@INRAE.fr & MORIN Pascale : pascale.morin@cirad.fr
https://umr-moisa.cirad.fr/l-unite/qualite-et-conformite-des-donnees

Présentez-vous en quelques mots :

- Votre corps de métier
- Avez-vous déjà réalisé une mise en conformité ?
  - Si non, allez-vous être amenés à en réaliser une ?
- Travaillez-vous avec des partenaires non Européen ?
- Travaillez-vous avec des partenaires privés ?

→ Quelles sont vos attentes, en quelques mots, vis-à-vis de cette formation ?

Les questions auxquelles vous serez en mesure de répondre à l’issue de la formation:

1. Le RGPD dans votre vie quotidienne :

- En tant que citoyen, dans quel cas pourrait-on vous enquêter sans vous demander votre consentement ? Cela signifie t’il que votre participation est obligatoire ?
- Si vous regrettez d’avoir participé à une enquête, savez-vous comment faire pour demander la suppression de vos données ?
- Pensez-vous être une personne vulnérable ? Qui, selon vous, peut être considéré comme une personne vulnérable ?

Les questions auxquelles vous serez en mesure de répondre à l’issue de la formation:

2. Le RGPD dans le cadre de vos recherches :

- Savez-vous dans quel cas une demande de mise en conformité doit être faite ?
- Dans quel cas êtes-vous responsable ? Responsable de quoi ? Responsable de toutes les données collectées et/ou traitées dans le cadre d’un projet de recherche ?
- Si vous travaillez avec des collègues localisés hors Europe, savez-vous ce que cela implique en termes de mise en conformité ?
- Qui est votre DPO ?

Droits fondamentaux :

1. *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »* - L'article nº 8 de la Convention européenne des droits de l'homme

2. Droit à la protection des données à caractère personnel : droit fondamental inscrit en 2000 dans la Charte des Droits Fondamentaux de l’Union Européenne

https://www.cnil.fr/fr/reglement-europeen-protection-donnees#haut

Qu’est ce que le RGPD ?
Pourquoi sommes-nous concernés ?

Le RDPD (Règlement Général sur la Protection des Données) est une règlementation européenne applicable depuis le 25 mai 2018. L’objectif est d’harmoniser, au niveau européen, les règles juridiques.

Ce règlement a pour but de renforcer la protection des **données à caractère personnel**. Elle s’applique à toute société présente dans **l’Union Européenne** et pour toute société extra européenne ayant à traiter des données de citoyens européens.

Protection des données dans le monde

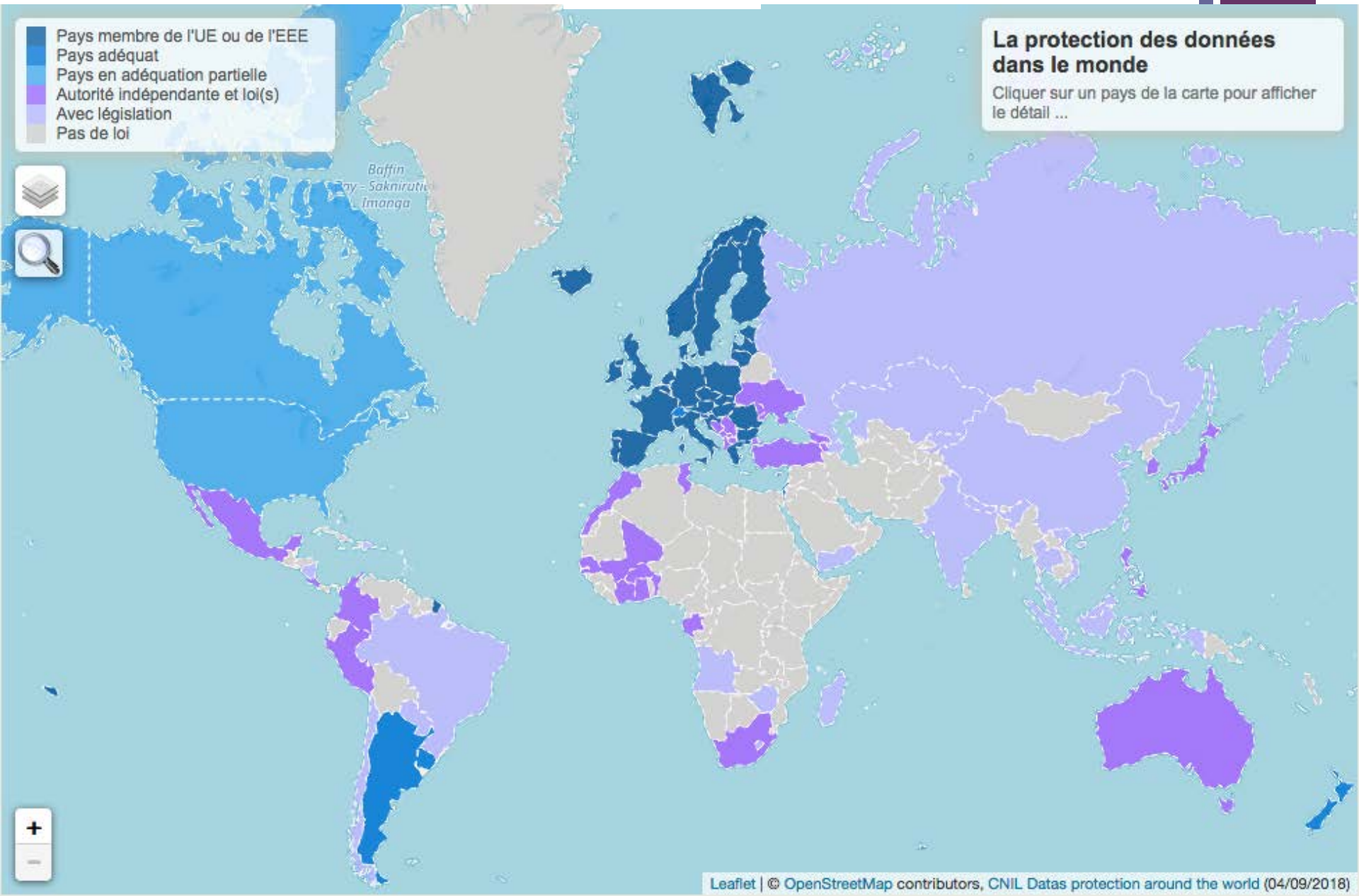
La CNIL a établi une carte internationale qui permet de visualiser les différents niveaux de protection des données des pays dans le monde

Il existe des niveaux de protection spécifique par pays : législation ou autorité de protection des données personnelles

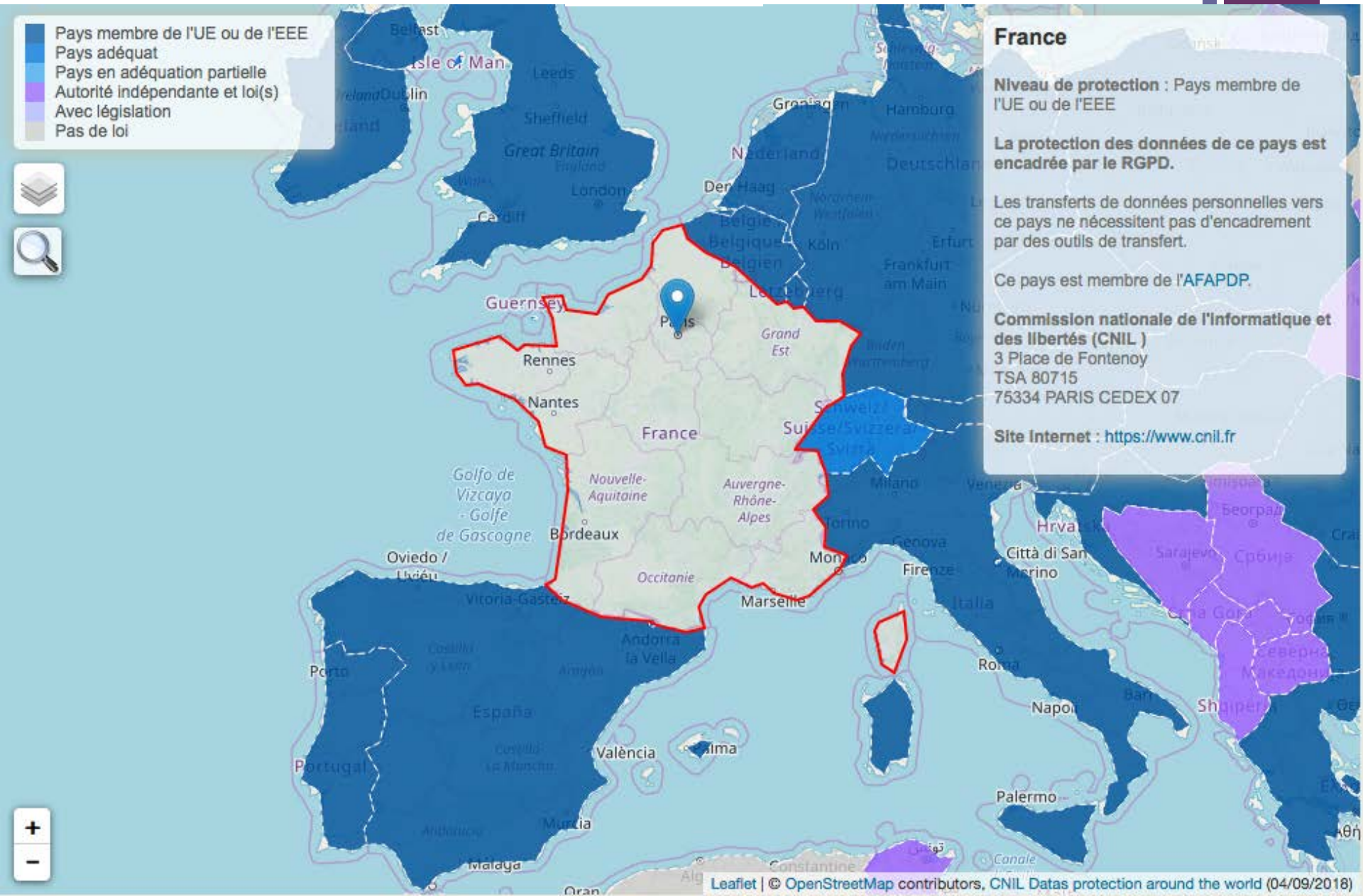
Lien : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

La CNIL vous accompagne : https://www.cnil.fr/fr/le-rgpd-cest-maintenant-les-changements-retenir-et-les-outils-pour-bien-se-preparer

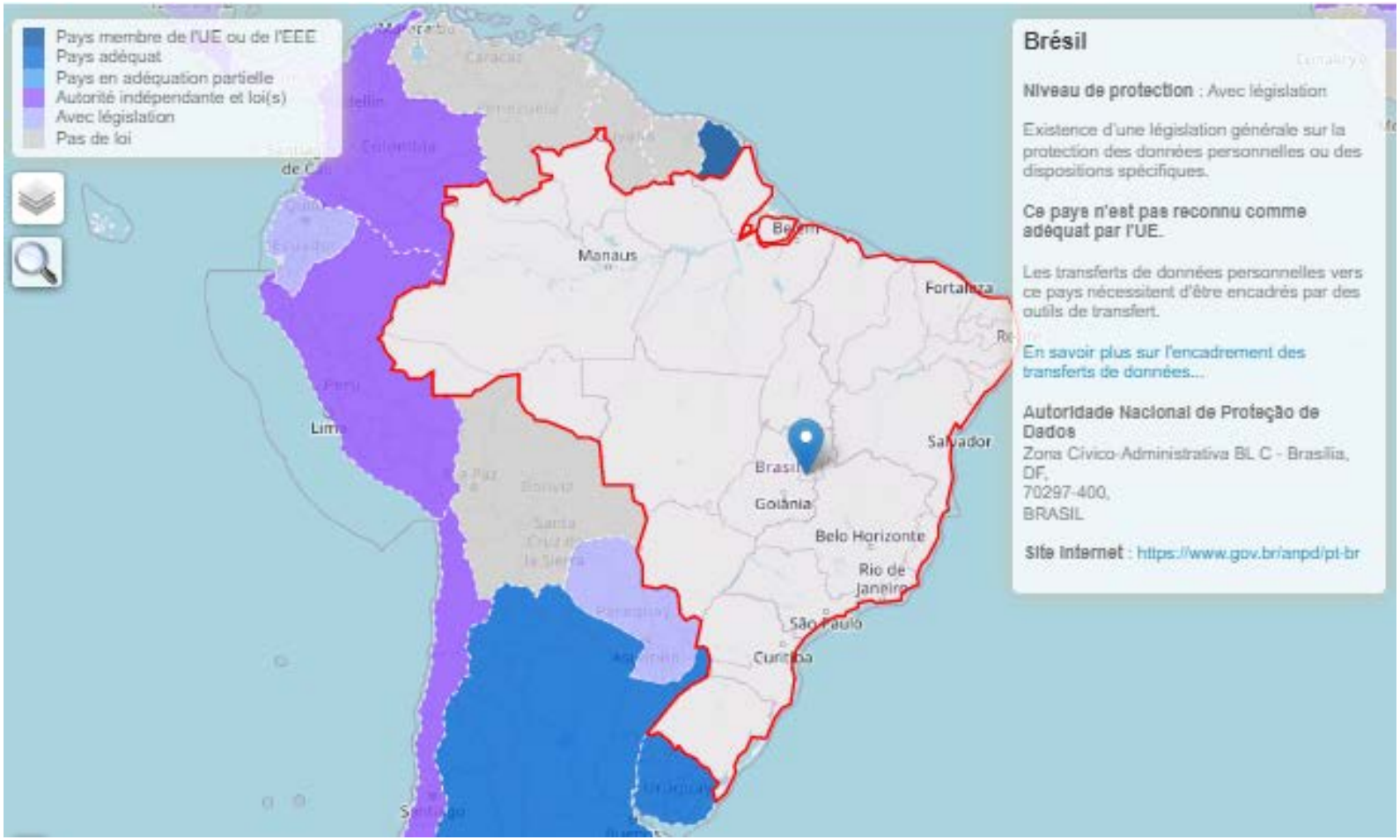
Protection des données dans le monde



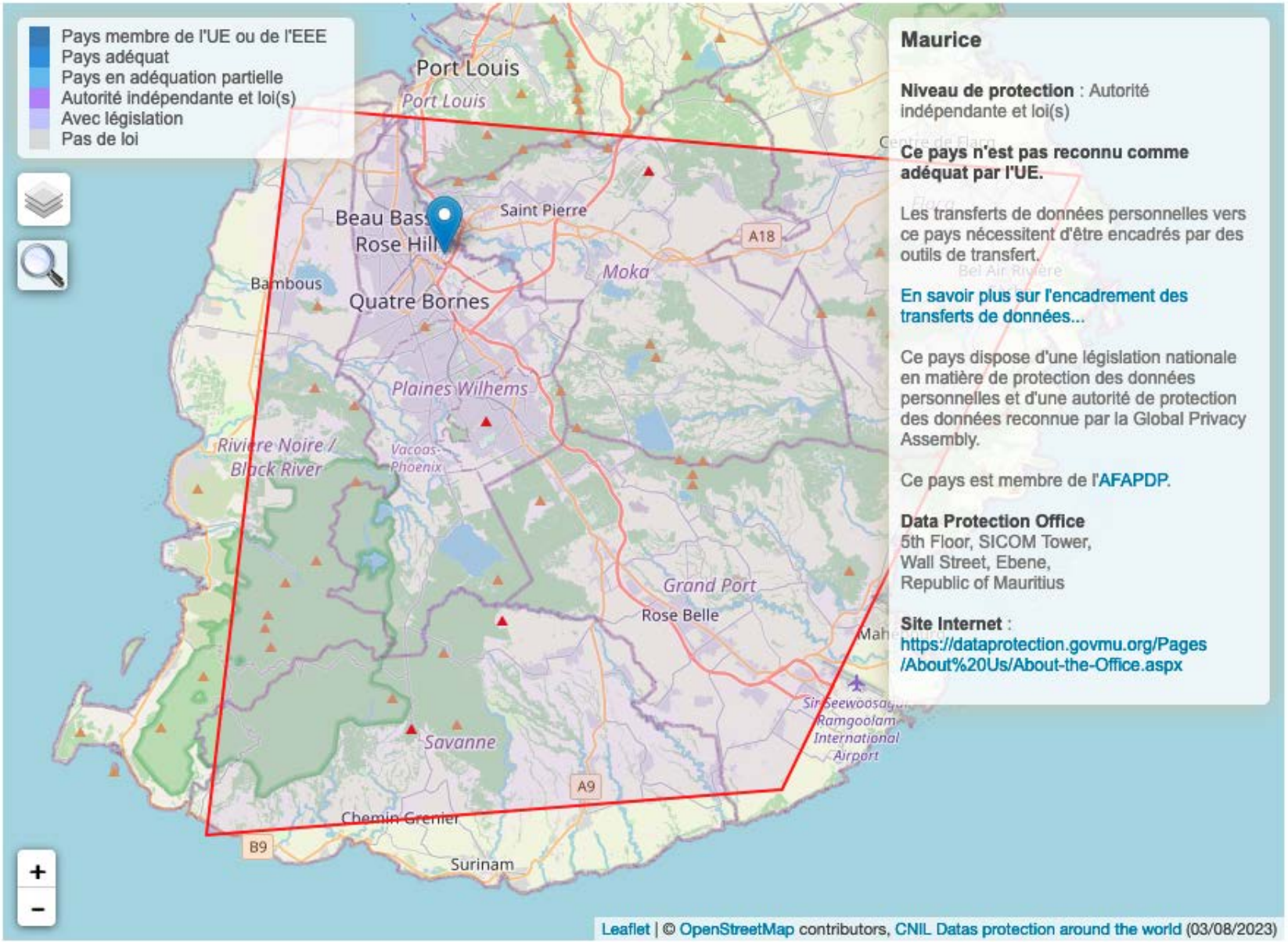
Protection des données en France



Protection des données en France



Protection des données en France



Maurice

Niveau de protection : Autorité indépendante et loi(s)

Ce pays n'est pas reconnu comme adéquat par l'UE.

Les transferts de données personnelles vers ce pays nécessitent d'être encadrés par des outils de transfert.

En savoir plus sur l'encadrement des transferts de données...

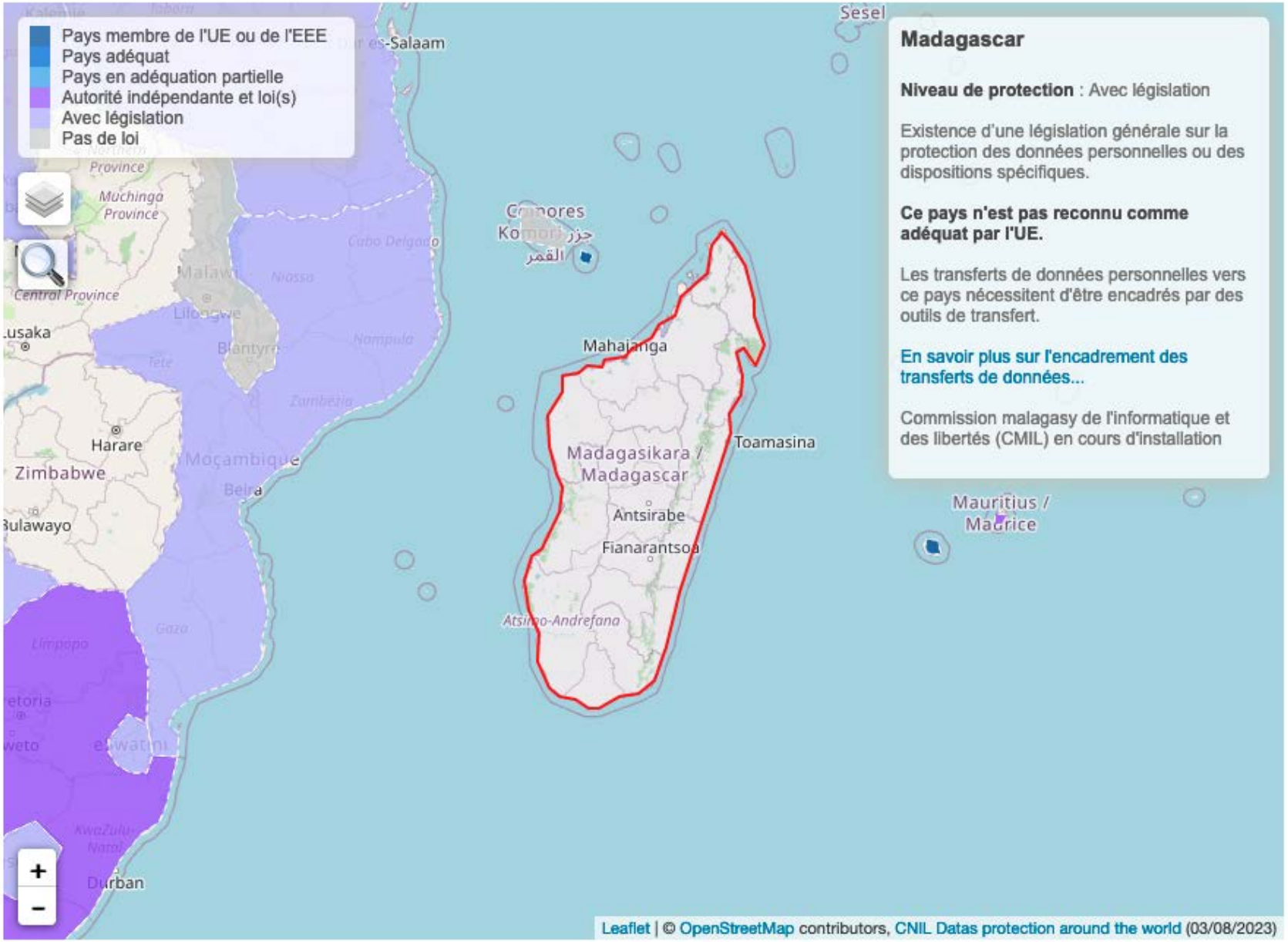
Ce pays dispose d'une législation nationale en matière de protection des données personnelles et d'une autorité de protection des données reconnue par la Global Privacy Assembly.

Ce pays est membre de l'AFAPDP.

Data Protection Office
5th Floor, SICOM Tower,
Wall Street, Ebene,
Republic of Mauritius

Site Internet :
https://dataprotection.govmu.org/Pages/About%20Us/About-the-Office.aspx

Protection des données en France



En cas de transfert des données hors UE :

- En informer les personnes enquêtées dans le cadre de la fiche d'information
- Si le pays destinataire a un niveau de protection adéquate (Cf. https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde)
- Pour les pays « non adéquat » :
  - USA : https://www.cnil.fr/fr/le-privacy-shield
  - Autres pays : Utiliser des clauses contractuelles adoptées par la Commission Européenne https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne

Qu'est ce que le RGPD ?
Pourquoi sommes-nous concernés ?

Les données à caractère personnel concernées sont celles collectées en Europe et hors UE mais qui sont, dans la plupart des cas, **traitées, sauvegardées et/ou archivées en Europe.**

Ex. 1 : Un chercheur-partenaire collecte des données dans un pays non Européen et un chercheur localisé en France les exploite

Ex. 2 : Un chercheur CIRAD expatrié hors UE collecte, traite, sauvegarde ces données depuis son institution d'affectation

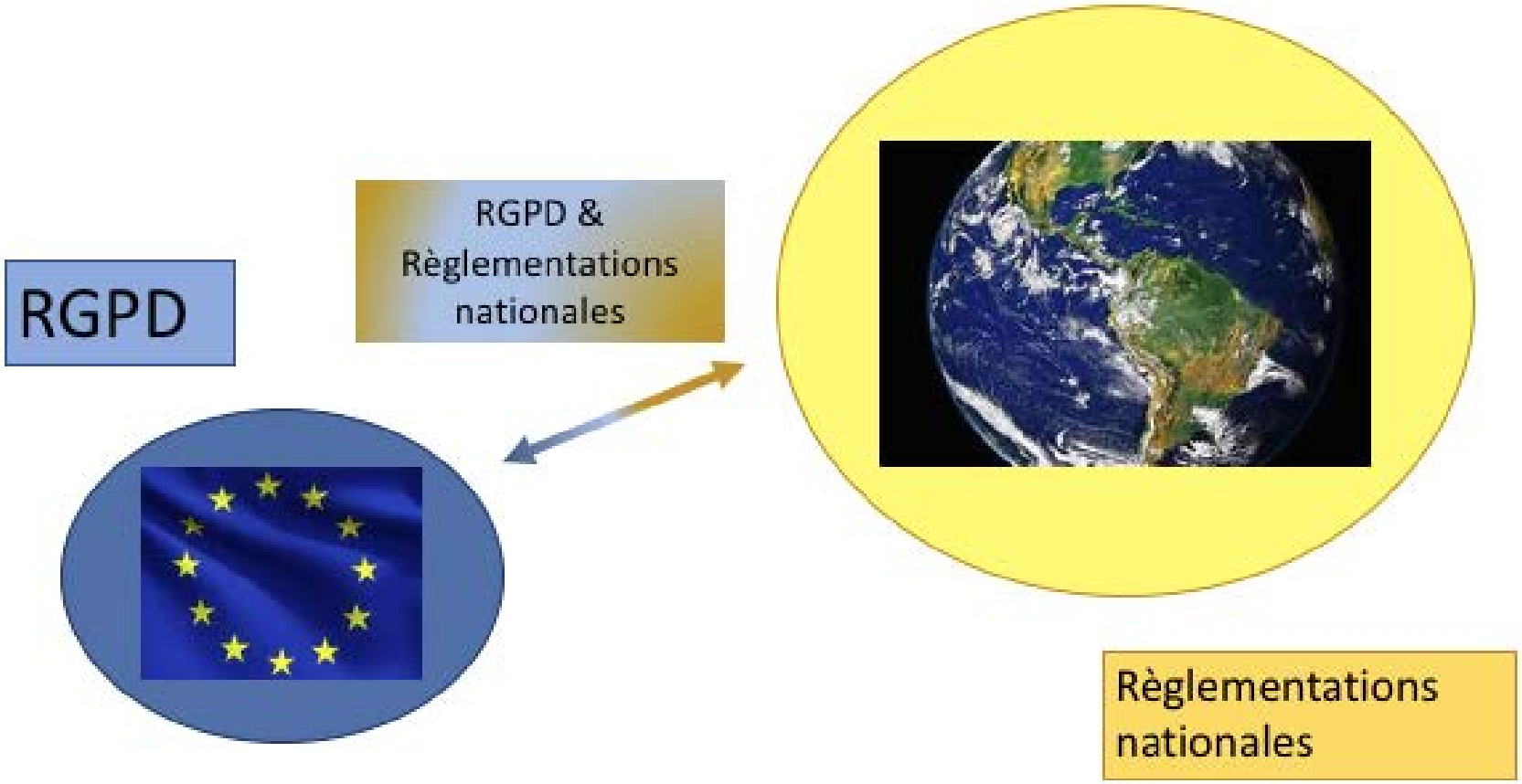
Ex. 3 : Un chercheur américain travaille sur des citoyens européens

Ex.4 : Un chercheur CIRAD expatrié hors UE encadre un doctorant qui travaille avec du matériel informatique local. Les données sont collectées, traitées, sauvegardées localement

Dans la plupart des cas, les données traitées dans nos unités de recherche sont soumises au RGPD

RGPD

Une vision simplifiée de la mise en conformité avec les différentes exigences règlementaires



Vos travaux de recherche portent sur des personnes morales ?

- Votre recherche n’entre pas dans le cadre du RGPD
- Vous êtes soumis à la loi 51-711 sur le secret statistique
  - Vous devez garantir la confidentialité des données et l’anonymat des personnes interrogées

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000888573&categorieLien=cid

Vos travaux de recherche portent sur des exploitations agricoles ?

Une exploitation agricole est une personne morale. Votre recherche n’est à priori non soumise au RGPD !

Souvent 1 exploitation = 1 personne (l’exploitant) ou 1 couple

Du fait de la taille de cette entité morale, les données relatives aux exploitations agricoles sont soumises au RGPD.

Le RGPD
Cadre général

1. Données à caractère personnel
2. Données sensibles
3. Analyse d'Impact relative à la Protection des Données (AIPD)
4. Consentement
5. Traitement
6. Responsable du traitement

- **Données à caractère personnel** :

« Toute information se rapportant à une personne physique identifiée ou identifiable; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, ***directement ou indirectement****, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » -* Article 4 du RGPD

Pour savoir si les données sont anonymes, trois types de critères sont à prendre en compte :

- **L’individualisation** : est-il toujours possible d’isoler un individu ?
- **La corrélation** : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?
- **L’inférence** : peut-on déduire de l’information sur un individu ?

En SHS, dans 97% des cas on est en mesure de lever l’anonymat en couplant vos données avec d’autres bases.

La pseudonymisation est une technique qui consiste à remplacer une donnée à caractère personnel comme le prénom par un pseudonyme ou un numéro. Cette technique permet la ré-identification ou l'étude de corrélations en cas de besoin particulier. Les données pseudonymisées sont donc considérées comme des données indirectement personnelles. A ce titre, elles sont donc soumises à la protection du RGPD.

- **Données sensibles** :

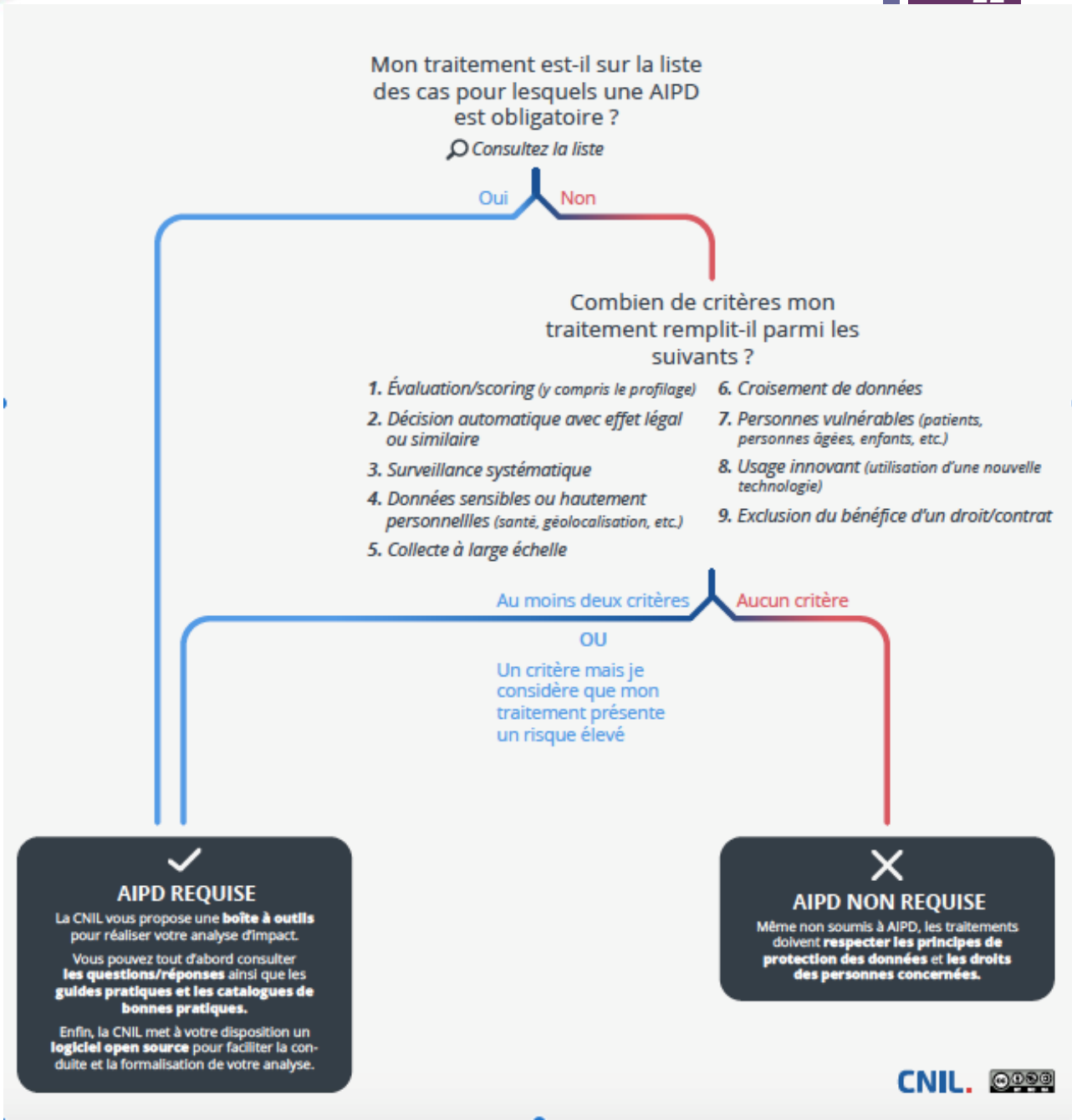
Origine raciale ou ethnique, opinion politique, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques aux fins d'identifier les personnes physiques de façon unique, santé, vie sexuelle ou orientation sexuelles, à des condamnations pénales ou infractions, numéro d'identification national unique

Analyse d'Impact relative à la Protection des Données (AIPD) :

La réalisation d'une AIPD est obligatoire quand le traitement est «***susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques***» - Article 35, paragraphe 1, illustré par l'article 35, paragraphe 3, et complété par l'article 35, paragraphe 4. Article 36.

AIPD : Outil de responsabilisation et de conformité qui permet de garantir les principes du RGPD de façon opérationnelle.

Source : https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia



Définitions
Les termes clefs à connaitre

Critère	Définition	Référence aux articles et/ou aux considérants RGPD	Plus simplement	Exemple
C1. Evaluation / scoring	*"Aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnel, sa fiabilité ou con comportement, ou sa localisation et ses déplacements"*	Considérants 71 et 91	Créer des profils d'individus / profilage de façon automatique sans intervention humaine	Analyse automatique d'une demande de crédit faite en ligne
C2. Prise de décision automatisée avec effet juridique ou effet similaire significatif	*"Des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire"*	Art. 35, paragraphe 3, a	Effets sur vos droits juridiques	Analyse de vos droits (CAF)
C3. Surveillance systématique	Traitement utilisé pour observer, surveiller ou contrôler les personnes concernées *"la surveillance systématique d'une zone accessible au public"*	Art. 35, paragraphe 3, c	Les personnes concernées ne savent ni qu'ils sont surveillés ni par qui et ils ne peuvent pas s'y soustraire	Surveillance d'un quartier à risque / manifestation
C4. Données sensibles ou données à caractère hautement personnel	Catégories particulières de données à caractère personnel (Art. 9) ainsi que des données à caractère personnel relatives aux condamnations pénales ou aux infractions (Art. 10)	Art. 9 et 10	Données sensibles (sens commun) ayant un impact sur l'exercice d'un droit fondamental où leur violation aurait une incidence grave sur la vie quotidienne des personnes	Dossiers médicaux contenus dans un hôpital / Condamnations pénales

Définitions
Les termes clefs à connaitre

Critère	Définition	Référence aux articles et/ou aux considérants RGPD	Plus simplement	Exemple
C5.Données traitées à grande échelle	Grande échelle : Nb de personnes Volume de données Durée ou pertinence du traitement Etendue géographique	Considérant 91	NB : "grande échelle" non définie explicitement dans le RGPD	Données collectées sur les réseaux sociaux
C6. Croisement ou combinaison d'ensemble de données	Réaliser des croisements ou combinaisons qui outrepasseraient les attentes de la personne concernée		Nouvelle finalité de la recherche	Enquête 1: mon poids comme indicateur de santé Enquête 2 : mes activités physiques pour le développement d'infrastructures
C7. Données concernant des personnes vulnérables	Les enquêtés sont dans l'incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits	Art. 8	Les personnes nécessitant une protection particulière	Enfants, personnes souffrant de maladie mentale, demandeurs d'asile, personnes âgées, salariés…
C8. Utilisation innovation ou application de nouvelles solutions technologiques ou organisationnelles	Les conséquences personnelles et sociales du déploiement d'une nouvelle technologie peuvent être inconnues	Art. 35, Considérants 89 et 91		Applications sur internet
C9. Traitements en eux-mêmes qui *"empêchent les personnes considérées d'exercer un droit ou de bénéficier d'un service ou d'un contrat"*	Opérations visant à autoriser, modifier ou refuser l'accès à un service ou à la conclusion d'un contrat	Art. 22, Considérant 91	Profilage	

Définitions
Les termes clefs à connaitre

AIPD = EIPV = PIA = DPIA

Analyse d'Impact relative à la Protection des Données (AIPD)

Etude d'Impact sur la Vie Privée (EIPV)

Privacy Impact Assessment (PIA)

Data Privacy Impact Assessment (DPIA)

Niveau 1 : aucune incidence sur les individus (nom de l'individu)

Niveau 2 : peu d'importance (nb enfants)

Niveau 3 : surmontable avec difficultés pour les individus (sexe du conjoint en France)

Niveau 4 : peut entraîner la mort de la personne en cas de divulgation de l'information (sexe du conjoint dans certains contextes)

Pour se renseigner : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Liste des traitements nécessitant une AIPD : https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf

Pour réaliser une AIPD, un logiciel PIA de la CNIL est à votre disposition: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

- **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. »* Articles 5 à 11 du RGPD

Le traitement couvre l'ensemble des étapes du processus du cycle de vie de la donnée

- Responsable du traitement :

*« Le **responsable** d'un **traitement** de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. »* (CNIL)

« Le Responsable de traitement prend les mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée »

Dans le cadre des unités de recherche,

le responsable du traitement est le Directeur d'Unité

Notion de responsabilité conjointe :

Avant le RGPD, seul un des partenaires pouvait être responsable de la bonne application de la règlementation. Aujourd'hui, la co-responsabilité permet aux partenaires d'être juridiquement responsables ensemble de la mise en œuvre de la règlementation. Les partenaires doivent déterminer ensemble les finalités et les moyens à mettre en œuvre,

Il est alors indispensable de répondre aux questions clés suivantes :

Qui fera la déclaration de mise en conformité ? Qui accède aux données à caractère personnel ? Comment est garanti la sécurisation des données ? Etc..

Il est primordial d'anticiper ces co-responsabilités entre partenaires du projet de recherche. Une clause spécifique devra être rédigée dans le contrat de partenariat. (à noter qu'un avenant est toujours possible). Les partenaires n'ayant pas besoin d'avoir accès aux DCP peuvent ne pas être considérés comme co-responsable de traitement.

Le processus de mise en conformité varie selon le statut juridique des partenaires.

- Il n’y a pas qu’un seul responsable du traitement

Pensez à identifier les responsables conjoints

Ils sont responsables devant la loi :

- Partenaires du projets
- Responsable de WP
- Coordinateur du projet

Indiquer dans les clauses contractuelles « Qui est responsable de quoi »

- **Consentement** :

  « Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair que des données à caractère personnel la concernant fassent l'objet d'un traitement » - Articles 4, 7 et 8 du RGPD.

- **Exigences règlementaires** :

  - Un consentement compréhensible par tous, formulé en des termes clairs et simples
  - Le responsable du traitement des données est responsable de la conservation des preuves de consentement
  - Obligation de conserver les preuves (écrites, électroniques, audio) des consentements. Attention : des cases à cocher ne peuvent pas permettre de recueillir un consentement
  - L'enquêté doit pouvoir retirer son consentement aussi facilement qu'il le donne

- Une finalité de la recherche unique :

  N’utiliser les données que pour les finalités dont la personne a été informée

  Prévoir dès la fiche de consentement la possibilité de leur réutilisation pour de futurs projets ou ne pas les réutiliser

  Ne pas collecter sur internet. Elles sont collectées dans le cadre d’une autre finalité. La collecte sera qualifiée de « déloyale » ! Sauf dans le cas de bases de données publiques pour lesquelles cette réutilisation est encadrée

- Les finalités, c’est-à-dire le but du traitement, doivent être définies en amont et indiquées dans la fiche d’information et le formulaire de consentement

Le RGPD & nous

1. Les principes sous la responsabilité du responsable du traitement
2. Transformer les principes en actions
3. Cadre règlementaire appliqué aux Unités de Recherche
4. Obligation de tenir, en interne, un « dossier de conformité »

Les principes sous la responsabilité du responsable du traitement

Articles 5 a 11 du RGPD

Le responsable de traitement doit veiller à ce que les données soient :

1. Traitées de manière **licite**, **loyale** et **transparente** au regard de la personne concernée

2. Traitées pour une **finalité déterminée**, **légitime** et **limitée** (Toute autre utilisation des données est interdite)

3. Collectées en respectant les principes de proportionnalité et pertinence de la recherche (Minimisation des données : Ne pas vouloir tout collecter)

Les principes sous la responsabilité du responsable du traitement

Article 5 du RGPD

Le responsable de traitement doit veiller à ce que les données soient :

4. Conservées
   - Avec une durée limitée et une identification stable des enquêtés
   - Dans le cadre de mesures techniques et organisationnelles établies pour garantir leur sécurité

5. Sécurisées selon des moyens appropriés et en adéquation avec leur niveau de risque (Cf. AIPD)

6. « Accessibles » aux enquêtés qui doivent pouvoir les modifier, supprimer… (articles 15 à 20)

Conservation des données

Les données à caractère personnel ne peuvent pas être conservées de façon illimitée.

Le chercheur doit définir une durée dite d'utilité et le mentionner aux personnes concernées.

Recommandation dans le cadre d'un projet de recherche :

Durée de conservation = Durée du projet + 5/10 ans

Cependant, elles peuvent être conservées à des fins archivistiques dans l'intérêt publique, à des fins scientifiques ou historiques (Art. 5).

Lorsque des jeux de données anonymisées suffisent pour les objectifs de la recherche, il faut anonymiser les données dès que possible et ne partager que des données anonymes.

Que faire des vos données à la fin de la durée d'utilité ?

A la fin de la durée d'utilité, vous devez :

- **Détruire** les données → voir procédure institutionnelle (cf.DPO)

  Il s'agit de détruire de manière irréversible, sécurisée et confidentielle des documents ou des données dont la durée de conservation est arrivée à échéance, qui n'ont plus d'utilité pour les unités, et qui n'ont pas d'intérêt scientifique, juridique ou historique pour l'Institut.

- Conserver à des fins archivistiques dans l'intérêt publique, à des fins scientifiques ou historiques (art 5) → vous devez **anonymiser** les données. Les individus ne doivent plus être identifiables directement ou indirectement

→ **dans tous les cas, vous devez le notifier à votre DPO**

Durée de conservation des données :
https://intranet-rgpd.cirad.fr/je-mene-un-sondage-et-ou-une-enquete/1-informez-les-personnes

Cadre règlementaire
Appliqué aux Unités de Recherche

Cadre règlementaire	En ce qui nous concerne
1. Le **renforcement des droits des personnes**	1. Dans le cadre de nos travaux, les personnes sont les enquêtés: individu, entreprise…
2. Le renforcement des **droits d'accès**, **de rectification et « d'oubli » -** Articles 15 à 21 du RGPD	2. L'enquêté a le droit d'obtenir du responsable de traitement qu'il modifie ou efface des données le concernant
3. L'obligation pour le **responsable de traitement** de rendre compte de sa conformité - Article 24 du RGPD	3. Déclarer le traitement au registre, établir un PGD (Plan de Gestion des Données)
4. La protection des données doit être garantie dès le démarrage de l'enquête - Articles 25 et 30 du RGPD	4. Le traitement des données personnelles doit être anticipé avant même la collecte des données c'est-à-dire au moment du montage du projet

Cadre règlementaire	En ce qui nous concerne
5. Obligation d'avoir un **système d'information sécurisé** – Article 32 du RGPD	5. Le dossier de conformité doit montrer que le système d'information permet de garantir la sécurité des données traitées, pour le niveau de risque identifié. ▪ Responsabilité institutionnelle & politique d'établissement (Direction des Systèmes d'Information) ▪ Responsabilité individuelle : mise en œuvre de bonnes pratiques, suivi du process interne de conformité dans le cadre d'un projet

6. Obligation d'informer de la fuite des données : dès qu'elle est identifiée, toute fuite de données doit être signalée à **l'autorité nationale de protection (la CNIL en France)** dans les meilleurs délais (72h) – Articles 33 et 34 du RGPD	6. Exemple: vol d'ordinateur (bureau ou domicile), problème de connexion non sécurisées, problème de confidentialité des données
	▪ Consigner l'information (origine de la fuite, nb d'enregistrements concernés…)
	▪ Informer l'équipe DPO (au Cirad)
	▪ Décrire les conséquences probables
	▪ Indiquer les moyens pris pour :
	  ▪ Eviter que l'incident ne se reproduise
	  ▪ Limiter les conséquences de cette fuite

Cadre règlementaire

7. Obligation de désigner un **Délégué à la Protection des Données** (DPO) et de définir ses fonctions et ses missions – Articles 37 à 39 du RGPD

Attention, le DPO institutionnel n'est compétent que pour les traitements mis en oeuvre sous la responsabilité de l'institution, ce qui n'est pas toujours le cas lorsque l'organisme n'est pas leader du projet

En ce qui nous concerne

7. Des DPO Institutionnels :
   - Au Cirad : l'équipe DPO, assurée par Lexagone (Margaux Bourgeois, Laura Martini) : dpo@cirad.fr

Attention : le DPO veille au respect du règlement, conseille, alerte la direction.

Il n'est pas responsable des non-conformités, chaque acteur traitant des données à caractère personnel doit rendre compte de la conformité des traitements qu'il opère.

Le DU doit *« associer le DPO (…) à toutes les questions relatives à la protection des données à caractère personnel »* Article 38 du RGPD

Rôle d'un DPO

- Informer et conseiller les instituts de recherche et les agents,
- Contrôler la conformité des activités internes avec les textes légaux en matière de données personnelles,
- Interlocuteur entre les instituts de recherche et une autorité de contrôle nationale, comme la CNIL,
- Au sein des instituts et des unités, il doit bénéficier d'un soutien organisationnel, financier et humain,
- Au niveau européen, il est en charge de la conformité au Règlement européen sur la protection des données (RGPD) au sein d'un nos instituts de recherche.

Cadre règlementaire

8. La **sanction** en cas de défaillance peut atteindre jusqu'à **20 millions d'euros pour les entités publiques** ou **4 % du chiffre d'affaires mondial** pour les entreprises privées. – Articles 83 et 84 du RGPD

En ce qui nous concerne

8. Au-delà de la sanction financière, la qualité / crédibilité scientifique des travaux des instituts et de l'unité est en jeu

De plus en plus de bailleurs de fonds demandent également des garanties de conformité, et les revues refusent de publier en leur absence

RGPD et sanctions financières

- Amendes infligées par la CNIL à deux médecins (3 et 6 K€) pour sécurité insuffisante des données de leurs patients

(configuration risquée de box internet, paramétrage de sécurité insuffisant du logiciel des données. Les données d'imagerie médicale pas sécurisée avant stockage (cf. article 32 : « mise en place de mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque »

- Données à caractère personnel (nom, adresse, date de naissance…)
- Données sensibles (données de santé)
- Personnes vulnérables (enfants…)
- Traitement grande échelle (tous les patients)

RGPD et sanctions financières pour la SNFC
Ficher d'évaluation des agents (1/2)

Plusieurs centres de bus ont intégré le nombre de jours de grèves des agents dans les fichiers d'évaluation

- **Une collecte de données non nécessaires (Art. 5.1.c et 5.2)**

Nombre de jours de grève : non nécessaire à l'évaluation des agents. Indépendant des objectifs à atteindre

Le nombre de jours d'absence aurait suffit → Principe de minimisation des données

RGPD et sanctions financières pour la SNFC
Ficher d'évaluation des agents (2/2)

- **Un manquement à l'obligation de limiter la durée de conservation des données (Art. 5.1.e)**

Conservation des dossiers jusqu'à 3 ans après la tenue des commissions → 18 mois recommandés

- **Un manquement à la sécurité des données (Art. 32)**

Tous les agents pouvaient extraire l'ensemble des données contenues dans l'outil → pas de différentiation d'habilitation

Cette configuration ne permettait pas de garantir la confidentialité des données

Une amende de 400 000 euros

https://www.cnil.fr/fr/fichiers-devaluation-des-agents-sanction-de-400-000-euros-lencontre-de-la-ratp

RGPD

Merci pour votre attention

et votre participation

Des questions ?

Sur cet atelier : pascale.morin@cirad.fr et magali.aubert@inrae.fr

Sur le RGPD au Cirad : dpo@cirad.fr

https://umr-moisa.cirad.fr/l-unite/qualite-et-conformite-des-donnees

Ce que nous verrons demain :
Le processus de mise en conformité

1. Saisir une fiche projet

2. Les documents obligatoires : fiche d'information, trame de demande de consentement, clauses : votre RDPO peut vous aider à compléter ces documents

3. Mise en application

Le Règlement Général sur la Protection des Données (RGPD)

Le processus de mise en conformité

1. Fiche d'information
2. Demande de consentement
3. Fiche projet
4. Étude de cas

Octobre 2023

cc BY NC ND

Chargées de Mission Qualité, Responsables Opérationnelles des Données (RDO), Correspondantes DPO
AUBERT Magali : magali.aubert@INRAE.fr & MORIN Pascale : pascale.morin@cirad.fr
https://umr-moisa.cirad.fr/l-unite/qualite-et-conformite-des-donnees

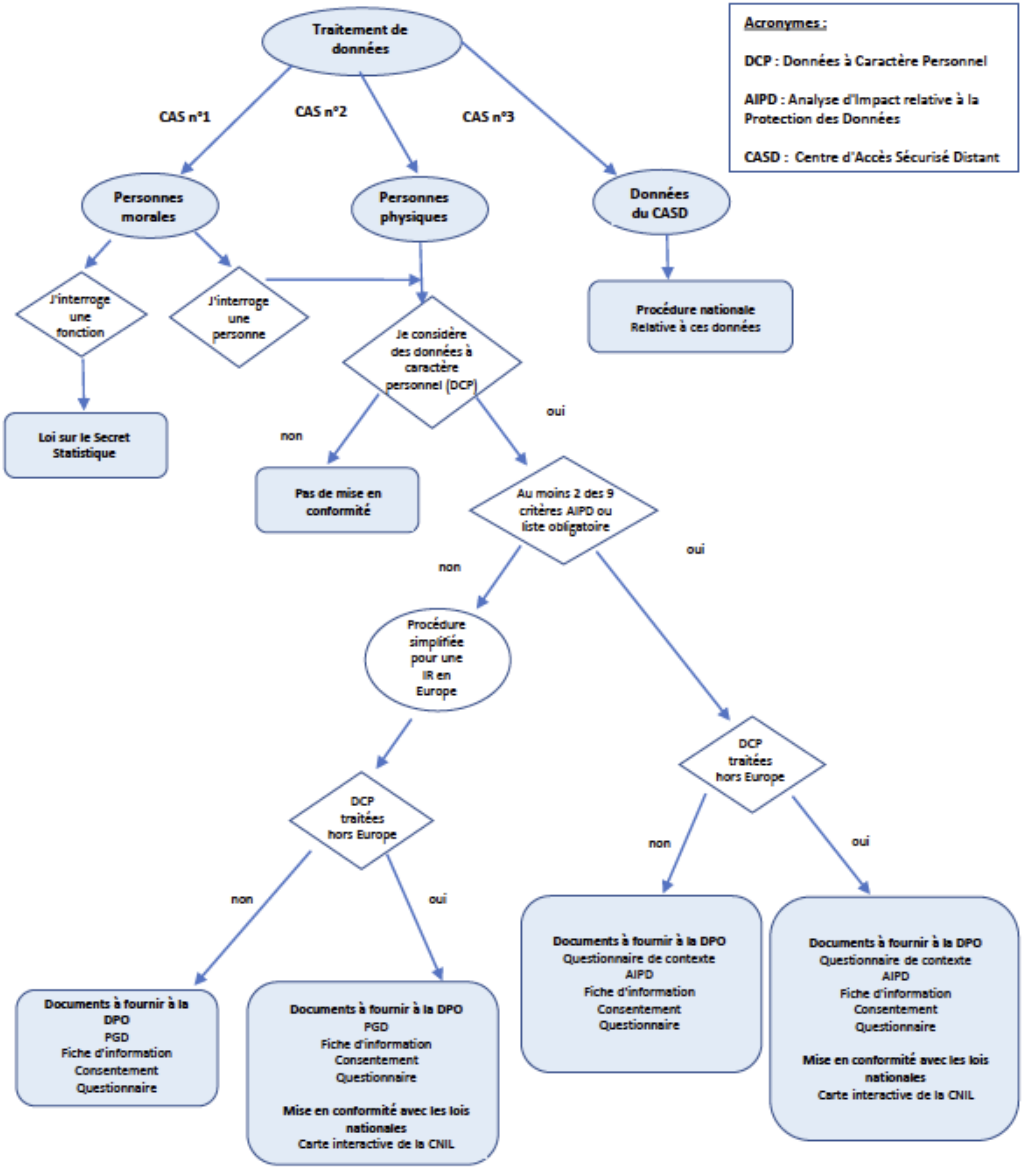
Le processus de mise en conformité

1. Saisir une fiche projet

2. Les documents obligatoires : fiche d'information, trame de demande de consentement, clauses : votre RDPO peut vous aider à compléter ces documents

3. Mise en application

Modélisation du processus d'inscription de vos données au registre
Le cas spécifique de l'UMR MoISA



Acronymes :

DCP : Données à Caractère Personnel

AIPD : Analyse d'Impact relative à la Protection des Données

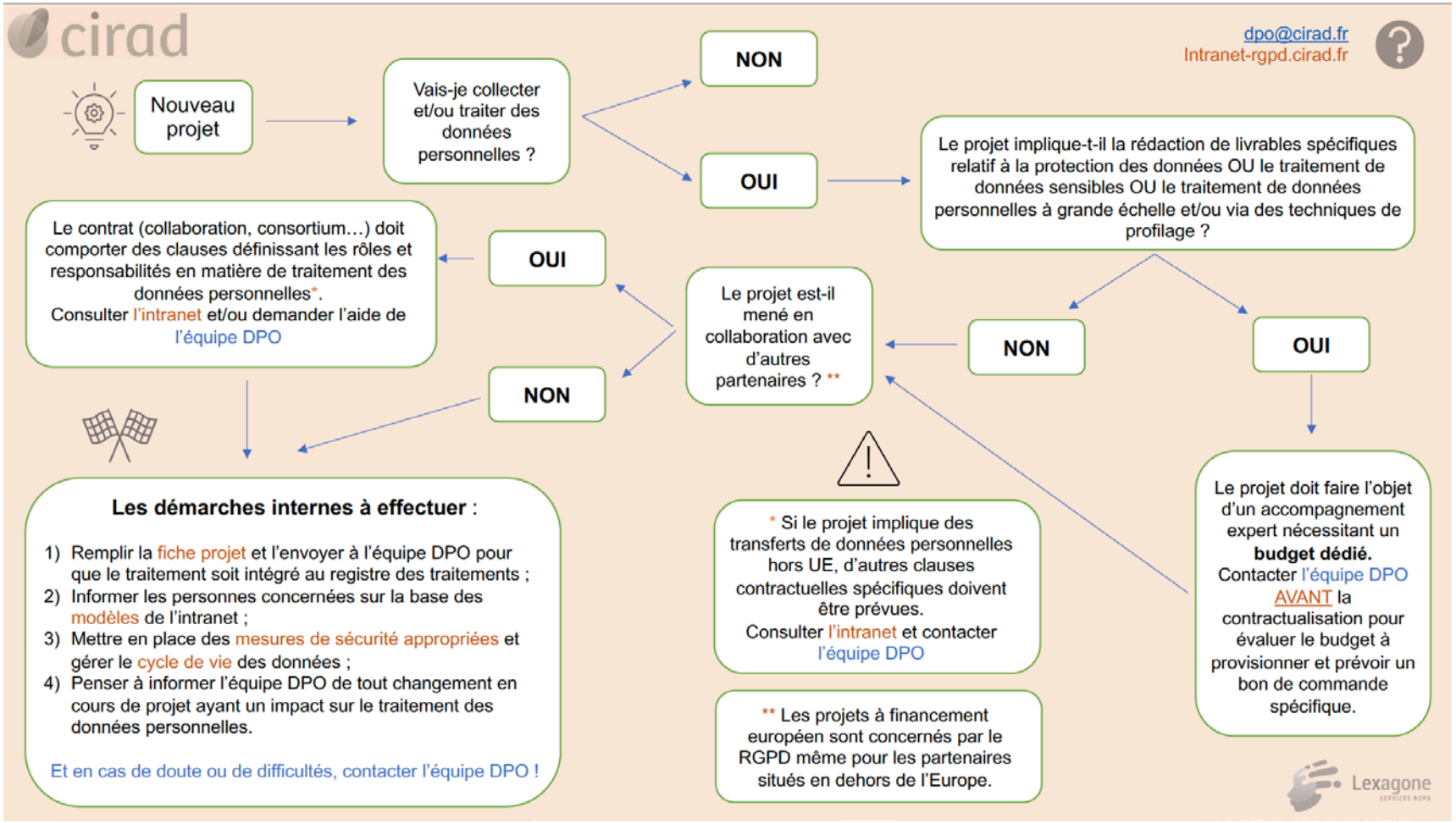
CASD : Centre d'Accès Sécurisé Distant

Magali **AUBERT** (INRAE, Département EcoSocio) magali.aubert@inrae.fr
Pascale **MORIN** (CIRAD, Département Environnements et Sociétés) pascale.morin@cirad.fr

v-mai 2022

Obligation de tenir, en interne, Un « dossier de conformité »

Consulter l'intranet RGPD (https://intranet-rgpd.cirad.fr/) et les outils méthodologiques :



Obligation de tenir, en interne, Un « dossier de conformité »

Consulter l'intranet RGPD (https://intranet-rgpd.cirad.fr/) et les outils méthodologiques :

Processus de mise en conformité par l'exemple

Le RGPD

1. **Fiche d’information**
2. Trame de consentement
3. Saisi de la fiche projet

Les exigences règlementaires : Informer devient une obligation

« Le règlement impose une information concise, transparente, compréhensible et aisément accessible aux personnes concernées »

Les informations contextuelles à transmettre obligatoirement à l'enquêté :

- **Identité et coordonnées** de l'institution responsable du traitement de données
- **La finalité de la recherche :** A quoi vont servir les données collectées ?
- **Le(s) destinataire(s) potentiels des données** : Qui aura accès aux données ? Chercheurs ? Bailleurs ? Revues ? …
- **Coordonnées du délégué à la protection des données personnelles** de l'organisme

Les informations sur les droits à transmettre obligatoirement à l'enquêté :

- **Durée de conservation des données**
- **Droits des enquêtés sur :**
  - Opposition, accès, rectification, effacement (art.16, 17, 21)
  - 2 nouveaux droits RGPD : limitation, portabilité (art.18 et 20)
- **Base juridique** du traitement

Le RGPD

1. Fiche d’information
2. **Trame de consentement**
3. Saisi de la fiche projet

- **Consentement** :

  « Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair que des données à caractère personnel la concernant fassent l'objet d'un traitement » - Articles 4, 7 et 8 du RGPD.

- **Exigences règlementaires** :

  - Un consentement compréhensible par tous, formulé en des termes clairs et simples
  - Le responsable du traitement des données est responsable de la conservation des preuves de consentement
  - Obligation de conserver les preuves (écrites, électroniques, audio) des consentements. Attention : des cases à cocher ne peuvent pas permettre de recueillir un consentement
  - L'enquêté doit pouvoir retirer son consentement aussi facilement qu'il le donne

Le RGPD

1. Fiche d’information
2. Trame de consentement
3. **Saisie de la fiche projet**

Obligation de tenir, en interne, Un « dossier de conformité »

Au Cirad, dès le montage du projet et avant de lancer les premières enquêtes, compléter la fiche projet : https://intranet-rgpd.cirad.fr/base-documentaire/process-interne et la transmettre à l'équipe DPO :

cirad

FORMULAIRE RGPD - Projets de recherche

Ce document a pour objet la présentation de votre projet sous l'angle RGPD. Il est destiné à la cellule DPO, afin de permettre une première analyse de conformité du projet à la règlementation applicable à la protection des données personnelles, et l'intégration du traitement au registre du CIRAD.

Merci de joindre à l'envoi de ce formulaire toute documentation utile pour l'analyse du projet : convention de partenariat/consortium, PGD, formulaire de consentement à la collecte …

En cas de doute ou de question complémentaire, l'équipe RGPD reste à votre écoute : dpo@cirad.fr

1. Description du projet	
Intitulé du projet	
But du projet	
Date de début du projet	
Date de fin du projet	
Référent RGPD du projet	

Le RGPD

Quelques points particulier :

- Réutilisation de jeux de données

- Publication

Vos obligations en cas de réutilisation / partage de données à caractère personnel :

- Le 1er responsable de traitement doit avoir obtenu le consentement des personnes enquêtées
- Les personnes doivent être informées de la réutilisation de leurs données
- Vous devez établir une convention qui définit le cadre d'utilisation des données
- Dans le cadre de données de santé, contactez l'équipe DPO pour étudier les possibilités

➢ Bonnes pratiques : partager des données anonymisées lorsque c'est possible, limiter la transmission des données à caractère personnel

Parlons publication

- Ne jamais transférer les données brutes personnelles à la demande d'un éditeur sans l'accord des personnes concernées
- Possibilité de publier des résultats agrégés ou anonymisés
- Pour les data paper : métadonnées OK mais pas les données !

- Open data :
  - Dans les projets Européens, c'est par défaut
  - Seuls les résultats agrégés, les métadonnées sont librement disponibles

Au Cirad, une référente institutionnelle sur la science ouverte : Sophie Fortuno (sophie.fortuno@cirad.fr)

Le RGPD

Des éléments de synthèse

Le processus de mise en conformité tout au long du processus du cycle de vie de vos données

DCP ? DS ?

Questionnaire d'enquête

Droit des personnes

Fiche d'information

Consentement

Questionnaire d'enquête

Renseigner les documents obligatoires

Le Plan de Gestion des Données

Responsable(s) de traitement ?

Plan de Gestion des Données

Envoyer vos documents pour validation

Inscription de vos données au registre

RGPD

Tenir un registre pour prouver sa conformité avec les exigences du RGPD :

Chaque Responsable de Traitement doit tenir un registre des traitements réalisés sous sa responsabilité.

Au Cirad, le registre est tenu au niveau institutionnel par l'équipe DPO.

En revanche chaque chercheur / chef de projet tient le dossier de conformité de son activité (conservation des fiches de consentement, documentation du process interne de conformité, PGD..)

Pour inscrire votre projet au registre :

https://intranet-rgpd.cirad.fr/base-documentaire/process-interne

1. Compléter la fiche projet (Formulaire RGPD – Projet de recherche)
2. Adapter les modèles de document (information, consentement, clauses : votre RDPO peut vous aider à compléter ces documents)
3. Transmettre l'ensemble de ces documents (fiche projet, documents adaptés, contrats fondateurs du projet, questionnaires d'enquête, étude d'impact sur la vie privée le cas échéant…) pour étude à l'équipe DPO et prévoir au besoin une réunion

Les documents sont à envoyer **avant le début des enquêtes** à l'équipe DPO (Délégué à la Protection des Données – Data Protection Officer) : dpo@cirad.fr

NB. les démarches liées à la conformité pouvant prendre du temps, l'équipe DPO, disponible à mi-temps, doit être contactée le plus en amont possible

Des exigences - Les outils pour vous aider

- L'intranet RGPD du Cirad : modèles de documents (fiche d'information, formulaire de consentement, clauses types pour les partenariats), outils méthodologiques (arbre décisionnel, checklist), actualités, foire aux questions,..
- Support atelier
- RGPD : Texte officiel
- Les contenus proposés sur le site de la CNIL https://www.cnil.fr/fr/comprendre-le-rgpd
- Des équipes dédiées au niveau institutionnel :
  - Chaque unité a désigné un relai DPO (RDPO)
  - dpo@cirad.fr pour contacter l'équipe DPO du Cirad
  - Des experts en matière d'éthique et de déontologie de la recherche (Philippe Feldmann), d'open data (Sophie Fortuno), de PGD (Laurence Dedieu)
  - La DIMS pour vous accompagner sur le montage des projets et les conventions associées
- L'équipe DPO propose des formations généralistes ou spécifiques métiers

Dans les faits

- Dans les UMR, c'est par principe le DPO de l'institution de rattachement du DU qui est compétent pour accompagner les projets, sauf lorsque l'unité a fait un choix différent (voir le DPO compétent par unité de recherche sur la page dédiée de l'intranet).
- Au Cirad, l'équipe DPO accompagne les traitements portés par les UMR rattachées au DPO Cirad sur la gestion courante de la conformité de leurs activités, la DPO adjointe étant présente sur site à Lavalette à raison de deux jours par semaine (les lundi et mardi)
- En cas de projet en partenariat, de fort enjeu avec des données à caractère personnel, de besoin spécifique, l'équipe DPO peut être sollicitée pour un accompagnement rapproché (sur bon de commande spécifique)

Les liens incontournables

- Côté CIRAD : https://intranet-rgpd.cirad.fr/
- Côté INRAE : https://intranet.INRAE.fr/cil-dpo
- RGPD : https://www.cnil.fr/fr/reglement-europeen-protection-donnees#haut
- CNIL : https://www.cnil.fr/fr/le-rgpd-cest-maintenant-les-changements-retenir-et-les-outils-pour-bien-se-preparer
- AIPD : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd
- Comité d'éthique INRAE CIRAD IFREMER IRD : https://www.cirad.fr/nous-connaitre/organisation-et-gouvernance/instances-et-comites#comit%C3%A9-consultatif-commun-d'%C3%A9thique-inrae-cirad-ifremer-ird-(c3e4)

Le RGPD

Le RGPD au prisme des outils qualité

Le Règlement Général sur la Protection des Données
Au prisme des Outils Qualité

Depuis le 25 mai 2018, les chercheurs doivent se mettre en conformité avec le RGPD - Règlement Général sur la Protection des Données. Dans de nombreuses disciplines, les données issues d'enquêtes de terrain sont, pour la plupart, des Données dites à Caractère Personnel. Les outils qualité offrent des grilles d'analyse pertinentes pour traiter les données de la recherche conformément à ces exigences règlementaires.

QQOQCP : Une méthode pour organiser sa mise en conformité

Cette méthode de questionnement simple et structurée, présente un caractère logique. A travers chacune de ces questions, vous aborderez les éléments clefs du RGPD. Chaque question renvoie à des notions indispensables pour lesquelles vous devez apporter des réponses précises pour garantir que le traitement des données de votre recherche est conforme avec les exigences règlementaires.

Qui

Qui sont les enquêtés ?
Personnes vulnérables ?
Mineurs (- de 16 ans) ?

Qui est responsable de traitement ?
Qui sont le ou les co-responsable(s) ?

J'ai pris contact avec mon DPO (Data Protection Officer) ?

Je fais appel à des prestataires extérieurs ?
J'ai rédigé des clauses contractuelles ?

Quoi

Est-ce que je traite des données à caractère personnel ?

Est-ce que je traite des données sensibles ?

Est-ce que je dois réaliser une AIPD ?
Est-ce que je valide au moins 2 des 9 critères ?

Est-ce que j'ai inscrit mon traitement au registre ?

Où

Est-ce que les données sont traitées en Europe ?

Est-ce que les données sont traitées hors Europe ?
Est-ce que je me suis mis en conformité avec les lois et réglementations nationales ?

Où sont stockées et sauvegardées les données ?

Quand

Est-ce que les données ont été collectées avant le 25 mai 2018 ?

A quel moment je dois supprimer / archiver les données ?

Combien

Est-ce que je traite des données "à grande échelle" ?

Quelle est la durée de conservation des données ?

Comment

Quelles sont les conditions de réutilisation / de partage des données traitées ?

Comment garantir la sécurité des données ?

Comment je garantis les droits et libertés des enquêtés ?
J'ai rédigé et diffusé une fiche d'information ?

Quels sont les logiciels mobilisés pour la retranscription / traitement ... des données ?
Sur quels supports sont les données ?

Pourquoi

Quelle est la finalité de la recherche ?

RGPD

Ishikawa : Un outil pour appréhender son enquête de terrain

Cet outil a été créé par le professeur Kaoru Ishikawa. Il est aussi appelé *« Méthode d'Ishikawa »*, 5M, diagramme en *« arêtes de poisson »* ou diagramme de *« causes à effet »*. Son utilisation permet de rechercher et d'identifier de manière synthétique les différentes causes possibles d'un problème (effet). Cet outil sert à l'amélioration du traitement et de la gestion des données de la recherche.

RGPD

Merci pour votre attention

et votre participation

Des questions ?

Sur cet atelier : pascale.morin@cirad.fr et magali.aubert@inrae.fr

Sur le RGPD au Cirad : dpo@cirad.fr

https://umr-moisa.cirad.fr/l-unite/qualite-et-conformite-des-donnees

RGPD

« Il ne faut pas penser à l'objectif à atteindre, il faut seulement penser à avancer. C'est ainsi à force d'avancer qu'on atteint ou qu'on double ses objectifs sans même s'en apercevoir »

Bernard Werber
La Révolution des Fourmis

Le RGPD
Ce qu'il faut retenir

Données à Caractère Personnel
(directement ou indirectement identifiantes)

Protection des citoyens **Traitement des données en Europe**

Fiche d'information

Consentement **Nouveaux droits**

Données Sensibles

DPO **Co-responsabilités**

AIPD

Données de santé **Personnes vulnérables**

Sécurisation des données