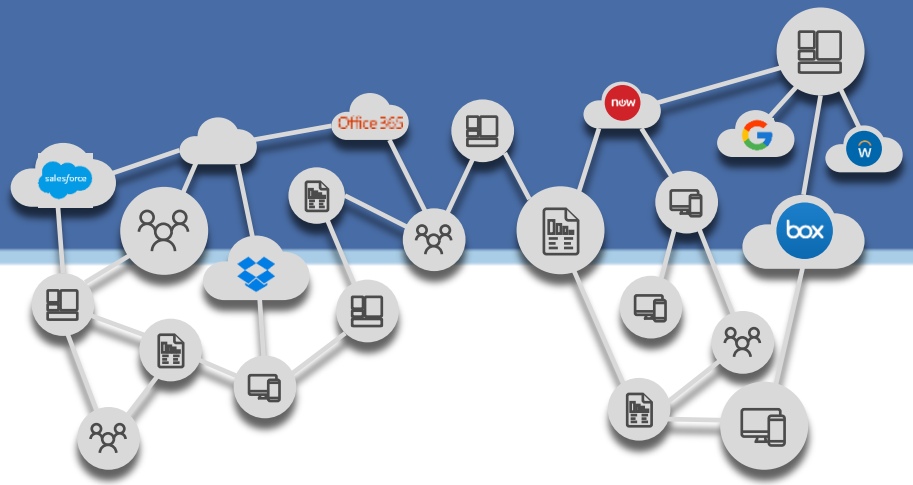
QuaRES
Association pour la Qualité
en Recherche et Enseignement Supérieur

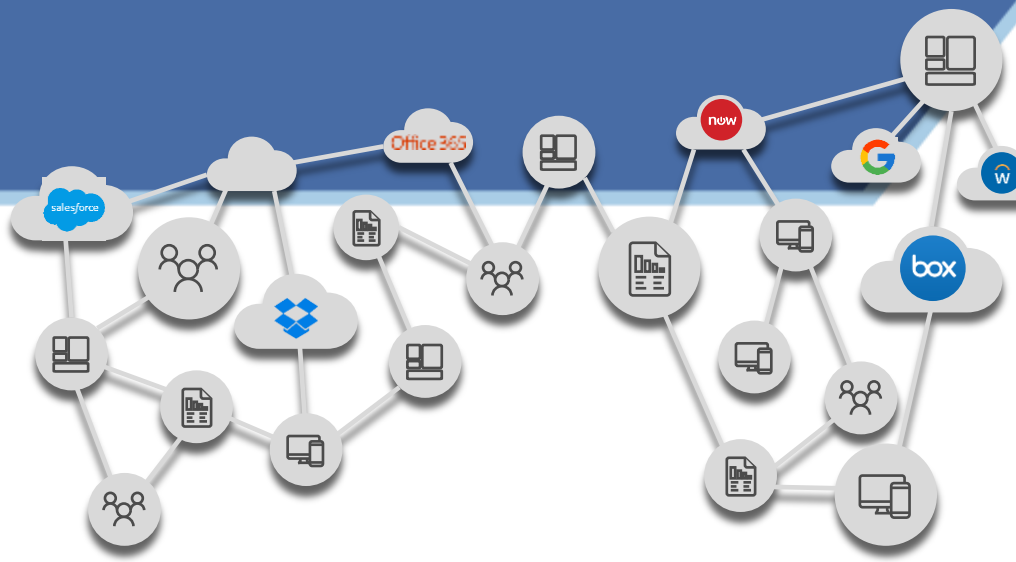
16ème
ÉCOLE QUALITÉ
du 10 au 12 Septembre 2018

La mise en conformité au RGPD à l'Ifremer

SINQUIN Jean-Marc
Délégué qualité Bretagne
DPD/DPO
Auditeur ICA



« La portée du RGPD est inégalée parce que les données personnelles sont tellement omniprésentes que pratiquement toutes les organisations d'une certaine taille traitent ou détiennent des quantités substantielles d'informations concernant leurs clients et leurs collaborateurs. »



<u>Seuls 25% des Français</u> estiment que la confidentialité de leurs données personnelles est correctement assurée sur Internet

- Les plus jeunes (moins de 35 ans : 16%) et les Français les plus actifs sur les réseaux sociaux (9%) sont les plus critiques sur la confidentialité de leurs données sur Internet.

Plus globalement, 7 Français sur 10 sont inquiets concernant… :

- …la sécurité de leurs données personnelles (73%),
- …l'utilisation de leurs données par les grandes entreprises d'Internet (72%),
- …celles transmises volontairement aux entreprises et services sur Internet (73%).

Cette inquiétude se conjugue à un faible niveau d'information à l'égard de ces sujets :

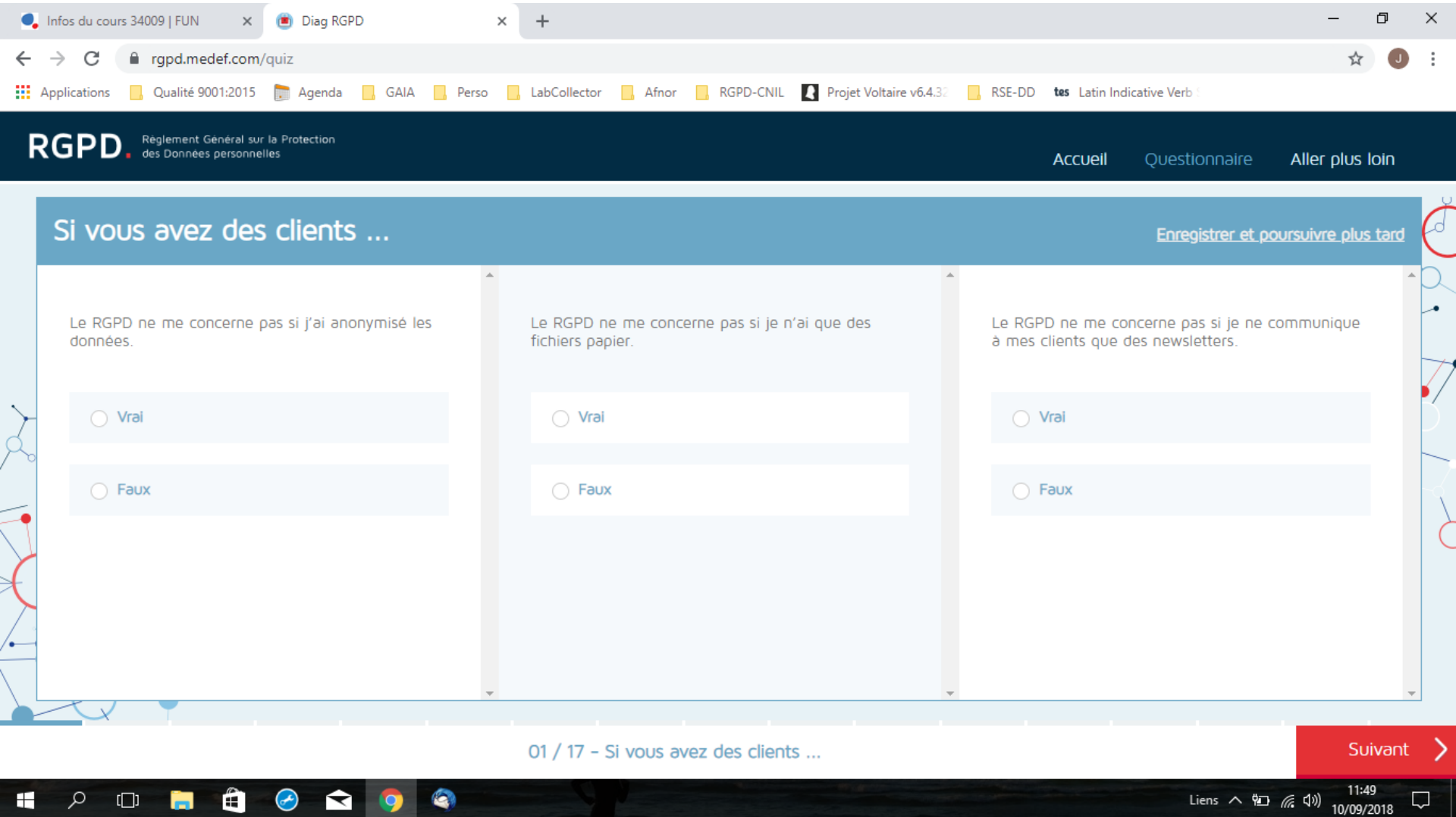
- Moins d'un quart des Français déclare être bien informé des mesures à prendre pour sécuriser leurs données (22%),
- Moins de 2 sur 10 s'estiment bien informés concernant l'utilisation de leurs données par les grandes entreprises d'Internet (17%) ou les services qu'ils utilisent sur Internet (15%).

Source sondage BVA-2017

Petit Quizz

G General D Data P Protection R Regulation

R Règlement G Général P Protection D Données

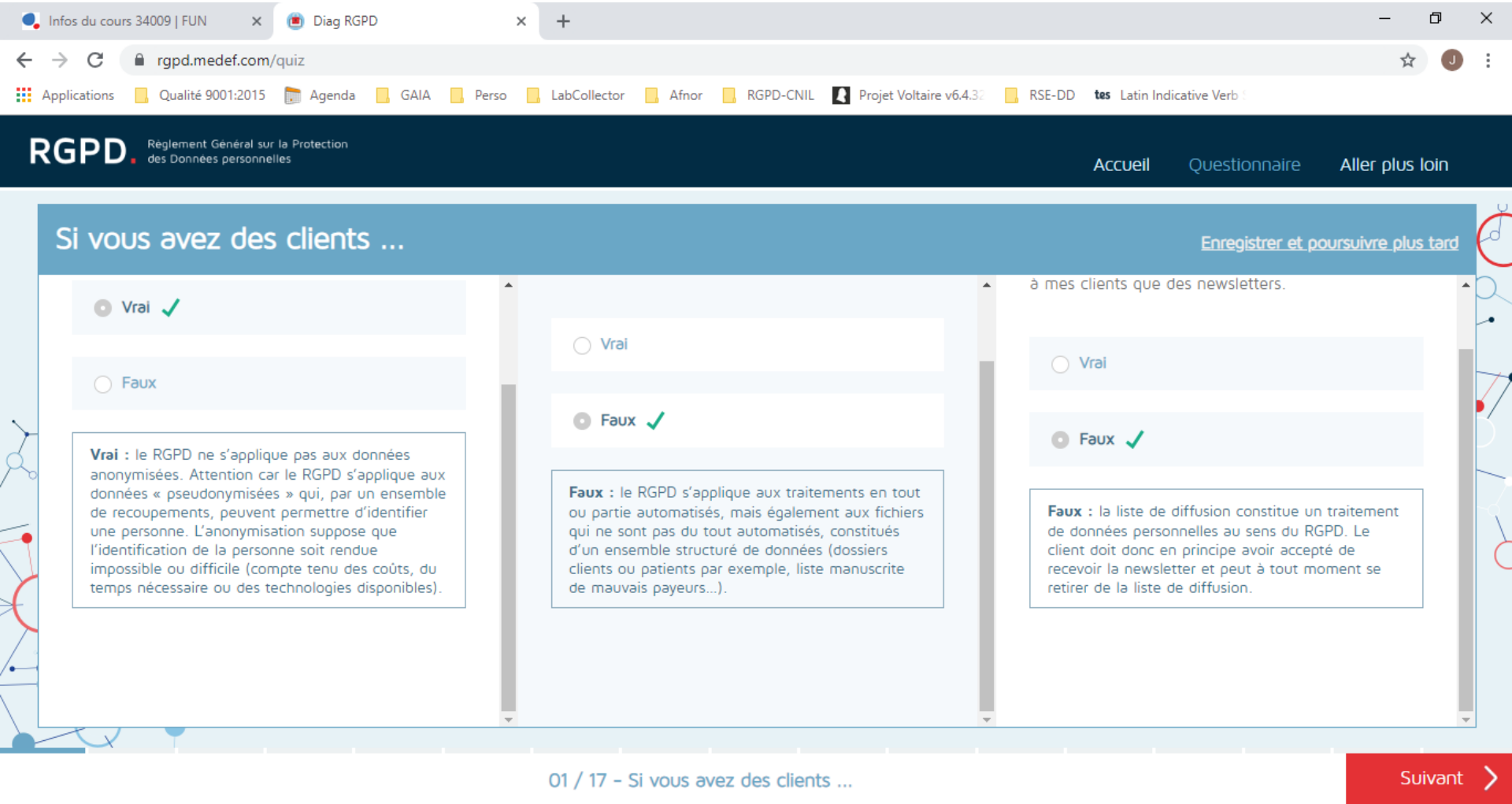


Etes vous RGPD compliant ?

G General D Data P Protection R Regulation

R Règlement G Général P Protection D Données

QuaRES ÉCOLE QUALITÉ



RGPD en quatre points

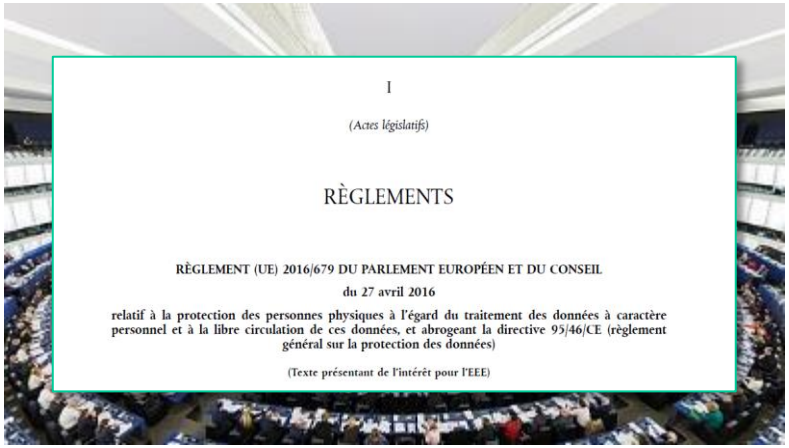
Règlement Européen applicable sans transposition dans tous les pays de l'UE

« Remplace » les lois nationales (Loi « Informatique & Libertés », LCEN, etc…)

Adopté en avril 2016 et effectif au plus tard le 25 mai 2018

Toutes les entreprises et collectivités sont concernées

Règlement Européen applicable sans transposition dans tous les pays de l'UE



I

(Actes législatifs)

RÈGLEMENTS

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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(Texte présentant de l'intérêt pour l'EEE)

N° 490

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

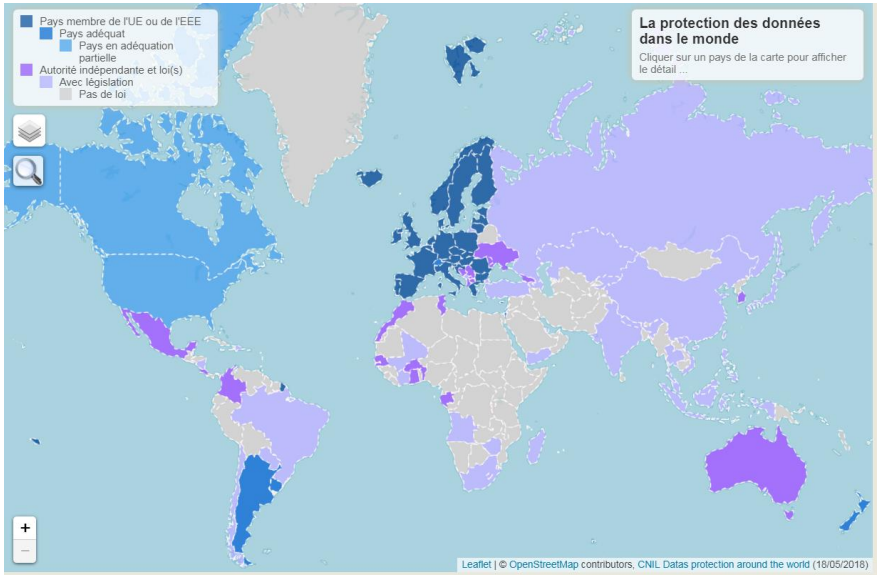
QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 13 décembre 2017.

PROJET DE LOI

relatif à la protection *des* données personnelles,

Partout ?



« Remplace » les lois nationales (Loi « Informatique & Libertés », LCEN, etc…)

1. La loi informatique & libertés (1978)
2. La directive européenne de 1995
3. La LCEN (2002)
4. Loi n° 2004-801 (Protection des données à caractère personnel)
5. Loi n° 2016-1321 « pour une république numérique »
6. Et maintenant le RGPD (règlement 2016/679 de l'UE)

Adopté en avril 2016 et effectif au plus tard le 25 mai 2018

Toutes les entreprises et collectivités sont concernées

De la bureaucratie à la preuve

- Finies les « déclarations CNIL » … mais la conformité devra être démontrée !
- Registre des traitements obligatoire si + de 250 personnes. Recommandé dans tous les autres cas
- Conservation des preuves

« Privacy by design » « Privacy by default »

- La sécurité des données personnelles doit être envisagée dès la conception des produits ou services. … Et être démontrable à l'utilisation
- La sécurité des données personnelles doit être gérée en permanence. Ce n'est pas une *option*.

Implication des sous-traitants

- Le sous-traitant doit présenter les mêmes garanties que le responsable de traitement.
- Le sous-traitant ne peut agir que sur instruction du responsable de traitement.
- Le sous-traitant est « co-responsable »
- Le sous-traitant a un devoir de conseil

Le DPO (DPD)

- Délégué à la Protection des Données
- Coordonne la conformité
- Point de contact
- Conseille et assiste
- Obligatoire ou « recommandé »

L'obligation de notification

- Les violations de données à caractère personnel devront obligatoirement être notifiées à l'autorité de contrôle.

Sous-traitant → Resp. de traitement → CNIL, Victimes

Renforcement des droits

- Information des personnes concernées
- Consentement « explicite et éclairé »
- Droit à l'oubli, portabilité, rectification, opposition
- Encadrement des « décisions automatisées »

Sanctions : 2 et 4% CA mondial, 10 et 20 M€

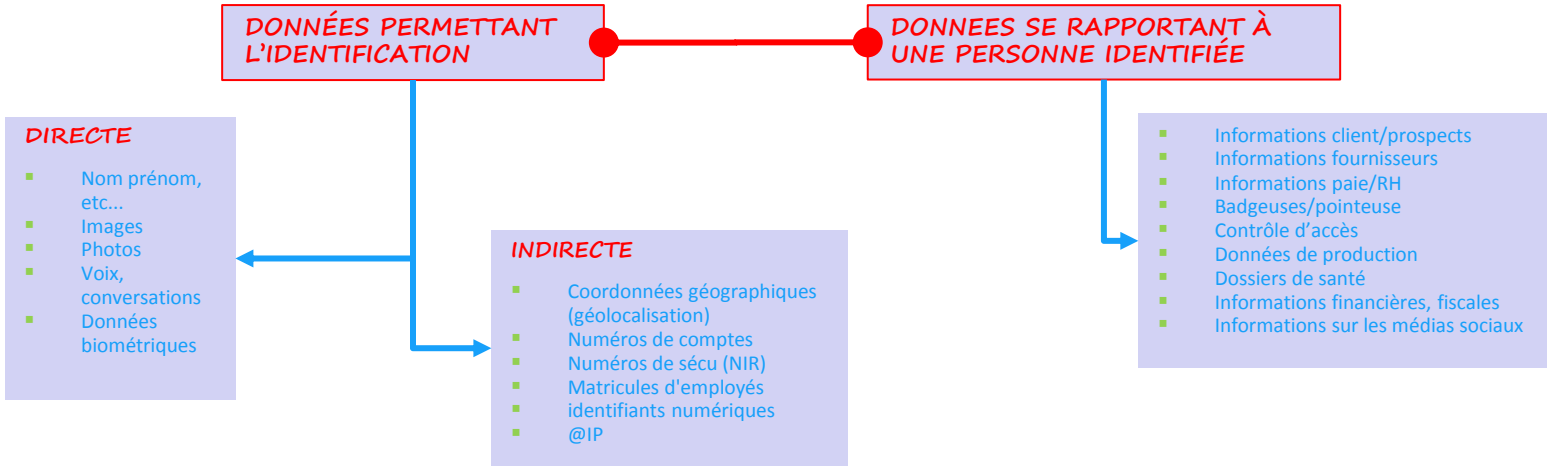
C’est quoi une donnée personnelle ?

Qu’appelle-t-on « Données à caractère personnel » ?

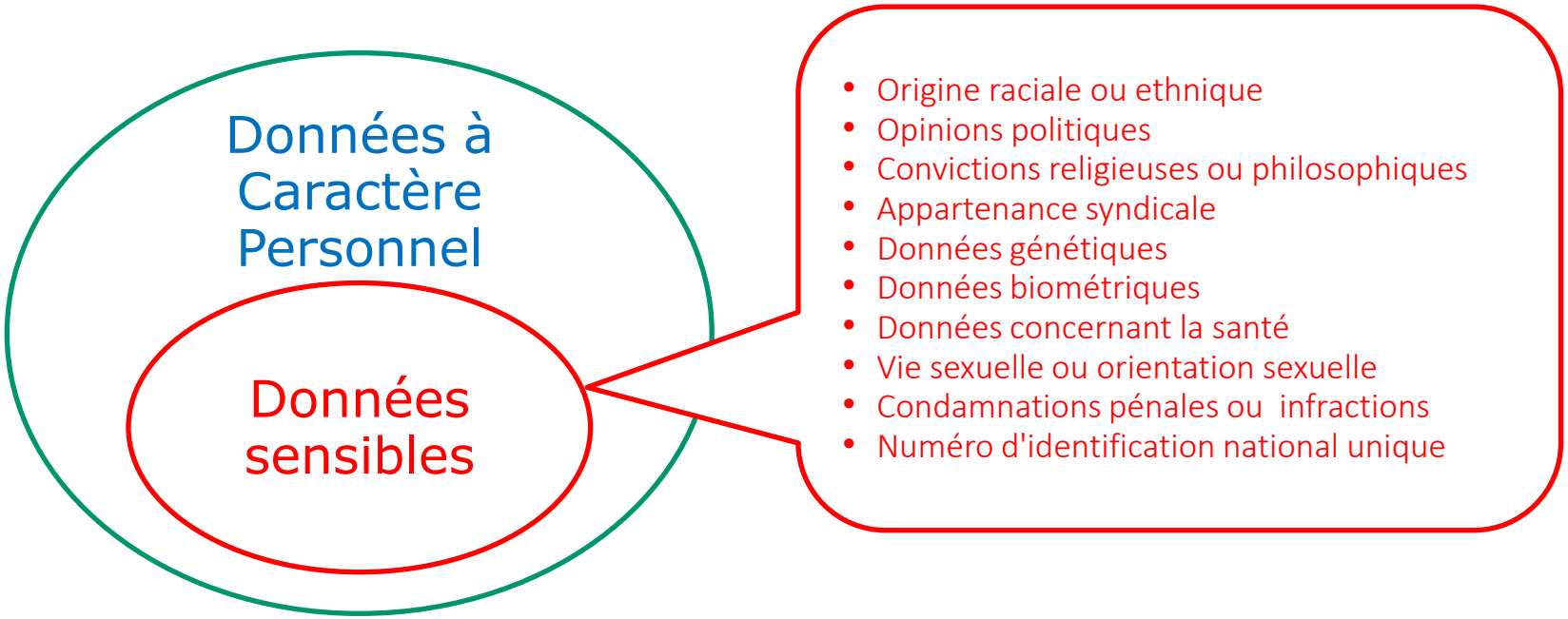
D C P

« 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 »*
(Art.4 RGPD)

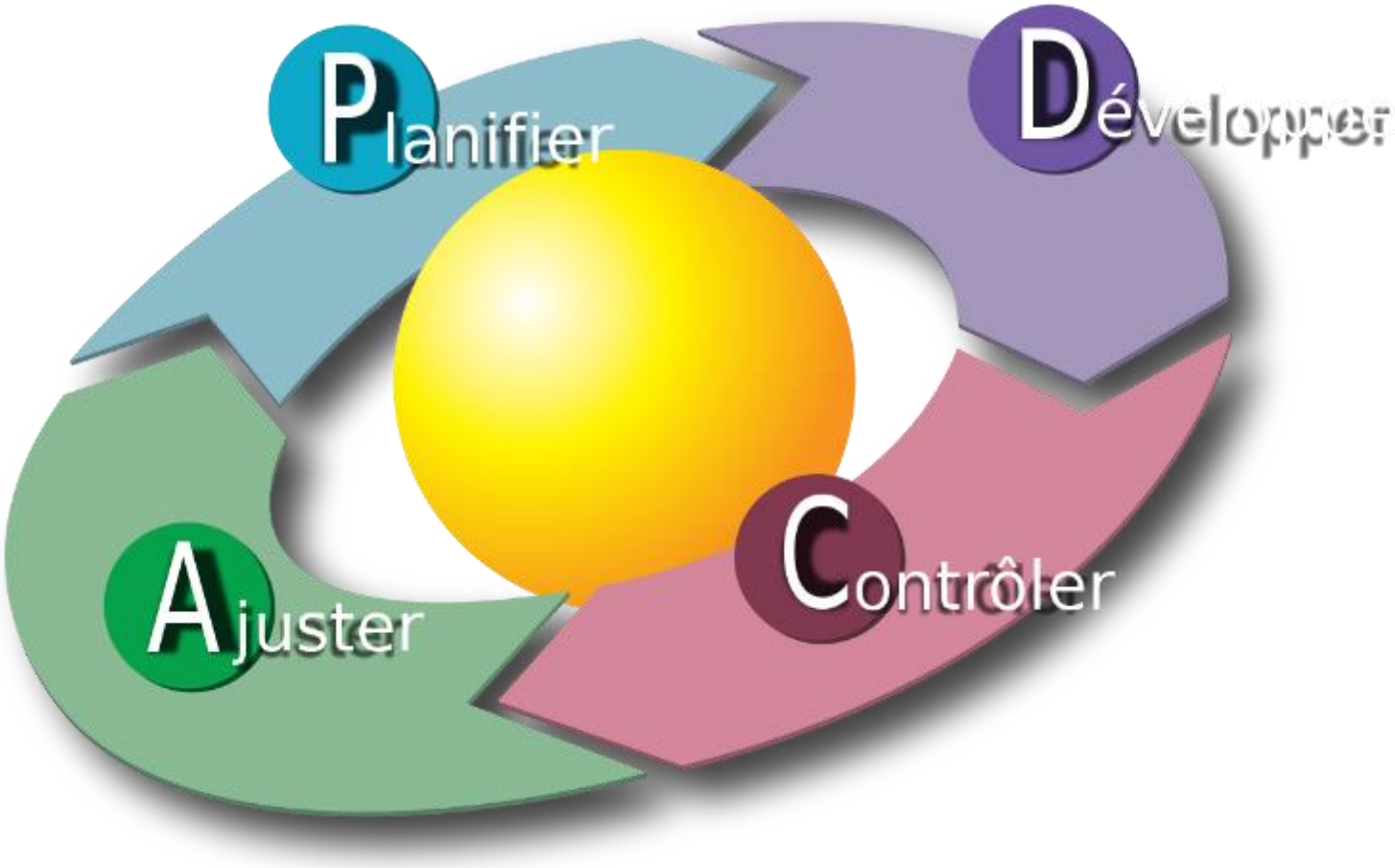


Et une donnée personnelle sensible ?



En pratique, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Le projet RGPD à l'Ifremer



Planification

- Constitution équipe projet
- Note de nomination Chef de projet
- Besoin de formation
  - Equipe projet
  - Salariés
- Elaboration PMP
- Identification des risques

Développement

- Trois sessions de formation / tutorat
- Identification du **niveau de conformité**
- Elaboration d'une première **carte heuristique**
- Elaboration **registre de traitement**
- **Procédure** Gestion des données personnelles
- Site **Intranet**

Niveau de conformité

Gestion de la conformité des traitements de DCP

Sommaire

Contexte de l'organisation

Connaître l'organisation et ses enjeux particuliers vis-à-vis de la mise en conformité des traitements de DCP.

Contexte général
Sensibilité
Priorités

Revue du 31/01/2018

Processus du SM DCP

Pratiques du Système de Management des Données à Caractère Personnel (SM DCP), groupées en processus

Tableau d'évaluation des pratiques
Synoptique
Points remarquables
Rosace
Histogramme

Glossaire

Politique sécurité applicable à la protection des DCP

Mesures de protection de l'information spécifiquement associées aux DCP (Disponibilité /Intégrité /Confidentialité /Paternité).

Tableau d'évaluation des pratiques
Points remarquables
Rosace
Histogramme

Suivi du SMDCP

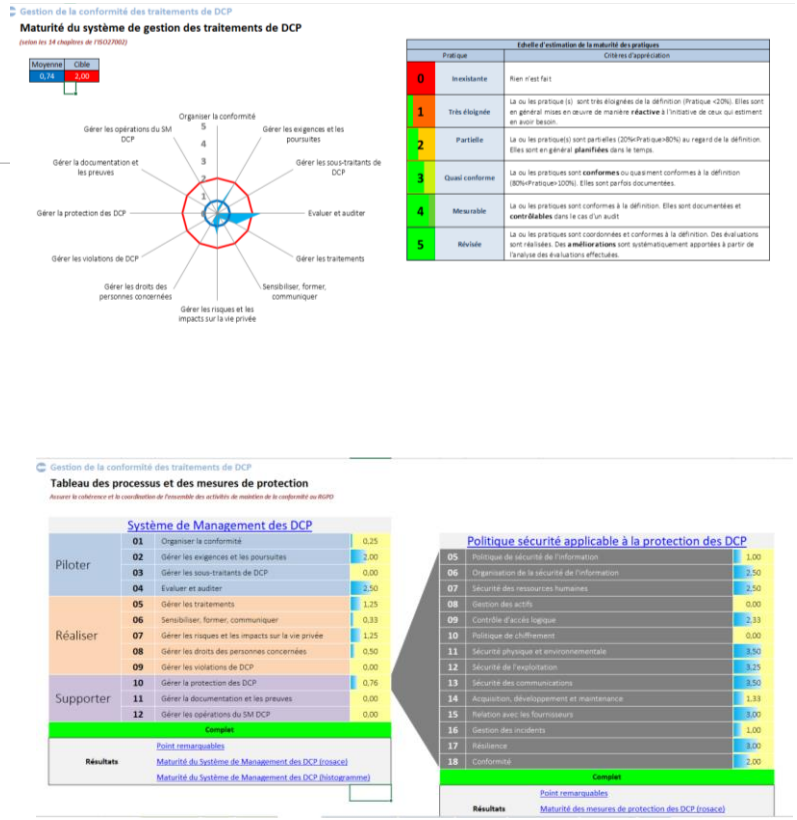
Gérer les preuves de conformité, Suivre les progrès de l'organisation, gérer l'amélioration continue.

Suivi des plans de progrès
Gestion des preuves opposables

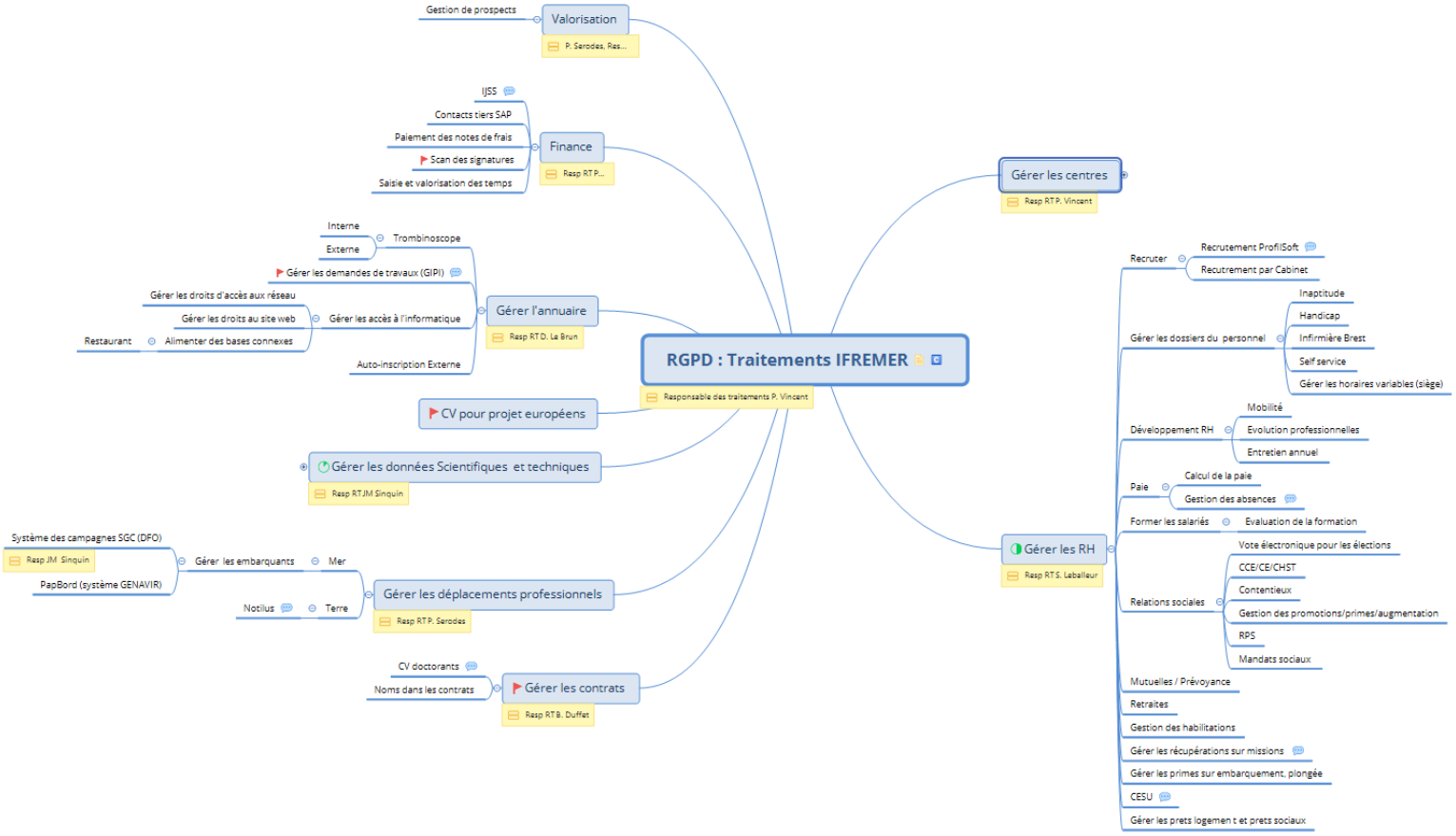
Echelles et listes de valeurs

Listes de valeurs, paramètres, nommage des processus, résultats intermédiaires…

Echelle de maturité
Résultats (données sources des graphes)
(PAR) Listes de valeurs



Première carte heuristique



Le registre de traitement (cf Art. 30)

RESPONSABLE DE TRAITEMENT
INSTITUT FRANCAIS DE RECHERCHE POUR L'EXPLOITATION DE LA MER
Représenté par Monsieur Patrick VINCENT
155 RUE JEAN JACQUES ROUSSEAU
92130 ISSY LES MOULINEAUX
FRANCE

Délégué à la protection des données
M. Jean Marc SINQUIN
IFREMER Centre Bretagne
ZI de la Pointe du Diable - CS 10070
29280 Plouzané

	Identification du traitement		Finalité	Catégories de personnes concernées	Catégories de données collectées		Catégories de destinataires	Transferts hors UE ?	Responsable du traitement	
N° / REF	Désignation		(Finalité principale)	(Employés, candidats, visiteurs, stagiaires, prestataires...)	Etat-civil, identité, données d'identification, images, Vie personnelle, vie professionnelle, informations d'ordre économique et financier, données de connexion , données de localisation, internet, autres catégories de données	Données sensibles (Oui/non)	(internes/externes/sous-traitants)	Oui /non	Responsable du traitement	Sous-traitant (le cas échéant)
DRH01	Recruter les salariés - candidats externes via Talent scream		Recrutement	Candidats	Etat-civil, identité, données d'identification, images, Vie personnelle, Vie professionnelle, informations d'ordre économique et financier	Oui	Internes :DRH, responsable hiérarchique:), Externe (Sous traitant): Talent Scream)	non	IFREMER	TALENT SCREAM
DRH02	Recruter les salariés - candidats externes via cabinet de recrutement		Recrutement	Candidats	Etat-civil, identité, données d'identification, images, Vie personnelle, Vie professionnelle, informations d'ordre économique et financier	Oui	Internes: Personnes habilitées chargées de la gestion du personnel, Supérieur hiérarchique	non	IFREMER	Cabinet de recrutement
DRH03	Gérer les données administratives du personnel (GA)		Gestion administrative des personnels	Employés, Intérimaires, personnel extérieur à l'Ifremer	Etat-civil, identité, données d'identification, images, Vie personnelle, Vie professionnelle, informations d'ordre économique et financier	Non	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH04	Gérer les données administratives du personnel (GA) - handicap		Gestion administrative des personnels	Employés	Etat-civil, identité, informations professionnelles	Oui	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH05	Gérer les données administratives du personnel (GA) - inaptitude		Gestion administrative des personnels	Employés	Etat-civil, identité, informations professionnelles	Non	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH06	Gérer les données administratives du personnel (GA) - infirmière		Gestion administrative des personnels	Employés	Etat-civil, identité, informations professionnelles	Non	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH07	Gérer les données administratives du personnel (GA) - self service HRA		Gestion administrative des personnels	Employés	Etat-civil, identité, données d'identification, images, Vie personnelle, Vie professionnelle, informations d'ordre économique et financier	Non	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH08	Gérer les données administratives du personnel (GA) - Badgeuse Issy		Gestion administrative des personnels	Employés	Etat-civil, identité, informations professionnelles	Non	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH09	Réaliser la paie des salariés - calcul de paie		Gestion administrative des personnels	Employés	Etat-civil, identité, Vie professionnelle, informations d'ordre économique et financier	Oui	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH10	Réaliser la paie des salariés - absences maladie		Gestion administrative des personnels	Employés	Etat-civil, identité Vie personnelle, Vie professionnelle	Non	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH11	Développer les RH -mobilité interne		Gestion des carrières et de la mobilité	Employés	Etat-civil, identité, données d'identification Vie professionnelle	Oui	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH12	Développer les RH - entretien annuel		Gestion des carrières et de la mobilité	Employés	Etat-civil, identité, données d'identification Vie professionnelle	Non	Internes: Personnes habilitées chargées de la gestion du personnel	non	IFREMER	
DRH13	Développer les RH - évolution professionnelle		Gestion des carrières et de la mobilité	Employés	Etat-civil, identité, données d'identification	Oui	Internes: Personnes habilitées chargées de la	non	IFREMER	

Registre OK | DAJF-001 | DAJF-002 | DAJF-003 | DAJF-004 | DAJF-005 | DAJF-006 | DAJF-007 | DAJF-008 | DAJF-009 | DAJF-010 | DAJF-011 ...

Notre niveau d'exposition

- **128 traitements**
- **23 traitements avec des données sensibles**
  - Dont 6 sous-traités

Recruter les salariés - candidats externes via Talent scream
Recruter les salariés - candidats externes via cabinet de recrutement
Assurer les relations sociales - RPS
Gérer la Prévoyance
Recruter les VSC
Gérer les départs autres que retraite

Désignation DPO & procédure interne de gestion des DCP

1. Données collectées à l'IFREMER

« L'IFREMER collecte certaines données personnelles vous concernant et qui sont **nécessaires à la gestion des relations de travail**: … »

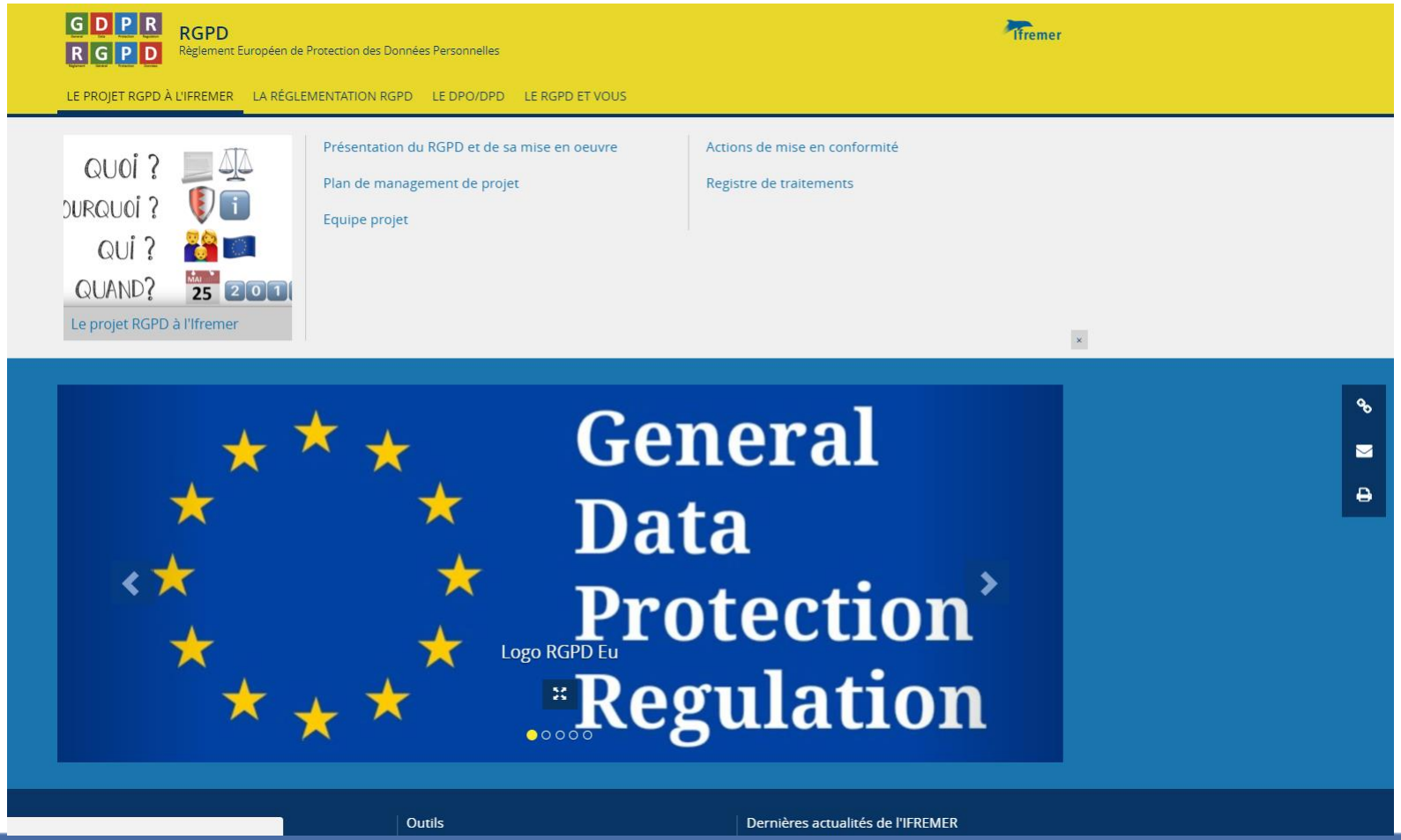
2. Finalité des traitements

« Ces données sont, pour certaines, collectées **à votre arrivée**, d'autres le sont **pendant la relation de travail** (vidéosurveillance, analyse de la navigation sur Internet, mise à jour des vos informations sur le système de gestion des ressources humaines par exemple) et traitées aux fins suivantes: … »

3. Vos droits

Le droit d'accès à vos données personnelles / Le droit de rectification de vos données personnelles si celles-ci sont erronées / Le droit d'opposition / Le droit au déréférencement / Droit à la portabilité des données

Un site *Intranet* RGPD dédié



Contrôler (approche ISO 9001:2015)

- Audit interne
- Indicateurs de suivi
- Revue de registre (traitements et sous-traitants)

Agir (approche ISO 9001:2015)

- Revue de Direction Annuelle spécifique RGPD
- Tableau de bord

Le RGPD est totalement soluble dans ISO9001:2015

- **4.1 « Compréhension de l'organisme et son contexte »**
- **4.2 « Compréhension des besoins et des attentes des parties intéressées »**
- **4.4.1.f) «… prendre en compte les risques et opportunités… », à la fois de manière globale et opérationnelle**
- **6.1 « Actions à mettre en œuvre face aux risques et opportunités »**
- **8.3 « Conception et développement de produits et services »**
- **8.5.3 « Propriété des clients ou des prestataires externes »**
- **9 « Évaluation des performances » et 10 « Amélioration »**

Principaux impacts à Ifremer

- **Révision de la charte informatique**
- **Ecriture d'une PSSI (Politique de sécurité du système d'information)**
- **Révision des sites de sciences participatives**
- **Nouvelles clauses dans les contrats de sous-traitance**

Pour aller plus loin :

- **Site de la CNIL :** https://www.cnil.fr/fr/rgpd-par-ou-commencer
- **RGPD et OS :** http://www.editions-legislatives.fr/content/donn%C3%A9es-personnelles-des-salari%C3%A9s-les-syndicats-doivent-exiger-des-r%C3%A9ponses-de-lentreprise
- **Relations responsable de traitement / sous-traitants :** https://syntec-numerique.fr/actu-informatique/pour-mise-en-place-responsable-obligations-contractuelles-rgpd
- **Durée de conservation :** http://www.marieannechabin.fr/2018/04/duree-de-conservation/
- **Petit Quiz :** https://rgpd.medef.com/