

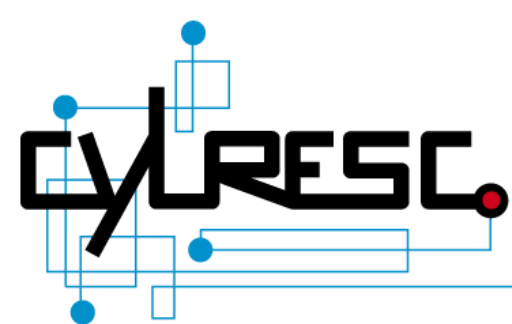


Aca
Nexia



Entre obligation et avantage concurrentiel, qu'implique le RGPD ?

→ Préparer sa mise en conformité



INTERVENANTS



**Xavier
BEAUSSAC**

*Chief Operations
Officer*



**Christophe
SZWEDO**

Team Leader



**Aurélie
SEGONNE-
MORAND**

*Avocat au Barreau
de Versailles*



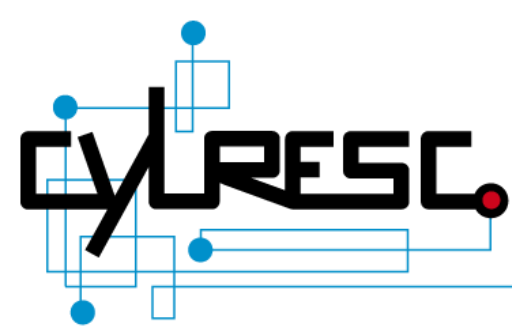
**Philippe
FOUCAULT**

*Directeur Audit et
conseil en
systèmes
d'information*



**Dominique
DESCOURS**

*Associé Risk
Management et
Contrôle Interne*



ORDRE DU JOUR

- I. Introduction au RGPD
- II. Le RGPD, pourquoi ?
- III. Les notions clés
- IV. Comment se mettre en conformité ?
- V. Anticiper les poursuites et les sanctions
- VI. Le vol de données personnelles (démonstration)



Aca
Nexia



Introduction au RGPD

Qui est concerné ?

- Entreprises traitant ou possédant des informations personnelles sur le citoyen européen

Sanction en cas de non-exécution

- 4% du chiffre d'affaires ou 20M€

Quand le règlement entre-t-il en vigueur ?

- 25 mai 2018

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

- Définition « *Loi informatique et liberté* » :

« Les données personnelles correspondent à toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

- Exemples de données personnelles

Identité, coordonnées, numéro de téléphone ou d'identifiant, données de localisation, adresse IP, habitudes de consommation...

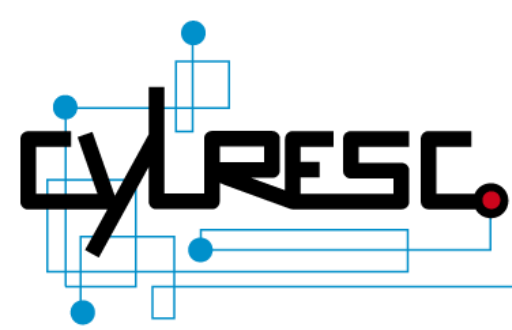
Qu'est-ce qu'un traitement ?

- Définition :

Toute opération, ou ensemble d'opérations, portant sur des données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction...).

- Exemples de traitements de données courants à caractère personnel

Gestion du personnel, des rémunérations, des fournisseurs, des clients, des opérations de fidélisation, modalités de surveillance (vidéos, systèmes d'alarme, contrôle d'accès,...)



I. INTRODUCTION AU RGPD

Qu'est-ce qu'un risque sur la vie privée ?

- Tout évènement pouvant porter atteinte aux droits et libertés des personnes (accès non autorisé, modification illicite ou données indisponibles) et toutes menaces qui permettraient qu'il survienne.



Aca
Nexia



Le RGPD, pourquoi ?

II. LE RGPD, POURQUOI ?

1.

Renforcement du droit des personnes

2.

Renforcement des vérifications sur les process

3.

Mise en place de véritable sanctions

4.

S'assurer d'une application de la loi à toute entité qui traite des données personnelles sur le territoire européen



Aca
Nexia



Les notions clés

III. LES NOTIONS CLES

Privacy « by design »

Security « by default »

Anonymisation

Chiffrement

Traçabilité des données et des traitements

Minimisation des données

Responsabilité

Consentement explicite

Droit de rectification

Droit à l'oubli

Désigner un DPO

- ✓ Obligation légale de désigner un DPO dans les 3 cas suivants :
- Traitement effectué par une autorité publique
 - Traitement des données personnelles réalisé à grande échelle : nécessite un suivi régulier
 - Traitement des données personnelles qui vise des données relatives à des condamnations pénales et à des infractions

Minimiser les données personnelles collectées

- ✓ Data Privacy by default : ne collecter QUE le strict nécessaire
- ✓ Nécessite la mise en place de nouveaux process
 - Purger l'ensemble des données qui ne sont pas strictement nécessaires au sein des applications existantes
 - Limiter les données collectées à l'avenir

La gestion et la portabilité des données personnelles

- ✓ Avoir la possibilité d'exporter les données dans un format structuré (XML)
- ✓ Donner la possibilité à l'utilisateur de récupérer ses données personnelles
- ✓ Droit de rectification : les données collectées doivent être tenues à jour
- ✓ Limitation de conservation : les données doivent être conservées pendant une durée limitée et cohérente avec le traitement
- ✓ Droit à l'oubli : les données doivent pouvoir être effacées sur demande

PIA (Privacy Impact Assessment)

- ✓ Lors d'un traitement à haut risque pour les droits et libertés des personnes, un PIA doit être effectué avant la mise en place du traitement
 - Permet d'évaluer les risques liés au traitement des données
- ✓ Cas dans lesquels un PIA est obligatoire :
 - Traitement des données personnelles fondé sur un traitement automatisé sur lequel sont prises des décisions juridiques
 - Traitement de données à caractère personnel relatives à des condamnations pénales
 - Surveillance à grande échelle d'une zone accessible au public



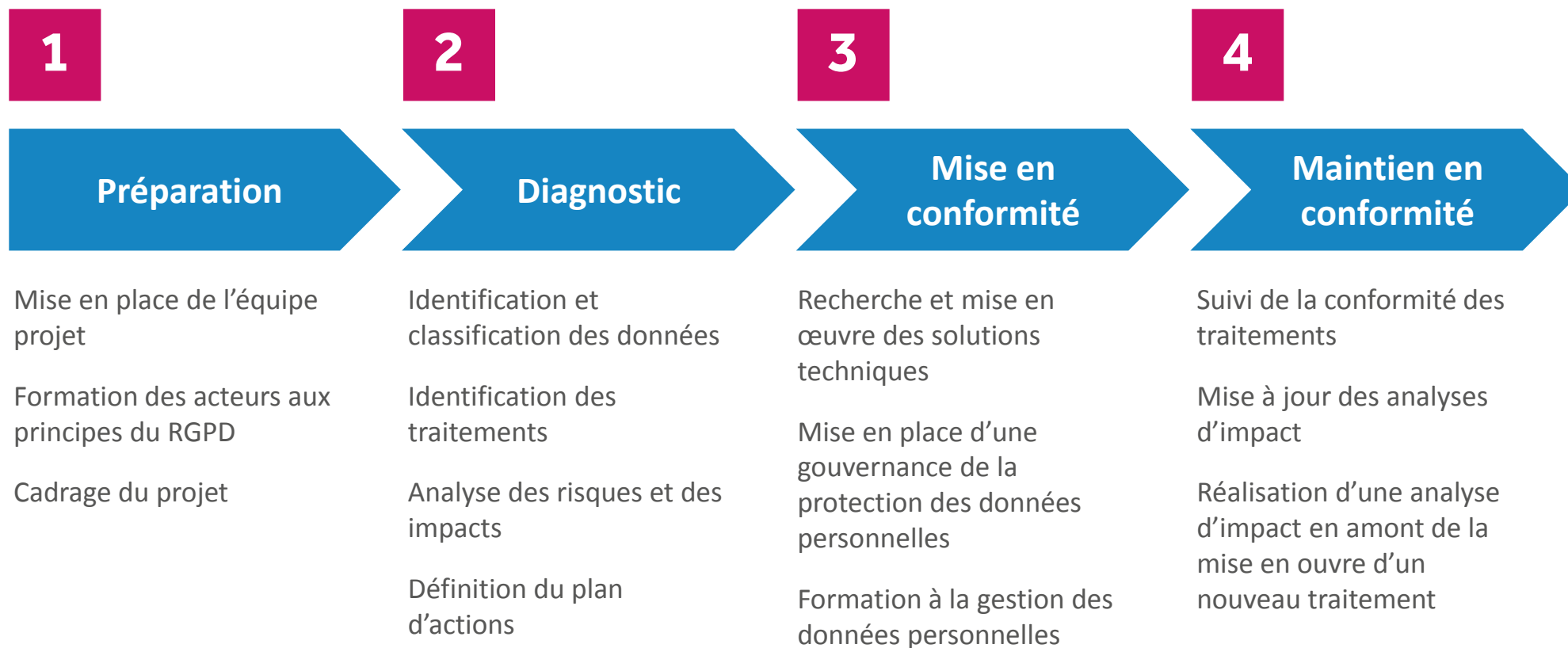
Aca
Nexia



Comment se mettre en conformité ?

IV. COMMENT SE METTRE EN CONFORMITE ?

Roadmap d'un projet RGPD – Le chemin vers la conformité



IV. COMMENT SE METTRE EN CONFORMITE ?

1

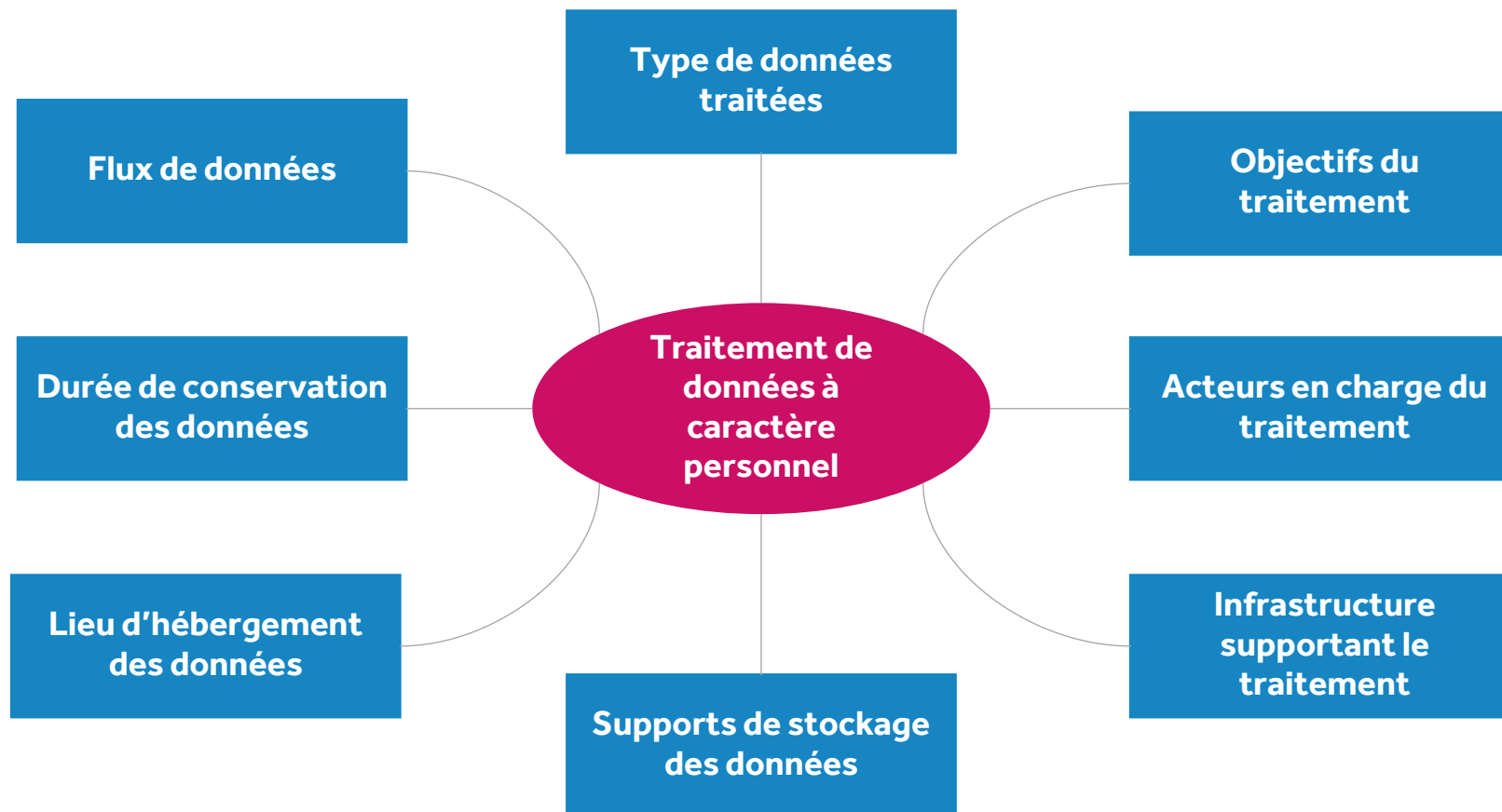
Préparation – La réussite passe par l'implication et la compréhension



IV. COMMENT SE METTRE EN CONFORMITE ?

2

Diagnostic – Recenser les données à caractère personnel



IV. COMMENT SE METTRE EN CONFORMITE ?

2

Diagnostic – Evaluer les risques engendrés par chaque traitement

Identifier les impacts potentiels

- Quels seraient les impacts en cas de perte de confidentialité, d'intégrité et/ou de disponibilité des données ?

Identifier les sources de risques

- Qu'est-ce qui pourrait être à l'origine d'un accès non autorisé, d'une modification illicite ou d'une indisponibilité des données ?

Identifier les menaces réalisables

- Qu'est-ce qui pourrait permettre qu'une menace se réalise (exemples : droits d'accès inappropriés, vol d'un ordinateur) ?

Identifier les mesures de prévention existantes

- Quelles solutions techniques permettent de couvrir les risques identifiés (exemples : contrôle d'accès, sauvegardes) ?

Estimer la gravité et la vraisemblance des risques pour les personnes concernées

IV. COMMENT SE METTRE EN CONFORMITE ?

2

Diagnostic – Déterminer et prioriser les actions de mise en conformité



IV. COMMENT SE METTRE EN CONFORMITE ?

3

Mise en conformité – Evaluer ou implémenter les mesures techniques

1

Protéger les données à caractère personnel

- Limiter les données au strict nécessaire (article 6 du RGPD).
- Réduire la durée de conservation des données (articles 6 et 36 du RGPD).
- Cloisonner les données via une gestion appropriée des droits d'accès.
- Chiffrer les données (disque dur, base de données, canal de communication...) en utilisant une solution certifiée par l'ANSSI.
- Anonymiser ou « pseudonymiser » les données.

2

Limiter les impacts sur les données à caractère personnel

- Sauvegarder les données pour assurer leur disponibilité.
- Contrôler l'intégrité des données en utilisant une fonction de hachage, une signature électronique... certifiée par l'ANSSI.
- Tracer l'activité via une journalisation des événements de sécurité.
- Mettre en place une organisation opérationnelle pour gérer les violations de données.

3

Réduire les risques sur les données à caractère personnel

- Authentifier les utilisateurs via des moyens adaptés et robustes.
- Gérer les accès (création/modification, désactivation et revue) de façon appropriée (y compris pour les tiers).
- Restreindre les droits d'accès de façon appropriée et limiter et encadrer l'utilisation des comptes génériques.
- Lutter contre les codes malveillants via l'installation et la mise à jour d'un logiciel antivirus.
- Contrôler les accès physiques via la mise en œuvre de moyens d'authentification (badge, code...).
- Mettre en place les dispositifs de protection environnementale des salles informatiques et en assurer la maintenance.

IV. COMMENT SE METTRE EN CONFORMITE ?

3 Mise en conformité – Evaluer ou implémenter les mesures techniques

4

Sécuriser les supports de stockage des données à caractère personnel

- Maintenir à jour les logiciels et matériels (applications métiers, base de données, systèmes d'exploitation, firewalls...).
- Protéger l'intégrité, la disponibilité et la confidentialité des codes sources des applications développées en interne.
- Surveiller les modifications apportées à certains fichiers ou répertoires.
- Sécuriser les postes de travail (câble de sécurité, masque de confidentialité...).
- Considérer l'usage des terminaux mobiles (smartphones, tablettes...).
- Maîtriser l'usage des réseaux sans fil.

5

Assurer la gouvernance de la protection des données à caractère personnel

- Définir les rôles et responsabilités des parties prenantes et mettre en place un comité de suivi.
- Mettre à jour la cartographie des risques des traitements de façon périodique (et a minima à chaque évolution).
- Formaliser les objectifs et les règles à appliquer en matière de protection de la vie privée.
- Former les parties prenantes.
- Intégrer la protection de la vie privée dans les projets.
- Superviser la protection de la vie privée à travers en particulier un contrôle régulier des traitements.

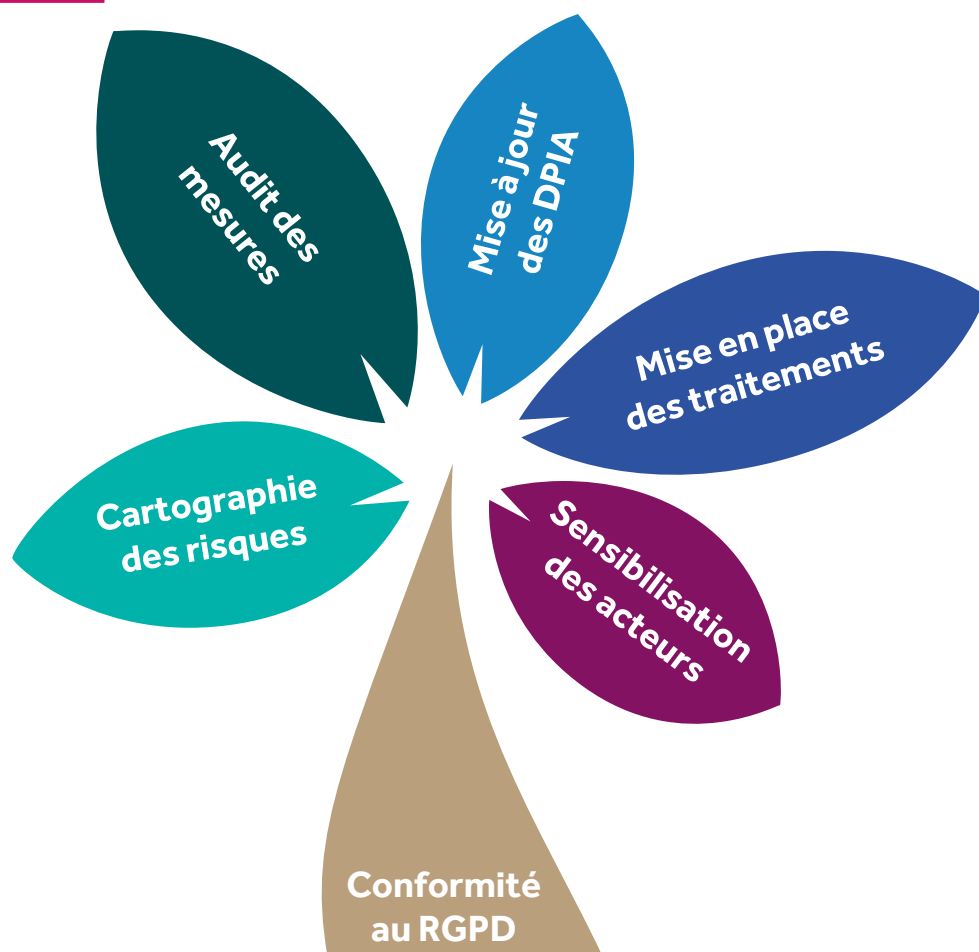


Il convient d'évaluer l'implémentation et l'efficacité des mesures techniques existantes.

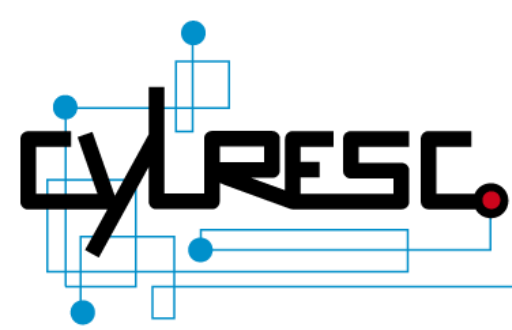
IV. COMMENT SE METTRE EN CONFORMITE ?

4

Maintien en conformité – Ce qu’il convient de faire pour rester conforme



- 
Cartographie des risques
 Réévaluer les risques à chaque évolution majeure des traitements et a minima chaque année.
- 
Audit des mesures
 Réaliser des audits de sécurité pour vérifier l'efficacité des mesures techniques.
- 
Mise à jour des DPIA
 Mettre à jour les DPIA en fonction de l'évolution des traitements, des risques et des mesures.
- 
Mise en place des traitements
 Réaliser un DPIA dès la conception d'un nouveau traitement.
- 
Sensibilisation des acteurs
 Mettre en place un programme de sensibilisation continue des parties prenantes.



IV. COMMENT SE METTRE EN CONFORMITE



Mettre en place un processus d'intervention en cas d'incident

- ✓ Outre les aspects techniques :
 - Gérer les relations publiques
 - Stratégie de communication

Former ses salariés à la cybersécurité

Le recours à la délégation de pouvoirs

- ✓ Transfert de la responsabilité au préposé



Aca
Nexia



Anticiper les poursuites et les sanctions

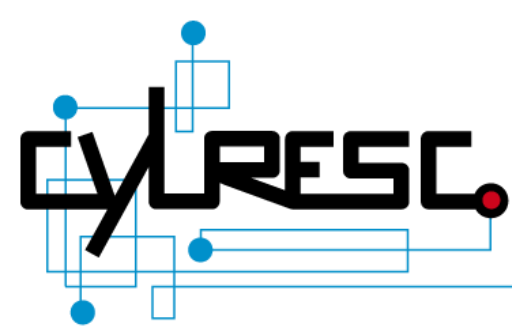
Les conséquences du vol de données personnelles

- **Pour les tiers**

- Le droit de réclamation de toute personne concernée auprès de l'autorité de contrôle :
 - Formulaire en ligne gratuit
 - Mesures correctrices de l'autorité de contrôle : avertissement, rappel à l'ordre, mise en conformité, audits, obtention de l'accès à toutes les données et aux locaux,...
 - Amendes administratives : amendes potentielles :
 - 10M€ ou 2% du CA annuel mondial (manquement au privacy by design, by default, etc.)
 - 20M€ ou 4% du CA annuel mondial total (manquements au droit des Personnes)
 - Action en justice à l'initiative de l'autorité de contrôle



Une règle essentielle : anticiper, coopérer et réagir !



V. ANTICIPER LES POURSUITES ET LES SANCTIONS



- **Pour les tiers**

- Le recours juridictionnel :

- L'action en justice des victimes de violation du traitement des données à caractère personnel pour vol, violation des règles en matière de protection des données, non respect de la vie privée, violation du secret professionnel, du secret de fabrique, atteinte à l'image,...
 - L'auteur de la violation : le responsable du traitement ou le sous-traitant
 - Les modalités : plainte pénale, citation directe, plainte avec CPC,...
 - Les conséquences : sanctions pénales et/ou civiles ou commerciales, demandes de cessation du dommage, ou de l'atteinte subi et la réparation du préjudice moral ou matériel subi
 - Le recours juridictionnel n'est pas exclusif d'une réclamation auprès de l'autorité de contrôle

- **Pour les entreprises**

- Perte de réputation
 - Risque de dépôt de bilan



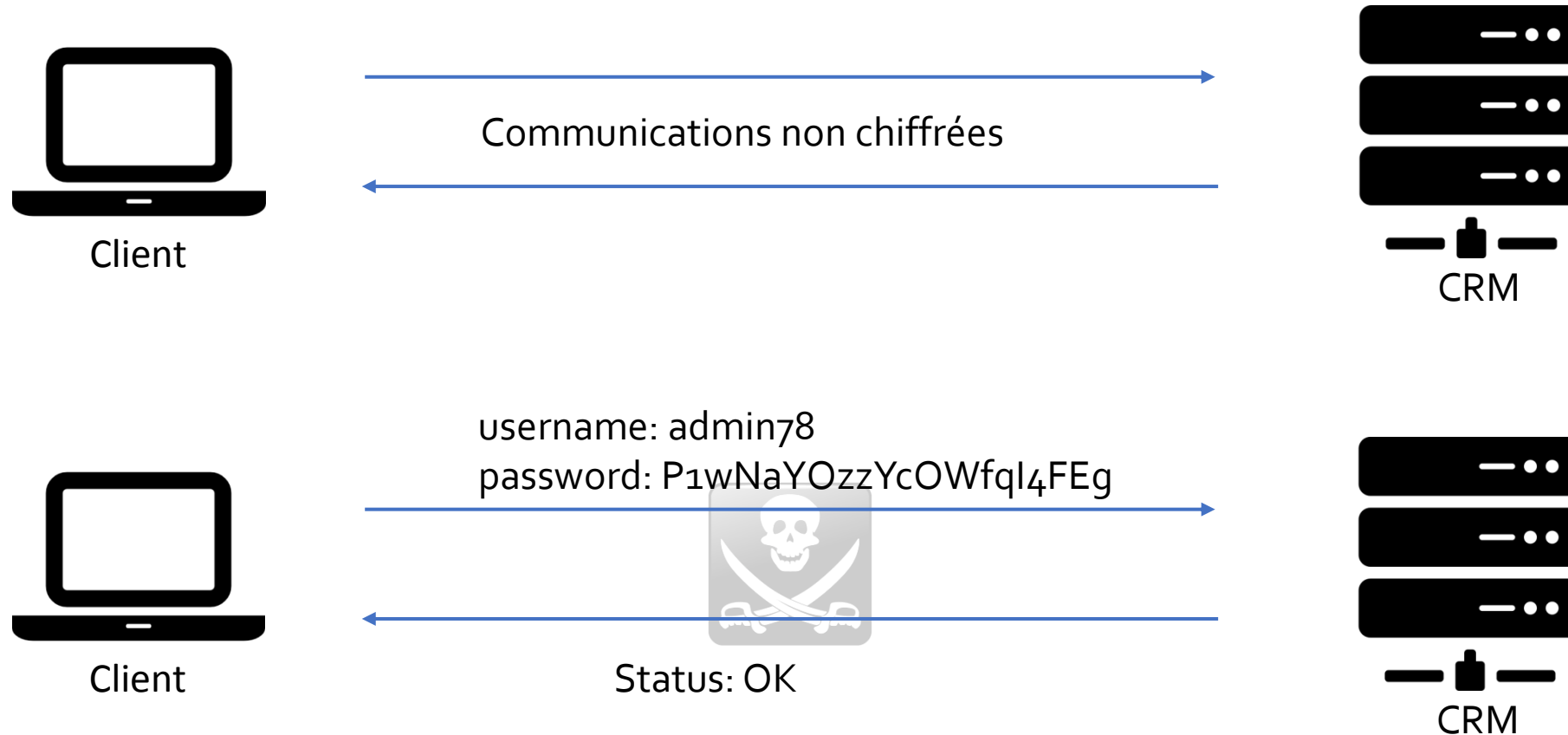
Aca
Nexia



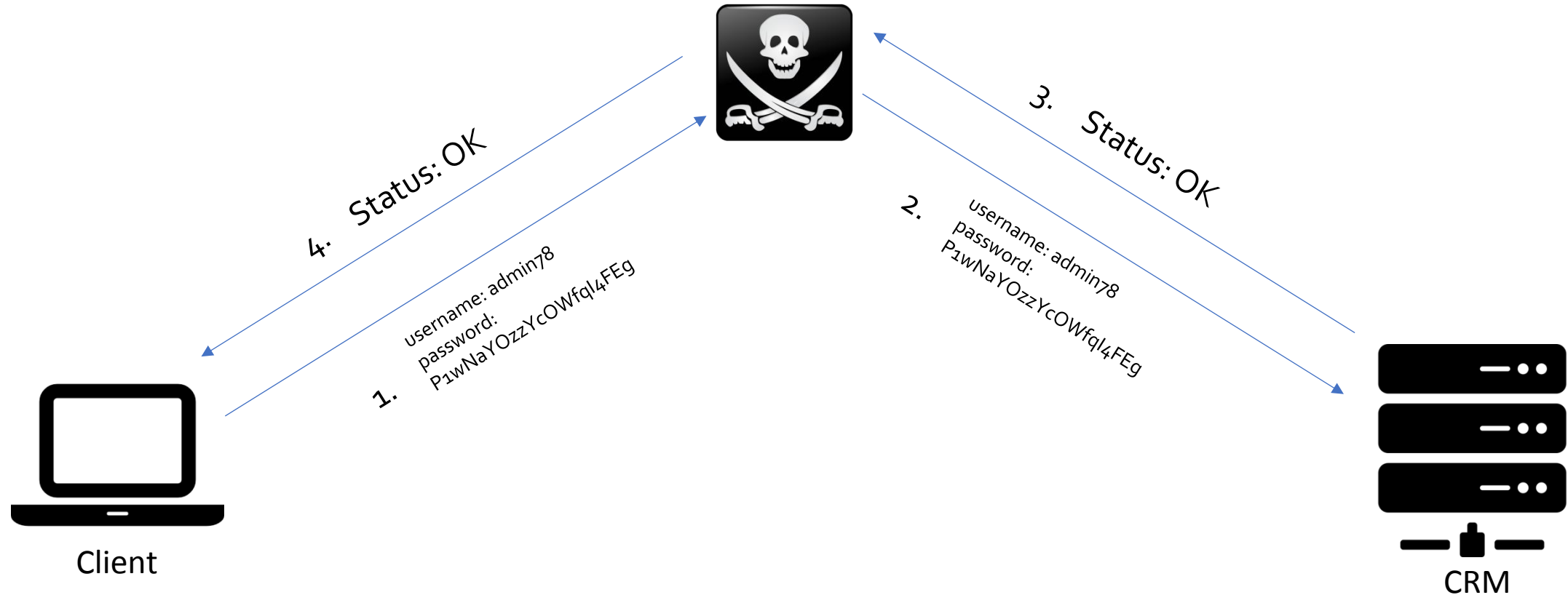
Le vol de données personnelles (démonstration)

VI. VOL DE DONNEES PERSONNELLES

Communication client-serveur



Attaque de l'homme du milieu (Man In The Middle)





Corbeille



Pro

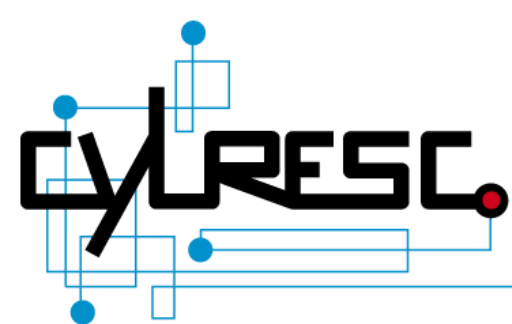


Posez-moi une question



17:48
30/11/2017





VI. VOL DE DONNEES PERSONNELLES

1	Nom	Prénom	Adresse	Tel
2	LEUNG	Colin	11 Rue Descartes	0608120151
3	MOISAN	Jade	8 rue madigan	0608123881
4	BOUABO	Samir	8 Rue Victor	0607995596
5	LEUNG	Hugues	27 Rue Pierre-Léon	0601312956
6	BOUABO	Nelly	27 rue Gambetta	0608887186
7	BOUABO	David	5 Rue Louis 1er de Malilly	0607994879
8	MOISAN	Laurence	21 Rue Jean-Louis-Méjoly	0603861989
9	BOUABO	Colin	20 rue de l'hôpital	0601207887
10	THOMAS	Benjamin	69 Rue Pascal	0607804799
11	LEUNG	Julien	18 Rue du Palais	0601206119
12	BOUABO	Benjamin	20 rue Gambetta	0601791829
13	BOUABO	Samir	69 Rue Andréa de l'École	0607887949
14	LEUNG	Hubert	11 Rue Beaumont	0601301959
15	BOUABO	Samir	20 rue de l'hôpital	0607812881
16	BOUABO	Julien	4 Rue Franklin	0608815489
17	BOUABO	Nathaniel	9 Rue Pierre-Léon	0601301959
18	BOUABO	Colin	22 rue Louis-Stanislas	0601307881
19	BOUABO	Samir	8 Rue André de l'École	0607887949
20	LEUNG	Colin	21 Rue Pierre-Léon	0601301959
21	THOMAS	Colin	7 rue Andréa de l'École	0608815489
22	BOUABO	Colin	79 Rue Louis 1er de Malilly	0604409887
23	BOUABO	Colin	8 Rue Descartes	0607887949
24	BOUABO	Colin	20 rue Andréa de l'École	0608815489
25	BOUABO	Colin	69 Rue Pascal	0607804799
26	BOUABO	Colin	21 Rue Beaumont	0601301959
27	BOUABO	Colin	20 rue de la Paix	0601207887
28	BOUABO	Colin	69 Rue Pascal	0607804799
29	BOUABO	Colin	21 Rue Beaumont	0601301959
30	BOUABO	Colin	20 rue de la Paix	0601207887
31	BOUABO	Colin	4 Rue Gambetta	0607887949
32	BOUABO	Colin	18 Rue du Palais	0601206119
33	BOUABO	Colin	20 rue Gambetta	0601791829
34	BOUABO	Colin	5 Rue Louis 1er de Malilly	0607994879
35	BOUABO	Colin	21 Rue Beaumont	0601301959
36	BOUABO	Colin	21 Rue Beaumont	0607804799
37	BOUABO	Colin	79 Rue Louis 1er de Malilly	0604409887
38	BOUABO	Colin	21 Rue Louis-Stanislas	0601307881

- Fichier récupéré pendant un test d'intrusion
- Base de données contenant l'intégralité des partenaires de l'audit (plus de 40 000 entrées, ...)
- Vecteurs d'entrées :
 - Services pas à jour
 - Politique de mot de passe trop faible

Vol de données personnelles

Maintenir un registre
des violations de
données personnelles
et des procédures de
notifications à la CNIL

Toute violation de
données personnelles
doit être notifiée à la
CNIL sous 24 heures

Notifier également la
(ou les) personne(s)
concernée(s)



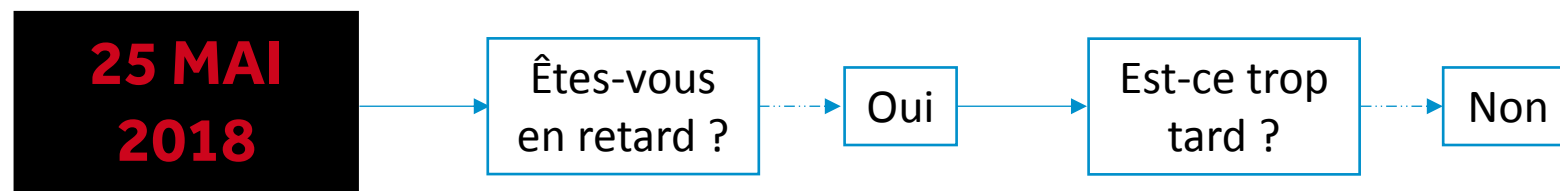
Aca
Nexia



Conclusion

HACKING DETECT

01010101110000101
01010101110000101



RGPD

- Un avantage concurrentiel pour votre entreprise
 - ✓ Accountability (sous-traitance, partenariats)
- Les mesures mises en place dans le cadre du RGPD permettent de protéger non seulement **les données personnelles** mais également **le système d'information** dans son ensemble

La mise en conformité :

- ✓ Etude de l'existant
- ✓ Analyse de risques
- ✓ Identification et correction des anciens process
- ✓ Mise en place de nouveaux process
- ✓ Formalisation des actions effectuées (documentation)
- ✓ Audits réguliers

Des questions?

CYLRESC

7 ter, rue aux Prêtres
78790 Montchauvet
Xavier BEAUSSAC

07 86 43 40 35

xbeaussac@cylresc.eu

Christophe SZWEDO

06 03 71 94 21

cszwedo@cylresc.eu

ACA NEXIA

31, rue Henri Rochefort
75017 Paris

Philippe FOUCAULT

06 84 21 49 59

p.foucault@aca.nexia.fr

Dominique DESCOURS

06 85 40 68 37

d.descours@aca.nexia.fr

SELARL LMC PARTENAIRES
Maître Aurélie SEGONNE-
MORAND

6, rue Jean-Pierre Timbaud
Immeuble Le Campus – Bât, B1
78180 Montigny-le-Bretonneux

01 30 21 18 92

mail@lmcpartenaires.fr