Les nouveaux guides de la CNIL

Comment gérer des risques dont l'impact ne porte pas sur l'organisme

Matthieu GRALL

CLUSIF – Colloque « conformité et analyse des risques »
13 décembre 2012

Service de l'expertise - Commission Nationale de l'Informatique et des Libertés

La CNIL en bref

Statut et composition

- Une autorité administrative indépendante composée de 17 membres (hauts magistrats, parlementaires, conseillers économiques et sociaux, personnalités qualifiées)
- Une présidente élue par ses pairs : Isabelle Falque-Pierrotin
- 160 agents

Missions

- Informer et conseiller : autorités, professionnels et grand public
- Contrôler les fichiers : déclaration et contrôles sur place
- Sanctionner en cas de non-respect de la loi

Le rôle de la CNIL dans l'encadrement des fichiers

EN AMONT

Pédagogie - Conseil - Expertise

- Action de sensibilisation à la loi : tutoriels, guides, etc.
- Recours au CIL (correspondant informatique et libertés) permettant :
  - allègement des formalités ;
  - conseil et suivi de la légalité des applications mises en place.
- Accomplissement des formalités préalables :
  - identifier les formalités ;
  - dispenses de déclaration ;
  - normes de simplification tant dans le régime déclaratif que d'autorisation ;
  - demandes d'avis, d'autorisation.
- Les demandes de conseil (RFID, nanotechnologies, etc.)
- De la conformité des codes de déontologie à la labellisation
- Le groupe des CNIL européennes (G29) et les standards internationaux

MISE EN ŒUVRE DU TRAITEMENT

EN AVAL

Plaintes - Contrôles – Sanctions

- Plaintes : 5738 plaintes reçues
- Contrôles : 385 contrôles réalisés, dont :
  - 24% à la suite d'une plainte ;
  - 40% dans le cadre du programme des contrôles européens ;
  - 25% en réaction à des sujets d'actualité et
  - 11 % dans le cadre de procédure de sanction.
- Sanctions : 65 mises en demeures et 19 sanctions, dont :
  - 13 avertissements :
  - 5 sanctions financières ;
  - 1 injonction de cesser le traitement.

(chiffres de 2011)

Pourquoi gérer les risques sur les libertés et la vie privée ?

1. Assurer la sécurité des données

Article 34 de la loi informatique et liberté

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et ***des risques présentés par le traitement****, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »*

(obligation de moyens)

Sanction administrative	Avertissement (privé ou public), Sanction financière (150 000 € d'amende la 1ére fois) Injonction de cesser le traitement
Sanction pénale	*Non respect de l'obligation de sécurité* (art. 226-17 du code pénal) : 5 ans d'emprisonnement et 300 000 € d'amende**.**

2. Assurer la maîtrise par les personnes concernées

Articles 38 à 43 de la loi informatique et liberté

Le responsable de traitement est tenu de garantir la maîtrise de leurs données aux personnes concernées et notamment **le libre exercice de leur droit** :

- d'opposition ;
- de rectification ;
- de suppression ;
- d'accès.

(obligation de résultats)

Sanction administrative

Avertissement (privé ou public),
Sanction financière (150 000 € d'amende la 1ére fois)
Injonction de cesser le traitement

Sanction pénale

Refus ou entrave aux droits des personnes (art. 131-13 du code pénal) :
1500 € par infraction constatée et 3 000 € en cas de récidive.

3. Assurer le respect de la loi Informatique et Libertés

Sanction administrative

Avertissement (privé ou public),
Sanction financière (150 000 € d'amende la 1ére fois)
Injonction de cesser le traitement

Sanction pénale

Détournement de finalité (art. 226.21 du code pénal) :
5 ans d'emprisonnement et 300 000 € d'amende.

Non-accomplissement des formalités (art. 226-16 du code pénal) :
5 ans d'emprisonnement et 300 000 € d'amende.

Dépassement de la durée de conservation (art. 226-20 du code pénal) :
5 ans d'emprisonnement et 300 000 € d'amende.

Non-respect de la confidentialité (art. 226-22 du code pénal) :
5 ans d'emprisonnement et 300 000 € d'amende,
par imprudence ou négligence 3 ans et 100 000 €

4. Préparer l'avenir

Nouveau règlement (En cours… ?)

– Le responsable de traitement serait tenu de mettre en œuvre des **mécanismes visant à garantir la protection des données dès la conception** et **d'effectuer une analyse d'impact** relative à la protection des données.

Sanction administrative

Avertissement (privé ou public),
Sanction financière (1 000 000€ d'amende ou 2% du CA)
Injonction de cesser le traitement

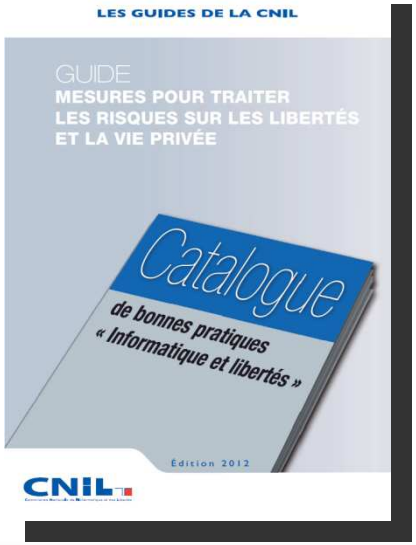
Comment gérer les risques sur les libertés et la vie privée ?

Différences entre SSI et protection de la vie privée

Sécurité des systèmes d'information	Protection de la vie privée
Objectif : protéger l'organisme	**Objectif** : protéger les personnes concernées et leurs droits
Sujet de l'étude : – Toutes les informations manipulées au sein de l'organisme (dont les données à caractère personnel) – Les processus métiers	**Sujet de l'étude** : – Les données à caractère personnel confiées à l'organisme – Les processus légaux
Impacts étudiés : sur l'image, juridiques (dont le non respect de la Loi Informatique & libertés), financiers…	**Impacts étudiés** : sur la vie privée, l'identité humaine, les droits de l'homme, les libertés publiques…

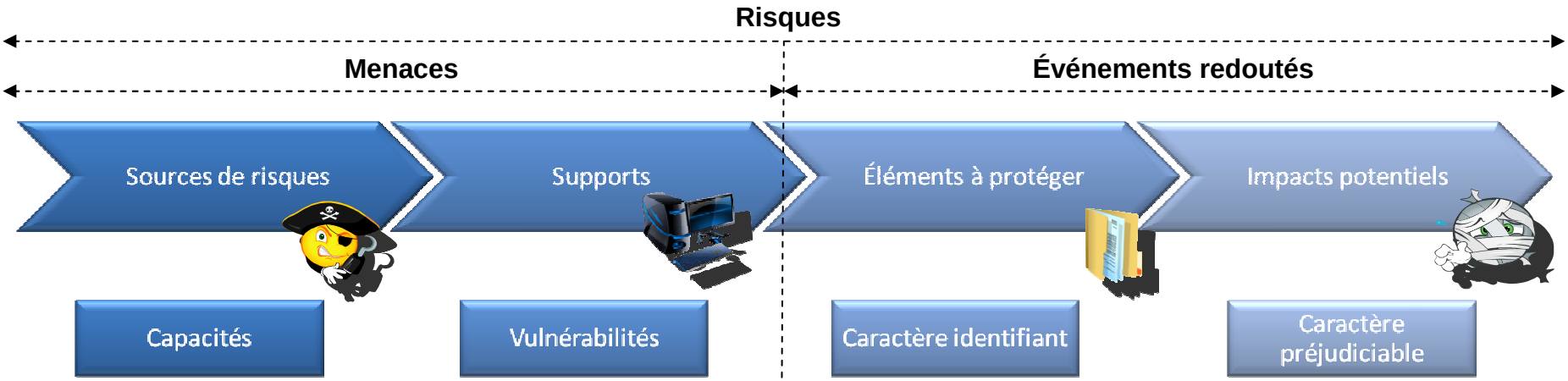
Comment gérer les risques sur la vie privée ?

- **Utiliser une méthode de gestion des risques reconnue**
  - Prendre en compte les spécificités de la protection de la vie privée
    - On étudie les risques et leurs impacts vis-à-vis des personnes concernées
    - On choisit des mesures respectueuses de la vie privée
- **Utiliser les guides de la CNIL**
  - Une méthode « Gérer les risques sur les libertés et la vie privée »
  - Un catalogue de mesures « Mesures pour traiter les risques sur les libertés et la vie privée »



1. Qu’est ce qu’un risque sur la vie privée ?

Un risque est un scénario décrivant un événement redouté et toutes les menaces qui le rendent possible.



Sources de risques
- Personnes externes
- Personnes internes
- Sources non humaines

Supports
- Matériels
- Logiciels
- Réseaux
- Personnes
- Supports papier
- Canaux papier

Éléments à protéger
- Processus
- Données à caractère personnel

Impacts potentiels
- Vie privée
- Identité humaine
- Droits de l’homme
- Libertés publiques

2. Principe de la méthode (application d'EBIOS)

I. Étude du contexte

1. Quels sont les processus (traitement et processus légaux) ?
2. Quelles sont les données à caractère personnel (DCP) ?
3. Quelles sont les références applicables ?
4. Quels sont les supports ?
5. Quelles sont les sources de risques ?

II. Étude des événements redoutés

1. Quel est le caractère identifiant des DCP ?
2. Quels seraient les impacts sur la vie privée si :
   - le traitement était modifié ?
   - les processus légaux n'étaient plus disponibles ?
   - une personne non autorisée accédait aux DCP ?
   - les DCP étaient modifiées ?
   - les DCP disparaissaient ?
3. Quel est le caractère préjudiciable de ces événements redoutés ?

III. Étude des menaces (si gravité élevée)

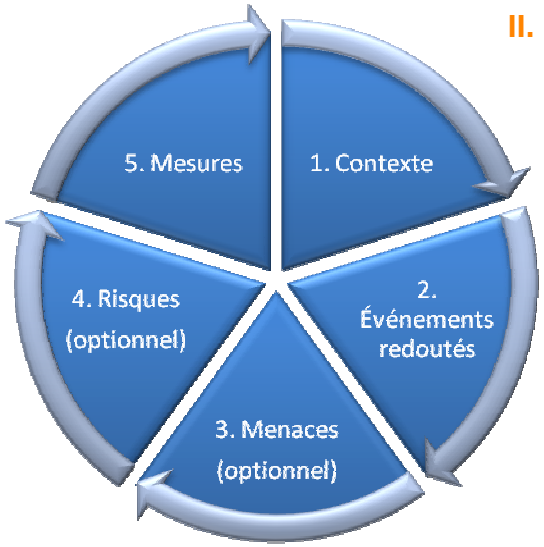
1. Quel est le niveau des vulnérabilités exploitables ?
2. Quelles sont les capacités des sources de risques à les exploiter ?

IV. Étude des risques (si gravité élevée)

1. Quelle est la cartographie des risques ?
2. Quels sont les objectifs de sécurité (modalités de traitement) ?

V. Étude des mesures

1. Quelles actions sur :
   - les éléments à protéger ?
   - les impacts ?
   - les sources de risques ?
   - les supports ?
2. Quels sont les risques résiduels ?



3. Vision projet : rôles des parties prenantes

- **La maîtrise d'ouvrage** (MOA) définit le traitement, identifie les événements redoutés et réalise la cartographie des risques.
- **La maîtrise d'œuvre** (MOE) étudie les menaces et propose des mesures pour traiter les risques.
- **Le CIL et/ou le responsable SSI** s'assure(nt) que les enjeux « Informatique et libertés » sont bien pris en considération. *(garant de la méthode)*
- **Le responsable de traitement** approuve l'étude et accepte les risques résiduels.

A réaliser	Responsable de traitement	CIL / RSSI	MOA	MOE
1. Etude du contexte	Approbateur	Consulté	Responsable	-
2. Etude des événements redoutés	Approbateur	Consulté	Responsable	-
3. Etude des menaces	Approbateur	Consulté	-	Responsable
4 . Etude des risques	Approbateur	Consulté	Responsable	Informée
5 . Etude des mesures	Approbateur	Consulté	Consultée	Responsable

4. Un catalogue de mesures

I. Agir sur les éléments à protéger

1. Minimiser les DCP
2. Gérer les durées de conservation des DCP
3. Informer les personnes concernées
4. Obtenir le consentement des personnes concernées
5. Permettre l'exercice du droit d'opposition
6. Permettre l'exercice du droit d'accès direct
7. Permettre l'exercice du droit de rectification
8. Cloisonner les DCP
9. Chiffrer les DCP
10. Anonymiser les DCP

II. Agir sur les impacts

21. Sauvegarder les DCP
22. Protéger les archives de DCP
23. Contrôler l'intégrité des DCP
24. Tracer l'activité sur le système informatique
25. Gérer les violations de DCP

III. Agir sur les sources de risques

31. S'éloigner des sources de risques
32. Marquer les documents contenant des DCP
33. Gérer les personnes qui ont un accès légitime
34. Contrôler l'accès logique des personnes
35. Gérer les tiers qui ont un accès légitime aux DCP
36. Lutter contre les codes malveillants
37. Contrôler l'accès physique des personnes
38. Se protéger contre les sources non humaines

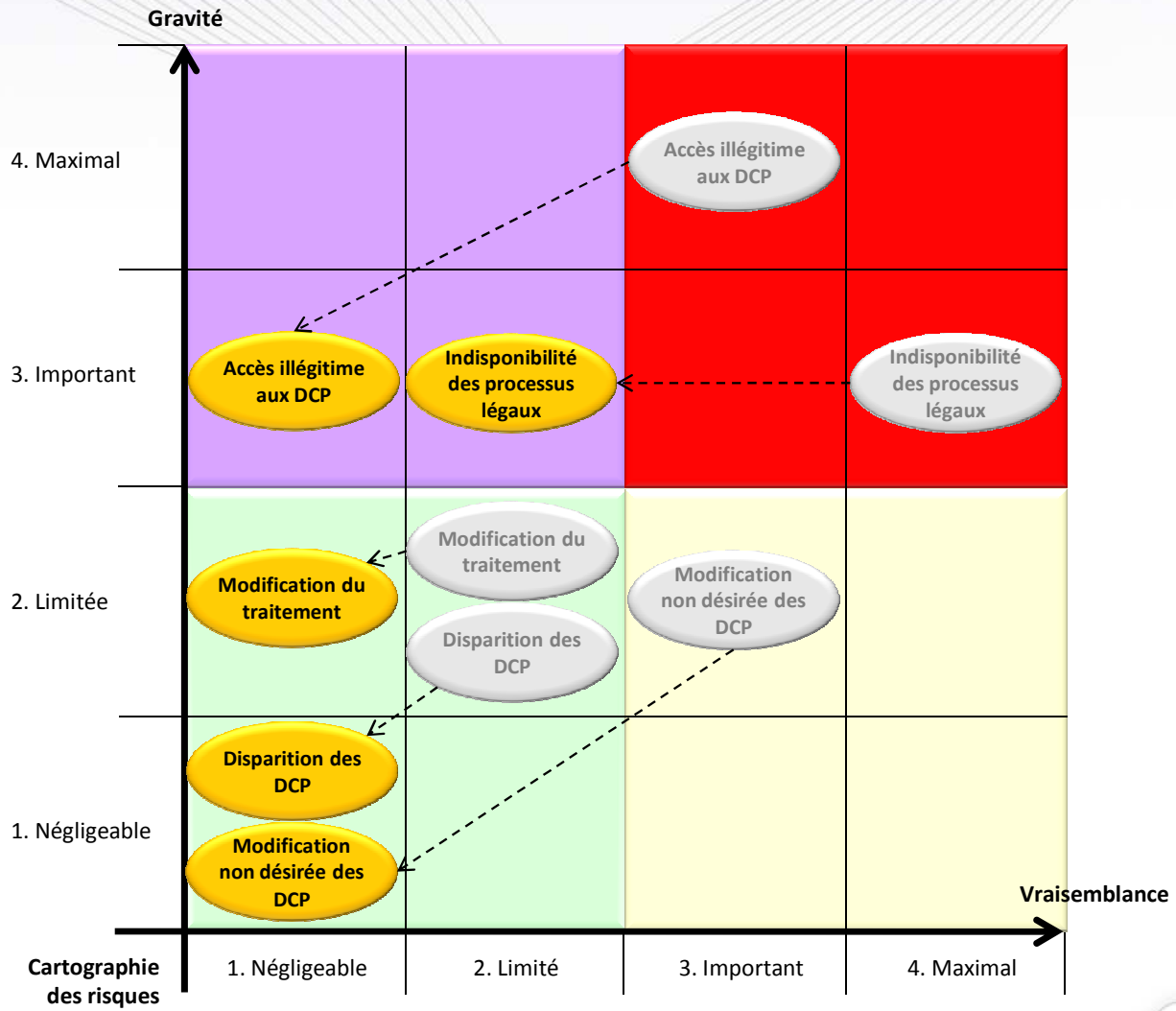
IV. Agir sur les supports

41. Réduire les vulnérabilités des logiciels
42. Réduire les vulnérabilités des matériels
43. Réduire les vulnérabilités des canaux informatiques
44. Réduire les vulnérabilités des personnes
45. Réduire les vulnérabilités des documents papier
46. Réduire les vulnérabilités des canaux papier

V. Mesures transverses (au niveau de l'organisme)

51. Gérer l'organisation de protection de la vie privée
52. Gérer les risques sur la vie privée
53. Gérer la politique de protection de la vie privée
54. Intégrer la protection de la vie privée dans les projets
55. Superviser la protection de la vie privée

5. Le résultat : la cartographie des risques



Pour aller plus loin…

- Les deux guides sont accessibles en ligne

  http://www.cnil.fr/en-savoir-plus/guides/

- Le Club EBIOS a publié deux études de cas
  - Gestion des patients d'un cabinet médical
  - Géolocalisation de véhicules d'entreprise

  http://www.club-ebios.org/site/productions.html