CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Rencontre AFCDP - CLUSIF

Apports de la CNIL pour la SSI
Une aide ou un risque ?

Levallois Perret, 25 octobre 2012

Eric Grospeiller

Fonctionnaire de Sécurité des Systèmes d'Information des ministères des affaires sosciales

Les objectifs

CNIL

- Protéger nos libertés à l'ère numérique en :
  - Garantissant l'anonymat,
  - Préservant l'identité humaine
  - Garantissant la transparence
  - Préservant la vie privée

RSSI

- Garantir la sécurité des systèmes d'informations et des données en fonction du besoin exprimé
  - Dans une démarche « Risque » métier
  - Selon une classification « DICP »
  - En utilisant des méthodes standardisés ou imposées

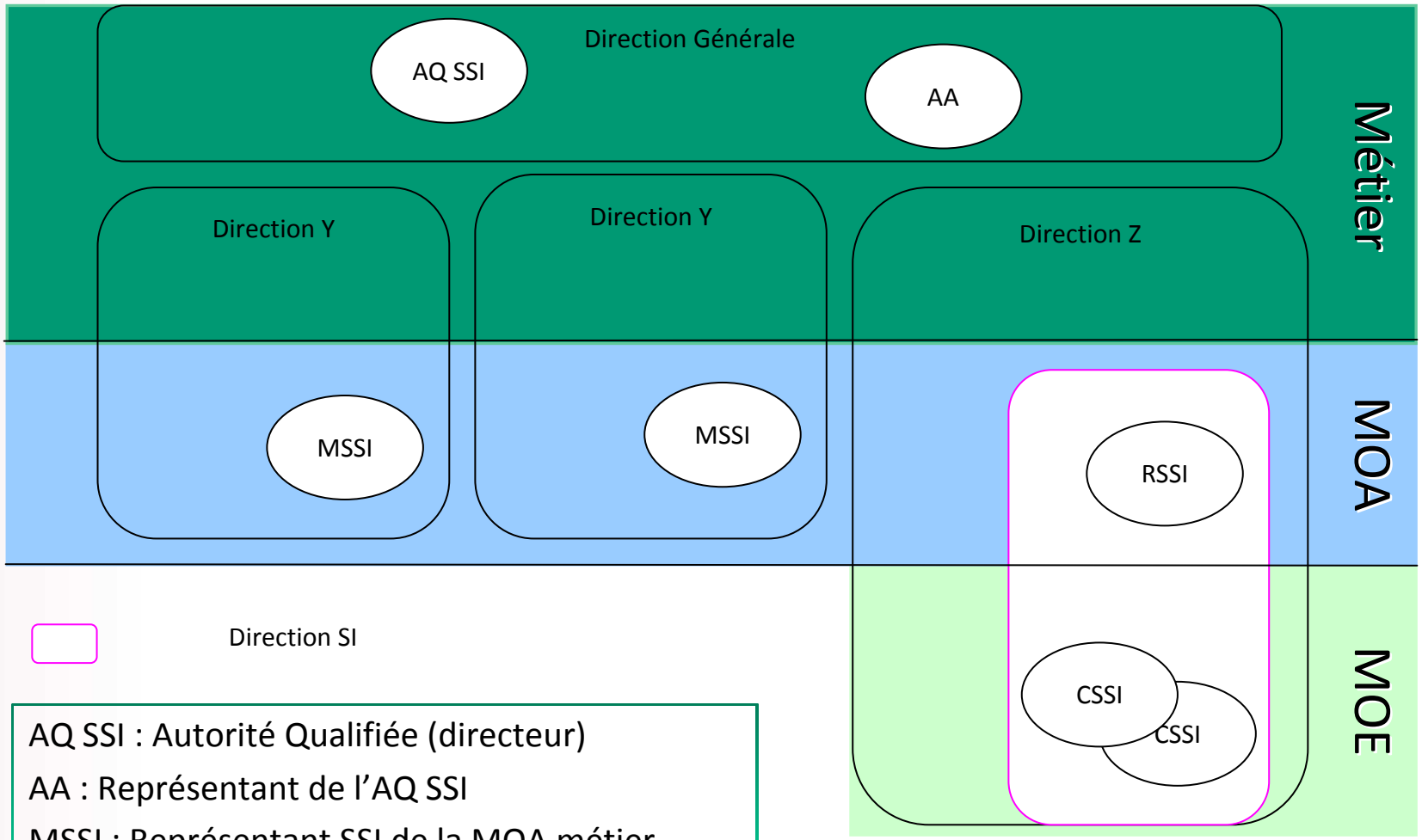
CNIL et LIL

- CNIL, organisme de
  - Définition :
    - D'obligations
    - De moyens
    - D'organisation
  - Recommandations,
  - Contrôle,
  - Sanction

- LIL :
  - Une loi, qui fixe le cadre de traitement des données à caractère personnel

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

L'organisation « SSI »



AQ SSI : Autorité Qualifiée (directeur)
AA : Représentant de l'AQ SSI
MSSI : Représentant SSI de la MOA métier
RSSI : Responsable sécurité SI
CSSI : Correspondant SSI

Synthèse des exigences « SSI »

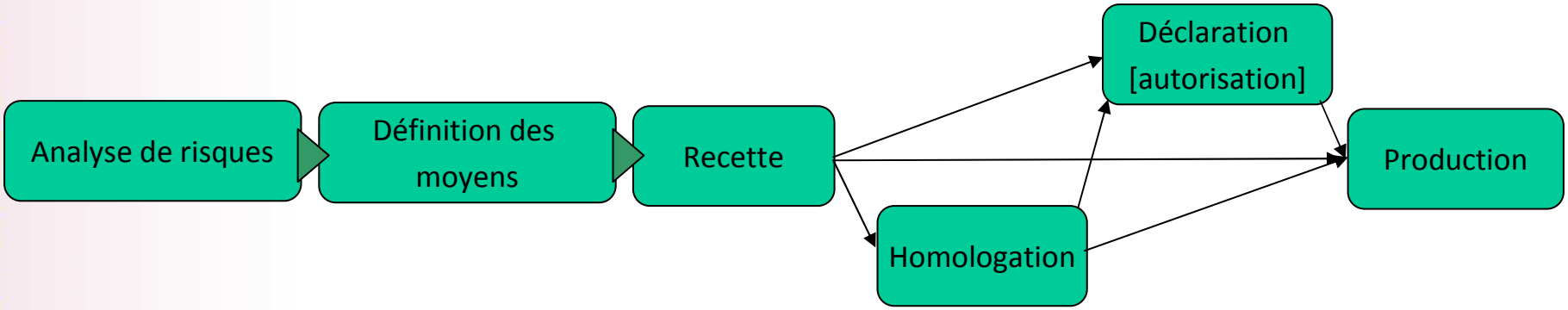
- **La sécurité des fichiers**
  - Tout responsable de traitement informatique de données personnelles **doit adopter des mesures de sécurité physiques** (sécurité des locaux), **logiques** (sécurité des systèmes d'information) et **adaptées** à la nature des données et aux risques présentés par le traitement.
  - **Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende.** art. 226-17 du code pénal
- **La confidentialité des données**
  - Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit **des destinataires** explicitement désignés pour en obtenir régulièrement communication et **des «tiers autorisés»** ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc).
  - **La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 € d'amende.**
  - **La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende.** art. 226-22 du code pénal
- **La durée de conservation des informations**
  - Les données personnelles **ont une date de péremption**.
  - Le responsable d'un fichier fixe **une durée de conservation raisonnable** en fonction de l'objectif du fichier.
  - **Le code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée de 5 ans d'emprisonnement et de 300 000 € d'amende.** art. 226-20 du code pénal

http://www.cnil.fr/vos-responsabilites/vos-obligations/

Synthèse méthodologique

- Démarche CNIL : Développement de la Délibération de la CNIL n° 81-094 du 21 juillet 1981 portant adoption d'une recommandation (la 3ème) relative aux mesures générales de sécurité des systèmes informatiques prévoyait déjà « que l'évaluation des risques et l'étude générale de la sécurité soient entreprises systématiquement pour tout nouveau traitement informatique, et réexaminées pour les traitements existants ».

- Cette démarche est cohérente avec l'approche ISO et RGS, ce dernier ajoutant la nécessité d'homologation.



http://www.cnil.fr/dossiers/securite/

Classification des données, un apport majeur

La classification en confidentialité est régie par un ensemble de textes nationaux avec des équivalences internationales. La préoccupation majeure porte sur les information classifiées défense. Pour les informations non classifiées défense, deux niveaux sont définis, ce qui nécessite d'être divisée en sous catégories.

Les niveaux de classification diffèrent d'un pays à l'autre. La plupart d'entre eux correspondent aux catégories ci-dessous.

Classifié défense / Non classifié défense — Habilitation et Besoin d'en connaître

Dénomination	Dénomination anglaise	Description
Très secret	*Top Secret*	Le plus haut niveau de classification de l'information. La divulgation publique de cette information pourrait causer un dommage exceptionnellement grave pour la sécurité nationale.
Secret	*Secret*	La divulgation publique d'une information classée secret pourrait nuire sérieusement à la sécurité nationale.
Confidentiel	*Confidential*	La divulgation publique d'une information classée confidentielle pourrait nuire ou être préjudiciable pour la sécurité nationale.
Restreint	*Restricted*	La divulgation publique d'une information classée restreinte pourrait causer des effets indésirables. Quelques pays n'utilisent pas cette classification.
Non classifié	*Unclassified*	Techniquement, ce n'est pas une classification, mais ce niveau est utilisé pour les documents gouvernementaux dont le niveau de sensibilité ne correspond pas à une des classifications ci-dessus. Ces documents peuvent être lus sans avoir une habilitation spécifique.

Propositions de sous catégories pour la dénomination « restreint ».

Secret	La diffusion d'information peut causer des dommages extrêmement graves pour l'organisme. Ces informations tomber sous le coups de la protection du patrimoine industriel et scientifique, du secret commercial, ou de la protection des données à caractère personnelles « sensibles ».
Confidentiel	La divulgation peut nuire sérieusement à l'organisme.
Restreint / Interne	L'information peut être préjudiciable à l'organisme, sans toutefois avoir d'impacts importants
Publique	Information destinée à être diffusée librement

Echelle des besoins relatives aux DCP

Echelle de classification des informations pour la confidentialité

Niveau	Libellé	Exemples
4	**Secret (LIL, données sensibles)**	**Informations nominatives :** - Informations de santé : pathologie, antécédents familiaux, observation médicale, - situations ou comportements à risques - Informations relatives aux infractions, condamnations ou mesures de sûreté (infractions, condamnations, mesures de sécurité) - Informations relatives à des suspicions de fraudes ou d'infractions - Origines raciales ou ethniques, opinions politiques, philosophiques, religieuses, appartenances syndicales des personnes, la vie sexuelle
		Informations non nominatives : - Informations liées à l'organisation et à la stratégie de l'organisme, dont la révélation aurait un impact négatif sur la conduite de ses missions -Informations liées aux mécanismes de fraudes et aux failles ou vulnérabilités de sécurité, dont la révélation pourrait être exploitée pour nuire aux missions de l'organisme - Données relevant du patrimoine scientifique et technique d'infrastructures vitales
3	**Confidentiel (LIL DCP directes)**	**Toute information nominative ne rentrant pas dans la classe « secret »** et notamment : - NIR, Etat-civil, identité, données d'identification (nom, prénom, adresse, photographie, date, lieu de naissance), - Appréciation sur les difficultés sociales des personnes - Informations d'ordre économique et financière (revenus, situation financière) - Vie personnelle : habitude de vie, situation familiale et sociale - Vie professionnelle : CV, Situation professionnelle, Scolarité, formation, Distinction - Informations biométriques : contour de la main, empreintes digitales, réseaux veineux, iris de l'œil, reconnaissance faciale, reconnaissance vocale, autre procédé
2	**Restreint (LIL, DCP indirectes)**	- Données de localisation (déplacement, données GPS, GSM, etc) par satellite, par téléphone mobile ou autre (adresse IP, logs, etc) - Identifiants des terminaux, Identifiants de connexions, Information d'horodatage… - procédures, description de processus, instructions, Intranet - enregistrements non nominatifs (dates, heures, actions, états, etc.) - informations personnelles que le salarié a identifiées explicitement comme tel dans le système d'information - Données de connexion
1	**Publique (Hors LIL)**	Informations ayant vocation à être publiées : éditoriaux, publication Extranet, statistiques publiables, campagnes de communication, etc.

Mais…

- Pour ce faire, il convient d'adopter une vision globale, qui dépasse le seul cadre des activités de l'organisme et des finalités prévues pour ses traitements, et qui permette d'étudier les impacts sur les personnes que ces données concernent. (Guide « gérer les Risques sur les libertés et la Vie Privée », CNIL 2012)

Incidence de la vision globale

- Critères DICP
  - Incompatibilité entre des solutions répondant à un besoin type D et la confidentialité
    - « Vital » pour l'entreprise
    - « Vital » pour la personne

- Organisation interne
  - En fonction du rattachement du CIL, de son positionnement, manque de légitimité, conflit d'intérêt ou absence de visibilité ?

Merci pour votre attention