



Move securely within the cyberworld

Séance d'information « Jonk Handwierk »
du 8/2/2018 à lalux

**Le RGPD
à la portée des PME**

**Dr. Carlo Harpes
Gérant**

itrust consulting s.à r.l.
55, rue Gabriel Lippmann
L-6947 Niederanven

Tel: +352 26 176 212 6
Fax: +352 26 710 978
Web: www.itrust.lu

Application dès le 27 mai 2018 (après 2 ans de temps d'adaptation) pour toute entité traitant des DCP.

Déf : DCP = Données à Caractère Personnel

toute information se rapportant à une personne physique identifiée ou **identifiable** (ci-après dénommée « **personne concernée** »); 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;

Acro.	Explication	Anglais	
AIPD	Analyse d'impact relative à la protection des données	DPIA	Data protection impact analysis
RGPD	Règlement général pour la protection des données	DPIA	
DCP	Donnée(s) à caractère personnel	PII	Personally identifiable information
DPD	Délégué à la protection des données	DPO	Data protection officer
	Mesure de protection		(Security) Control
	Personne concernée		PII principle (legal: data subject)
	Responsable du traitement		PII controller
	Processeur de DCP		PII processor

Décisions automatisées

Règles d'entreprise contraignantes

Transferts de DCP vers des pays tiers ou à des organisations internat.

Autorités de contrôle indépendantes (CNPD)

Coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées

Dispositions relatives à des situations particulières de traitement (-> Lois)

journalistes, auteurs, artistes, info publique, identité national, archivage (historique et scientifique), contrat de travail, associations religieuses

Dispositions liées au fonctionnement

a) Principe de légitimité

Le consentement, obligation de service public, une obligation légale, ou protection de la vie. Intérêt justifié à condition que le traitement des données n'affecte la vie privée que de façon minime.

b) Principe de finalité

Strictement limitée à une finalité explicitement déterminée au préalable.
à ce qui est nécessaire pour atteindre des buts expressément fixés d'avance.

c) Principe de nécessité et de proportionnalité

Se limiter aux données liées directement et nécessaire à la finalité initiale.

d) Principe d'exactitude

Données traitées soient correctes et actuelles, rectifiées le cas échéant ou bien effacées.

e) Principe de loyauté

De bonne foi, et non pas à l'insu de la personne concernée.

En outre, les données doivent être effacées ou rendues anonymes le plus rapidement possible. L'utilisation ultérieure de données personnelles à des fins autres que celles initialement prévues est en principe interdite.

f) Principe de sécurité et de confidentialité

Protégé contre traitements non autorisés (manipulations, vols, perte).

Le responsable engage sa responsabilité en cas de non-respect de ce principe.

g) Principe de transparence

Possibilité d'un contrôle personnel.

h) Protection renforcée pour certaines données

origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont **interdits sauf explicitement autorisé** par la CNPD.

i) Principe du respect du droit des personnes

- informer les intéressés sur le respect des droits d'accès et de rectification
- agir sur base du droit d'opposition
- effacer les DCP si non conforme à la loi.

Registre des activités de traitements

- a) Nom et coordonnées du responsable (ou des responsables) et du délégué à la protection des données (DPO) (s'il est nommé).
- b) Finalités
- c) Catégories de personnes concernées et de données (p. ex. données médicales d'enfants)
- d) Catégories de destinataires
- e) Garanties appropriés en cas de destinataires dans un pays tiers
- f) Délais pour l'effacement (si possible)
- g) Description générale des mesures de sécurité (si possible)

Obligatoire sauf

- si moins de 250 employés
- pas de risques pour les droits et libertés,
- occasionnel, **et** données non sensibles.

Le Responsable du Traitement

- a) notifie la CNPD dans les meilleurs délais et, si possible, **72 heures** au plus tard après en avoir pris connaissance (accompagné d'une justification en cas de retard),
- b) à moins que la violation en question ne soit **pas** susceptible d'engendrer **un risque** pour les droits et libertés des **personnes physiques**,
- c) décrit les faits, la nature de la violation, les catégories et le nombre approximatif de personnes concernées, le nombre approximatif d'enregistrements concernés...
- d) donne un point de contact (DPO) pour des questions complémentaires,
- e) décrit les conséquences probables et les mesures prises.
- f) En cas de risque élevé pour des personnes physiques, **communiquer la violation aux personnes concernées**, en termes clairs et simples, incluant les conséquences probables et mesures prises (exception possible, après mûres réflexions...).

Le Processeur de DCP

- a) notifie immédiatement le responsable du traitement.

Toute personne concernée :

- a le droit d'introduire une réclamation auprès de la CNDP,
- peut faire un recours juridictionnel si pas de réponse après 3 mois,
- peut passer par une représentation (UCL, Syndicats...),
- a le droit à une réparation du préjudice subi du responsable ou du processeur.

Le responsable ou processeur DCP :

est exonéré, s'il **prouve** que le fait qui a provoqué le dommage ne lui est nullement imputable.

Amendes administratives (décidées par le CNPD, sans processus judiciaire)

- a) doivent être effectives, proportionnées et dissuasives,
- b) ne sont pas cumulables.
- c) Au maximum : 20 Mio € ou 4 % de votre chiffre d'affaires mondial du dernier bilan annuel
-- le chiffre le plus élevé étant retenu.

La CNPD a le droit d'arrêter votre traitement s'il est non conforme.

L'analyse d'impact relative à la protection des données est obligatoire

- pour le traitement de données sensibles (médicales. financières...)
- pour traitement de données susceptibles d'engendrer **un risque élevé** pour les droits et libertés des personnes physiques.

But de l'AIPD :

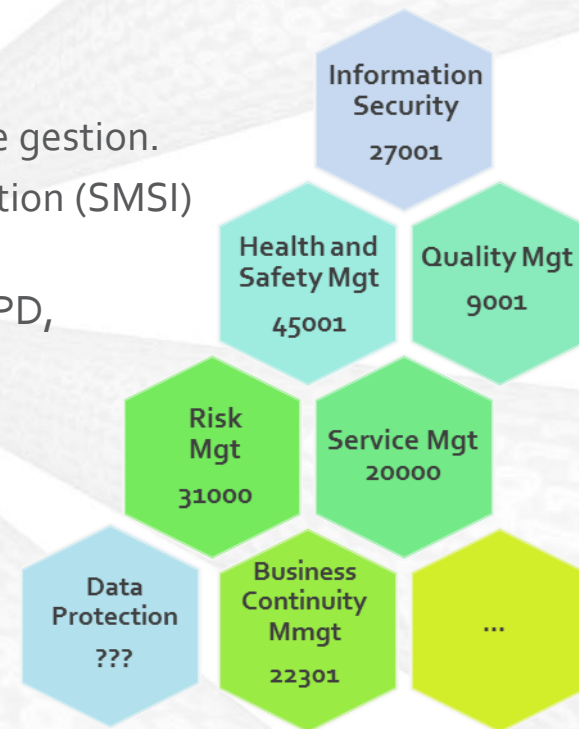
- a) évaluer, l'origine, la nature, la particularité et la gravité de ce risque;
- b) déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le GDPR.

Note : Consultation préalable de la CNPD en cas de risque élevé et traitement impossible compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre.

Nos convictions : Run a single management system!

Pour plus d'efficacité

- Évitez les silos, les conflits d'influences, les inefficacités de gestion.
- ISO 27001- Système de gestion de la sécurité de l'information (SMSI) la première qui utilise une nouvelle structure.
- Elle s'étend (facilement) pour couvrir les exigences du RGPD, de façon intelligente.



Pour plus de recours de pratiques éprouvées :

- Ne reposez pas sur l'enthousiasme de quelques personnes.
- Assurez que la sécurité est bien gérée, par chaque employée.

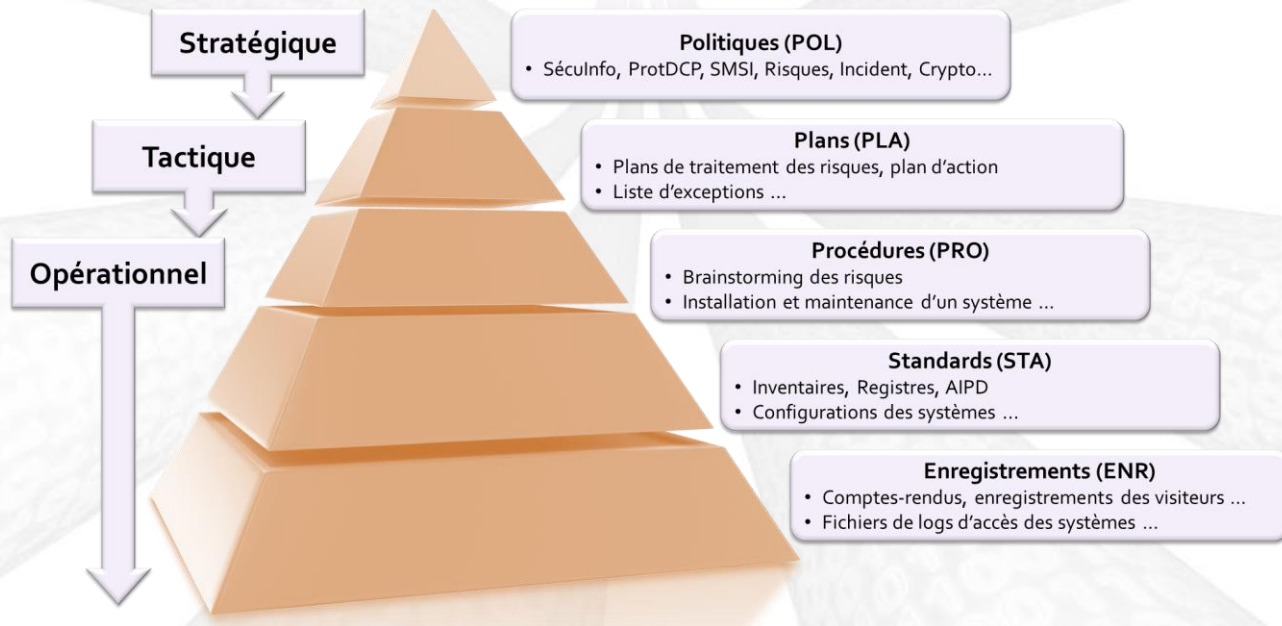


- Un système de management contemporain est organisé autour de 7 activités.



Pour disposer de preuves :

Avec une procédure de gestion de documents, donnez une forme adéquate et une valeur à vos documents, afin de prouver que vous avez pris les bonnes décisions au bon moment.



Mesures techniques :

- imposer des mots de passe forts;
- configuration correctement vos systèmes (et vérifier ceci par audit ou test d'intrusion);
- mettre à jour régulièrement;
- chiffrer, pseudonymiser, anonymiser, où possible;
- limiter les accès;
- détruisez avec soin les DCP (disques des imprimantes, stick USB,...).

Mesures de gestion

- charte avec règles à respecter;
- sensibilisation (formation et test d'ingénierie social);
- attribution de responsabilité;
- classification (pour ne pas pénaliser le traitement d'informations peu sensibles);
- contrats solides (avec control du respect).

Nos convictions : Ensuite, préparez les spécificités !

- a) Assurer la **légitimité** (typiquement obtenir un **consentement valable**).
- b) Assurer la capacité technique (et procédure) pour **informer les personnes concernées**.
- c) Établir un contrat avec un **expert** pour vous aider en cas de violation ou vous conseiller en permanence).
- d) Établir un **contrat avec un DPD, le cas échéant**.
- e) Documenter les finalités et les mesures de sécurité.
- f) Faites votre **analyse de risque (AIDP)**, le cas échéant, avec assistance externe.
- g) Implémenter les mesures issues du traitement des risques.
- h) Compléter les **contrats de sous-traitance**.
- i) Écrivez une **déclaration de respect de la vie privée** (privacy notice).
- j) Préparer (et entraîner) la gestion d'un incident (cyber et vol classique).

Integrated ISMS: Information Security Management System



Information Security Management System (ISMS)

General policy (ITR-General)

General information

Type	Policy
Sequence number	base
Version	3.1
State	Final
Approved by	C. Harpe
Date	2010/02/07
Classification	Internal

The currently applicable version of this document is on slide 10/11.

Information Security Managem (ISMS)

Information Security Pol

General information

Reference number	0-0
Version	1.0
State	Final version
Approved by	CMC
Approval date	23/02/2015
Classification	Internal

But du document

Cette politique sectorielle définit les directives relatives appliquées et respectées pour protéger de manière adéquate les informations du Centre des technologies de l'Etat.

Informations générales

Numéro de séquence	15-0
Etat	Final
Classification	Interne

Relation avec les fo

Système de Gestion de la Sécurité de l'Information (SGSI)

Gestion des risques

Information générale

Numéro de séquence	05-00
Suivi de documentation	Version: 1.0 / Etat: Approuvé
Approuvé par	Philippe Mathieu
Date d'approbation	04/03/2016
Classification	Restreinte

Politique de Sécurité de l'Information de l'Etat luxembourgeois

Politique générale (PSI-LU)

Informations générales

Numéro de séquence	0-0
Version	1.0
Etat	Version finale
Propriétaire	ANSSI
Classification	Vert

Avant-propos du Premier Ministre, Ministre d'Etat

La protection des informations est une priorité majeure pour le gouvernement du Grand-Duché de Luxembourg, et nécessite une politique dédiée à la sécurité de l'information. Elle concerne la confidentialité, l'intégrité et la disponibilité des informations gérées dans les systèmes d'information classifiés et non classifiés installés et exploités par l'Etat et les opérateurs d'infrastructures critiques pour leurs besoins propres.

La formulation de cette politique permet de mettre en œuvre la stratégie de cybersécurité approuvée et rendue exécutoire par le Conseil de gouvernement. Elle constitue l'outil principal de la gouvernance de la sécurité des informations internes à l'Etat et prépare le développement de la société numérique dans l'esprit de l'initiative « Digital Letzebuerg ».

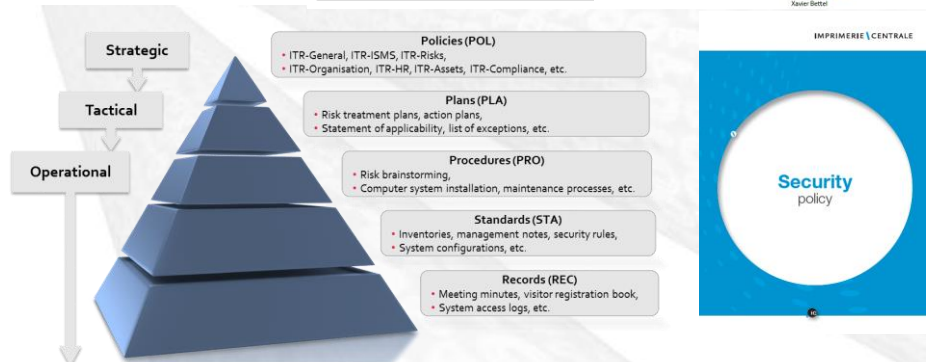
Cette politique énonce des objectifs généraux et définit un cadre de gestion d'objectifs spécifiques par domaines et par entité. La mise en application de cette politique crée un Système de Management de la Sécurité de l'Information (SGSI) pour les départements ministériels, les administrations et services de l'Etat luxembourgeois ainsi que pour les opérateurs d'infrastructures critiques. Ce SGSI définit, met en œuvre, surveille et améliore des objectifs de sécurité, ainsi que des actions et congrès appropriés pour répondre à ces exigences.

La gouvernance de la sécurité s'articule autour de dix principes élaborés par l'ANSSI, dont voici trois éléments clés :

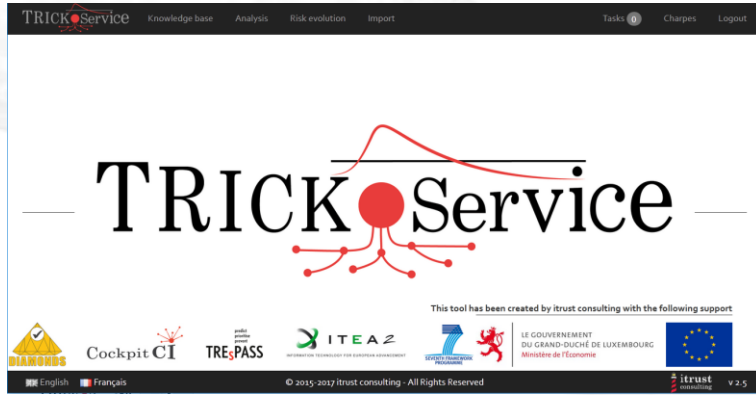
- Afin d'atteindre les objectifs énoncés et de minimiser les risques liés aux traitements des données, la sécurité de l'information, incluant la sécurité des systèmes d'information, s'inscrit au cœur de toutes les activités de l'Etat luxembourgeois.
- Le système de gestion prévoit que les départements ministériels, les administrations et services de l'Etat luxembourgeois établissent des mesures appropriées de protection de l'information contre toute modification, destruction et divulgation non autorisée, quelle que soit accidentelle ou intentionnelle. Le cas échéant il protège aussi la fiabilité et la non-répudiation de ces mêmes informations. Il prévoit une analyse des objectifs et à une analyse des risques.
- Ce document, ainsi que toutes exigences émises dans ce cadre et tout document annexé ont un caractère obligatoire pour tout le personnel dès leur publication par l'ANSSI et leur mise en application par le dirigeant des départements ministériels, administrations et services de l'Etat luxembourgeois concernés.

Je vous invite à prendre connaissance de l'engagement demandé à chaque agent, et à contribuer avec toutes vos compétences à la réalisation de l'objectif ultime qui est la protection adéquate des informations que vous devez traiter en vous assurant la confiance des citoyens, des entreprises et surtout une activité au Luxembourg, et des Etats partenaires dans les services de l'Etat luxembourgeois.

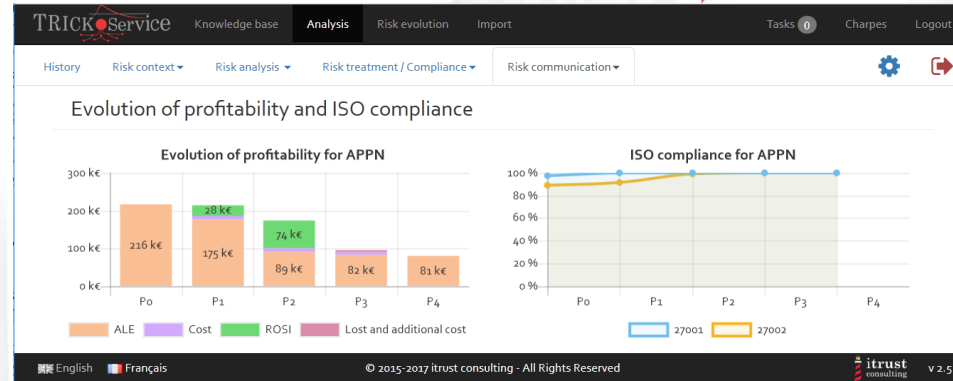
Xavier Bietter



- Nous écrivons vos documents.
- Nous aidons à prendre des décisions.
- Nous livrons un ensemble de politiques et procédure adaptées à vos besoins.



- 1) Contexte & valeurs de vos actifs (cf. 27005, 29134)
- 2) Analyse d'écart (27002, 29151, 27552, RGPD...;
- 3) Analyse des menaces, vulnérabilités, risques;
- 4) Évaluation des conséquences et probabilités;
- 5) Plan de traitements des risques, triés phase et rentabilité (ROSI);
- 6) Analyse d'impact sur la vie privée conforme au RGPD (et 27001, CSSF...).



CERT: Computer Emergency Response Team

- Incident Response
- Forensic Investigation
- Malware Analysis
- R&D
- Participation to international conferences (Defcon Las Vegas, hack.lu)
- Knowledge transfer (APT1: technical backstage)



TF-CSIRT
Trusted Introducer

itrust consulting CERT respects the incident-handling guidelines provided by NIST:

- | | | |
|------------------|---------------|-------------|
| • Preparation | • Containment | • Recovery |
| • Identification | • Eradication | • Follow-up |

What we learned operating a CERT

- a lot on threats and malware,
- that in the future, all organisations SHALL manage how to react to security incidents, i.e., have CERTs as partners / subcontractors.



Pour vous assurer de votre sécurité :

- a) Scan de vulnérabilité externe pour PME (à partir de 200 €)
- b) Analyse de vulnérabilité (~5 jours pour un portail web)
- c) Test d'intrusion (vous donnez le budget)
- d) Audit de configuration (1 jour par élément, FW, serveur, Exchange)
- e) Audit de conformité (ISO ou RGPD, < ~1 semaine)
- f) Test d'ingénierie social (logique ou physique) (1-3 jour)

Le top :

Certification des produits et services

Cf. Europrise, ou sur mesures.





Ne changez pas votre focus !

Profiter des exigences du RGPD pour améliorer votre gestion :

- plus de documentation;
- formulation plus claire des responsabilités;
- des finalités plus claires;
- moins de données – moins de risques.

C'est utile pour votre business !



Move securely within the cyberworld

