PRONEWTECH

CONSULTING & ENGINEERING

Analyse des risques et mesures à considérer pour sécuriser le système informatique et protéger les données à caractère personnel

MADE IN LUXEMBOURG

PRONEWTECH

Introduction

- **Le GDPR demande de réaliser sa mise en conformité selon une <u>approche basée sur les risques.</u>**

- **Un des 6 principes à respecter concerne <u>l'intégrité et la confidentialité</u> des données.**

- **Une approche méthodologique implique:**

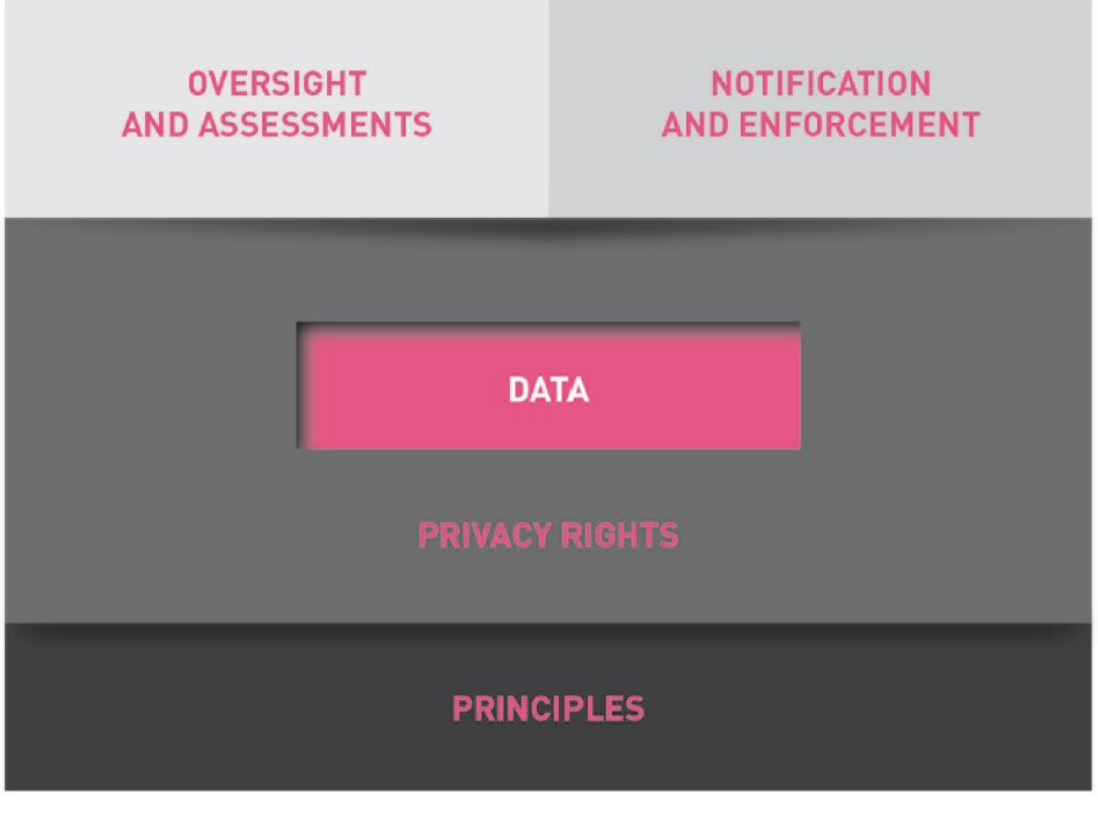
1. **La mise en place de mesures appropriées afin de sécuriser les données à caractère personnel et leur traitement**
2. **La réalisation d'une analyse des risques (le cas échéant)**
3. **La mise en place de solutions techniques permettant de détecter toute violation de données privées.**
4. **Diminution du risque**
5. **Gestion des violations**

LUXEMBOURG GREEN BUSINESS AWARDS 2015

GREEN IT AWARD

1. Mesures de sécurité

- **Le responsable du traitement et le sous-traitant mettent en œuvre des mesures appropriées pour assurer un niveau de sécurité approprié au risque, y compris la capacité d'assurer en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement.**



CORE ELEMENTS OF GDPR

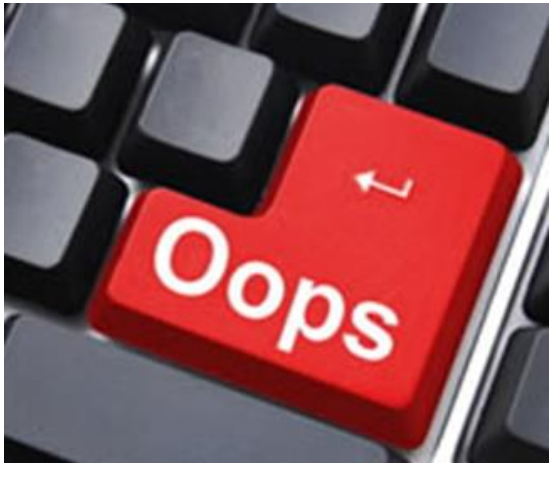
1. Mesures de sécurité

- **Mesures au niveau de l'infrastructure physique et informatique:**
  - **Alarmes**
  - **Contrôle d'accès à code / sans code**
  - **Détection intrusion**
  - **Armoires à code**
  - **Vidéosurveillance**
  - **Firewall**
  - **Logiciels Antivirus**
  - **Logiciels Antispam / Anti phishing / …**
  - **Sécurisation et délimitation des serveurs virtuels au sein de cloud**




1. Mesures de sécurité

- **Mesures de mise à jour de la sécurité informatique:**
  - **Antivirus à jour**
  - **Utiliser des logiciels GDPR « compliant by design / default »**
  - **Limiter l'accès aux données, aux data bases**
  - **Limiter l'accès aux logiciels qui manipulent les données**
    - **Politique mot de passe**
    - **Contrôle de la mac adresse**
    - **VPN sécurisé**
  - **Test d'intrusion**
    - **Audit d'architecture du réseau IT**
    - **Audit de configuration**
    - **Audit de vulnérabilité**
    - **…**



PRONEWTECH

1. Mesures de sécurité

- Le GDPR ne décrit pas de liste exacte des contrôles que les organisations devraient mettre en œuvre pour être conforme. Néanmoins, les meilleures pratiques en matière de sécurité générale suggèrent que les éléments suivants pourraient constituer un bon point de départ:

1 DATA CLASSIFICATION	2 CONFIGURATION CHANGE MANAGEMENT	3 ADMINISTRATOR CONTROLS AND SEPARATION OF DUTIES	4 SECURE SYSTEM CONFIGURATION
5 ACCESS CONTROL	6 NETWORK-BASED SEGMENTATION	7 ENCRYPTION AND PSEUDONYMISATION	8 DATA LEAK PREVENTION
9 DDOS PREVENTION	10 USER ACTIVITY MONITORING	11 VULNERABILITY MANAGEMENT	12 DISASTER RECOVERY

LUXEMBOURG GREEN BUSINESS AWARDS 2015
GREEN IT AWARD

1. Mesures de sécurité

- **Mesures informatiques:**

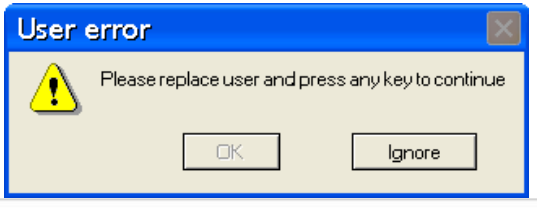
  - **Limiter les possibilités d'export des données**
    - **Cryptage / blocage des ports USB**
    - **Empêcher les manipulations copier/coller**
    - **Restrictions pour les envois par mail ou via web**
  - **Sécuriser les transferts, crypter les données**
  - **Demande d'identification au niveau de l'imprimante avant impression (via code, lecteur de badge,..)**

1	2	3	4
THE PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA	THE ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES	THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT	A PROCESS FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING

PRONEWTECH

1.1 GDPR Firewall Compliance module

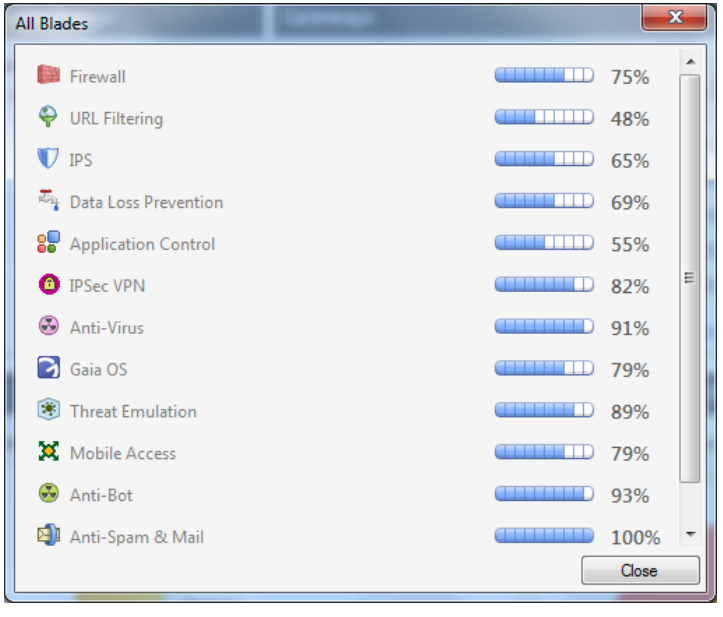
99% des failles de sécurité auraient pu être évitées par une configuration correcte des équipements de sécurité.

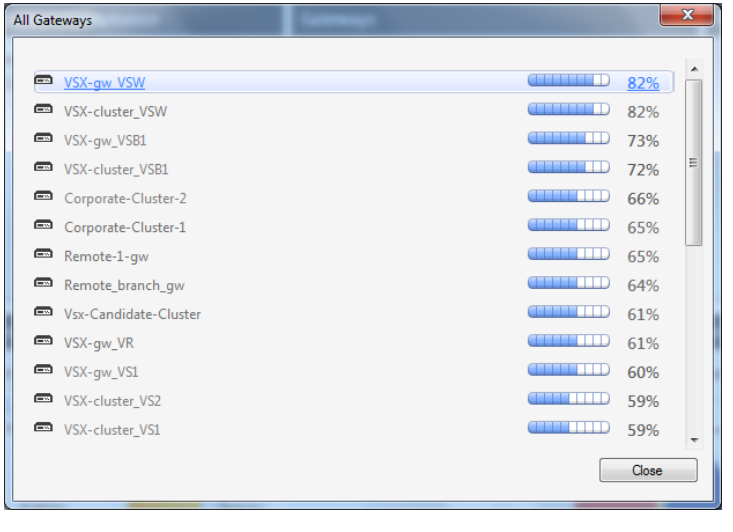


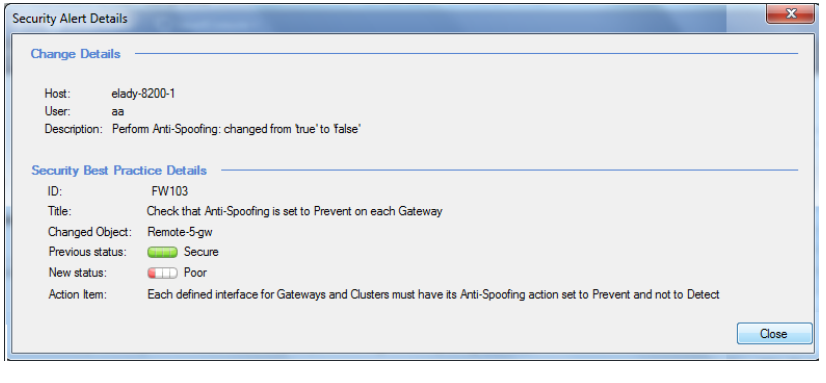
LUXEMBOURG GREEN BUSINESS AWARDS 2015
GREEN IT AWARD

1.2 Eléments à surveiller

- ❑ Analyse des blades
  - Validez vos politiques et paramètres de configuration
  - Identifiez les erreurs en temps réel
  - Utilisez des tableaux de bord GDPR Dashboard au sein de votre infrastructure Firewall
- ❑ Analyse des Gateways
- ❑ Alerte de sécurité en ligne





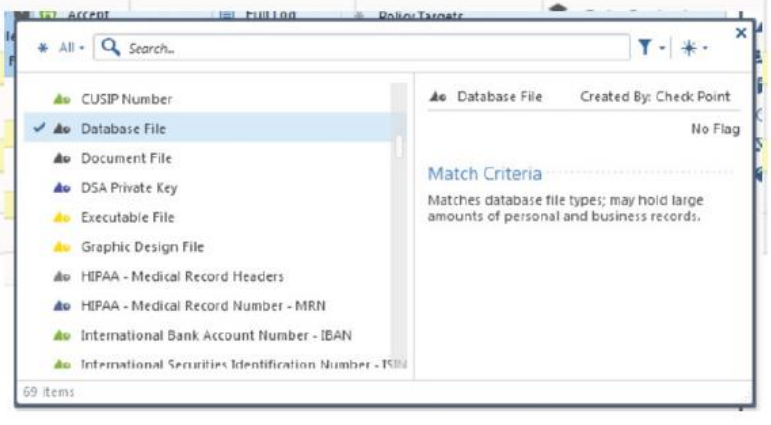


PRONEWTECH

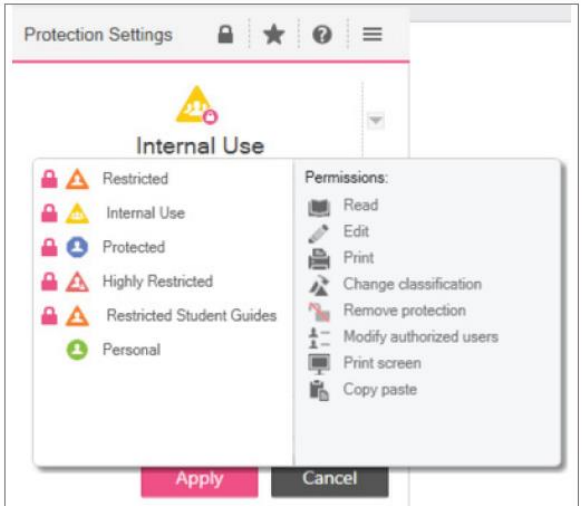
1.2 Eléments à surveiller

- Network segmentation

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action
8	Customers to ftp servers	ExternalZone	FTP_Ext	Any	ftp-Protocol-Signat...	Any Direction Archive File	Accept
9	Policy for access to Data Center servers	Any	Data Center LAN				
Temporary Access Grant (10)							
10	Special policy for temp guest rules using wireless LAN	WirelessZone	Any				
Clean Up (11-12)							
11	Clean up	Any	Any				
Cleanup		Any	Any				



- Protection Settings
- DDOS Prevention
- User Activity Monitoring
- Vulnerability Management



LUXEMBOURG GREEN BUSINESS AWARDS 2015
GREEN IT AWARD




2. Analyse des risques

- **DPIA : Data Protection Impact Assessment / Analyse d'impact relative à la protection des données privées**
- **Article 35 du GDPR.**
- **Nécessaire dans les cas suivants :**
  - **Traitement automatisé visant l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage**
  - **Traitement à grande échelle de catégories particulières de données (biométriques, ethnique, appartenance syndicale, …) ou relatives à des condamnations pénales**
  - **Surveillance systématique à grande échelle d'une zone accessible au public**
- **Les autorités de contrôle nationales (CNPD au Luxembourg) seront en charge d'éditer la liste des traitements nécessitant une DPIA (RGPD, article 35 – 4)**




2. Analyse des risques

- **Analyse de risques liés au vol, à la perte ou à la modification d'une donnée ou d'un groupement de données**
- **Priorisation des risques et des mesures à appliquer en fonction de leur criticité et des coûts d'implémentation**
- **Conception d'un plan d'action pour les risques importants**
- **Exemple de moyens à mettre en place:**
  - **Pseudonymisation**
  - **Réduction du nombre d'infos au strict minimum**
  - **Sécurisation du système informatique (antivirus, firewall, SIEM, cryptage de données,…)**
- **Pour les traitements actuels (mise en conformité) et futurs (privacy by design)**
- **Documenter l'analyse des risques**




2. Analyse des risques

- **Evaluer la gravité du risque :**
  Caractère identifiant & caractère préjudiciable

GRAVITE		
CARACTERE IDENTIFIANT		
Note	**Importance**	**Description**
1	Négligeable	Impossible d'identifier la personne
2	Limité	Difficile d'identifier la personne
3	Important	Il est relativement facile d'identifier la personne
4	Maximal	Il est facile d'identifier la personne

1. Prénom seul à l'échelle d'un pays ; 2. Prénom et nom; 3. Prénom, nom et date de naissance;
4.Prénom, nom, date de naissance, adresse postale

CARACTERE PREJUDICIABLE		
Note	**Importance**	**Description**
1	Négligeable	Peu d'impacts ou quelques désagréments
2	Limité	Des désagréments significatifs mais surmontables
3	Important	Des conséquences significatives
4	Maximal	Des conséquences irrémédiables

1. Perte de temps, agacement, énervement ; 2.Frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress ; 3. Détournement d'argent, interdiction bancaire, perte d'emploi, assignation en justice, aggravation de l'état de santé; 4. Péril financier, affection psychologique ou physique de longue durée, décès.

2. Analyse des risques

- **Evaluer la gravité du risque :**
  Caractère identifiant & caractère préjudiciable

CARACTERE IDENTIFIANT + PREJUDICIABLE	
<5	Négligeable
=5	Limité
=6	Important
>6	Maximal




2. Analyse des risques

- **Evaluer la vraisemblance du risque :**

Vulnérabilité des supports & capacités des sources de risques

VRAISEMBLANCE		
VULNERABILITE DES SUPPORTS		
Note	**Importance**	**Description**
1	Négligeable	Les supports ne sont pas vulnérables
2	Limité	Les supports sont peu vulnérables
3	Important	La menace est sérieuse et les supports vulnérables
4	Maximal	La réalisation de la menace ne fait pas de doute

1. Vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès; 2. l'accès est contrôlé par badge uniquement; 3. L'accès est contrôlé par une personne à l'acceuil ; 4. Vol de supports papiers stockés dans le hall public de l'organisme

CAPACITES DES SOURCES DE RISQUES		
Note	**Importance**	**Description**
1	Négligeable	Les sources de risque ont une capacité nulle
2	Limité	Le sources de risque ont une capacité limitée
3	Important	Les sources de risque ont une capacité importante
4	Maximal	Les sources de risque ont une capacité illimitée

1. Une personne seule pour des motifs personnels; 2. Un groupe de personnes à des fins financières; 3. Un groupe important à des fins politiques; 4. Un gouvernement à des fins d'espionnage

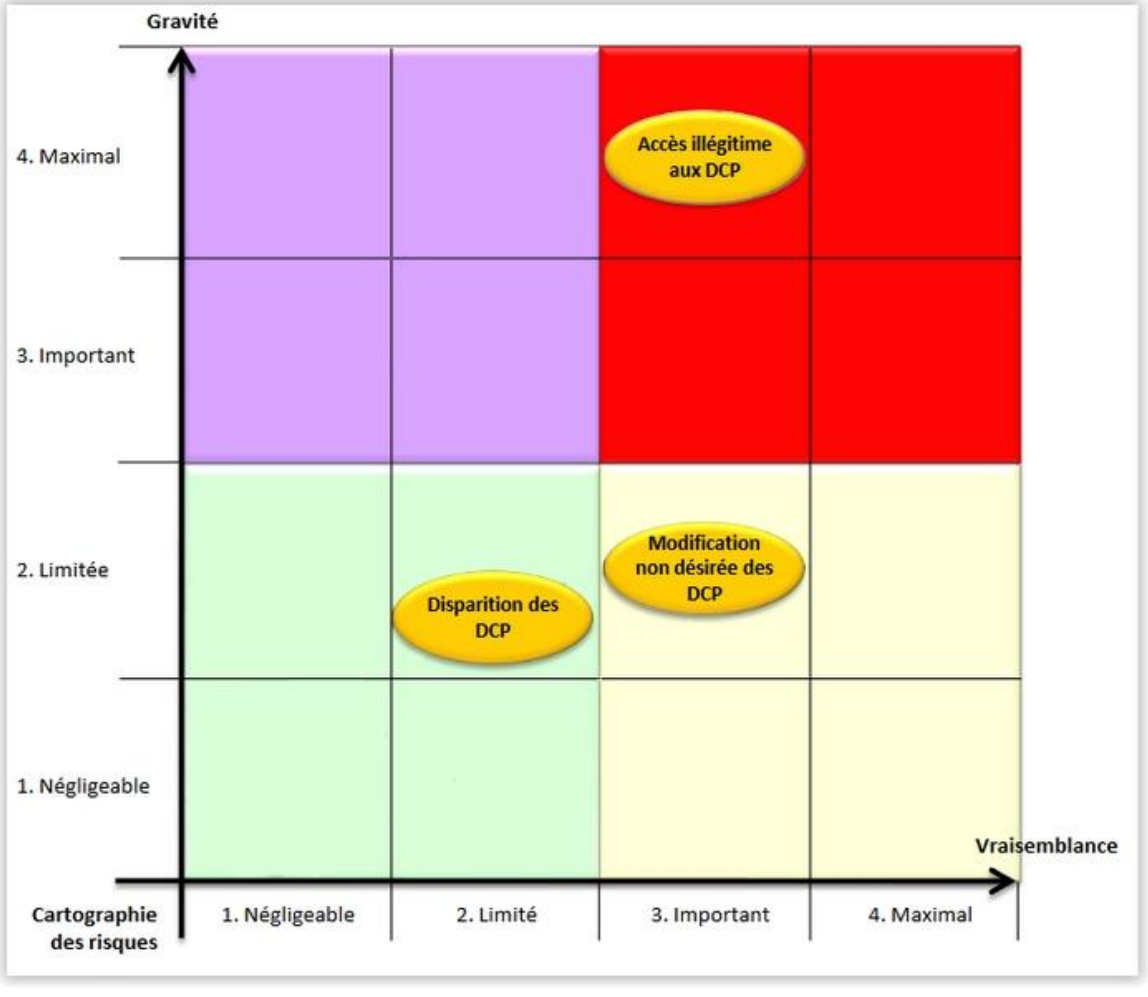
2. Analyse des risques

- **<u>Evaluer la vraisemblance du risque :</u>**
  Vulnérabilité des supports & capacités des sources de risques

VULNERABILITE DES SUPPORTS + CAPACITES DES SOURCES DE RISQUES	
<5	Négligeable
=5	Limité
=6	Important
>6	Maximal

2. Analyse des risques

- **Cartographie de l'ensemble des risques recensés :**
  En fonction de la gravité et de la vraisemblance



DCP : Données à caractère personnel

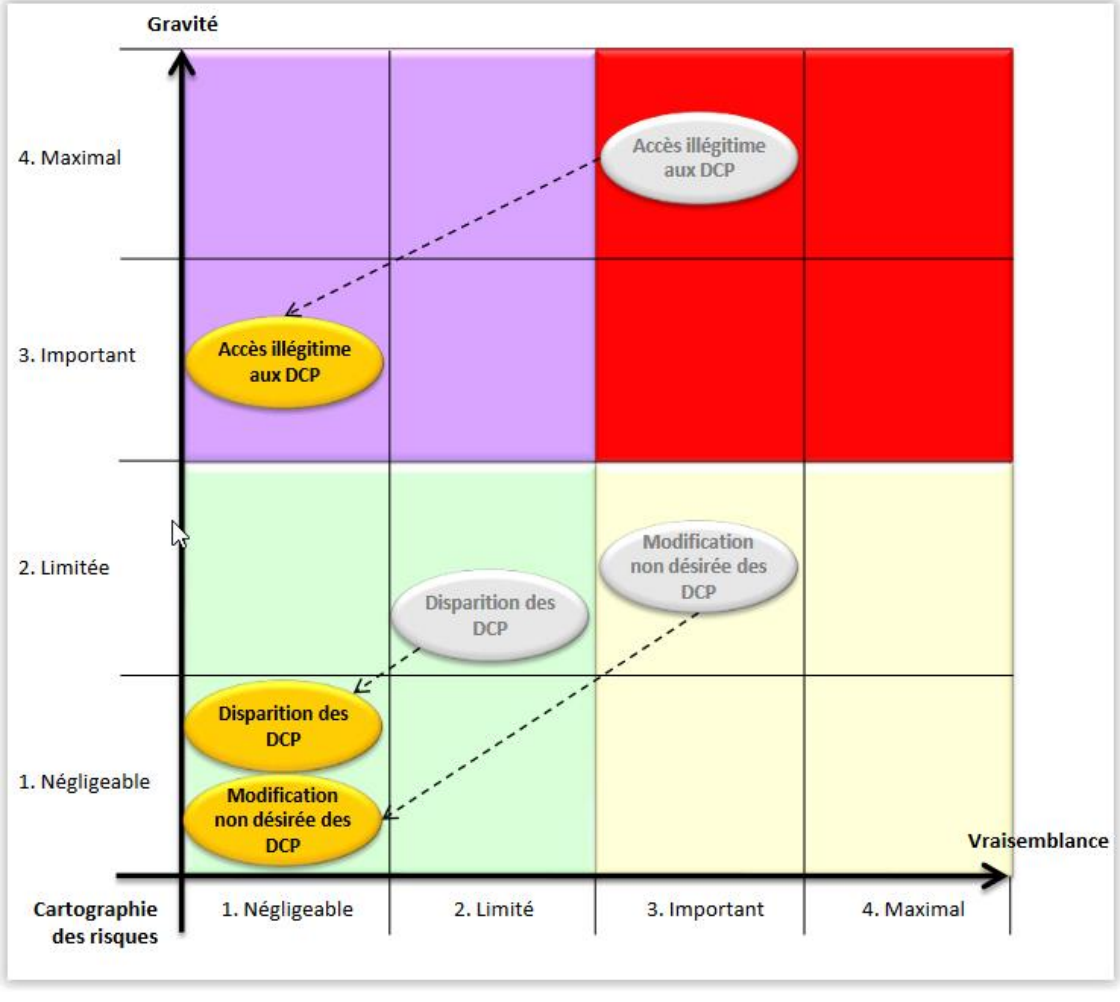
3. Mesures de sécurité procédurales




- **Mesures organisationnelles:**
  - **Clauses de confidentialité**
  - **Procédures internes**
  - **Règles de bonne conduite**
  - **Information et sensibilisation du personnel**
  - **Réalisation d'une analyse des risques (DPIA)**
  - **Pseudonymisation voir anonymisation des données**
  - **Minimisation des données au maximum possible**

4. Diminution du risque

- **Analyse du niveau de risque suite aux mesures prises**






5. Gestion des violations

Détection et traçabilité des violations:

- **Journalisation des activités– système de log file**
  - **Au niveau du réseau informatique**
  - **Au niveau des logiciels**
- **DLP (data loss prevention)**
  - **Logiciel de détection des pertes de données**
- **Modules firewall qui scannent le réseau**
- **SIEM (security information and event management)**
  - **Centralisation de tous les évènements afin de relier les causes aux effets**
- **Conformité des sous-traitants**
  - **Firewall**
  - **Cryptage des données**
  - **Limitation des accès**
  - **Information du responsable dans les plus brefs délais**




5. Gestion des violations

Notification des violations: (vol, modification, perte, accès non autorisé,…)

Qui	Auprès de	Délais à compter de la prise de connaissance	Contenu
Responsable de traitement	Autorité de contrôle : CNPD	72 heures	• Nature de la violation • Identification DPO, point de contact • Conséquences probables • Mesures de remédiation
Responsable de traitement	Personnes concernées	Dans les meilleurs délais	• Nature de la violation • Identification DPO, point de contact • Conséquences probables • Mesures de remédiation
Sous-traitant	Responsable de traitement	Dans les meilleurs délais	• Nature de la violation • Identification point de contact

PRONEWTECH

GREEN IT AWARD

tango

BGL BNP PARIBAS

Q8

KPMG
cutting through complexity

Raiffeisen
Naturellement ma banque

Carnegie

European Investment Bank

POST LUXEMBOURG

Cactus

Administration des Ponts et Chaussées

uni.lu
UNIVERSITÉ DU LUXEMBOURG

TRAXYS

G4S

orange™

Loterie Nationale

ACL

TOTAL

THE SOLARWIND PROJECT

VILLE DE LUXEMBOURG

交通銀行
BANK OF COMMUNICATIONS

lalux
ASSURANCES

LE FONDS BELVAL

ROCKHAL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

Microtis




Contact

ProNewTech S.A.

55, Allée de la Poudrerie

L-1899 Kockelscheuer

- Tél : +352 32 99 20 - 1
- Fax : +352 32 99 20 - 11
- Mobile : +352 691 26 30 25
- E-mail : info@pronewtech.lu
- Internet : http://www.pronewtech.lu

CEO : Roland STREBER