# RegTech for CNPD
# Collaboration LIST / CNPD

**Juin 2017**

Digital Lëtzebuerg

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

# RegTech for CNPD

## Objectifs de la CNPD

- Guidance, sensibilisation et « vulgarisation » de la protection des données
- **Permettre** aux entreprises de **s'évaluer** et d'identifier les actions à mettre en œuvre
- De la théorie vers l'opérationnel: **outiller** le reporting et **la gouvernance internes** de la protection des données
- Mobiliser différents corps de métier (hors juridique): IT, Sécurité information, Chefs de projets, analystes, communication …
- Montée en puissance « continue » des connaissances: **mises à jour du contenu** en fonction de l'évolution de la matière: avis (article 29), guidances, jurisprudences, prises de position
- Modèle générique vers modèles contextuels (sectoriels)

# RegTech for CNPD

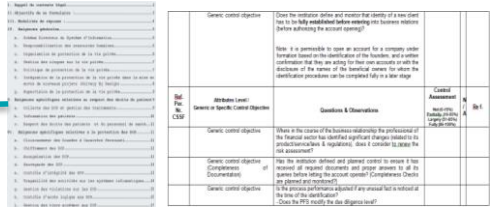
## Définition du projet

- **3 partenaires** : CNPD / Digital Lëtzebuerg / LIST.
- Collaboration de recherche sur **3 ans**.
- **Participation essentielle d'entreprises :**
  - 3 dans la première phase / BGL BNP Paribas - Croix Rouge - Hôpitaux Robert Schumann
  - 12 dans la deuxième phase (cf. appel à volontaires)
- Plusieurs domaines de travail :
  - 1 – veille
  - 2 – **assessment et compliance**
  - 3 – DPIA
  - …

# RegTech for CNPD

## RGPD « Assessment & compliance »

- **Un référentiel d'exigences**

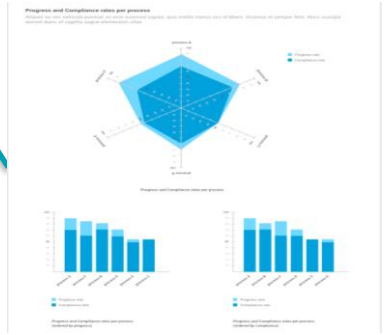


*Exigences*
*Questions*
*Notice/exemple*
*Recommandations*
*Domaines-processus*

- **Un outil**

*Niveaux de satisfaction (aux exigences)*
*Justifications*
*Elements de prevue*
*Commentaires*

- **Un reporting dynamique**



*Registre de traitement / risques*
*Visualisation*
*Indicateurs clé*

# RegTech for CNPD

## RGPD « Assessment & compliance »

- Un modèle d'exigences **évolutif**.
  - + des modèles sectoriels en cours de construction.
- Un outil **évolutif**.
- Un outil **multi-modèles**…(ISO 27001, PSDC…)
- Une ouverture en **octobre** (cybersecurity week).
- Plusieurs modes de déploiement en réflexion.

# RegTech for CNPD

## Le modèle

I. Organisation

- Obligations générales: responsabilités du responsable du traitement
- Droits de la personne: généralités
- Délégué à la protection des données
- Notification violation

II. Les traitements

Registre des activités de traitements

| Traitement 1 | Traitement 2 | Traitement 3 | Traitement x |
|---|---|---|---|
| Responsables conjoints | Responsables conjoints | Responsables conjoints | Responsables conjoints |
| Principes relatifs aux traitements | Principes relatifs aux traitements | Principes relatifs aux traitements | Principes relatifs aux traitements |
| Licéité du traitement | Licéité du traitement | Licéité du traitement | Licéité du traitement |
| Droits de la personne | Droits de la personne | Droits de la personne | Droits de la personne |
| DPIA | DPIA | DPIA | DPIA |
| Transferts Pays Tiers | Transferts Pays Tiers | Transferts Pays Tiers | Transferts Pays Tiers |
| Catégories particulières de données | Catégories particulières de données | Catégories particulières de données | Catégories particulières de données |

III. Sous-traitance

- Sous-traitance
- Sécurité des traitements
- Protection des données dès la conception / Protection des données par défaut

# RegTech for CNPD

## Le modèle

### Exemple: Droits de la personne concernée / Droit à la portabilité des données

Eléments issus du RGPD :

1) Les personnes concernées peuvent recevoir les données à caractère personnel les concernant qu'elles ont fournies, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque:
   - le traitement est fondé sur le consentement ou un contrat et
   - le traitement est effectué à l'aide de procédés automatisés

2) La personne concernée qui exerce son droit à la portabilité des données a le droit d'obtenir que les données à caractère personnel soient transmises directement à un autre responsable du traitement, lorsque cela est techniquement possible.

3) L'exercice de la portabilité ne porte pas atteinte aux droits et libertés de tiers.

# RegTech for CNPD

## Le modèle

### Exemple: Droits de la personne concernée: droit à la portabilité des données

Eléments d'aide pour répondre aux exigences du RGPD:

1) Une information quant à l'exercice du droit à la portabilité est fournie aux personnes lors de l'obtention de leur données à caractère personnel.
2) Une information quant à la différence entre le droit à la portabilité et le droit d'accès est disponible. Cette information comporte notamment le type de données auquel les personnes peuvent avoir accès en exerçant ce droit afin que celles-ci puissent déterminer au mieux quel droit exercer.
3) Une information additionnelle est communiquée sur le droit à la portabilité avant la fermeture d'un compte.
4) Le jeu de données issu d'un exercice du droit à la portabilité contient des métadonnées permettant d'identifier et de décrire les données (bonne pratique).
5) Les données sont-elles transférées aux personnes concernées de manière sécurisée?

6) …

# RegTech for CNPD

## Le modèle

### Exemples de types de preuves possibles pour démontrer ce qui est mis en oeuvre

Licéité du traitement : exécution d'un contrat

*1) Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou l'exécution de mesures précontractuelles prises à la demande de celle-ci.*

⇒ Contrat et description du mécanisme d'acceptation du contrat par les personnes concernées

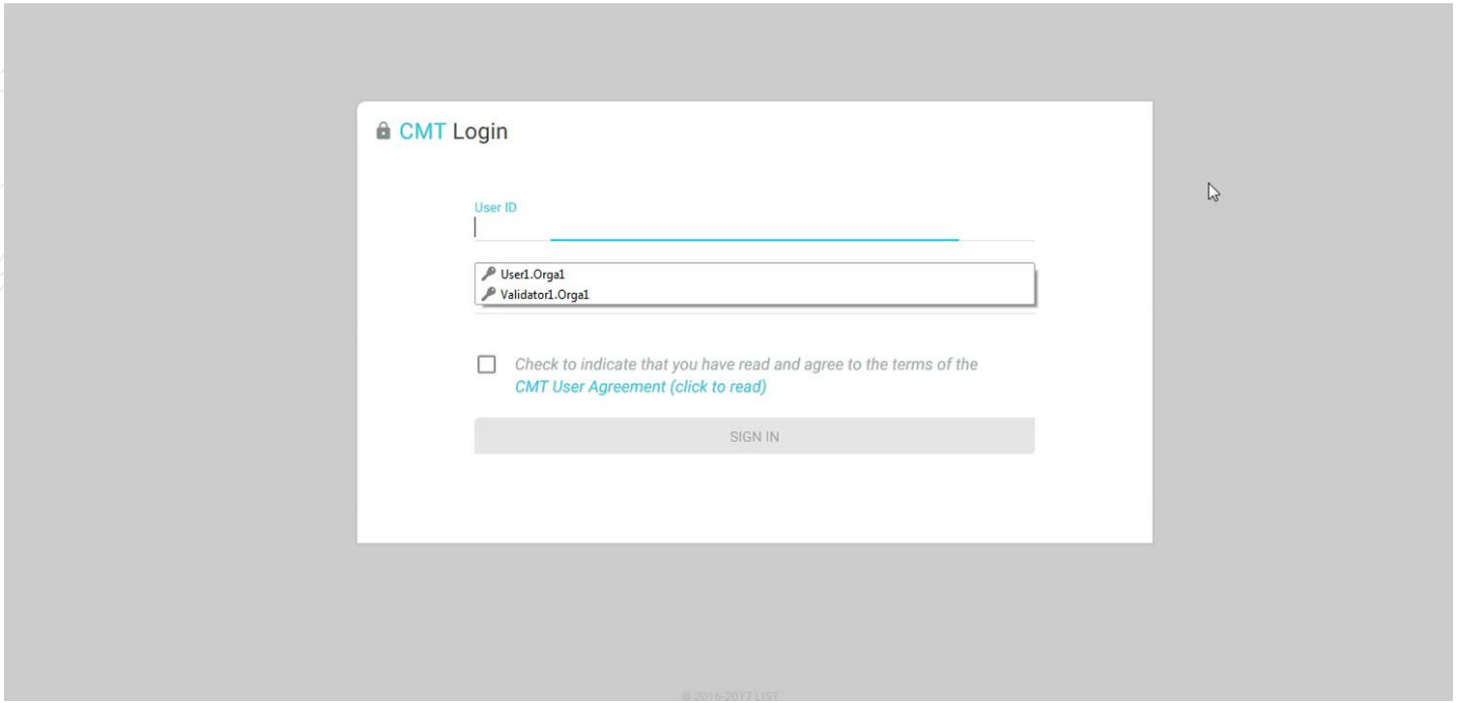
*2) L'acceptation du contrat implique un traitement supplémentaire de données que les données strictement nécessaires : Les personnes concernées sont-elles informées des finalités supplémentaires et leurs acceptations est-elle volontaire?*

=> Type de preuves possibles:

- les informations fournies à la personne concernée;
- quand ces informations sont-elles fournies à la personne concernée;
- comment le / les traitement(s) supplémentaire(s) sont-ils acceptés? (description du mécanisme de choix volontaire)

# RegTech for CNPD

## L’outil CMT



record of processing activities (pdf)

## GDPR Partie 1 : Organisation

*Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce vel orci bibendum, sodales turpis nec, pharetra ligula. Vivamus pharetra consectetur.*

add new GDPR Part 1

| type | project title | created on | created by | updated on | updated by | status | locked by |
|---|---|---|---|---|---|---|---|
| GDPR Partie 1 : Organisation | Project v1 | 14 April 2017 | Rob Arvutz | 15 April 2017 | Rob Arvutz | Draft | |

Open
Edit
Duplicate
Delete

## GDPR Partie 2 : Traitements

*Quisque pellentesque mattis eros vitae placerat. Nunc et pharetra quam, commodo sagittis arcu* ***download example***

add new GDPR Part 2

| type | project title | created on | created by | updated on | updated by | status | locked by |
|---|---|---|---|---|---|---|---|
| GDPR Partie 2 : Traitements | Gestion administrative des clients | 14 April 2017 | Rob Arvutz | 15 April 2017 | Rob Arvutz | Draft | |
| GDPR Partie 2 : Traitements | Prise en charge individualisée | 14 April 2017 | Rob Arvutz | 15 April 2017 | Rob Arvutz | Validated | |
| GDPR Partie 2 : Traitements | Echange avec intervenants extern ... | 14 April 2017 | Rob Arvutz | 15 April 2017 | Rob Arvutz | Draft | Peter Wurtz |

## GDPR Partie 3 : Sous-Traitance

*Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Vestibulum eu pellentesque sapien.*

add new GDPR Part 3

| type | project title | created on | created by | updated on | updated by | status | locked by |
|---|---|---|---|---|---|---|---|

## Partie 1: Organisation

Partie 1: Organisation

Created on: 30 May 2017
Created by: Validator1 Orga1

Draft

## Partie 2: Traitements

Partie 2: Traitements

Project title: test

Created on: 30 May 2017

Partie 2: Traitements

Project title: Gestion des contrats

Created on: 09 June 2017

DOWNLOAD CHECKLIST FILE (.XLSX)

PRINT AS PDF

IMPORT PREFILLED FILE (.XLSX)

### *Information CNPD*

- *Informations complémentaires à fournir par la CNPD*

## 1 • Obligations générales: Responsables conjoints du traitement

/ *GDPR Art. 26*

Les obligations respectives aux fins d'assurer le respect des exigences du RGPD sont définies de manière transparente entre les responsables conjoints du traitement.

L

/ GDPR Art. 26

## General Informations

* informations obligatoires

*Quisque pellentesque mattis eros vitae placerat. Nunc et pharetra quam, commodo sagittis arcu* ***download example***

**Titre ***

*Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce vel orci bibendum, sodales turpis nec, pharetra ligula.*

Gestion administrative des clients

**Description**

*Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce vel orci bibendum, sodales turpis nec, pharetra ligula.*

Description

**Catégorie de destinatires ***

*Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce vel orci bibendum, sodales turpis nec, pharetra ligula.*

Catégorie de destinataires

**Finalité ***

*Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce vel orci bibendum, sodales turpis nec, pharetra ligula.*

Finalité

**Sous traitants**

*Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce vel orci bibendum, sodales turpis nec, pharetra ligula.*

Sous traitants

project status Draft

## 1 • Licéïté du traitement

*Quisque sed ipsum aliquet | feugiat libero a, consectetur dolor | Fusce volutpat blandit odio non viverra.*

## 2 • Droit de la personne

*Aliquet, ex nec vehicula pulvinar, ex eros euismod sapien, quis mattis metus orci id libero. Vivamus et semper felis. Nunc suscipit laoreet diam, et sagittis augue elementum vitae.*

***CR761 / ESMA RTS Art.85.1.a***

Sed eleifend ullamcorper bibendum. Sed eget quam sed ante luctus sagittis. Suspendisse dignissim ornare tempus.

help | GDPR ref. | comments | linked docs. | internal chat

**comments**

Fully
Largelly
Partially
None
Not Applicable

Do Not Know

***CR761 / ESMA RTS Art.85.1.a***

Sed eleifend ullamcorper bibendum. Sed eget quam sed ante luctus sagittis. Suspendisse dignissim ornare tempus.

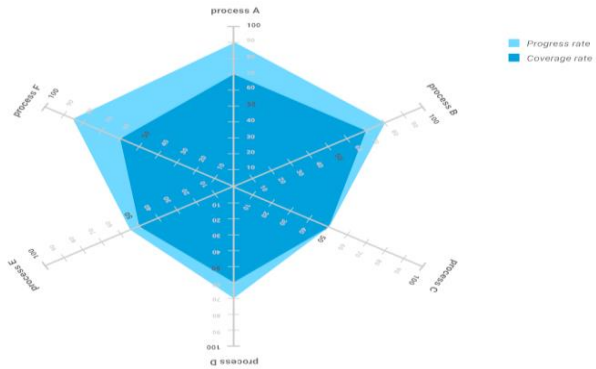
F

help | GDPR ref. | comments | linked docs. | internal chat

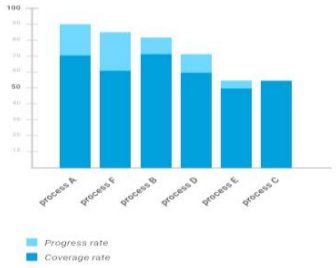
***CR761 / ESMA RTS Art.85.1.a***

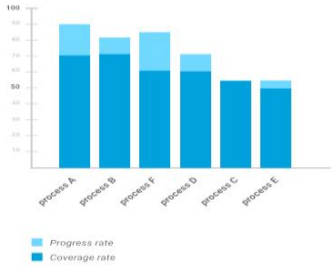
## Progress and Coverage rates per process

*Aliquet, ex nec vehicula pulvinar, ex eros euismod sapien, quis mattis metus orci id libero. Vivamus et semper felis. Nunc suscipit laoreet diam, et sagittis augue elementum vitae.*



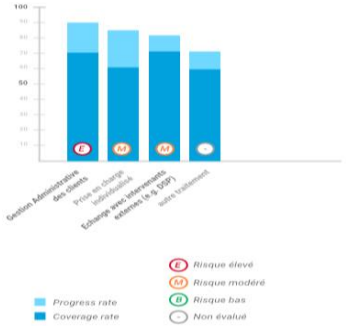

Progress and Coverage rates per process



## Progress and Coverage rates : Partie 2 - Traitements

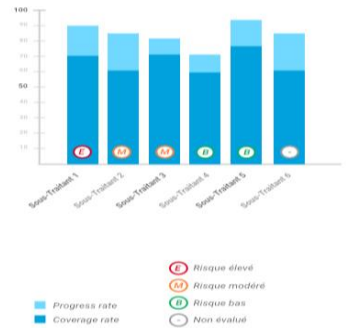
*Aliquet, ex nec vehicula pulvinar, ex eros euismod sapien, quis mattis metus orci id libero. Vivamus et semper felis. Nunc suscipit laoreet diam, et sagittis augue elementum vitae.*




**Progress and Coverage rates : Partie 2 - Traitements**
***(ordered by risk)***

## Progress and Coverage rates : Partie 3 - Sous-Traitance

*Aliquet, ex nec vehicula pulvinar, ex eros euismod sapien, quis mattis metus orci id libero. Vivamus et semper felis. Nunc suscipit laoreet diam, et sagittis augue elementum vitae.*



# RegTech for CNPD

## Phase de bêta-test

- Appel à **volontaires** / environ **12** entreprises retenues.
- **Représentatives** de l'écosystème luxembourgeois.
- **2 mois** de test du 3 juillet au 8 septembre 2017.
- Retours sur **le modèle et l'outil**.
- A la fin du bêta-test: réunion de concertation avec les bêta-testeurs.
- **Demande de participation** auprès de la CNPD : regtech@cnpd.lu
  - Eléments à fournir: personne de contact, fonction, nom de l'entreprise, domaine d'activité
  - Date limite: 26 juin 2017

# Q&R

**Juin 2017**

Digital Lëtzebuerg

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST