GDPR Compliance Support Tool

Information Session – 19th October 2017

eProseedRTC
WE SIMPLIFY COMPLEXITY.

Digital Lëtzebuerg

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

GDPR CST Presentation

Goals

- Guidance, awareness raising and « vulgarization » of data protection.
- **Allow companies** to **assess** themselves and identify actions to be taken.
- From theory to operational: **Providing tools** for data protection internal reporting and governance.
- **Involve** various trades (besides legal): IT, Information Security, project managers, business analysts, communication …
- Continuous growth of knowledge: **Update of the content** depending of the evolution of matter: opinions (article 29, future EDPB), guidance, jurisprudences, positions taken.
- Generic model to contextual models (sectoral).

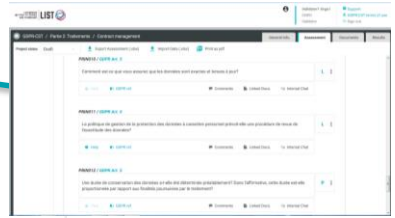
GDPR CST Presentation

Components

- **Requirements framework**

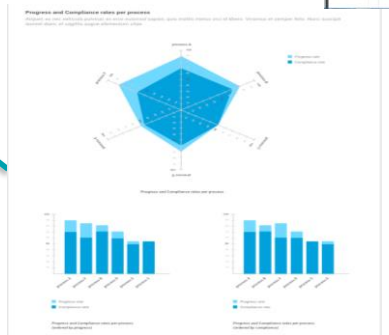
Requirements
Questions
Recommendations
Domains

- **Assessment interface**



Quotation
Comments
Elements of proof
Internal chat
Record of processing activities

- **Dynamic reporting**



Key indicators
Ranking of processing activities, data processors
Visualization by domains

GDPR CST Presentation

Functionalities

- A **logical and detailed approach** of the regulation, based on a set of more than 350 requirements and recommendations, developed by the CNPD.
- A dedicated evaluation for each dimension of the company: **department, site,** …(Part 1), **processing activities** (Part 2), **data processors** (Part 3).
- Editing and management of the **record of processing activities**.
- A **visualization framework** to facilitate the internal reporting tasks.
- Management of **evidences** (links between requirement and documents).
- The possibility of **exporting and importing** the ongoing evaluation data for continuing the assessment out of the tool.
- **Upcoming scalable features** in version 2.0 such as multi-user mode as well as importing and storing proof documents.

GDPR CST Presentation

The requirements framework

I. Organisation

- General obligations: accountability of the data controller
- Rights of the data subject: general points
- Data Protection Officer
- Data Breach Notifications

II. Data processings

Records of processing activities

Processing 1	Processing 2	Processing 3	Processing x
Joint Controllers	Joint Controllers	Joint Controllers	Joint Controllers
Processing's principles	Processing's principles	Processing's principles	Processing's principles
Processing's lawfullness	Processing's lawfullness	Processing's lawfullness	Processing's lawfullness
Rights of the data subjects	Rights of the data subjects	Rights of the data subjects	Rights of the data subjects
DPIA	DPIA	DPIA	DPIA
Transfers to third countries	Transfers to third countries	Transfers to third countries	Transfers to third countries
Special categories of pers. data	Special categories of pers. data	Special categories of pers. data	Special categories of pers. data

III. Processors

- Data processing with processors
- Security of processing
- Data Protection by Design/ Data Protection by Default

GDPR CST Presentation

The requirements framework

Example: Rights of the data subject/ the right to data portability

Extract from the GDPR:

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.

GDPR CST Presentation

The requirements framework

Example: Rights of the data subject/ the right to data portability

Possible criteria to meet the requirements of the GDPR:

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 transférées aux personnes concernées de manière sécurisée.

6) …

GDPR CST Presentation

The requirements framework

Examples of possibles types of evidences to demonstrate what has been setup

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).

Registre des activités de traitement

Partie 1: Organisation

Le règlement général sur la protection des données requiert, en fonction du contexte, la mise en œuvre d'éléments de gouvernance et d'organisation interne en matière de gestion de la protection des données. D'autres exigences de protection des données à mettre en œuvre sont communes à tous les traitements de données à caractère personnel de l'organisation responsable d'un traitement. La section « Organisation ...

Partie 1: Organisation

Title: **Kirchberg**

Creat. on: **11 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Belval**

Creat. on: **18 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Merl**

Creat. on: **24 July 2017** Updat. on: **05 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Registre des activités de traitement

Partie 1: Organisation

Le règlement général sur la protection des données requiert, en fonction du contexte, la mise en œuvre d'éléments de gouvernance et d'organisation interne en matière de gestion de la protection des données. D'autres exigences de protection des données à mettre en œuvre sont communes à tous les traitements de données à caractère personnel de l'organisation responsable d'un traitement. La section « Organisation ...

Partie 1: Organisation

Title: **Kirchberg**

Creat. on: **11 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Belval**

Creat. on: **18 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Merl**

Creat. on: **24 July 2017** Updat. on: **05 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Kayl**

Registre des activités de traitement

Partie 1: Organisation

Le règlement général sur la protection des données requiert, en fonction du contexte, la mise en œuvre d'éléments de gouvernance et d'organisation interne en matière de gestion de la protection des données. D'autres exigences de protection des données à mettre en œuvre sont communes à tous les traitements de données à caractère personnel de l'organisation responsable d'un traitement. La section « Organisation ...

Partie 1: Organisation

Title: **Kirchberg**

Creat. on: **11 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Belval**

Creat. on: **18 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Merl**

Creat. on: **24 July 2017** Updat. on: **05 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Draft

Partie 1: Organisation

Title: **Kayl**

Registre des activités de traitement

Partie 1: Organisation

Le règlement général sur la protection des données requiert, en fonction du contexte, la mise en œuvre d'éléments de gouvernance et d'organisation interne en matière de gestion de la protection des données. D'autres exigences de protection des données à mettre en œuvre sont communes à tous les traitements de données à caractère personnel de l'organisation responsable d'un traitement. La section « Organisation ...

Partie 1: Organisation

Title: **Kirchberg**

Creat. on: **11 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Validated

Partie 1: Organisation

Title: **Belval**

Creat. on: **18 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Validated

Partie 1: Organisation

Title: **Merl**

Creat. on: **24 July 2017** Updat. on: **06 October 2017**
Creat. by: **Paul Richard** Updat. by: **Paul Richard**

Validated

Partie 1: Organisation

Title: **Kayl**

GDPR CST Presentation

Limits

- The tool does not offer a guarantee of compliance with the legislation for your processing activities.
- As data controller, you remain responsible for managing your processing activities (accountability).
- The tool is not to be considered as a solution to all the problems related to the processing of personal data.
- The CNPD does not have access to the information you put in the tool (neither today nor in the future).

GDPR CST Presentation

1 SOLUTION, 3 FLAVORS

- **Public (CNPD website)**
  - Full application features
  - Limited Identity & Access Management (i.e. only individual registration)
  - Accessible to ALL (hosted on a publicly accessible IP)
  - All data are stored securely on a shared system
- **Private SaaS (Paid)**
  - Full application features
  - Full Identity & Access Management (i.e. multi user registration & delegation)
  - Accessible only to the subscriber (VPN and/or limited IP access)
  - All data are stored securely on a private system (dedicated to the subscriber)
- **Private OnPrem (Paid)**
  - Full application features
  - Full Identity & Access Management (i.e. multi user registration & delegation)
  - Accessible only to the subscriber (intranet)
  - All data are stored securely on the subscriber systems

Questions

eProseedRTC
WE SIMPLIFY COMPLEXITY.

Digital Lëtzebuerg

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST