GDPR Compliance Support Tool

Séance d'information 18 octobre 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

Les objectifs

- 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).

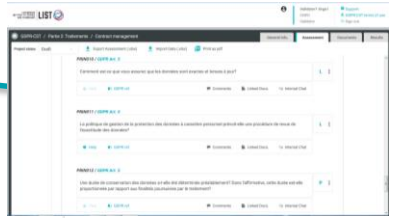
GDPR CST Presentation

Les composants

- **Un référentiel d'exigences**

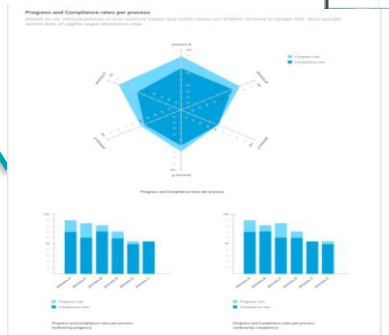
Exigences
Questions
Notice/exemple
Recommandations
Domaines

- **Une interface**



Niveaux de couverture
Justifications
Elements de preuve
Commentaires
Registre des traitements

- **Un reporting dynamique**



Registre de traitement / risques
Visualisation
Indicateurs clé

GDPR CST Presentation

Les fonctionnalités

- Une approche logique et détaillée du règlement, basée sur un **référentiel de plus de 350 exigences et recommandations associées**, élaboré par la CNPD.
- Une évaluation distincte pour chaque partie de l'organisation : **département, site, filiale**…(Partie 1), pour chaque **traitement** (Partie 2) et pour chaque **sous-traitant** (Partie 3).
- La possibilité de gérer son **registre des traitements** sur base des traitements renseignés dans la Partie 2.
- La **visualisation et l'export de résultats et graphiques** spécifiques à une évaluation ou consolidés.
- La **gestion des documents** de preuve.
- **L'export et l'import des évaluations** en cours pour partager le travail ou le continuer sous d'autres formats.
- Des fonctionnalités évolutives à venir dans la version 2.0 comme le mode multi-utilisateur ainsi que l'import et le stockage de documents de preuve.

GDPR CST Presentation

Le référentiel d'exigences

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

GDPR CST Presentation

Le référentiel d'exigences

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.

GDPR CST Presentation

Le référentiel d'exigences

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 transférées aux personnes concernées de manière sécurisée.

6) …

GDPR CST Presentation

Le référentiel d'exigences

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

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

Les limites

- L’outil n’offre pas de garantie de conformité par rapport à la législation pour vos traitements.
- En tant que responsable de traitement, vous restez responsable de la gestion de vos activités de traitement (accountability).
- L’outil n’est pas à considérer comme une solution à toutes les problématiques liées au traitements de données à caractère personnel.
- La CNPD n’a à aucun moment accès aux informations que vous mettez dans l’outil (ni aujourd’hui, ni dans le futur).

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

Q&R

eProseedRTC
WE SIMPLIFY COMPLEXITY.

Digital Lëtzebuerg

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST