

28/01/2025



Data protection awareness toolbox for SMEs and startups

Jérôme Comodi
Legal advisor, Project manager

DATA PROTECTION DAY
Take Control of your Privacy

Introduction



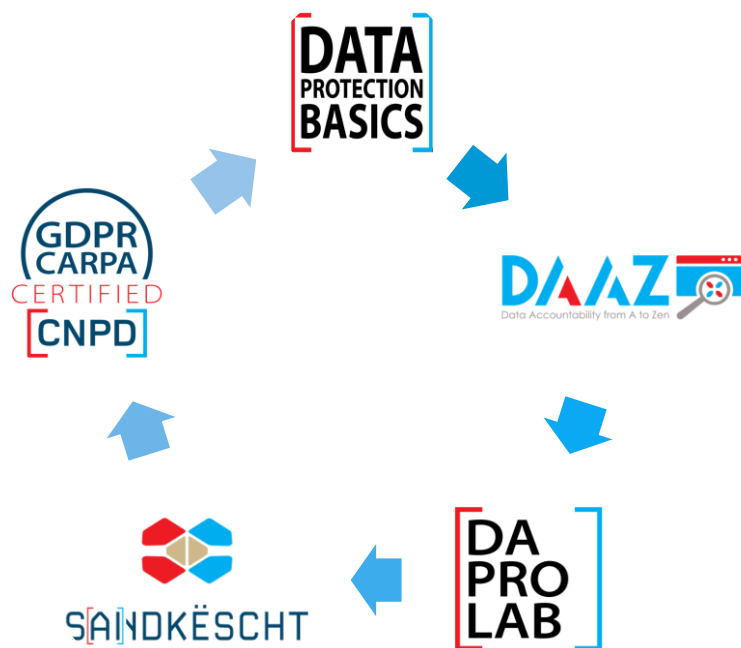
- **CNPD mission**
 - To actively engage in promoting and enabling a trusted digital economy with an innovation ecosystem respectful of privacy and personal data
- **Observations after 6 years of GDPR**
 - **Maturity of organisations** in terms of privacy and data protection is still quite weak, especially in non regulated sectors, in SMEs, startups and with independent entrepreneurs
 - **Generative AI** triggers a new wave of technologies and innovation
 - **New incoming EU/LU legislation** (DGA, DA, AI Act, DSA, DMA, ...) is putting additional “pressure” on organisations, increasing potential compliance gaps and barriers for innovation
 - Common shared **vision of stakeholders** to promote a development of a digital economy built on responsible innovation and aligned on the new legal framework
 - **Collective effort** needed to increase awareness and promote data governance and accountability



La Commission Nationale pour la Protection des Données (CNPD) s'engage activement à promouvoir une économie responsable et respectueuse de la protection des données à caractère personnel et de la vie privée. Elle fait cela depuis sa création en 2002, mais c'est avec l'entrée en vigueur du Règlement général sur la protection des données (RGPD) en 2018 et l'évolution rapide des nouvelles technologies numériques, en particulier l'intelligence artificielle (IA), que le CNPD considère ceci comme une priorité.

Dans cette optique, la CNPD a lancé en janvier 2024 un appel à contribution visant à mieux comprendre les problématiques des acteurs de l'écosystème luxembourgeois par rapport à l'utilisation de l'intelligence artificielle et à esquisser des mesures d'accompagnement appropriées, conformément à sa mission de guidance.

CNPD initiatives



■ Data Protection Basics

- Training sessions introducing basic data protection concepts and the GDPR with the general public and professionals without prior knowledge as a key target

■ DAAZ

- Interactive GDPR eLearning through gamified story-telling targeting small companies

■ DaProLab

- In person closed workshops encouraging exchange of experiences between professionals with the support of the CNPD as a moderator

■ Sandkëscht

- Regulatory sandbox for innovative use cases to test and enhance GDPR compliance.

■ GDPR certification

- Framework allowing professionals with an advanced maturity level in data protection to demonstrate their compliance with the GDPR



“Data Protection Basics” training sessions

DP-Basics training sessions



▪ Objectif

- To explain the **key principles** of data protection and privacy so that the GDPR can be properly understood and applied.

▪ Target public:

- General public from any organisation or at individual **without any prior knowledge** of legal background
- Not aimed at an expert audience and not intended to train professionals in the field

▪ Format

- one day **5h on-site** course
- Pre scheduled sessions, 1 per month,
- **20-25 participants**
- 2 CNPD trainers per session
- Sessions in French; in English (starting October 2024)
- **Certificate of attendance** on request
- **Free participation**

▪ Main topics covered

- **Key elements:** definitions, life cycle of personal data, controller/sub-processor, the RGPD
- **Main principles:** purpose limitation, transparency, lawfulness, data minimisation, retention periods, security, accountability, etc.
- **Data subject rights:** right to information, right of access, right to object
- **Obligations of organisations:** register of processing operations, data breach notification, impact assessment
- **Voluntary compliance tools:** certifications, codes of conduct, ...
- The **DPO**
- **Supervisory authorities**

DP-Basics : figures



- **(Re)Launch**

- Development / update of former CNPD course from 2018
- Integrating elements from GDPR eLearning for civil servants developed in collaboration with CGPD and INAP
- First 2 test sessions in December 2023

- **Sessions**

- 12 sessions held (2023-2024), 5 announced (2025)
- 200 participants since start; 22 participants effectively present on average per session
- 9 CNPD trainers

DP-Basics : continued development



- **Widen the public**
 - sessions in English language (oct 2024)
 - sessions outside of Belval
 - Integration into the Digital Learning Hub (DLH) programme starting 2025

- **Widen the scope**
 - Specific sessions « artificial intelligence et data protection» (4 sessions in 2024 and 5 announced in 2025)
 - based on simple and specific examples
 - in the context of the GDPR (not AI Act)
 - Interaction of GDPR and AI Act
 - Prerequisites: attend the “data protection basics” training or have completed DAAZ



Interactive eLearning and compliant tool DAAZ

Origin of the initiative



- **GDPR Compliance Assessment Tool (CST) available online between 2017 and 2022**
- **EU Project ALTO (2022-2024)**
 - programme CERV (Citizens, Equality, Rights and Values Programme)
 - In collaboration with LHC - NC3

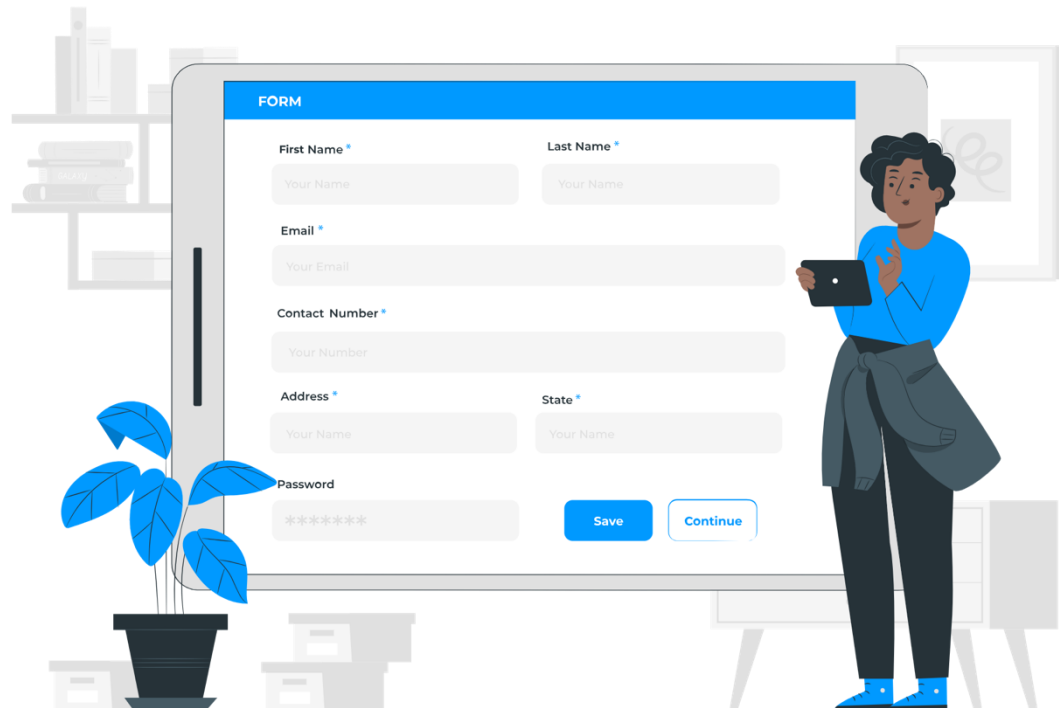
Objective

- Supporting very small businesses, startups and SMEs
- ... in understanding, strengthening and maintaining their **compliance with the GDPR**
- ... by creating an **enjoyable educational tool** based on story learning, gamification, UX and immersion
- ...free of legal language



1. Identification of the « users' needs »

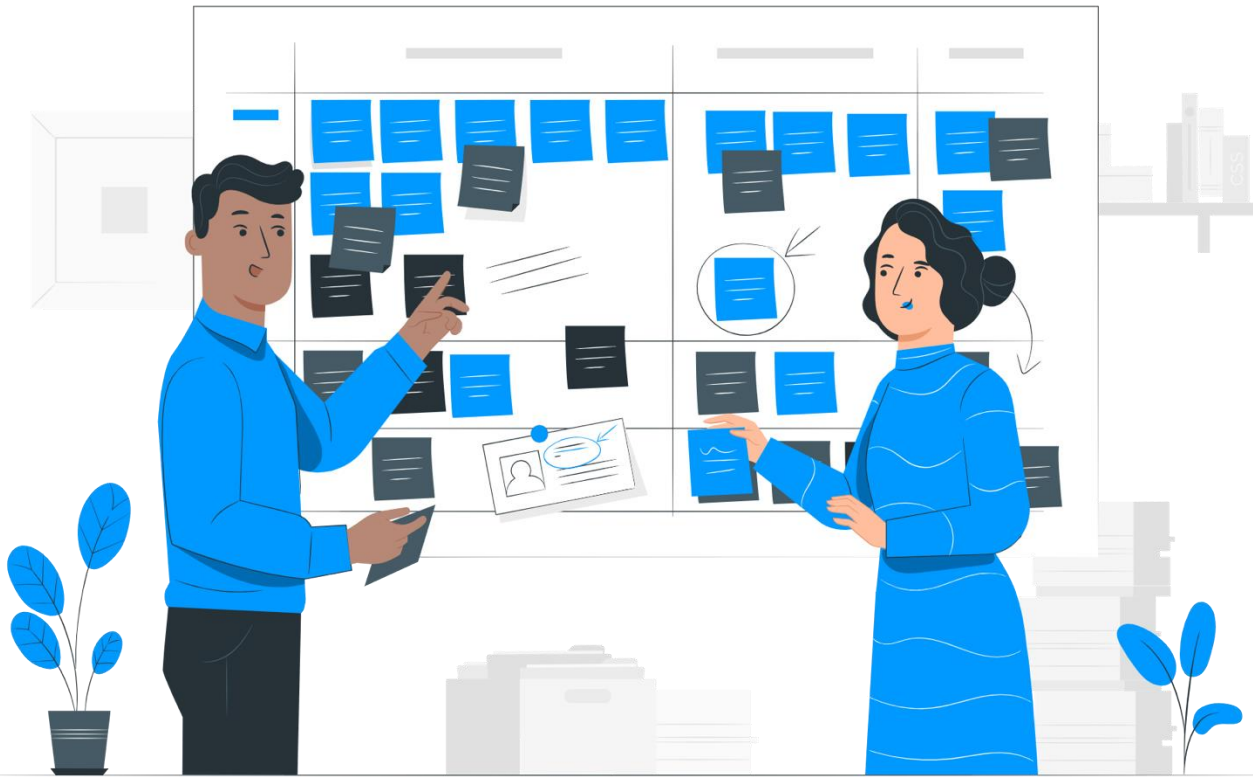
Drafting of the online Survey



Collaboration with SMEs



2. Design



- 9 GDPR Model criteria
- 4 maturity levels
- Learning by Doing methodology
- Integration of UX concepts
- Narration and immersion
- Gamification
- Accessibility and gender neutrality

Double objective :

- ✓ Focus on user experience
- ✓ Ensure user commitment

2. Design

Connaissances



- 9 “GDPR Model” criteria

Double objective :

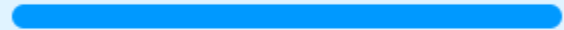
- ✓ Focus the tool on user experience
- ✓ Ensure user commitment

2. Design

Bases
Level 1



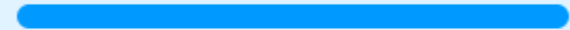
Progression: **100%**



Conception
Level 2



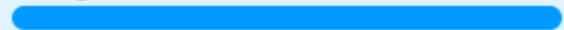
Progression: **100%**



Implementation
Level 3



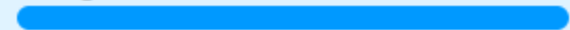
Progression: **100%**



Governance 2.0
Level 4



Progression: **100%**

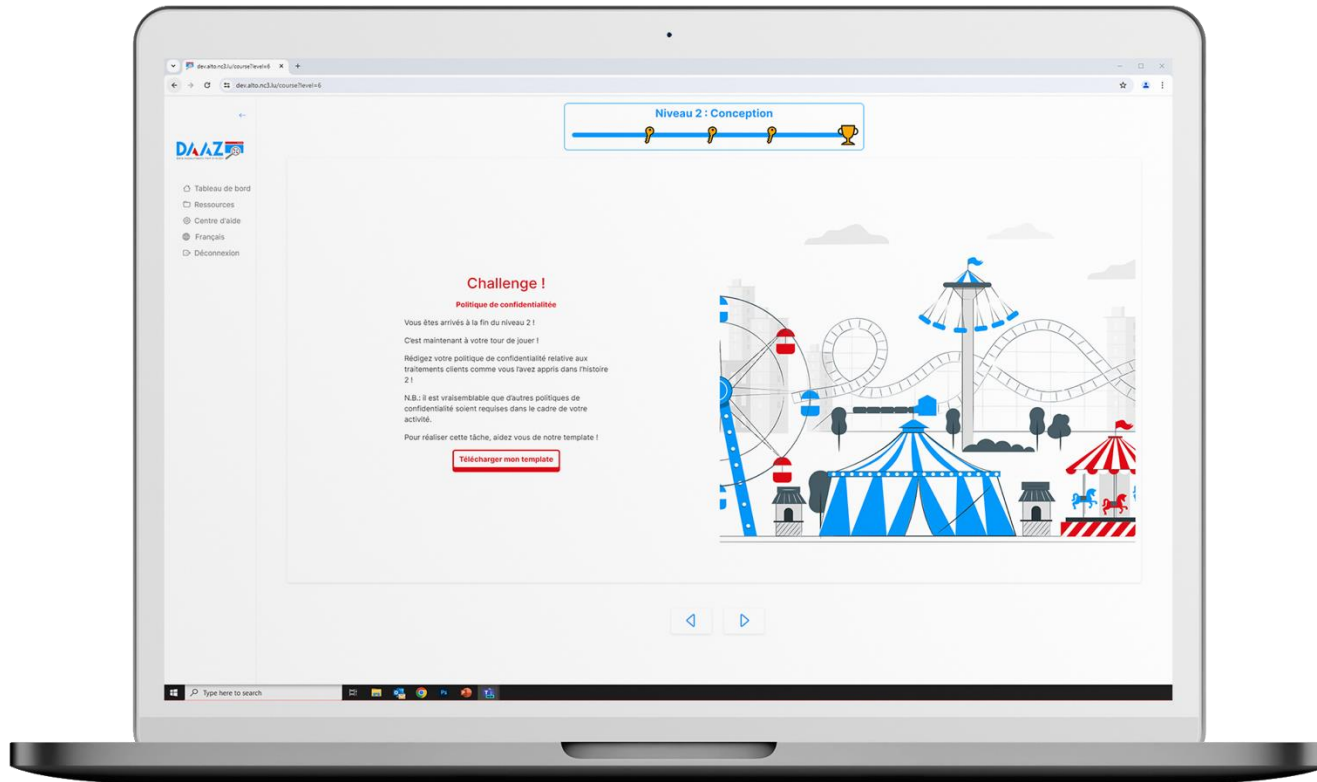


- 9 GDPR Model criteria
- **4 maturity levels**

Double objective :

- ✓ Focus the tool on user experience
- ✓ Ensure user commitment

2. Design

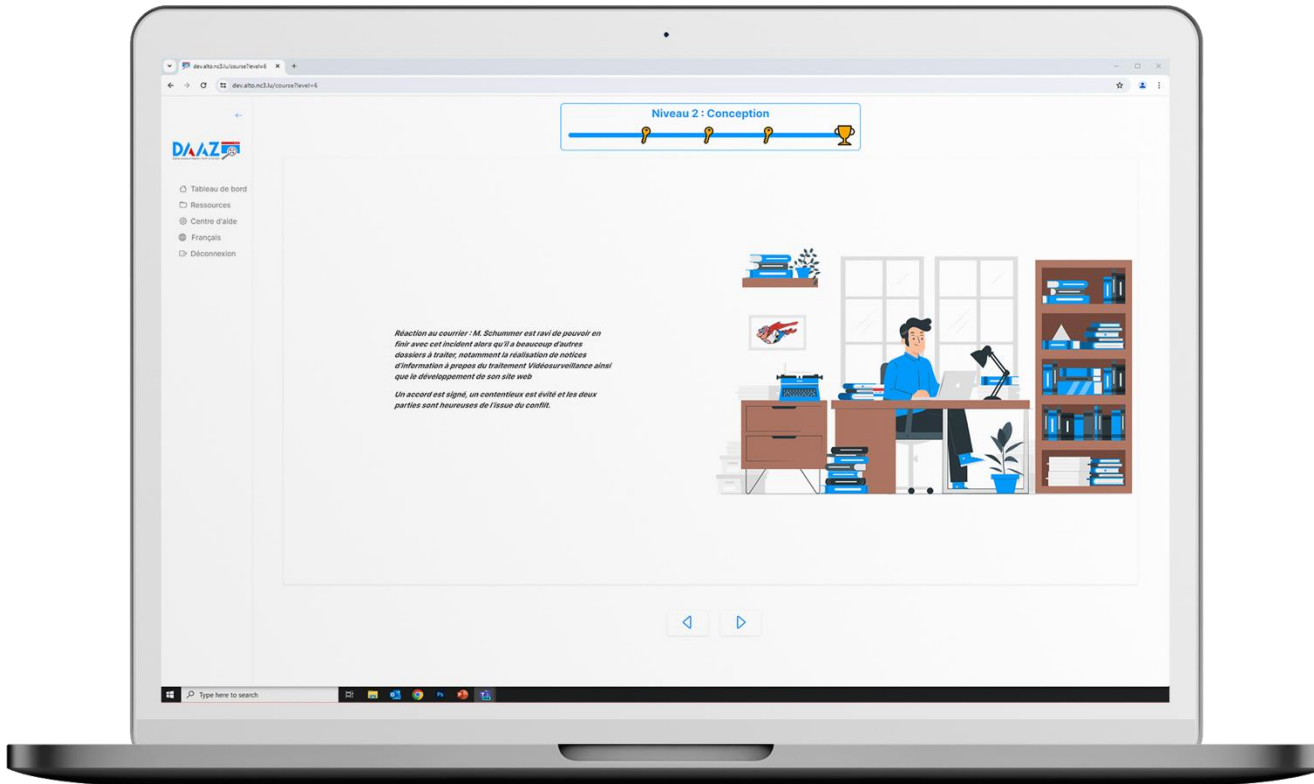


- 9 “GDPR Model” criteria
- 4 levels of maturity based on the “design science” method
- **“Learning by Doing” methodology**

Double objective :

- ✓ Focus the tool on user experience
- ✓ Ensure user commitment

2. Design

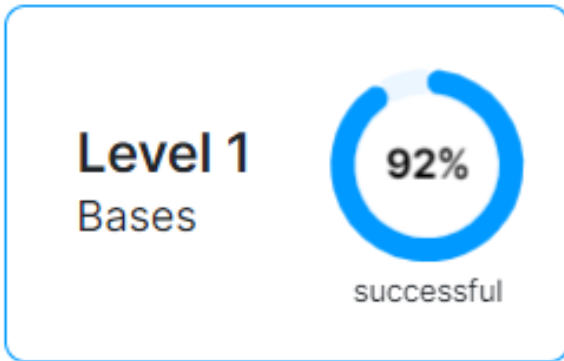


- 9 “GDPR Model” criteria
- 4 levels of maturity based on the “design science” method
- “Learning by Doing” methodology
- **Narration and immersion**

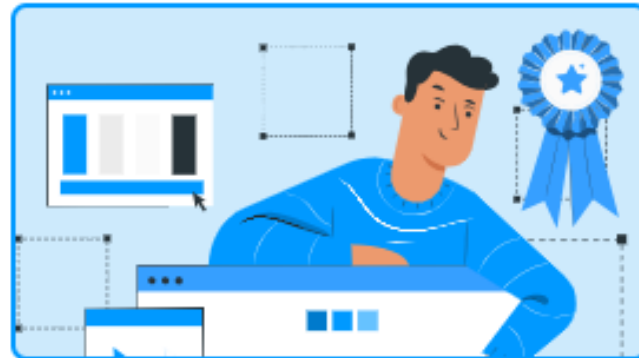
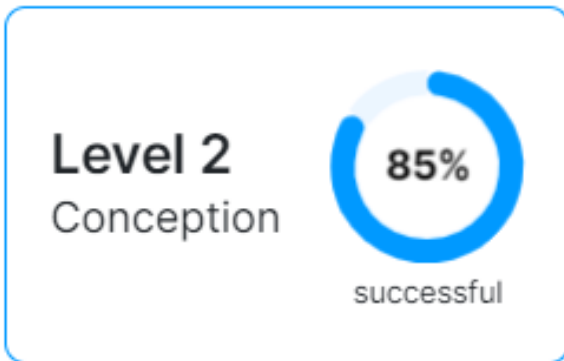
Double objective :

- ✓ Focus the tool on user experience
- ✓ Ensure user commitment

2. Design



- 9 “GDPR Model” criteria
- 4 levels of maturity based on the “design science” method
- “Learning by Doing” methodology
- Narration and immersion
- **Gamification**



Double objective :

- ✓ Focus the tool on user experience
- ✓ Ensure user commitment

2. Design

Dominique

Il faut bien vivre avec son temps !
A ce propos, voici un courrier de votre confrère,
Me Gilles
Mertens. Lisez-le et dites-moi comment réagir.
J'ai vraiment besoin de vos conseils !

Me P. Boodhun

Apparemment, il s'agit d'une affaire délicate en
matière de
droit du travail et de protection des données
personnelles...

Dominique

Ça concerne aussi les données personnelles ?
Alors, ça tombe
bien !
Je termine justement de remplir mon registre de
traitements,
via le template de la CNPD.



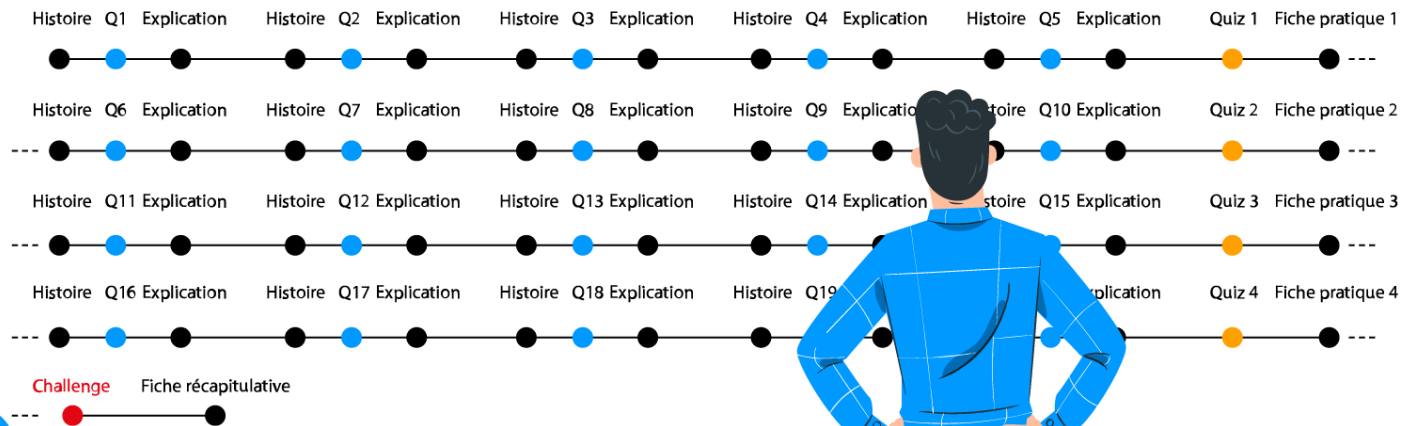
- 9 “GDPR Model” criteria
- 4 levels of maturity based on the “design science” method
- “Learning by Doing” methodology
- Narration and immersion
- Gamification
- **Accessibility and gender neutral**

Double objective :

- ✓ Focus the tool on user experience
- ✓ Ensure user commitment

3. User Interface

Schéma d'un niveau



3. User Interface

Niveau 4 : Gouvernance 2.0



Question 17
Veuillez ordonner les étapes d'un P.D.C.A. appliqué à la gestion de données personnelles.

1. Planifier – convenir des finalités, bases légales, évaluer les risques vis-à-vis des personnes concernées, notamment
2. Mettre en œuvre – rédiger les procédures et notices en protection des données et les fonctions des ressources, notamment
3. Vérifier – vérifier régulièrement la conformité du traitement au RGPD de bout en bout, vérifier les connaissances du personnel, vérifier les mise à jours des recommandations de la CNPD, notamment
4. Ajuster – améliorer et ajuster au besoin les traitements, la documentation, la formation du personnel, notamment

ONLINE TEST

1. A B C D

2. A B C D

NEXT >



Navigation arrows: < >

3. User Interface

Quiz 1.1


Script: 3 catégories de données vont vous être proposées, à savoir celles dont le traitement est en principe interdit, celles dont le traitement est effectué sous le contrôle de l'autorité publique et celles qui n'appartiennent à aucune de ces 2 catégories.

Quiz : Parmi les données suivantes, cochez celles dont le traitement est en principe interdit:

- Les condamnations pénales.
- L'origine ethnique.
- Les données industrielles.
- Les opinions politiques.
- Les convictions religieuses.
- L'appartenance syndicale.
- Les infractions ou les mesures de sûreté connexes.
- Les données génétiques.
- Des données biométriques.
- Le savoir-faire d'une entreprise.
- Des données concernant la santé.
- Des données concernant l'orientation sexuelle.



3. User Interface



Fiche pratique 1: Les principales notions

Depuis le 25 mai 2018, le Règlement général sur la protection des données (RGPD) est applicable. Le RGPD vise principalement à donner aux individus le contrôle de leurs données à caractère personnel et demande aux entreprises qui gèrent des données de justifier la collecte et la conservation des données personnelles, d'assurer leur sécurité et leur confidentialité, d'informer les personnes concernées sur leurs droits (modification, suppression, portabilité des données...) et nommer un délégué à la protection des données (DPO) dans certains cas.

Par « Responsable du traitement », on entend tout organisme qui détermine les finalités et les moyens du traitement de données à caractère personnel (Administration publique, entreprise privée, association, notamment).

Le « DPO » n'est pas obligatoire sauf condition. Une personne de contact en matière de protection des données est fortement recommandée afin de centraliser les mesures qu'implique la gestion des données. Nommer un DPO ou DPO ne dégage le gérant de ses responsabilités en matière de gestion des données.

Par « Données à caractère personnel », on entend toute information concernant une personne physique identifiable ou identifiable. Une « personne physique identifiable » est définie comme 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 un ou plusieurs éléments spécifiques

Fiche pratique 2: Traitement d'un droit

Sur base du droit d'accès, un client, un salarié ou toute personne concernée peuvent vous adresser une demande de communication de toutes ou certaines des données que vous possédez à son sujet (Art. 15 du RGPD).

Les notions qui entourent la réponse à une demande de droit d'accès :

- **Respect de la forme** : Si le droit d'accès est exercé sous une forme électronique, les informations sont à fournir par voie électronique lorsque cela est possible, à moins que la personne ait demandé qu'il en soit autrement.
- **Les éléments d'information** doivent être compréhensibles et aisément accessibles, en des termes clairs et simples.
- **La réponse** doit être communiquée dans les meilleurs délais et au plus tard, dans un délai d'un mois à compter de la réception de la demande.
- **Aucun paiement ne peut être exigé** pour fournir les éléments d'information demandés, sauf si les demandes sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif.
- **Vous pouvez demander des informations supplémentaires nécessaires** pour obtenir confirmation de l'identité du demandeur, s'il y a des doutes raisonnables quant à son identité.

Fiche pratique 3: Les critères du consentement et bases de licéité

Le consentement de la personne concernée est défini comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » (Art. 4.1 du RGPD). Pour être valide, le consentement de la personne concernée doit présenter différentes caractéristiques.

- Le consentement doit être « libre ». La personne concernée doit disposer d'un véritable choix entre le refus ou de retirer son consentement sans subir de préjudice.
- Le consentement doit être « spécifique ». Le consentement doit correspondre à une finalité spécifique et déterminée à l'avance. Lorsqu'un traitement comporte plusieurs finalités, la personne doit pouvoir consentir à chacune d'elles.
- Le consentement doit être « éclairé ». La personne concernée doit être informée de l'identité du responsable du traitement et des finalités du traitement auxquelles sont destinées ses données. Par ailleurs, il convient de préciser, dans le formulaire de consentement, que la personne a le droit de retirer son consentement à tout moment. Les informations fournies doivent permettre à la personne concernée de comprendre ce qu'il va advenir de ses données. Pour ce faire, les informations ne doivent être « noyées » dans des notices générales.
- Le consentement doit être « univoque ». Le consentement doit être donné sans ambiguïté par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement de données la concernant. Cet acte positif peut prendre la forme d'une déclaration écrite ou comprise par voie électronique. Cela peut

Fiche pratique 4: Le registre des activités de traitement

Le registre des activités de traitement (« registre ») doit être tenu par le responsable du traitement sous forme écrite ou électronique. Son format est libre. Il permet au responsable de traitement de documenter sa conformité au RGPD, ce qui est un élément important du principe de responsabilité ou d'« accountability ».

Le contenu du registre doit comprendre des informations sur tous les traitements de données effectués par l'organisation (Art. 30 du RGPD). Il comporte, pour chaque traitement, notamment les informations suivantes, lesquelles nécessitent de comprendre les principes fondamentaux du RGPD :

 - le nom et les coordonnées du responsable du traitement et du DPO (v. fiche pratique n° 2) ;
 - les finalités du traitement. La finalité est l'objectif en vue duquel le traitement des données est opéré. Les objectifs poursuivis doivent être choisis et connus avant le début du traitement (v. encart sur les critères des finalités) ;
 - les catégories de personnes concernées ;
 - les catégories de données. Le principe de minimisation doit être appliqué. Il prévoit que vous devez traiter uniquement les données qui sont nécessaires (et non seulement utiles) à la réalisation des finalités ;
 - les catégories de destinataires (y compris dans des pays tiers) ;
 - les délais de conservation des données (si non les critères pour justifier cette durée). Le principe de limitation de la conservation doit être appliqué, lequel prévoit que les données doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.
 - une description générale des mesures de sécurité techniques et organisationnelles en place pour protéger les données. Le principe d'intégrité et de confidentialité doit être appliqué, lequel prévoit que vous devez assurer l'intégrité et la confidentialité des données à l'aide de mesures techniques et organisationnelles appropriées, notamment contre un traitement non-autorisé ou illégal et contre la perte, destruction ou altération accidentelle des données.
 - le cas échéant : les transferts de données vers des pays tiers (c'est-à-dire hors de l'espace économique européen) et les coordonnées du responsable conjoint du traitement.

RED FLAG: En cas de demande émanant de la CNPD, le registre devra lui être mis à disposition.

Les finalités doivent être :

 - **Déterminées** : la finalité vise effectivement à limiter les opérations de traitement à une finalité précise et prédéfinie.
 - **Explicites** : l'explication donnée doit être à même de permettre à tout un chacun de comprendre la finalité poursuivie, indépendamment des différences sociales ou linguistiques pouvant exister entre les individus.
 - **Légitimes** : l'utilisation des données personnelles aux fins indiquées doit être conforme à la loi.




RED FLAG: Les données personnelles ne doivent pas être traitées ultérieurement d'une manière incompatible avec les finalités initialement déterminées (Art. 5.1.c. du RGPD).



3. User Interface




3. User Interface

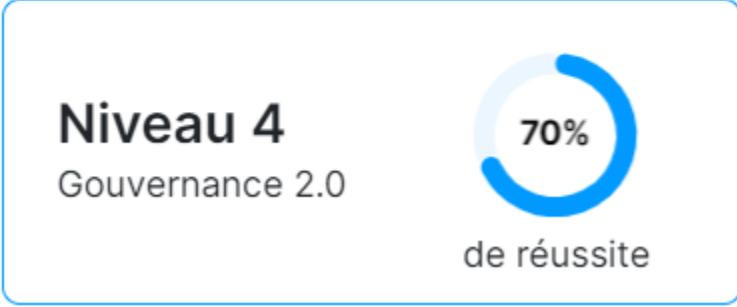
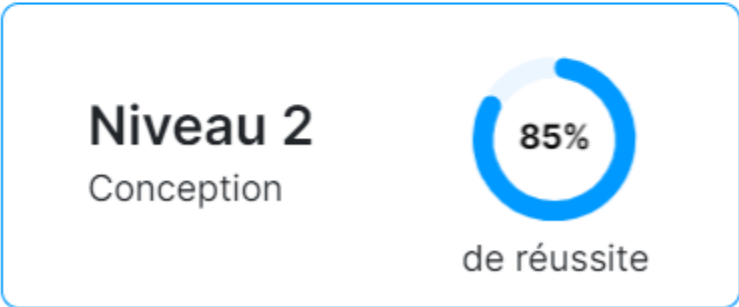
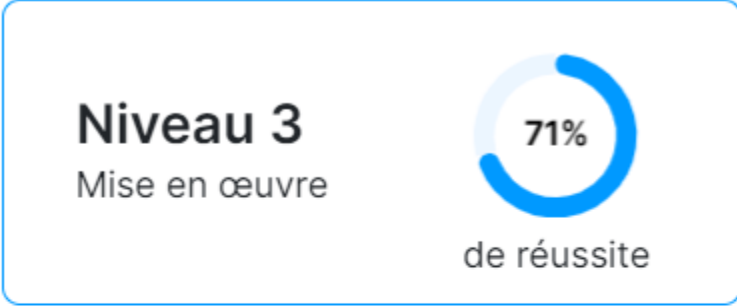
AutoSave Off    Le registre des activités de traitement.xlsx - Protected... • Saved to this PC

File Home Insert Page Layout Formulas Data Review View Automate Help

Graphic 2 *fx*

	A	B	C
1		<p><u>Illustration d'un registre des activités de traitement sur base de l'article 30 du règlement général sur la protection des données</u></p> <p><i>Attention : Ce document constitue uniquement un modèle de registre des activités de traitement, qui reprend une liste exemplative et non exhaustive des traitements habituels d'une entreprise. Les différentes rubriques doivent donc être complétées et adaptées au cas par cas en fonction des activités et des finalités des traitements de données de l'entreprise.</i></p>	
2			
3			
4			
5			
6			
7			
8			
9			
10			
11		Nom et coordonnées du responsable du traitement	Nom de la société ou de l'entreprise, nom du gérant/responsable/président, adresse postale, numéro de téléphone, adresse mail, site internet
12			
13		Le cas échéant, coordonnées du représentant du responsable de traitement	
14			
15		Le cas échéant, coordonnées du représentant du délégué à la protection des données (ou Data Protection Officer (DPO))	
16			
17		Dernière mise à jour du registre	xx/xx/202x

3. User Interface



First feedbacks

DAAZ after the first 6 months (since July 2024)





“DaProLab” Workshops

“DaProLab” workshops



- **Objective:**
 - To **exchange** knowledge, experiences and good practices
 - ... on **pre-selected topics** in the field of personal data protection and the GDPR
 - ... in order to **foster accountability** with the participants by **discussing opposing views**
- **Target public**
 - aimed at data protection professionals and technical experts on the topic covered during the session
 - not aimed at identifying commercial opportunities
- **Format**
 - **Closed, interactive 2-hours sessions, in person**
 - in French as the guiding language
 - selection of one topic per session by CNPD or together with actors
 - 10-15 participants per session, selected according to the topic
 - **CNPD is only the organizer and moderator**, not a participant, ensures that discussions are productive
 - Technical experts to present specific topics

“DaProLab” workshops : figures



- **(Re) launch of the initial CNPD workshop concept from 2018**
 - 5 sessions in 2024
 - April 2024: *L'Intelligence artificielle et la protection des données*
 - May 2024: *Privacy by Design dans le contexte de l'intelligence artificielle*
 - Juillet 2024 : *L'IA et la gouvernance des données personnelles au sein des organisations*
 - Septembre 2024: *Décisions automatisées*
 - Octobre 2024: *Sécurité IA ou OSINT (Open Source Intelligence)*
 - 2 sessions planned in 2025
 - February 2025: *Regulatory sandbox on AI in collaboration with LIST*
 - 17 April 2025: *AI and Use case in collaboration with UNESCO*



GDPR Certification

Commission Nationale pour la Protection des Données

GDPR Art. 42 & art. 46

GDPR Certification – Art. 42 & 43



GDPR Art. 42 Certification (Data processing certification)

- a **voluntary process** that helps to demonstrate compliance with the GDPR. The GDPR does not introduce any right or obligation for controllers and processors to be certified.
- an **accountability tool**. It enables companies, public authorities, associations and other bodies to demonstrate their compliance with the GDPR.
- a **legally binding tool**, unlike, for example, ISO certification of management systems.
- National certifications / EU Seal Certifications

GDPR Art. 43 Accreditation of Certification bodies

- In LU, the CNPD handles the accreditation activities for GDPR certifications.

GDPR - CARPA Certification



- Certification scheme developed by the CNPD
- Covers internal governance systems
- Based on ISAE 3000, ISCQ1 and ISO17065 standards
- 3 certification bodies approved by the CNPD

Actions to encourage GDPR Certifications

- Communications addressed to C-Level
- Voluntary tool -> Difficult to convince decision makers



GDPR Certification – What will happen?



GDPR Art. 46 – Certification as a tool for transfers

- First certification of this kind
 - GDPR Art. 46.2.f: *“an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.”*
- CNPD competent supervisory authority to get it approved at EDPB level
- Forecast regarding the availability of the tool: 2nd Quarter 2025

Actions to encourage GDPR Certifications

- Communications addressed to C-Level
- Voluntary tool -> Difficult to convince decision makers



“A.I. and Data Protection” training sessions

AI and Data Protection training sessions



▪ Objectif

- To explain the **key principles** of data protection and AI regulation so as to ensure that AI systems can be developed and deployed in compliance with the regulations.

▪ Target public:

- Any organisation or/and any individual **with minimum prior knowledge** of legal background
- Not aimed at an expert audience and not intended to train professionals in the field

▪ Format

- one day **3h/4h on-site** course
- Pre scheduled sessions, 5 per years,
- **20-25 participants**
- 2 CNPD trainers per session
- Sessions in French; in English
- **Certificate of attendance** on request
- **Free participation**

▪ Main topics covered

- **Key element of AI** : how it works and what it's used for. AI impact on data protection.
- **Main principles**: Technical aspects of AI with a focus on supervised learning. Review of data protection and points relevant to AI. Connections between the AI Act and the RGPD.
- **Concrete examples of applications** : focus on AI systems using personal data.
- **Highlight on** : automated decisions, the use of special categories of personal data and further processing of personal data.

AI and Data Protection: figures



■ Launch

- Integrating elements from AI Act
- First 4 sessions in November and December 2024

■ Sessions

- More than 100 participants since the Beginning
- 20 participants effectively present on average per session
- 5 CNPD trainers
- 4 sessions held (2024)
- Next 4 Publics Sessions : 03/02, 17/02, 03/03 and 17/03



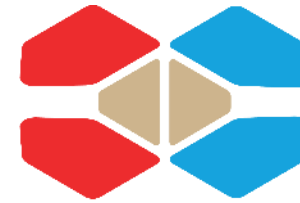
Regulatory Sandbox (RSB)

Commission Nationale pour la Protection des Données

Regulatory Sandbox



- The "Regulatory Sandbox" program aims to provide
 - a dedicated space
 - to test and assess the legal implications of new technologies and personal data use,
 - especially in artificial intelligence,
 - in collaboration with innovation players in Luxembourg.



S[A]NDKËSCHT

The evolutive approach



- The “Sandkëscht” regulatory sandbox designed to evolve:
 - by enabling skill development as a supervisory authority, and
 - by fostering practical experience in managing the Sandbox.
 - **Regulatory**: supporting innovation actors in their compliance with the GDPR and soon, with the AI ACT.
 - **Artificial Intelligence**: Implementing a sandbox dedicated to artificial intelligence, focused on personal data protection, follows a specific plan over a set period.
 - A measure of support for effective innovation **IA act**:
 - Operational AI regulatory sandbox (**horizon 2026**).

The Entry Mechanism



Participating Organisation:

- Any entity registered in Luxembourg, regardless of its size, sector of activity, or status.

Innovation :

- Projects can focus on the development, integration, or use of new technologies, particularly artificial intelligence systems.

Benefits for individuals or society in general :

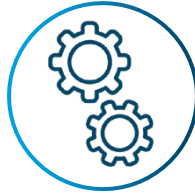
- This includes products or services that provide benefits to consumers or optimize the use of resources such as digital transformation, ecological transition, and more.

The benefits



Safe Space

Support data protection in the era of AI complexity



Experiment

Address new processing activities



Compliance

Strengthen the foundations for upcoming regulations



Open discussion

Direct collaboration with the data protection authority



Trusted innovation

Respectful of data subjects rights

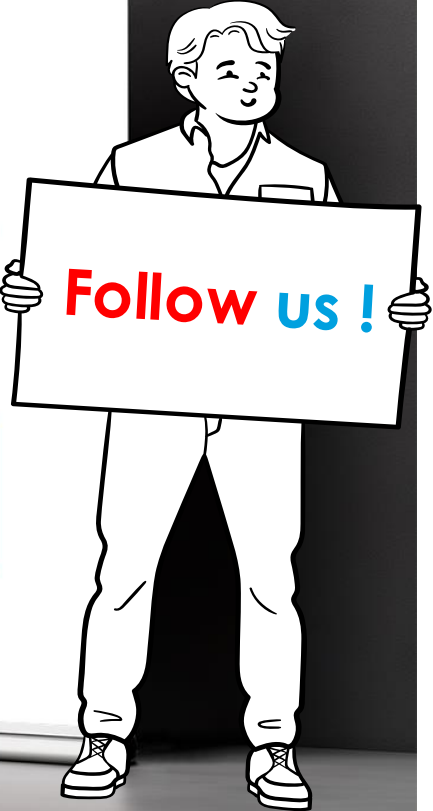
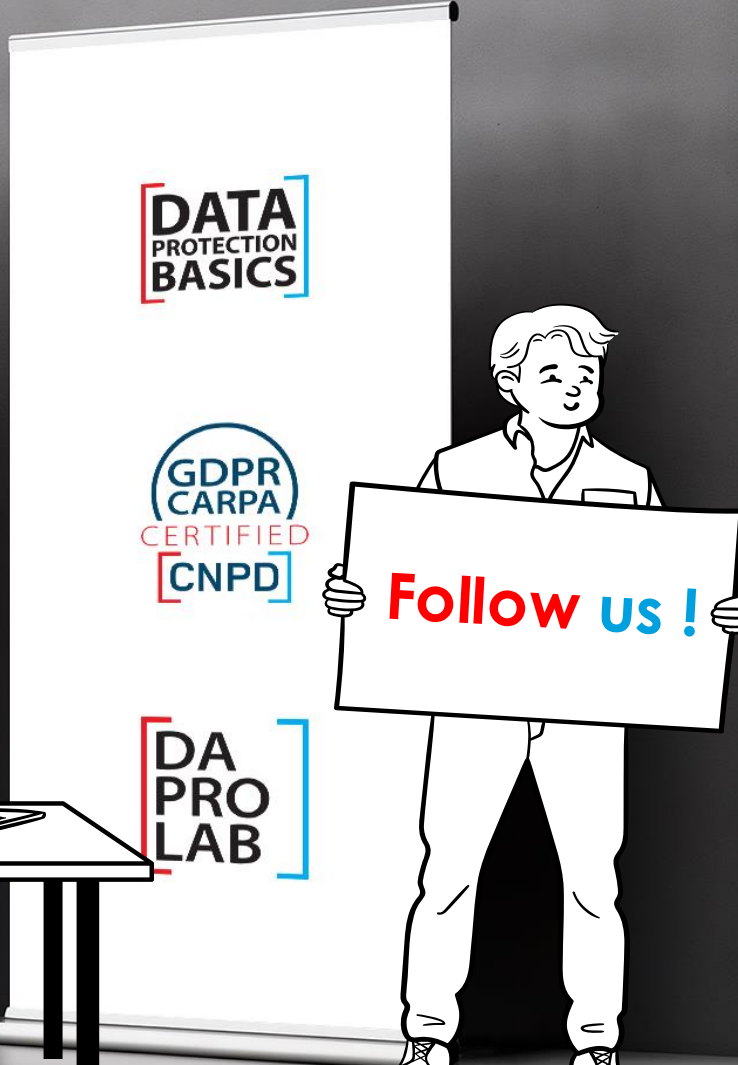


Reduce the costs

Prevent corrective actions and remediation costs

Any question ?

Visit the dedicated page!



MERCI! THANK YOU! DANKE!

Commission nationale pour la protection des données
15, Boulevard du Jazz
L-4370 Belvaux

261060-1 | www.cnpd.lu | info@cnpd.lu