

DAAZ & Leonora: Building Digital Competences for a Trusted Digital Society

Jérôme COMMODI

Head of Digital Literacy

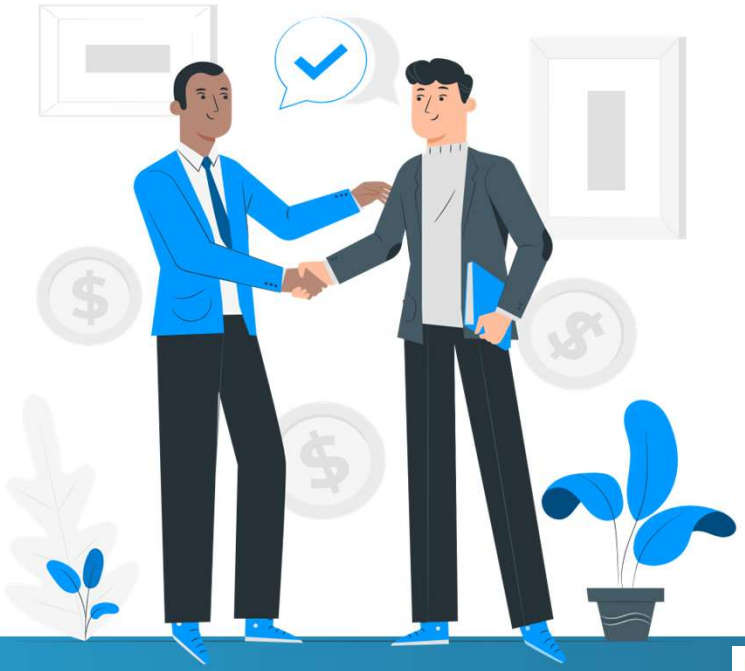
Fostering data protection risk assessment for SMEs and raising risk awareness among the general public



A Practical Interactive Learning Tool for SMEs

1. Origin of the tool

Grant Agreement



- Wish of the CNPD

Supporting SMEs in assessing, strengthening and maintaining their compliance with the provisions of the GDPR.

- Objective of the project :

Create a tool to facilitate GDPR compliance for SMEs.

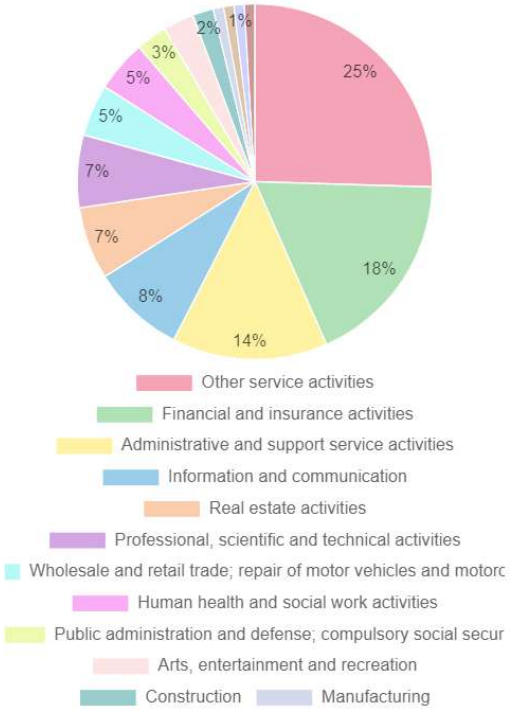
Co-funded by the European Union

1. Origin of the tool
Identification of the « end-users »

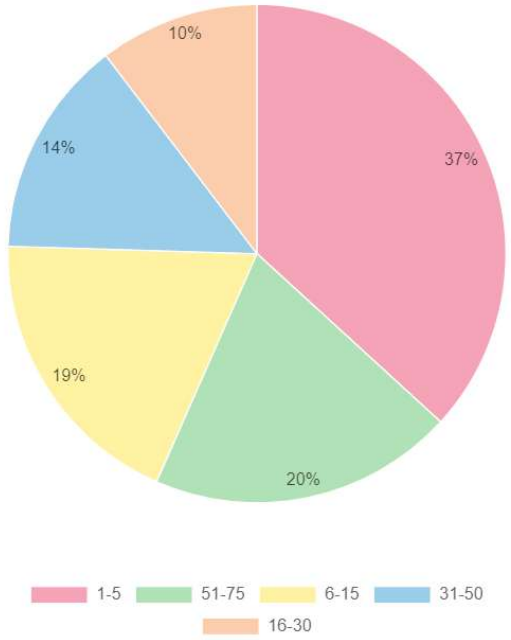
Collaboration with SMEs



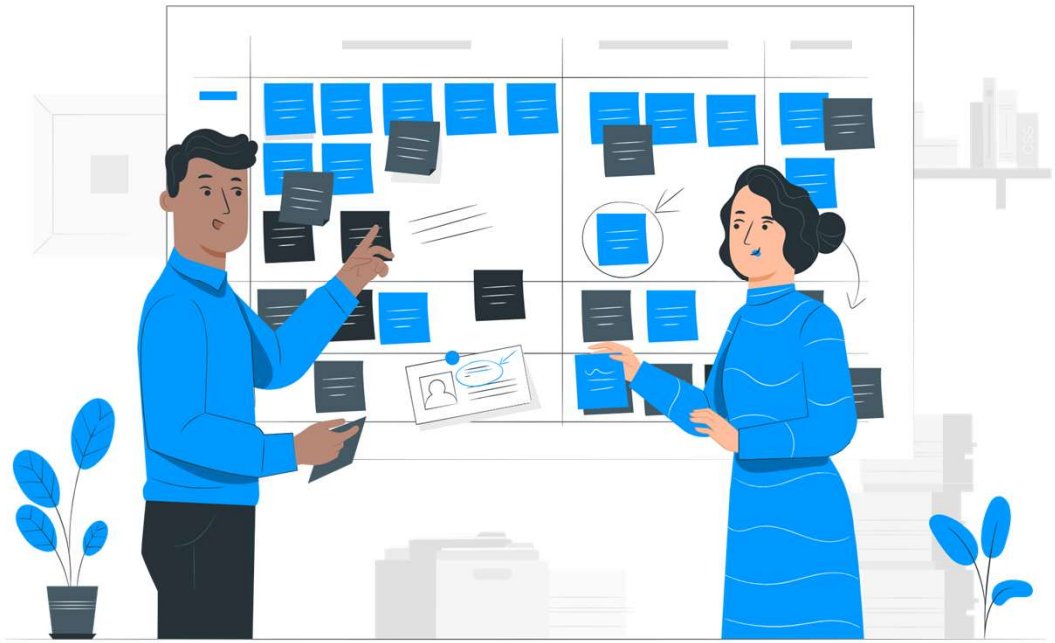
Surveys company sector



Surveys company size



2. Conception of a suitable tool



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

Double objective :

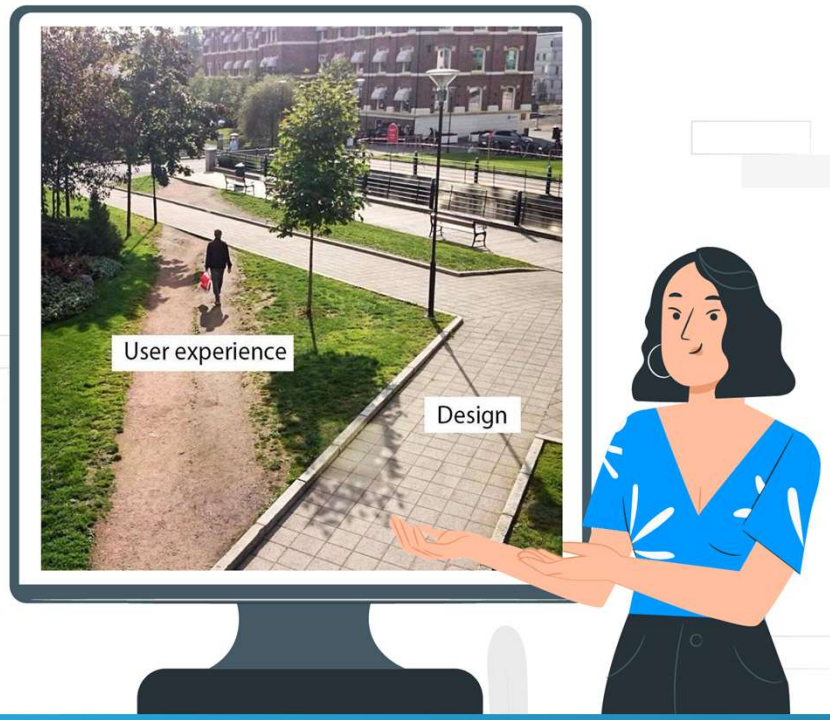
✓ Focus the tool on the user experience

✓ Ensure user commitment

Co-funded by the European Union

2. Conception of a suitable tool

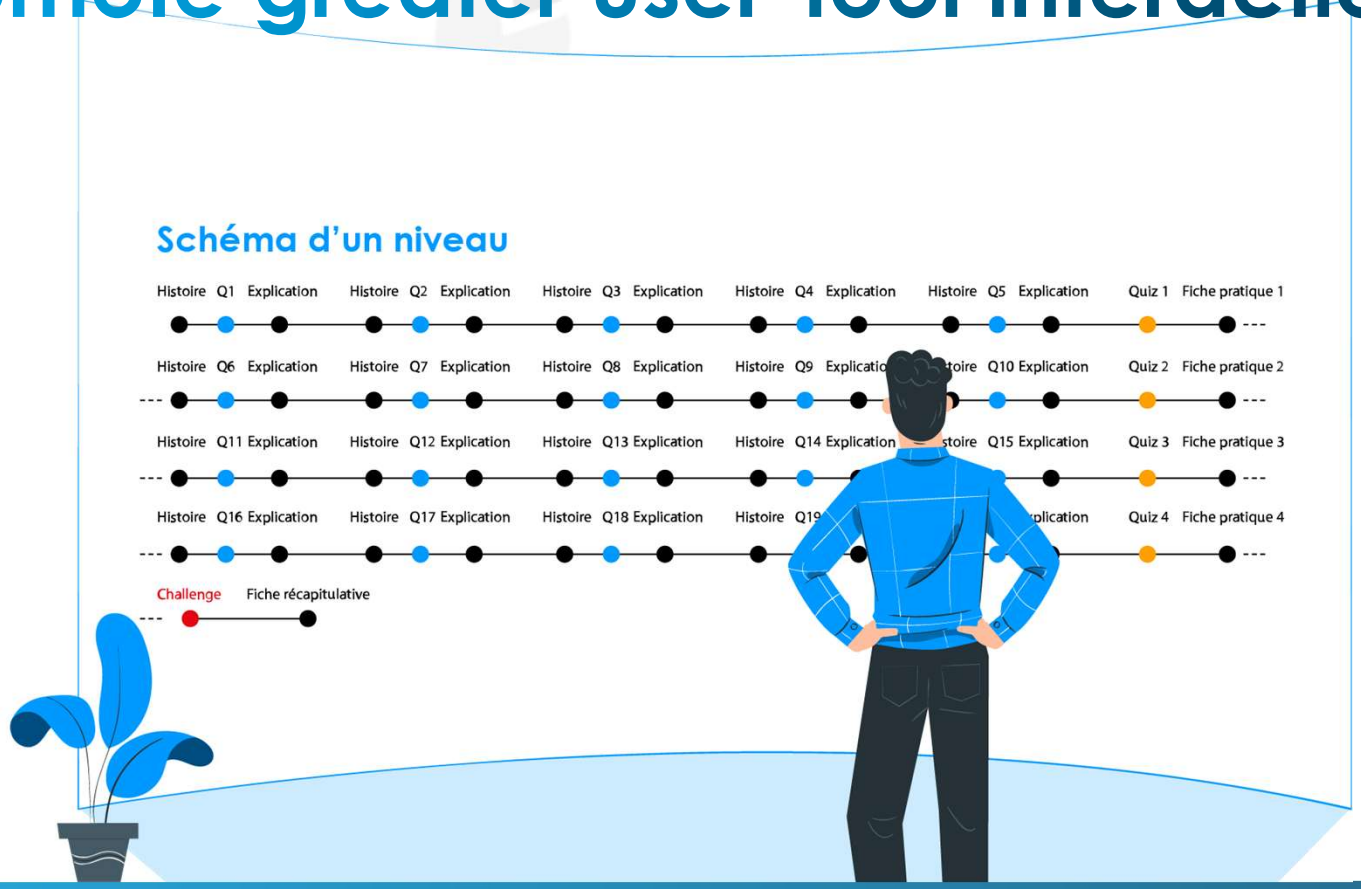
Technical point – User Experience



- The Advantage of **UX Design**
- Step 1 : **User search**
  interviews, questionnaire and persona
- Step 2 : **Conception**
  affordance, interaction cost and friction

Co-funded by the European Union

3. Promote greater user-tool interaction



Co-funded by the European Union

3. Promote greater user-tool interaction



Co-funded by the European Union

3. Promote greater user-tool interaction

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

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.

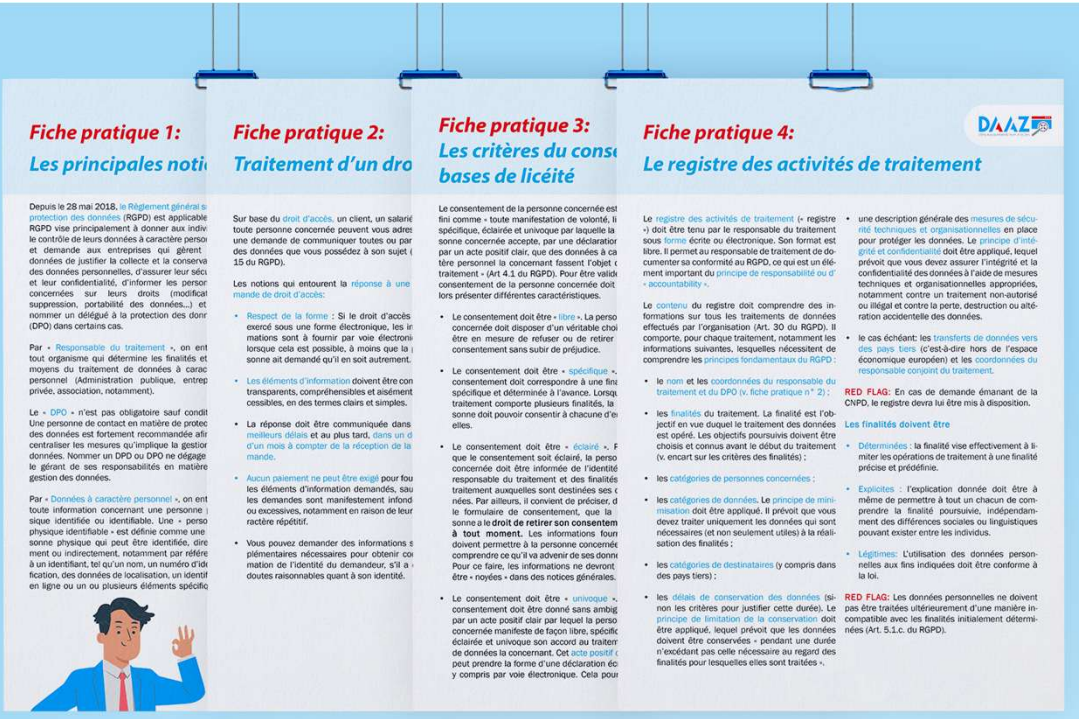
Quiz : Parmi les données suivantes, cochez celles dont le traitement est en principe interdit:

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



3. Promote greater user-tool interaction

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES



Fiche pratique 1:
Les principales noti

Depuis le 28 mai 2018, le Règlement général s protection des données (RGPD) est applicable RGPD vise principalement à donner aux indiv le contrôle de leurs données à caractère perso et demande aux entreprises qui gèrent données de justifier la collecte et la conserva des données personnelles, d'assurer leur séc et leur confidentialité, d'informer les perso concernées sur leurs droits (modificat suppression, portabilité des données,...) et nommer un délégué à la protection des donr (DPO) dans certains cas.

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

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

Par « Données à caractère personnel », on ent toute information concernant une personne sique identifiée ou identifiable. Une « perso physique identifiable » est définie comme une sonne physique qui peut être identifiée, dire ment ou indirectement, notamment par référe à un identifiant, tel qu'un nom, un numéro d'id fication, des données de localisation, un identif en ligne ou un ou plusieurs éléments spécifiq

Fiche pratique 2:
Traitement d'un dro

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

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

- Respect de la forme : Si le droit d'accès exercé sous une forme électronique, les in mations sont à fournir par voie électroni lorsque cela est possible, à moins que la sonne ait demandé qu'il en soit autrement.
- Les éléments d'information doivent être con transparents, compréhensibles et aisément cessibles, en des termes clairs et simples.
- La réponse doit être communiquée dans meilleurs délais et au plus tard, dans un d d'un mois à compter de la réception de la mande.
- Aucun paiement ne peut être exigé pour fou les éléments d'information demandés, sau les demandes sont manifestement infond ou excessives, notamment en raison de leur ractère répétitif.
- Vous pouvez demander des informations s plémentaires nécessaires pour obtenir co mation de l'identité du demandeur, s'il a doutes raisonnables quant à son identité.

Fiche pratique 3:
Les critères du cons bases de licéité

Le consentement de la personne concernée est fini comme « toute manifestation de volonté, li spécifique, éclairée et univoque par laquelle la sonne concernée accepte, par une déclaratior par un acte positif clair, que des données à ca tère personnel la concernant fassent l'objet tratement » (Art 4.1 du RGPD). Pour être valid consentement de la personne concernée doit lors présenter différentes caractéristiques.

- Le consentement doit être « libre ». La perso concernée doit disposer d'un véritable choi être en mesure de refuser ou de retirer consentement sans subir de préjudice.
- Le consentement doit être « spécifique ». consentement doit correspondre à une fin spécifique et déterminée à l'avance. Lorsq traitement comporte plusieurs finalités, la sonne doit pouvoir consentir à chacune d'e elles.
- Le consentement doit être « éclairé ». F que le consentement soit éclairé, la perso concernée doit être informée de l'identité responsable du traitement et des finalités traitement auxquelles sont destinées ses nées. Par ailleurs, il convient de préciser, d le formulaire de consentement, que la sonne a le **droit de retirer son consentem à tout moment.** Les informations foun doivent permettre à la personne concernée comprendre ce qu'il va advenir de ses donn Pour ce faire, les informations ne devront être « noyées » dans des notices générales.
- Le consentement doit être « univoque ». consentement doit être donné sans ambig par un acte positif clair par lequel la perso concernée manifeste de façon libre, spécifiq éclairée et univoque son accord au traiter de données la concernant. Cet acte positif peut prendre la forme d'une déclaration éc y compris par voie électronique. Cela pour

Fiche pratique 4:
Le registre des activités de traitement

DAAZ

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 (sinon 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 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.

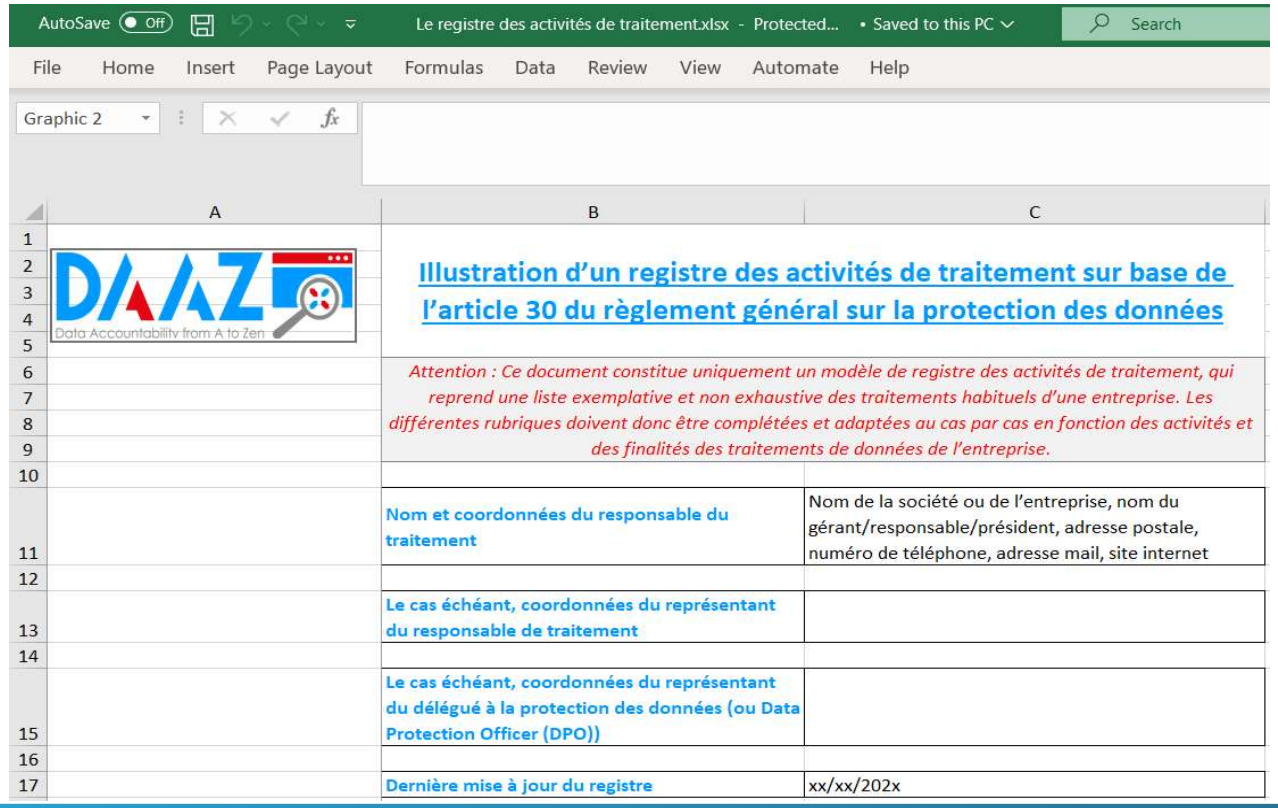
RED FLAG: Les données personnelles ne doivent pas être traitées ultérieurement d'une manière incompatible avec les finalités initialement déterminées (Art. 5.1.c. du RGPD).

Co-funded by the European Union

3. Promote greater user-tool interaction



3. Promote greater user-tool interaction



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

File Home Insert Page Layout Formulas Data Review View Automate Help

Graphic 2

DAAZ Data Accountability from A to Zen

Illustration d'un registre des activités de traitement sur base de l'article 30 du règlement général sur la protection des données

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.

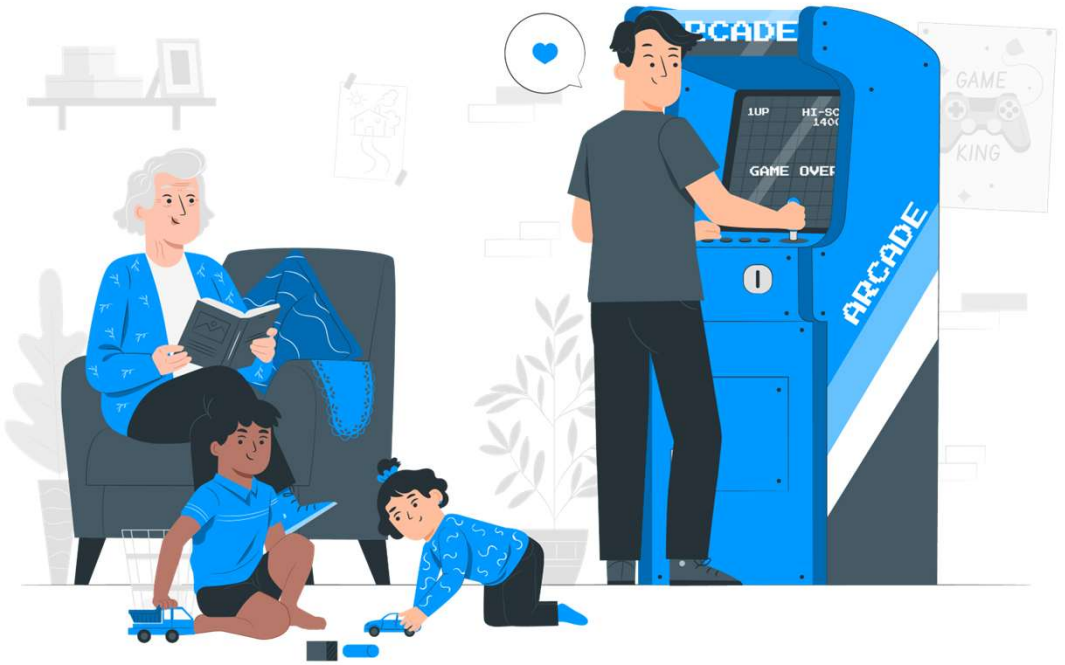
Nom et coordonnées du responsable du traitement	Nom de la société ou de l'entreprise, nom du gérant/responsable/président, adresse postale, numéro de téléphone, adresse mail, site internet
Le cas échéant, coordonnées du représentant du responsable de traitement	
Le cas échéant, coordonnées du représentant du délégué à la protection des données (ou Data Protection Officer (DPO))	
Dernière mise à jour du registre	xx/xx/202x

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Co-funded by the European Union

3. Promote greater user-tool interaction
Technical point

- **Narration**
  - Memorization
  - Structure
- **Gamification**
  - Motivation
  - Engagement
- **Immersion**
  - Identification with the Characters
  - Reproduced lessons learned



Co-funded by the European Union

DAAZ

www.daaz-gdpr.lu

CNPD

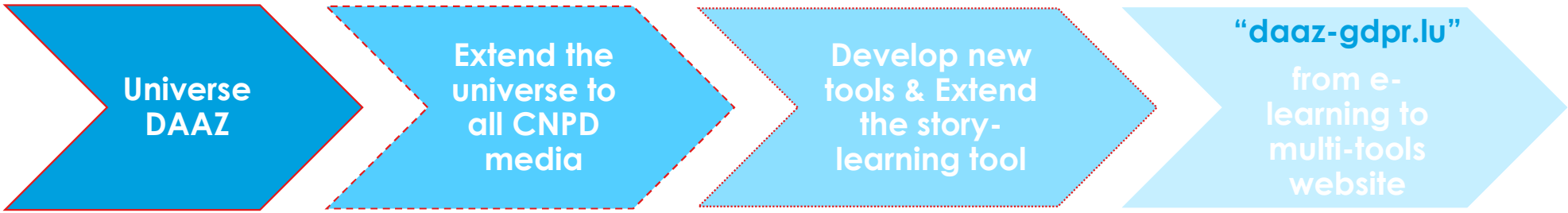
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Data accountability ...

... from A to Zen



Future of DAAZ Universe




LEONORA

Présentation du projet WTOON

- **Target audience**: Adolescents (12–16 years old)
- **Objectives**:
  - Raise awareness about online risks (addiction, cyberbullying, mobbing, sextortion, scams, etc.)and the protection of their personal data,
  - Share positive experiences and good practices, and
  - Inform them about their rights, and
  - Help adolescents become true digital citizens.

Educative transmedia Approach

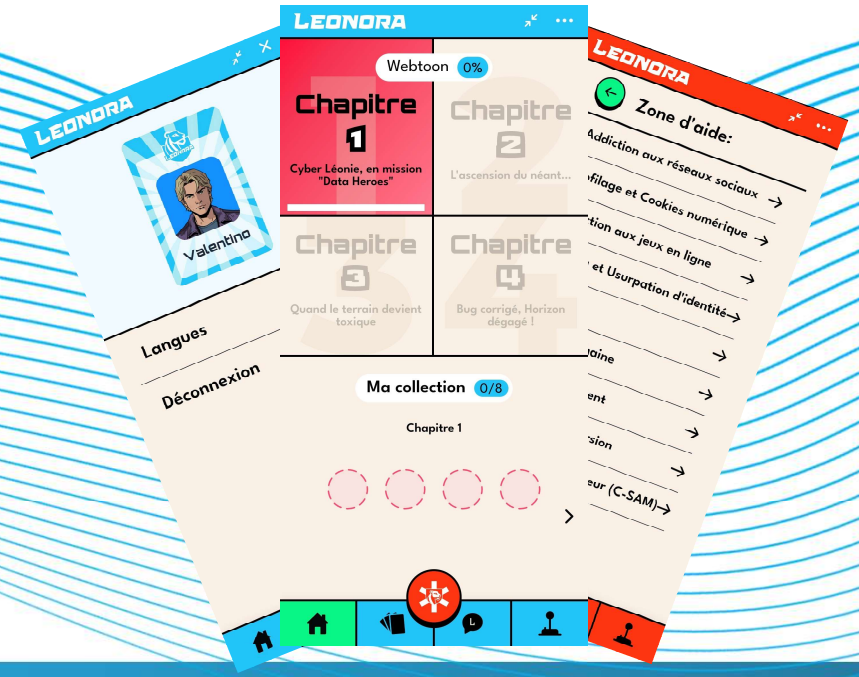
to guide teenagers from isolation in the virtual world toward trusted actors in the real world

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

The Webtoon



The LMS



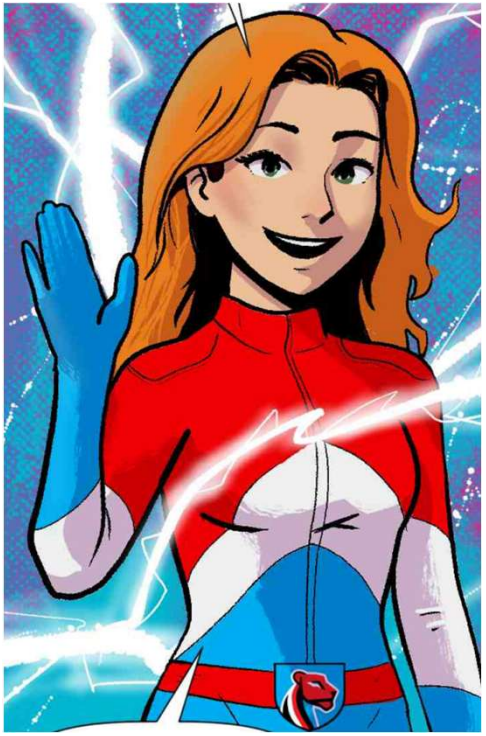
The Ed'tech Games

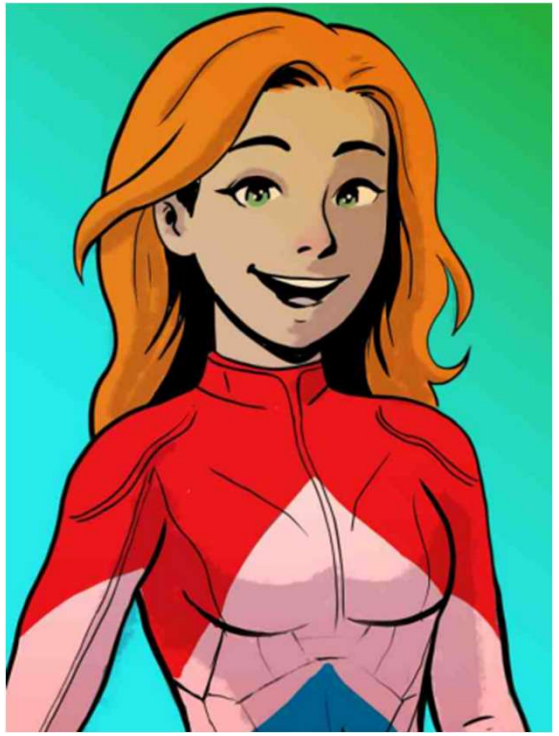


Co-funded by the European Union

The CNPD's Cyber-heroine

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES






Co-funded by the European Union

The Characters

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES



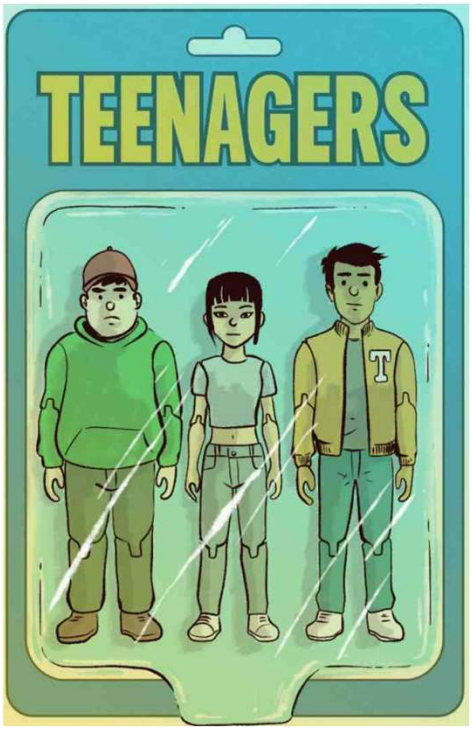






The Webtoons
Learning Objectives

Webtoon 1
Age: 12 -13 years old
Addiction to Social Media
Cookies, Algorithm, Profiling, Influencer, Digital footprint
Access, Object, Transparency







Co-funded by the European Union

The Webtoons
Learning Objectives

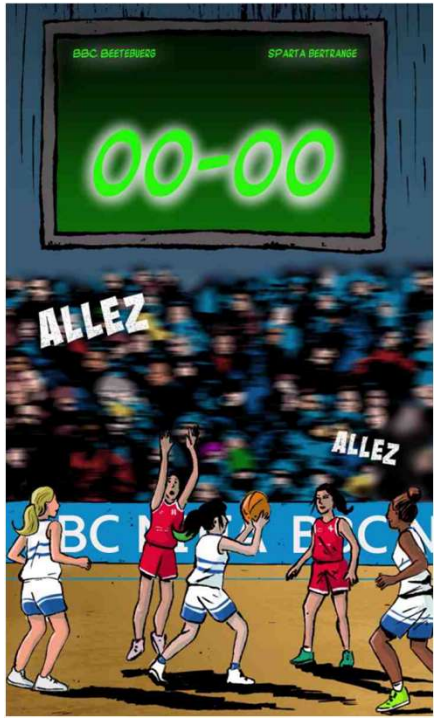


Webtoon 2
Age: 12 -13 years old
Addiction to Games
Dark patterns, Hate Speech, Money Premium, hacking
Erasure





The Webtoons
Learning Objectives



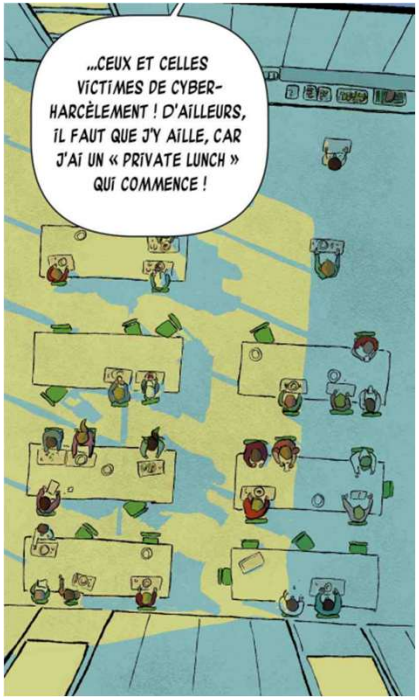


Webtoon 3
Age: 14 -16 years old
Cyberbullying
IA/Deepfake, Fake account, OSINT Data, Sharenting
Portability, Right to Your Image



Co-funded by the European Union

The Webtoons
Learning Objectives







Webtoon 4
Age: 14 -16 years old
Sexting
Nudes, Grooming, Sextorsion, Algospeak, Fake account, C-SAM
Rectification, Right to Complain

Co-funded by the European Union

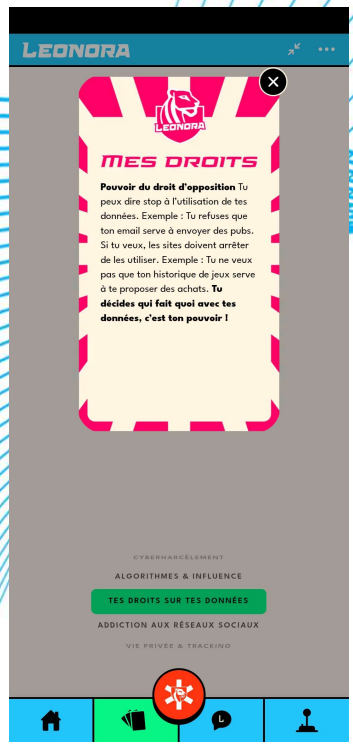
The Learning Managment System

Visual of the Dashboard and Interactions Learning Points









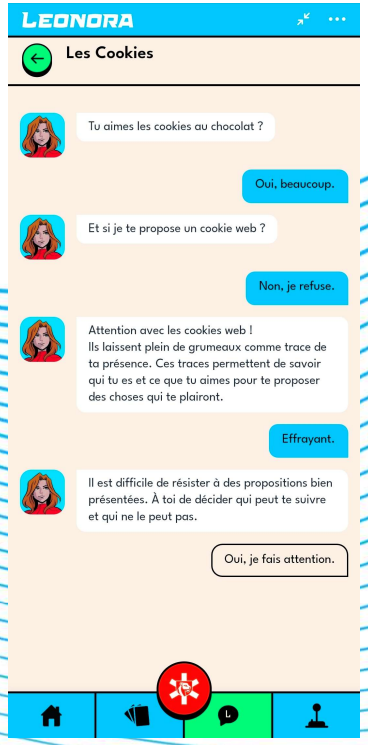
Co-funded by the European Union

Managment System

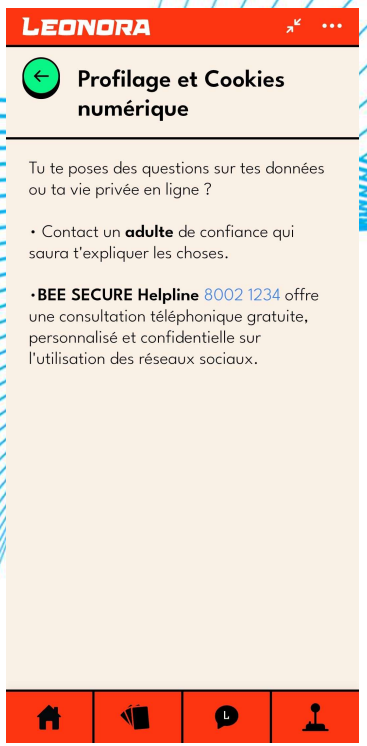
Visual of the Dashboard and Interactions Learning Points







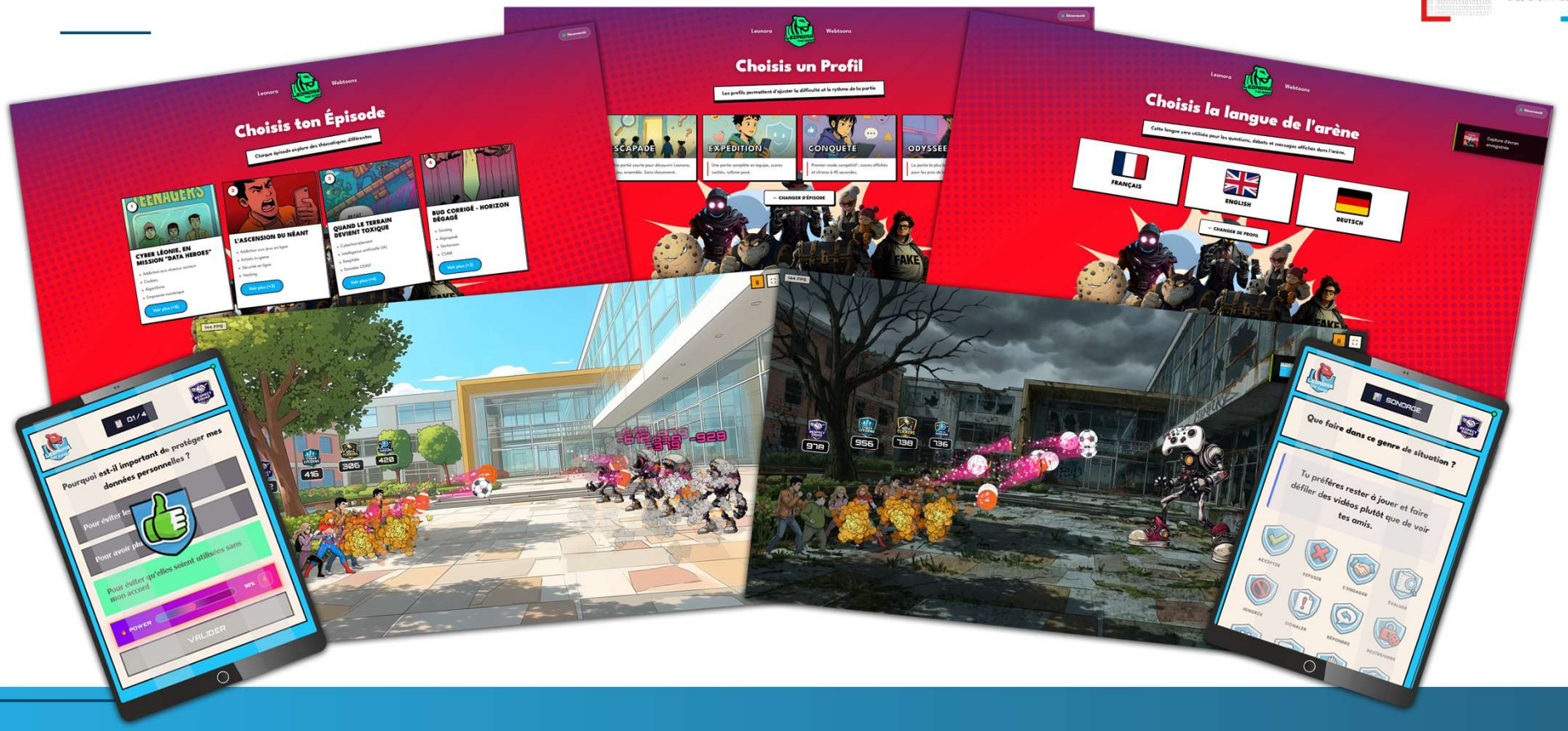




Co-funded by the European Union

The Digital Collaborative Game

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES



the European Union



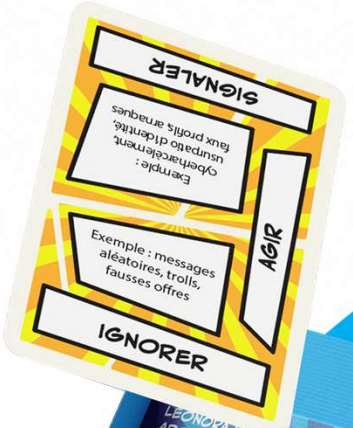
The Card Game

Peer-2-peer learning

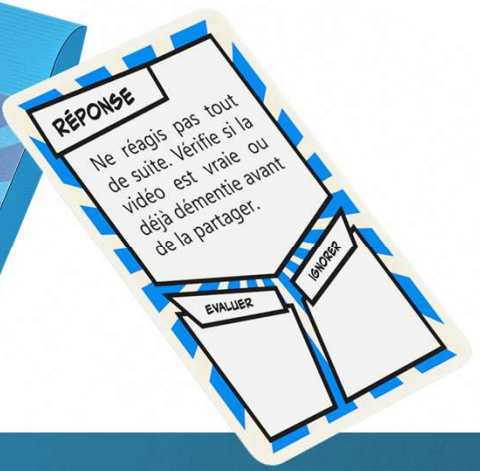
CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES















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