



Cyber sécurité et protection des données personnelles



Micro - Entreprise Cybersecurity

MECyS

Un projet en partenariat avec



Introduction

Comprendre la Cyber
Sécurité

01

En pratique

Protection de données et
Smishing

02

Cyberviolences

RGPD

03

En concret

Quelles sont les situations
rencontrées ?

04

1. Qu'est-ce que permet la Cyber Sécurité ?



Elle protège les utilisatrices et utilisateurs des dangers d'Internet et a pour objectif d'informer la population des menaces numériques récentes pour prévenir les dommages intellectuels, techniques ou financiers.

02. Quels sont les Cyber Risques ?

Des e-mails qui nous menacent d'effacer nos données, des SMS qui nous annoncent des gains exceptionnels ou des contacts sur Facebook qui nous promettent le grand amour: souvent, les rencontres inespérées que l'ont fait en ligne ne tiennent pas leurs promesses. Apprenez-en plus sur les arnaques sur Internet, les techniques des criminels et les façons de vous protéger



02. Comment reconnaître un hameçonnage (Phishing)?



02. Que faire si vous recevez un message d'hameçonnage par SMS ?

1. Ne communiquez jamais d'informations sensibles suite à un SMS

car aucune administration ou société sérieuse ne vous contactera par ce type de message pour vous demander vos informations personnelles, vos données bancaires ou vos mots de passe.

2. Ne téléchargez jamais d'application en dehors des sites ou magasins officiels.

Si, après avoir cliqué sur un lien dans un SMS, une alerte s'affiche et vous invite à télécharger ou mettre à jour une application, ne donnez pas suite et fermez la page.

3. Signalez le message frauduleux sur la plateforme 33700 ou transférez-le par SMS au **33700 (service gratuit).**

Ce service fera bloquer l'émetteur du message.



03

RGPD & MECyS

Comprendre l'importance de la protection des données en tant qu'entrepreneurs en France

03. Introduction à la protection de données

Que signifie réellement "protection des données" ?

La protection des données fait référence à la protection des individus "contre les conséquences indésirables (...) dues à l'accès aux données (stockées) ou à la perte involontaire de données."

→ Droit à la vie privée... y compris dans l'espace numérique !

Que faut-il pour une protection des données efficace ?

- 1.Des réglementations, telles que les lois sur la protection des données ;
- 2.L'engagement de chaque organisation qui traite des données personnelles ;
- 3.Des mesures d'auto-protection par les individus et les systèmes.

→ Quelles sont les réglementations pertinentes ?

03. Introduction à la protection de données

En cas de traitement des données
concernant des personnes résidant dans
l'UE :

RGPD de l'UE

en vigueur depuis le 25.05.2018

Obligatoire

pour les organisations avec...



03. Introduction à la protection de données

En France, toutes les organisations qui traitent des données personnelles de résidents de l'Union Européenne sont tenues de se conformer au RGPD. Cela inclut :

- **Entreprises**

Peu importe leur taille, toutes les entreprises qui collectent, stockent ou traitent des données personnelles doivent respecter le RGPD.

- **Organisations à but non lucratif**

Les associations et fondations qui traitent des données personnelles doivent également se conformer.

- **Administrations publiques**

Les organismes gouvernementaux et les collectivités locales sont soumis au RGPD.

- **Entreprises hors UE**

Même les entreprises situées en dehors de l'UE doivent se conformer si elles traitent des données de résidents de l'UE.

En résumé, toute entité qui manipule des données personnelles de citoyens de l'UE doit mettre en place des politiques conformes au RGPD. Si vous avez besoin de plus de détails ou d'exemples spécifiques, n'hésitez pas à demander !

03. Comment s'y prendre

Data Protection Assessment



Scan it

Assess the data protection level of your organization in just few minutes

- Your result will be not be stored and the assessment is anonymous (data sparse code base; no printing).
- You can determine your top 3 data protection priorities based on the assessment result.

// You can repeat the assessment as often as you wish. //

04

En concret

Un outil IA mis à disposition gratuitement

04. Que faire ?



Principes clés

- **Transparence** : Informer clairement sur l'utilisation des données.
- **Minimisation** : Collecter uniquement ce qui est nécessaire.
- **Sécurité** : Protéger contre les violations de données.
- **Limitation** : Conserver les données seulement pour la durée nécessaire.

Droits des individus

- **Accès** et rectification.
- **Effacement** ("droit à l'oubli").
- **Portabilité** vers un autre service.
- **Opposition** au traitement, notamment publicitaire.

Obligations des entreprises

- Obtenir un **consentement explicite**.
- Assurer une **conformité stricte** (registre, DPO).
- Notifier les **violations sous 72h**.

Sanctions

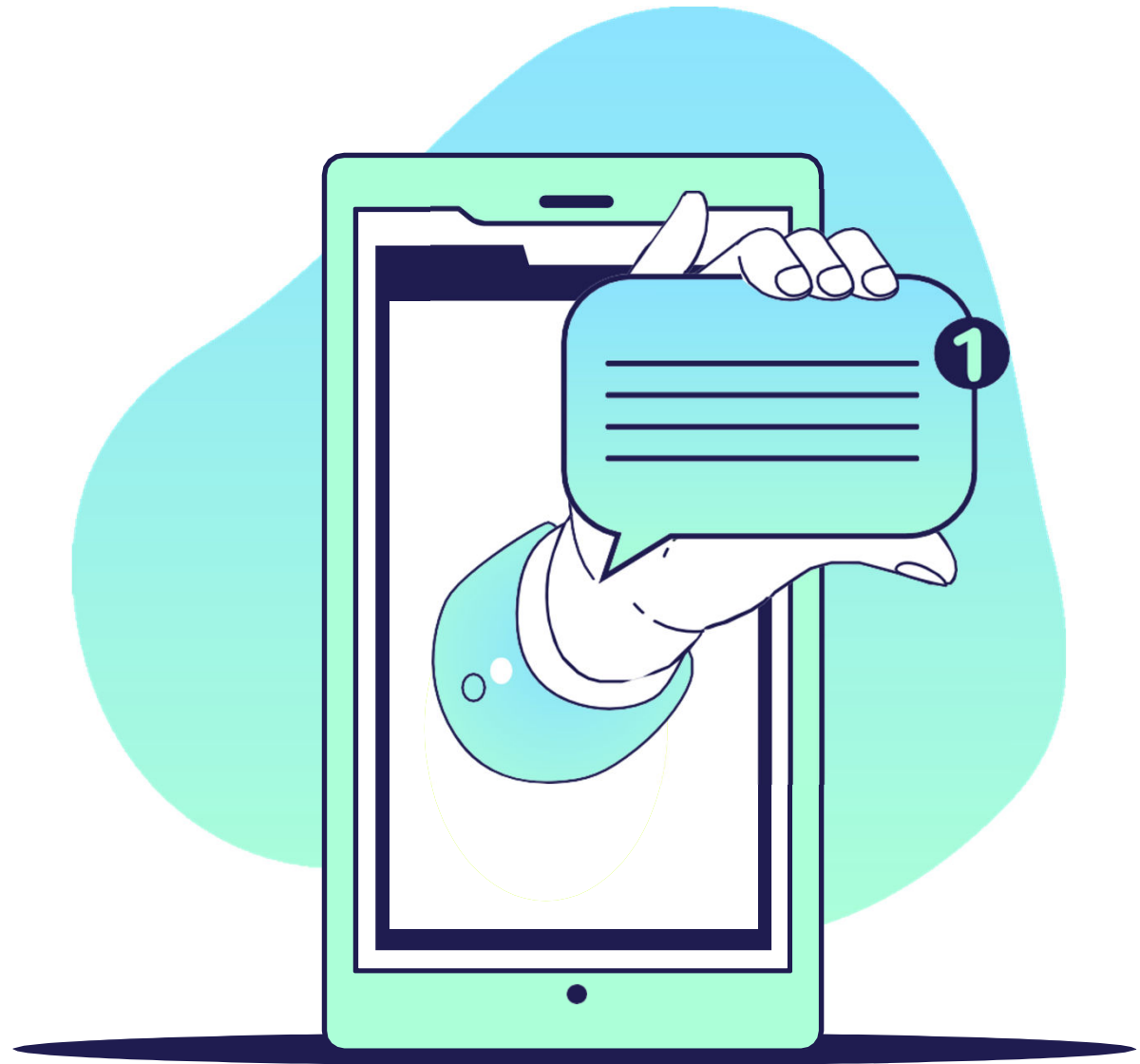
Jusqu'à **20 M€** ou **4 %** du chiffre d'affaires annuel mondial.

MERCI!

Restons en contact
Juan E. MARCOS
contact@anemo.co
+33 6 72 66 51 79



CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#) and illustrations by [Stories](#)





Cyber sécurité et protection des données personnelles



Micro - Entreprise Cybersecurity

MECyS

Un projet en partenariat avec



Introduction

Comprendre la Cyber
Sécurité

01

En pratique

Protection de données et
Smishing

02

Cyberviolences

RGPD

03

En concret

Quelles sont les situations
rencontrées ?

04

1. Qu'est-ce que permet la Cyber Sécurité ?

Elle protège les utilisatrices et utilisateurs des dangers d'Internet et a pour objectif d'informer la population des menaces numériques récentes pour prévenir les dommages intellectuels, techniques ou financiers.



02. Quels sont les Cyber Risques ?

Des e-mails qui nous menacent d'effacer nos données, des SMS qui nous annoncent des gains exceptionnels ou des contacts sur Facebook qui nous promettent le grand amour: souvent, les rencontres inespérées que l'ont fait en ligne ne tiennent pas leurs promesses. Apprenez-en plus sur les arnaques sur Internet, les techniques des criminels et les façons de vous protéger



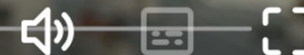
02. Comment reconnaître un hameçonnage (Phishing)?



1:15

LUMÉNA DULUC - DÉLÉGUÉE GÉNÉRALE - CLUSIF
MEMBRE DE CYBERMALVEILLANCE.GOUV.FR

1:49



02. Que faire si vous recevez un message d'hameçonnage par SMS ?

1. Ne communiquez jamais d'informations sensibles suite à un SMS

car aucune administration ou société sérieuse ne vous contactera par ce type de message pour vous demander vos informations personnelles, vos données bancaires ou vos mots de passe.

2. Ne téléchargez jamais d'application en dehors des sites ou magasins officiels.

Si, après avoir cliqué sur un lien dans un SMS, une alerte s'affiche et vous invite à télécharger ou mettre à jour une application, ne donnez pas suite et fermez la page.

3. Signalez le message frauduleux sur la plateforme 33700 ou transférez-le par SMS au **33700** (service gratuit).

Ce service fera bloquer l'émetteur du message.

03

RGPD & MECyS

Comprendre l'importance de la protection des données en tant qu'entrepreneurs en France

03. Introduction à la protection de données

Que signifie réellement "protection des données" ?

La protection des données fait référence à la protection des individus "contre les conséquences indésirables (...) dues à l'accès aux données (stockées) ou à la perte involontaire de données."

→ Droit à la vie privée... y compris dans l'espace numérique !

Que faut-il pour une protection des données efficace ?

- 1.Des réglementations, telles que les lois sur la protection des données ;
- 2.L'engagement de chaque organisation qui traite des données personnelles ;
- 3.Des mesures d'auto-protection par les individus et les systèmes.

→ Quelles sont les réglementations pertinentes ?

03. Introduction à la protection de données

En cas de traitement des données
concernant des personnes résidant dans
l'UE :

RGPD de l'UE

en vigueur depuis le 25.05.2018

Obligatoire

pour les organisations avec...



03. Introduction à la protection de données

En France, toutes les organisations qui traitent des données personnelles de résidents de l'Union Européenne sont tenues de se conformer au RGPD. Cela inclut :

- **Entreprises**

Peu importe leur taille, toutes les entreprises qui collectent, stockent ou traitent des données personnelles doivent respecter le RGPD.

- **Organisations à but non lucratif**

Les associations et fondations qui traitent des données personnelles doivent également se conformer.

- **Administrations publiques**

Les organismes gouvernementaux et les collectivités locales sont soumis au RGPD.

- **Entreprises hors UE**

Même les entreprises situées en dehors de l'UE doivent se conformer si elles traitent des données de résidents de l'UE.

En résumé, toute entité qui manipule des données personnelles de citoyens de l'UE doit mettre en place des politiques conformes au RGPD. Si vous avez besoin de plus de détails ou d'exemples spécifiques, n'hésitez pas à demander !

03. Comment s'y prendre

Data Protection Assessment



Scan it

Assess the data protection level of your organization in just few minutes

- Your result will be not be stored and the assessment is anonymous (data sparse code base; no printing).
- You can determine your top 3 data protection priorities based on the assessment result.

// You can repeat the assessment as often as you wish. //

04

En concret

Un outil IA mis à disposition gratuitement

04. Que faire ?



Principes clés

- **Transparence** : Informer clairement sur l'utilisation des données.
- **Minimisation** : Collecter uniquement ce qui est nécessaire.
- **Sécurité** : Protéger contre les violations de données.
- **Limitation** : Conserver les données seulement pour la durée nécessaire.

Droits des individus

- **Accès** et rectification.
- **Effacement** ("droit à l'oubli").
- **Portabilité** vers un autre service.
- **Opposition** au traitement, notamment publicitaire.

Obligations des entreprises

- Obtenir un **consentement explicite**.
- Assurer une **conformité stricte** (registre, DPO).
- Notifier les **violations sous 72h**.

Sanctions

Jusqu'à **20 M€** ou **4 %** du chiffre d'affaires annuel mondial.

MERCI!

Restons en contact
Juan E. MARCOS
contact@anemo.co
+33 6 72 66 51 79



CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#) and illustrations by [Stories](#)

