PR3 : Outils pour organiser des événements numériques à l'international

Module 5: Enjeux concernant la protection des données et la confidentialité lors de l'organisation d'événements virtuels

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the European Union

Module 5: Sommaire

- Les données et leur protection
- Les étapes pour une approche conforme en matière de protection et de confidentialité des données

Co-funded by the European Union

DONNEES ET PROTECTION DES DONNEES

Co-funded by
the European Union

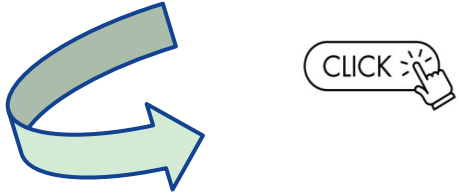
À QUOI SERVENT VOS DONNÉES ? QUE PEUT-IL LEUR ARRIVER ?

- Marketing numérique hyper-segmenté
- Espionnage industriel
- Vol d'identité
- Fraudes
- Chantage
- Clonage de carte de crédit
- Ransomware, phishing (exigez une rançon pour restituer l’intégrité de vos données)
- Ouverture de comptes bancaires à votre nom pour blanchir de l'argent
- Demander de faux remboursements d'assurance maladie en votre nom

Co-funded by the European Union

Ginni Rometry, PDG d'IBM de 2012 à avril 2020, sait exactement ce qui se passe et en a parlé à plusieurs reprises :

« Les données sont la nouvelle ressource de notre époque. Elles sont à la base de l'avantage concurrentiel et elles transforment toutes les professions et toutes les industries. Ainsi, la cybercriminalité constitue la plus grande menace pour tous les secteurs et toutes les entreprises du monde. »

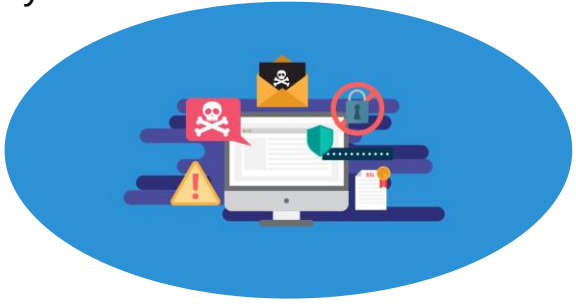


Co-funded by the European Union

Le sujet de la confidentialité et de la sécurité des données est abordé dans les médias grand public, et les gens ont commencé à prendre conscience de la valeur de leurs données personnelles.

- Cela se passe comme dans les films. Quiconque a regardé « Les termes et conditions peuvent s'appliquer » et « The Great Hack » sait de quoi nous parlons.

- Si vous n'êtes toujours pas convaincu, regardez comment l'hypersegmentation des campagnes publicitaires arrive sur votre téléphone portable immédiatement après que vous ayez manifesté votre intérêt pour un sujet spécifique.



Co-funded by the European Union

Protection des données et événements virtuels

- Les événements virtuels offrent de nombreux avantages : de la portée et de l'interaction accrue à l'évaluation optimale des données obtenues.
- Une préparation systématique est nécessaire pour garantir que les données requises et collectées sont sécurisées et peuvent également être utilisées ultérieurement en marketing.

Les points les plus importants à retenir ici sont :

- Principes de base du RGPD
- Chiffrement
- L'outil utilisé
- Politique de confidentialité
- Double inscription
- Confidentialité des données des participants

Co-funded by the European Union

Principes de base du RGPD

L'un des principes de base les plus importants du RGPD est ce que l'on appelle **l'économie des données** : seules les données réellement nécessaires peuvent être collectées.

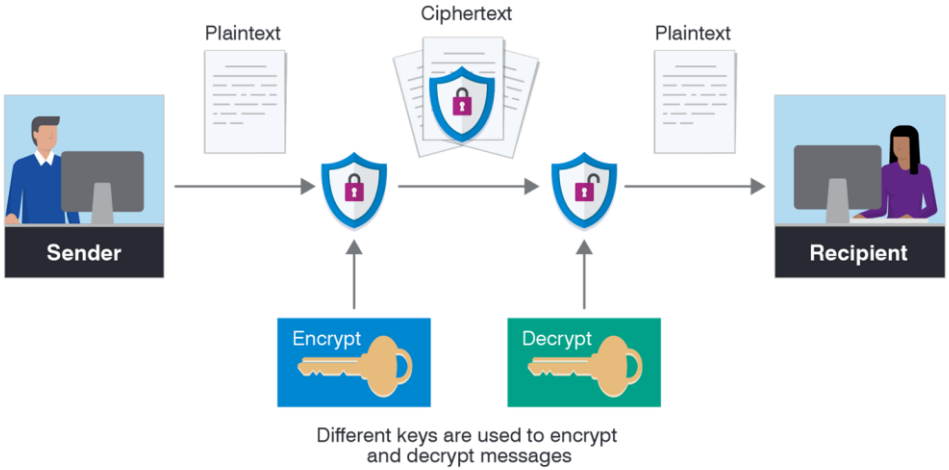
Par exemple, le lieu de résidence des participants n'a généralement pas d'importance.
En principe, vous n'avez même pas besoin d'un nom, une adresse e-mail et éventuellement le nom de l'entreprise suffisent déjà pour une inscription.

Co-funded by the European Union

Cryptage

Les données personnelles sont collectées lors de l'inscription : celles-ci doivent être protégées

Un cryptage suffisant du site Web et de la transmission des données est obligatoire : respectez toujours les normes en vigueur



Co-funded by the European Union

L'outil utilisé

L’événement dépend de l’outil de vidéoconférence ou de l’outil d’événement en ligne utilisé.

- Recherchez un outil qui répond aux exigences techniques et, surtout, aux exigences en matière de protection des données.
- Vérifiez si les données personnelles sont traitées via l'outil (la réponse est oui dans 99% des cas) et où ces données sont stockées ou traitées.
- Vous avez besoin d'un contrat clair sur ces points avec fournisseur de l'outil.

S’il s’agit d’un outil non européen qui traite également les données en dehors de l’UE, rappelez-vous que le protocole UE-États-Unis Le Privacy Shield n’est plus en vigueur et vous devez donc convenir de dispositions contractuelles supplémentaires avec le fournisseur de l'outil.

Co-funded by
the European Union

Politique de Confidentialité

Quelles données sont collectées, à quelles fins et comment sont-elles traitées? Quels outils sont utilisés, quand et pourquoi ?

- Vous devez mettre toutes les réponses à ces questions à la disposition des participants dans un langage simple et compréhensible en un seul clic - avant l'événement.
- La politique de confidentialité doit donc toujours être tenue à jour, en fonction des outils utilisés
- Si vous souhaitez également utiliser les données à des fins de marketing, ces finalités doivent également être expliquées dans la politique de confidentialité et les participants doivent avoir la possibilité de s'y opposer à tout moment. De plus, une double confirmation est requise dans ce cas.

Co-funded by the European Union

Double Confirmation

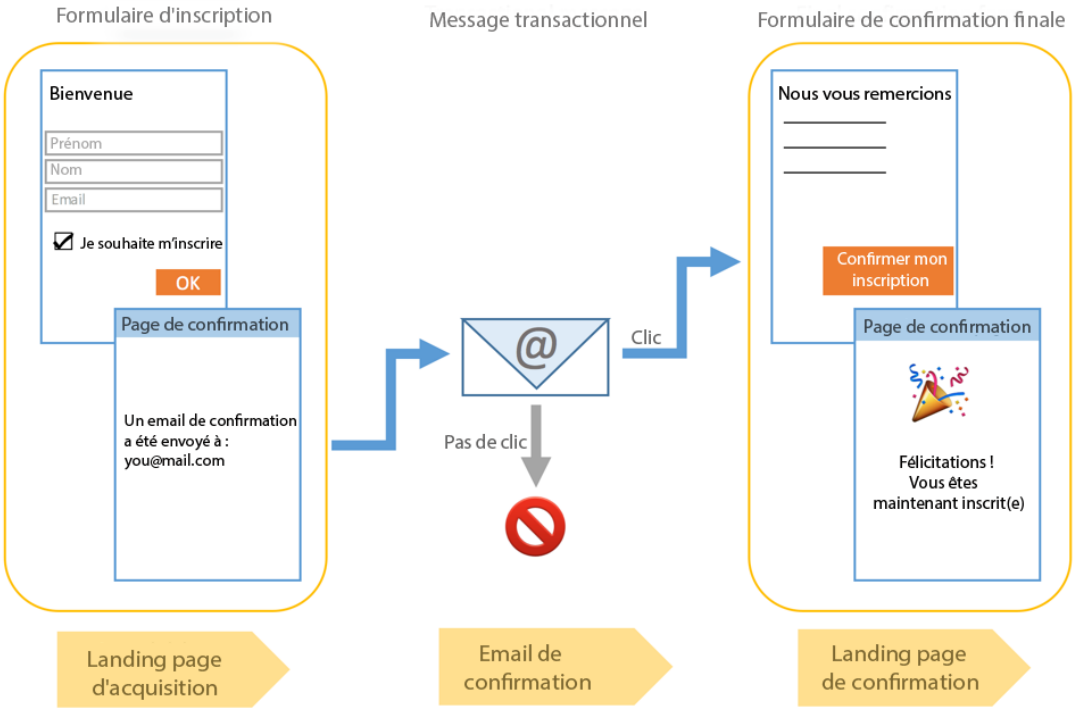
Afin de protéger les parties intéressées contre les informations indésirables, l'utilisation des données à d'autres fins publicitaires nécessite généralement le consentement conformément à **l'art. 6 (1) a) DSGVO et § 7 (2) et (3) UWG**.
Dans ce cas, un **email de confirmation** doit être envoyé après l'inscription, contenant **un lien de confirmation.**

Ce n'est que lorsque ce lien est confirmé que le traitement des données à des fins publicitaires est licite.

IMPORTANT!!!

Si les personnes intéressées s'inscrivent à l'événement numérique mais n'effectuent pas de double confiration, l'adresse e-mail ne peut pas être utilisée à des fins de publicité ultérieure (voir également l'article 7 (2) n° 2 et 3 UWG).

Co-funded by the European Union



Co-funded by the European Union

Confidentialité des données des participants

Avant, pendant et **après** l'événement, les données des participants doivent être protégées au mieux par vous en tant que responsable**.**

Cela signifie par exemple qu'aucune liste des participants ne peut être publiée sans leur consentement exprès, que les noms des personnes présentes ne peuvent être affichés en ligne sauf accord de leur part, ou encore qu'aucune image ou enregistrement sonore ne peut être réalisé sans leur consentement, donné à l'avance

DE PLUS, vous avez également besoin d'un processus concret sur la manière de procéder en interne en cas de violation de la protection des données.

Co-funded by the European Union

LES ÉTAPES VERS UNE APPROCHE PROFESSIONNELLE ET CONFORME EN MATIÈRE DE PROTECTION DES DONNÉES ET DE CONFIDENTIALITE

Co-funded by the European Union

1. Trouver les bonnes personnes en interne
2. Réaliser un diagnostic détaillé pour définir l'étendue des mesures à prendre pour se conformer à la législation
3. Nommer un DPO (Délégué à la Protection des Données)
4. Mettre en place des règles précises
5. La confidentialité et la sécurité des données nécessitent une approche professionnelle
6. Culture, engagement, communication et formation en matière de sécurité de l'information

Co-funded by the European Union

1. TROUVER LES BONNES PERSONNES EN INTERNE

C'est une question qui dépend directement de la direction de l'entreprise: direction générale, conseil d'administration et/ou comités exécutifs.

1. **LA PREMIÈRE LIGNE DE DÉFENSE :** est un service informatique solide

2. **LA DEUXIÈME LIGNE DE DÉFENSE** : des analyses de risques appropriées et la conformité à la loi

3. **LA TROISIÈME LIGNE DE DÉFENSE :** est un audit interne, incluant le choix de fournisseurs qui ont cette préoccupation comme priorité absolue

Co-funded by the European Union

2. RÉALISER UN DIAGNOSTIC DÉTAILLÉ POUR DÉFINIR L'ÉTENDUE DE CE QUI DOIT ÊTRE FAIT POUR SE CONFORMER À LA LÉGISLATION

- Cartographier les informations qui doivent être protégées, les zones, les systèmes, les environnements, les plates-formes et les professionnels qui doivent être impliqués
- Identifier les politiques qui doivent être créées ou celles existantes qui doivent être mises à jour
- Identifiez les documents qui doivent être examinés, comme les conditions de consentement

Co-funded by the European Union

3. DÉSIGNER UN DPD (DELEGUE A LA PROTECTION DES DONNEES

Fonctions principales:

- Coordonner les efforts de protection des données dans tous les départements concernés
- Participer à des projets visant à garantir la confidentialité dès la conception depuis le tout premier projet
- Mener et surveiller une AIPD
- Promouvoir la sensibilisation en tant que meilleure pratique en matière de protection des données
- Insérer la protection des données à l'agenda de l'organisation jusqu'à ce que le sujet fasse partie de la culture
- Être le point de contact avec les autorités réglementaires

Co-funded by the European Union

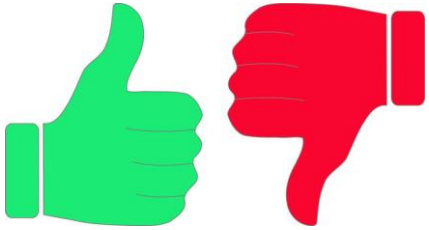
4. DEFINIR DES REGLES

- Classer les informations (publiques, restreintes, sensibles, confidentielles ou critiques) ;
- Communiquer fréquemment avec les autorités,
- Mettre en œuvre un programme solide de sécurité de l'information, comprenant une surveillance et des tests périodiques ;
- Tester régulièrement la vulnérabilité et le cryptage des données sur le réseau interne ;
- Sensibiliser les collaborateurs et les parties prenantes.

Co-funded by the European Union

5. LA CONFIDENTIALITÉ ET LA SÉCURITÉ DES DONNÉES NÉCESSITENT UNE APPROCHE PROFESSIONNELLE

- Le consentement doit être donné par écrit ou par tout autre moyen démontrant la manifestation effective de la volonté du titulaire dans une clause détachée des autres conditions contractuelles.
- Si le consentement est modifié par rapport à ses finalités initiales, un nouveau consentement doit être obtenu du titulaire → le consentement peut être révoqué.



- Les modèles de consentement présentent les spécificités.
- Les messages marketing ou commerciaux ne sont envoyés qu'à ceux qui expriment leur consentement préalable et explicite à les recevoir..

Co-funded by the European Union

6. CULTURE DE SÉCURITÉ DE L'INFORMATION, ENGAGEMENT, COMMUNICATION ET FORMATION

Délégué à la Protection des Données (DPD): un responsable du traitement légal ou physique qui collecte des données personnelles et prend toutes les décisions concernant la forme et la finalité du traitement des données.

- Le pont entre les parties prenantes et l'équipe informatique opérationnelle ;
- Responsable de guider les employés qui ne suivent pas les pratiques de traitement des données, en promouvant une culture de protection des données claire et objective.

Co-funded by the European Union

- Le traitement de toute opération effectuée avec des données personnelles, telle que la collecte, l'utilisation, le traitement, le stockage et l'élimination, doit être supervisé par un spécialiste des données.
- Les employés doivent être sensibilisés à la cyber sécurité afin de comprendre comment protéger leurs données personnelles.

Co-funded by
the European Union

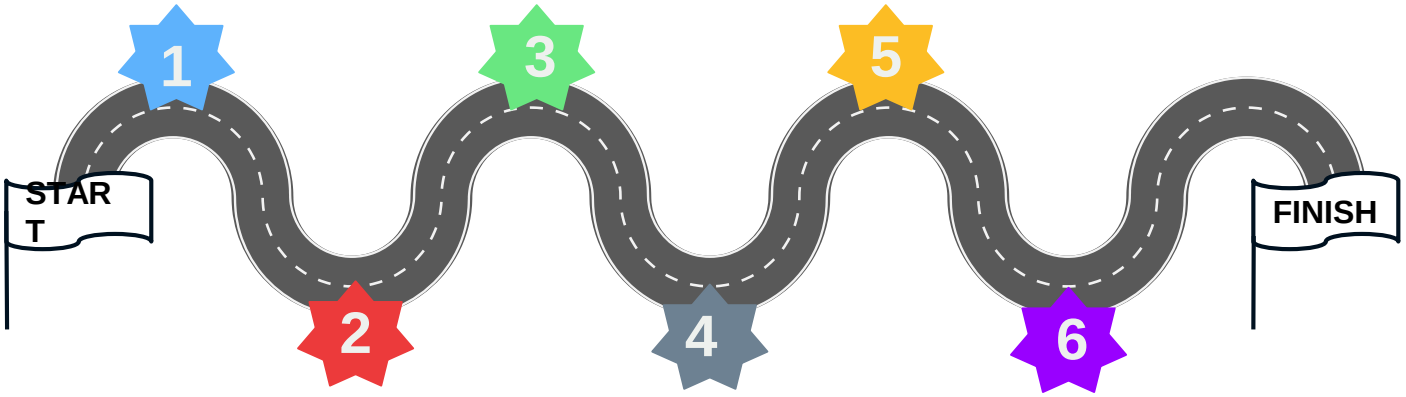
A VOUS DE JOUER!

Créez votre feuille de route pour la protection et la confidentialité des données

Suivez les étapes et remplissez la feuille de route dans la diapositive suivante pour obtenir une protection parfaite des données pour votre événement en ligne.

Co-funded by the European Union

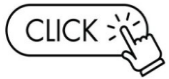
Votre feuille de route en matière de protection des données



Co-funded by
the European Union

Questionnaire Général d’Evaluation

Si vous avez parcouru tous les modules, veuillez remplir le questionnaire d'évaluation générale suivant



Co-funded by
the European Union

Merci!

Co-funded by
the European Union

Co-funded by the European Union