SCENARIO

RGPD : respect des règles de protection des données

Page d'accueil du jeu et tutoriel :

À propos :

Ce jeu sérieux a pour objectif de sensibiliser les salariés aux principes du RGPD. Vous allez apprendre les fondamentaux du RGPD, les bonnes pratiques et les erreurs à éviter.

Vous incarnerez un employé et devrez prendre des décisions pour faire avancer les différentes histoires proposées.

Les situations présentées dans le jeu sont fictives et toute ressemblance avec des personnes ou des situations réelles serait purement fortuite.

Partie 1 :

Chapitre 0 : Connaissance des bases du RGPD :

Tout d'abord, le joueur doit répondre à un questionnaire sur le RGPD qui comprend principes fondamentaux, les droits des personnes concernées …
Ce questionnaire va être récompenser par des points pour toutes bonnes réponses.

Quiz :

1) Qu'est-ce que le RGPD ?

a. Une loi européenne sur la protection des données personnelles

b. Une organisation internationale sur la protection des données personnelles

c. Un organisme de certification pour les entreprises

Réponse : a. Une loi européenne sur la protection des données personnelles

Explication en cas de mauvaise réponse : Le RGPD est une réglementation européenne qui vise à garantir la protection des données personnelles des citoyens européens.

2) Quelles sont les personnes protégées par le RGPD ?

a. Les citoyens européens

b. Les citoyens du monde entier

c. Les citoyens français

Réponse : a. Les citoyens européens

Explication en cas de mauvaise réponse : Le RGPD protège les citoyens européens, quel que soit leur lieu de résidence ou le lieu où les données sont traitées.

3) Qu'est-ce que la protection des données personnelles ?

a. La garantie de la confidentialité et de la sécurité des données personnelles

b. La collecte et l'utilisation de données personnelles sans autorisation

c. La diffusion de données personnelles à des fins commerciales

Réponse : a. La garantie de la confidentialité et de la sécurité des données personnelles

Explication en cas de mauvaise réponse : La protection des données personnelles implique la garantie de la confidentialité et de la sécurité des données personnelles, ainsi que le respect des droits des personnes concernées en matière de protection de leur vie privée.

4) Les entreprises doivent-elles obtenir le consentement des personnes concernées pour collecter leurs données personnelles ?

a. Oui, toujours

b. Non, pas toujours

Réponse : b. Non, pas toujours

Explication en cas de mauvaise réponse : Les entreprises n'ont pas toujours besoin d'obtenir le consentement des personnes concernées pour collecter leurs données personnelles, mais elles doivent respecter d'autres principes du RGPD, tels que la minimisation des données et la finalité du traitement.

5) Les données personnelles doivent-elles être stockées de manière sécurisée ?

a. Oui

b. Non

Réponse : a. Oui

Explication en cas de mauvaise réponse : Le RGPD exige que les données personnelles soient stockées de manière sécurisée pour garantir la protection de la vie privée des personnes concernées. Si les données ne sont pas stockées de manière sécurisée, il y a un risque accru de fuite de données ou de violation de la vie privée.

6) Une entreprise peut-elle stocker des données personnelles pendant une période illimitée ?

a. Oui

b. Non

Réponse : b. Non

Explication en cas de mauvaise réponse : Les entreprises ne peuvent pas stocker des données personnelles pendant une période illimitée. Le RGPD exige que les entreprises ne stockent les données personnelles que pour une période strictement nécessaire. Si les données sont stockées pendant une période plus longue que nécessaire, cela peut entraîner des sanctions graves pour l'entreprise.

7) Dans quel cas est-il nécessaire d'informer les personnes concernées sur le traitement de leurs données personnelles ?

a. Uniquement lorsqu'on leur demande

b. À tout moment

c. Seulement si la loi l'exige

Réponse : c. Seulement si la loi l'exige

Explication en cas de mauvaise réponse : Les personnes concernées doivent être informées sur le traitement de leurs données personnelles uniquement si la loi l'exige. Il est important de respecter les obligations de notification pour éviter les sanctions.

8) Les employés peuvent-ils accéder aux données personnelles des clients sans autorisation ?

a. Oui, s'ils en ont besoin pour leur travail

b. Non, ils n'ont accès qu'à ce qui est strictement nécessaire pour leur travail

Réponse : b. Non, ils n'ont accès qu'à ce qui est strictement nécessaire pour leur travail

Explication en cas d'une mauvaise réponse : Les employés ne peuvent pas accéder aux données personnelles des clients sans autorisation. Le RGPD exige que les employés n'aient accès qu'à ce qui est strictement nécessaire pour leur travail. Si les employés accèdent à des données personnelles sans autorisation, cela peut entraîner des sanctions graves pour l'entreprise.

9) Qui est responsable d'assurer la sécurité des données personnelles dans une entreprise ?

a. Les employés

b. Le responsable de la protection des données (DPO)

c. Les deux

Réponse : c. Les deux

Explication en cas de mauvaise réponse : Tous les employés d'une entreprise sont responsables de garantir la sécurité des données personnelles. Le responsable de la protection des données (DPO) est également responsable de veiller à ce que les données soient traitées de manière conforme au RGPD. C'est donc une responsabilité partagée entre les employés et le DPO.

10) Une entreprise peut-elle transférer des données personnelles à un pays tiers sans garanties appropriées en matière de protection des données ?

a. Oui

b. Non

Réponse : b. Non

Explication en cas de mauvaise réponse : Les entreprises ne peuvent pas transférer des données personnelles à un pays tiers sans garanties appropriées en matière de protection des données. Le RGPD exige que les données personnelles soient protégées, même lorsqu'elles sont transférées à un pays tiers. Les entreprises doivent s'assurer que les pays tiers disposent de niveaux adéquats de protection des données avant de transférer des données personnelles vers eux.

Partie 2 :

Pratique de bonnes démarches :

Dans cette partie, le joueur va être confronté à des cas concret sur la manière de traiter les données personnelles de manière conforme au RGPD.
Il doit prendre des décisions sur la collecte, le traitement et la protection des données personnelles en fonction des situations présentées.

Entreprise : **Amaton**

Personnages **: Hasan**, **Céline**, **Eve**, **Adam**, **Marie**, **Tom**, **Jean**, **Rémi**, **Partenaire commercial**, **M. Juste**

CAS n°1 : Consentement

Les employés reçoivent un appel d'un client qui se plaint de la manière dont ses données personnelles ont été utilisées par l'entreprise.

Les employés doivent résoudre la plainte en respectant les règles RGPD. Ils doivent prendre des décisions sur la collecte, le traitement et la protection des données personnelles.

Les employés de l'entreprise, **Adam** et **Eve**, reçoivent un appel d'un client nommé **M. Juste** qui se plaint de la manière dont ses données personnelles ont été utilisées par l'entreprise.

Dialogue :

Eve : Bonjour, ici **Eve** de la société **Amaton**. Comment puis-je vous aider aujourd'hui ?

M. Juste : C'est **M. Bastien Juste**, je suis client d'**Amaton**. Bonjour **Eve**, je suis très mécontent de la façon dont votre société a utilisé mes informations personnelles. Je veux savoir comment vous allez résoudre ce problème.

Eve : Je suis vraiment désolée de l'entendre, M. Juste.
Pourriez-vous me donner plus de détails de ce qui vous pose un problème ?

M. Juste : Oui, j'ai reçu une offre publicitaire pour un produit que je n'ai jamais demandé. Et je soupçonne que mes informations ont été utilisées sans mon autorisation.

Eve : Je comprends. Nous prenons ce genre de situation très au sérieux. Adam, pourrais-tu nous rejoindre pour aider à résoudre ce problème ?

Adam : Bien sûr, Eve. Bonjour M. Juste, je suis Adam **d'Amaton** du département commercial. Comment puis-je vous aider ?

Eve : M. Juste se plaint d'avoir reçu une offre publicitaire pour un produit qu'il n'a jamais demandé et qu'il soupçonne que ses informations ont été utilisées sans son autorisation.

Adam : Je comprends.

Le joueur doit prendre une décision sur la façon de traiter les informations de M. Juste pour résoudre le problème de manière conforme au RGPD.

Choix possible :

- **Demander à M. Juste s'il autorise la vérification de son compte.**
- Vérifier son compte sans lui demander.

Si le joueur décide de demander à M. Juste s'il autorise la vérification de son compte :

Adam : Merci, M. Juste. Pourrais-je vous demander de nous donner votre autorisation pour accéder à votre compte pour vérifier les informations liées à cette offre publicitaire ?

M. Juste : Bien sûr, allez-y.

Adam : Merci beaucoup, M. Juste. Nous allons vérifier votre compte dès que possible et nous vous tiendrons informé des résultats de notre enquête.

La décision de demander l'autorisation de M. Juste pour accéder à son compte a permis à l'entreprise de se conformer aux règles du RGPD et de respecter les droits de protection des données de M. Juste.

Cette décision montre également que l'entreprise accorde une grande importance à la confidentialité et à la protection des données personnelles de ses clients. En conséquence, l'entreprise peut maintenir la confiance de ses clients et éviter des conséquences négatives potentielles telles que des sanctions financières ou juridiques.

Si le joueur décide de vérifier le compte de M. Juste sans lui demander son autorisation :

Adam : Merci, M. Juste. Nous allons vérifier votre compte dès que possible pour trouver la source du problème.

Si les employés décident de vérifier le compte de M. Juste sans lui demander son autorisation, ils peuvent enfreindre les droits de protection des données de M. Juste et violer les règles énoncées dans le RGPD. Cela peut également entraîner une perte de confiance de la part des clients et une réputation négative pour l'entreprise, ainsi que des conséquences potentielles sous forme de sanctions financières ou juridiques. En général, il est préférable de demander toujours l'autorisation des utilisateurs avant de traiter leurs données personnelles.

CAS n°2 : Partage de mot de passe

Un employé est absent ce jour, son collègue lui demande le mot de passe de son poste pour accéder aux documents qu'il a besoin pour continuer son travail.
Les employés doit déterminer les risques s'il partage leurs données personnelles comme leur mot de passe.

Il est 10h00 et **Marie** est en train de travailler à son poste. Soudain, son collègue **Tom** vient à son bureau et lui demande :

Tom : Bonjour Marie, je sais que tu es occupée, mais j'ai besoin de ton aide.
Mon collègue **Jean** est absent aujourd'hui et j'ai besoin de ses documents pour terminer mon projet. Pourrais-tu me donner son mot de passe pour que je puisse accéder à son ordinateur ?

Marie : Je ne pense pas que c'est une bonne idée.

Tom : Fait moi confiance, je vais juste récupérer les documents. Ça ne va même pas prendre 2 minutes.

Choix de l'utilisateur :

Si l'utilisateur décide de partager le mot de passe de **Jean** avec **Tom** :

Marie envoie un email à Jean à ce sujet. Elle précise dans son email que pour finir le travail, Tom a besoin de son mot de passe le plus rapidement possible.

Marie : D'accord**, je vais te donner le mot de passe**. Mais tu dois promettre de le protéger et de ne pas l'utiliser pour autre chose que ce dont tu as besoin.

Tom : Merci beaucoup, Marie. Je te promets de le protéger et de ne l'utiliser que pour ce dont j'ai besoin.

Plus tard dans la journée, un audit découvre que le mot de passe a été utilisé pour accéder à des données sensibles qui n'ont rien à voir avec le projet de Tom. Le département de la conformité au RGPD de l'entreprise reçoit une plainte de l'un des clients pour violation de ses données personnelles.

Marie se rend compte que son choix a entraîné des conséquences négatives pour l'entreprise et pour la protection des données personnelles. Elle peut se sentir coupable et déçue d'avoir contribué à cette situation.

Si l'utilisateur décide de demander l'autorisation à Jean :

Marie : D'accord, je vais envoyer un e-mail à Jean pour lui demander s'il autorise la vérification de son compte.

30 minutes plus tard.

Marie : J'ai reçu une réponse négative de la part de **Jean**.

Tom : C'est dommage, mais au moins nous avons respecté les règles du RGPD en demandant son autorisation. Et je tiens à féliciter Jean pour ne pas avoir partagé son mot de passe, c'est une bonne pratique de sécurité en ligne.

Marie : Tout à fait d'accord. Je vais envoyer un autre e-mail à Jean tout de suite.

CAS n°3 : Piratage

Les employés doivent gérer une fuite de données à la suite d'une attaque informatique.
Les employés doivent prendre des mesures immédiates pour minimiser les dommages et gérer la situation de manière responsable en respectant les règles RGPD.

Céline et **Hasan** discutent lorsqu'une notification étrange attire l'attention de Céline.

Céline : Oh non, je viens de recevoir une alerte de sécurité indiquant qu'il y a eu une violation de données. Nous avons été piratés.

Hasan : Quoi ? Quels types de données ont été volés ?

Céline : Ils ont obtenu l'accès à des informations personnelles des clients, y compris des noms, des adresses et des numéros de téléphone. Je ne sais pas comment ils ont pu pirater mon ordinateur alors qu'il y a que moi qui l'utilise.

Hasan : Je suppose que tu n'as pas suffisamment protéger tes données.

Céline : Comment ça ?

Hasan : Il fallait que tu protèges tes données. Je peux te donner des conseils pour éviter ces attaques informatiques.

Tu dois mettre en place des mesures de contrôle d'accès, c'est-à-dire, utiliser des mots de passe forts, des identifiants uniques et des permissions de niveau d'accès appropriées. Par exemple, un bon mot de passe doit être assez long (au moins 12 caractères) et doit contenir tout type de caractères.

Céline : Merci pour tes conseils Hasan. Que devons-nous faire maintenant ?

Hasan : Nous devons agir rapidement pour minimiser les dommages et nous assurer que nous sommes en conformité avec le RGPD.

Le joueur doit prendre une décision sur la façon de gérer la fuite de données.

Choix possible :

• Isoler le système compromis et informer le responsable de la protection des données, mais ne pas informer les clients pour éviter une panique inutile.

Céline : Nous devons immédiatement isoler le système compromis pour minimiser les dommages. Et nous devons informer le responsable de la protection des données pour qu'il puisse prendre des mesures supplémentaires pour protéger les données des clients. Cependant, nous devons être prudents quant à la divulgation de l'incident aux clients pour éviter une panique inutile.

Hasan : Je suis d'accord, Céline. Nous ne voulons pas causer de l'inquiétude chez nos clients. Nous devrions attendre de recevoir des instructions de la part du responsable de la protection des données avant de communiquer quoi que ce soit aux clients.

Céline : Très bien. Je vais isoler le système tout de suite et informer le responsable de la protection des données de l'incident.

Le responsable de la protection des données a pris des mesures pour sécuriser le système et a enquêté sur l'incident. Cependant, en raison du retard dans la divulgation de l'incident, l'autorité de contrôle compétente a infligé à l'entreprise une amende importante pour violation des règles RGPD.

• Isoler le système compromis, informer le responsable de la protection des données, signaler l'incident à l'autorité de contrôle compétente et informer tous les clients dont les données ont été compromises.

Céline : Nous devons immédiatement isoler le système compromis pour minimiser les dommages. Nous devons également informer le responsable de la protection des données, signaler l'incident à l'autorité de contrôle compétente et informer tous les clients dont les données ont été compromises.

Hasan : Tout à fait d'accord, Céline. Nous devons être transparents et informer nos clients dès que possible pour qu'ils puissent prendre des mesures de protection.

Céline : Très bien. Je vais isoler le système tout de suite, informer le responsable de la protection des données, signaler l'incident à l'autorité de contrôle compétente et informer tous les clients concernés.

L'entreprise a agi rapidement pour minimiser les dommages, et les clients dont les données ont été compromises ont pu prendre des mesures pour protéger leurs informations personnelles.

Bien qu'il y ait eu des coûts associés à la notification des clients et à la mise en place de mesures supplémentaires pour renforcer la sécurité des données, l'entreprise a finalement évité des amendes importantes pour violation des règles RGPD.

CAS n°4 : Transmission de données aux partenaires

Les employés reçoivent une demande d'un partenaire commercial pour utiliser des données personnelles à des fins de marketing.
Les employés doivent déterminer si l'utilisation des données est autorisée en conformité avec les RGPD. Ils doivent évaluer les risques et les avantages de l'utilisation des données pour le marketing et prendre une décision éthique.

Nous sommes en fin de journée, il est 17h30. Adam, qui travaille dans le département commercial, reçoit un appel de la société Dépathlon, avec qui ils ont travaillé par le passé.

Adam : Bonjour, je suis Adam de la société Amaton. Comment puis-je vous aider ?

Partenaire commercial : Bonjour, je suis le représentant de la société Dépathlon. Nous avons travaillé ensemble par le passé et j'aimerais savoir si nous pourrions avoir accès à des données personnelles de vos clients pour nos campagnes marketing. Nous sommes persuadés que cela augmenterait notre taux de conversion et améliorerait nos ventes.

Adam : Puis-je vous mettre en attente un instant, s'il vous plaît ? Je vais appeler Rémi, notre DPO, pour qu'il nous rejoigne sur cette conversation.

Adam appelle Rémi et l'invite à se joindre à l'appel.

Rémi : Bonjour, je suis Rémi et je m'occupe de la conformité RGPD. Pourriez-vous nous fournir plus de détails sur la façon dont vous allez utiliser ces données ?

Partenaire commercial : Bien sûr. Nous voudrions utiliser les noms, adresses email et numéros de téléphone de vos clients pour leur envoyer des publicités ciblées sur nos produits. Nous sommes confiants que cela aura un impact positif sur les ventes.

Adam : Nous devons nous assurer que nous respectons les règles RGPD en matière de protection des données personnelles. Nous allons devoir examiner vos demandes avec soin.

Le joueur doit prendre une décision sur la façon de traiter la demande du partenaire commercial.

Choix possible :

• Accepter la demande du partenaire commercial et partager les données avec eux.

• Refuser la demande du partenaire commercial et ne pas partager les données avec eux.

Si le joueur choisit d'accepter la demande du partenaire commercial :

Adam : Nous avons pris en compte votre demande et nous sommes prêts à partager certaines de nos données avec vous.

Partenaire commercial : Bien sûr, nous comprenons. Nous sommes prêts à signer l'accord. Merci beaucoup.

Rémi : Très bien, nous allons vous fournir les données que vous avez demandées. Cependant, si nous avons des doutes quant à votre utilisation des données, nous nous réservons le droit de mettre fin à l'accord.

En vertu du RGPD, les personnes ont le droit de savoir quelles données sont collectées, comment elles sont utilisées et avec qui elles sont partagées. Si l'entreprise ne respecte pas ces règles, elle peut être tenue responsable en vertu de la loi. En outre, cela peut nuire à la réputation de l'entreprise et conduire à une perte de confiance des clients.

Dans le cas où le partenaire commercial utilise les données à des fins non autorisées, cela peut également entraîner des conséquences négatives pour les personnes concernées, telles que des atteintes à la vie privée ou des escroqueries.

Si le joueur choisit de refuser la demande du partenaire commercial :

Adam : Nous avons examiné votre demande et nous avons décidé que nous ne pouvons pas partager ces données avec vous en raison de nos obligations en matière de protection des données. Nous

comprenons que cela pourrait être décevant, mais nous sommes tenus de respecter les lois et les règlements en vigueur.

Partenaire commercial : Je suis déçu, mais je comprends votre position. Si jamais vous changez d'avis, n'hésitez pas à me contacter à nouveau.

Rémi : Nous sommes désolés de ne pas pouvoir satisfaire votre demande, mais nous sommes tenus de respecter les lois et les règlements en vigueur en matière de protection des données personnelles. Nous sommes ravis de travailler avec vous dans d'autres domaines qui pourraient être bénéfiques pour nos deux entreprises.

Les conséquences pour l'entreprise peuvent inclure une perte potentielle de revenus de la part du partenaire commercial, ainsi qu'une réputation d'être une entreprise qui ne partage pas les données de ses clients. Cependant, cela peut également renforcer la confiance des clients envers l'entreprise en montrant que leur confidentialité est prise au sérieux et peut renforcer la conformité aux règles RGPD.

La fin du jeu :

Récapitulation des leçons apprises pendant le jeu.
Le joueur reçoit un score final qui montre sa connaissance du RGPD de façon théorique et pratique.
Une remarque s’il a la moyenne ou pas.
Et des conseils pour lui pour approfondir ces connaissances.