Leto

GUIDE POUR SENSIBILISER VOS COLLABORATEURS AU RGPD

COMMENT FAIRE DU RGPD UNE RÉALITÉ OPÉRATIONNELLE

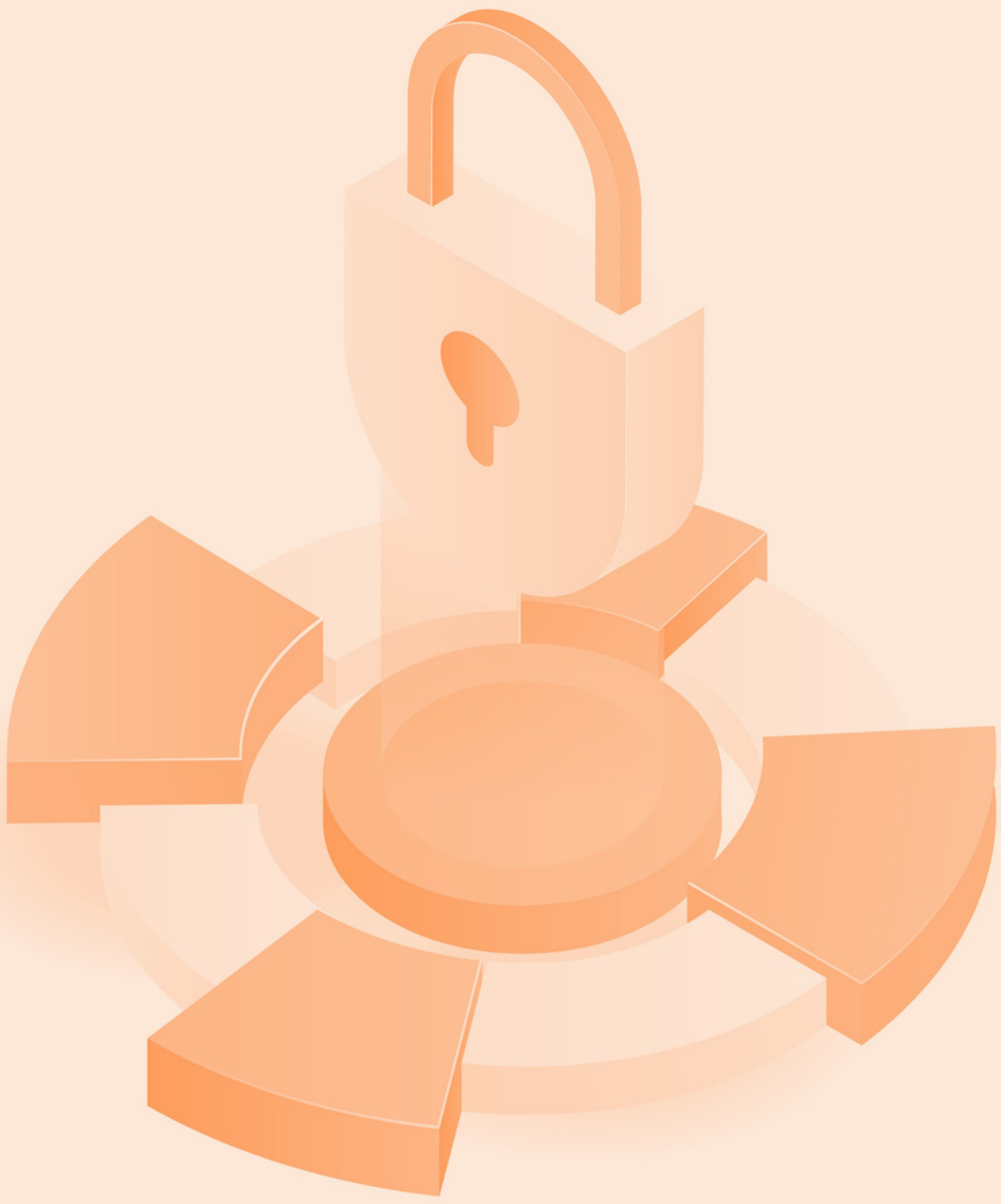
LETO LEGAL

SOMMAIRE

LES POINTS CLÉS

1. Introduction
2. Pourquoi sensibiliser ses collaborateurs au RGPD : les enjeux
3. Comment sensibiliser ses collaborateurs au RGPD : les méthodes
4. Bonus : 30 questions de sensibilisation issues de notre module
5. À propos de Leto

1. INTRODUCTION



Pourquoi faire de la protection des données personnelles votre priorité

INTRODUCTION

L'imprudence est la première cause des failles de sécurité et de fuite de données. Or, il ressort du rapport annuel pour 2022 de la Commission nationale de l'information et des libertés (CNIL) que plus d'un tiers des sanctions prononcées concernent un manquement à la sécurité des données ayant entraîné une fuite des données personnelles des individus. Ces manquements représentent plus de 100 millions d'euros de sanctions prononcées en 2022.

Et pour cause, ces dernières années ont été émaillées de nombreux scandales en matière de vol de données en Europe et dans le monde. On pense par exemple au scandale Facebook-Cambridge Analytica (en 2018) avec près de 87 millions d’utilisateurs visés par un vol de données.

Plus récemment en France, la société DEDALUS BIOLOGIE a été sanctionnée par la CNIL d’une amende de 1,5 million d’euros en 2021 pour des défauts de sécurité ayant conduit à la fuite de données de santé de près de 500 000 personnes. En plus du coût financier évident, c’est un coût réputationnel incalculable pour l’organisme visé par une telle procédure.

Alors, comment éviter cela ? La réglementation sur la protection des données (RGPD) a pour objet de garantir la sécurité des données personnelles qui circulent. Le RGPD a donc deux fonctions :

- Protéger la vie privée des individus,
- Encourager les entreprises à assurer la sécurité de leurs données contre tout vol, fuite et détournement.

Pour cela, le RGPD impose un certain nombre d'obligations aux responsables de traitement, c'est-à-dire à tout organisme collectant et utilisant des données personnelles. Cependant, le Règlement général sur la protection des données est souvent perçu, à tort, comme un immense parcours à obstacles juridiques et techniques.

S'il n'est pas faux qu'une partie de la mise en conformité consiste à construire un certain nombre de documents juridiques déclaratifs sur la manière dont sont traitées les données personnelles, une majeure partie de la démarche consiste à adopter de bonnes pratiques et à monter en maturité sur la manipulation de la data.

Contrairement aux idées reçues, lors de ses contrôles, la CNIL adopte une attitude bienveillante et pragmatique. Ce qui compte, c'est votre bonne foi dans cette démarche : adoptez-vous au quotidien de bonnes pratiques en matière de sécurité ?

À titre d'illustration, le 10 novembre 2022, la CNIL a prononcé une sanction à l'encontre de la société DISCORD INC "en tenant compte des efforts réalisés par la société pour se mettre en conformité tout au long de la procédure". La CNIL a pris en compte les efforts de l'entreprise, même tardivement, pour mettre en place des dispositifs de sécurité, même imparfaits.

Il en résulte que, faire de la protection des données personnelles votre priorité, contribue à votre mise en conformité au RGPD et à réduire vos risques en matière de sécurité des systèmes informatiques. Ces deux sujets sont aujourd'hui indissociables.

L'objet de ce guide est donc de vous donner toutes les clés pour vous mettre en conformité avec la réglementation et faire de la sécurité une réalité opérationnelle.

Voyons plus en détail :

- Pourquoi sensibiliser ses collaborateurs au RGPD : les enjeux de la sensibilisation.
- Comment sensibiliser ses collaborateurs au RGPD : les méthodes.

2. POURQUOI SENSIBILISER SES COLLABORATEURS AU RGPD

Les enjeux de la sensibilisation des collaborateurs

LES ENJEUX DE LA SENSIBILISATION

L'enjeu de la sensibilisation est avant tout d'abandonner l'idée que la protection des données personnelles ne concerne qu'une poignée d'individus au sein de votre entreprise.

Au contraire, chaque collaborateur est directement concerné dès lors qu'il manipule des données au quotidien. Ils sont les acteurs clés de toute votre démarche.

Pourquoi votre structure est concernée

Il est quasiment impossible de se trouver en dehors du champ d’application du RGPD : il s’applique à tout organisme et à toutes les données personnelles. Chaque membre de votre organisation est donc concerné.

Le RGPD s’applique à tous les organismes

La taille ne compte pas.

En effet, si l'on se réfère à la lettre du RGPD, l'article 2 du RGPD est explicite : le RGPD s'applique à toutes les activités professionnelles exercées dans l'Union européenne. Sont donc exclus les traitements de données personnelles opérés dans le cadre d'une activité "strictement personnelle ou domestique".

En d'autres termes, tout organisme, qu'il soit privé ou public, quelle que soit sa taille, est concerné par la réglementation en matière de protection des données personnelles. Auto-entrepreneurs, microentreprises, TPE, PME, ETI ou grandes entreprises, administrations, collectivités territoriales, ministères, ONG, États, associations, fondations : aucun organisme n'est exclu du champ d'application du RGPD.

Où que vous soyez.

De plus, le RGPD (article 3 RGPD) à vocation à s’applique en dehors des frontières de l’Europe. Ainsi, votre structure est soumise à cette réglementation si :

- Votre organisme est établi sur le territoire d'un pays membre de l'Union européenne, même si vous n'exercez vos activités qu'en dehors de l'UE.
- Votre organisme est établi en dehors du territoire d'un pays membre de l'Union européenne et que des données de personnes issues de l'Union européenne sont concernées.

Le RGPD s’applique à toutes les données personnelles

Le RGPD ne s'applique qu'aux données à caractère personnel qui sont traitées par un organisme dans le cadre d'une activité professionnelle. La définition d'une donnée à caractère personnel est volontairement très large de sorte que toute donnée est incluse dans la définition.

En effet, les données à caractère personnel correspondent à toutes les informations se rapportant à une personne physique identifiée ou identifiable directement (par exemple, nom et prénom) ou indirectement (par exemple, numéro de sécurité sociale, adresse e-mail, enregistrement des conversations) (article 4 RGPD).

Par conséquent, toutes les données qui permettent de remonter à une personne physique, même indirectement, sont des données à caractère personnel.

Par exemple :

- Lors du recrutement d'un salarié, votre entreprise est amenée à recueillir les données suivantes : CV, lettre de motivation, lettres de recommandation, coordonnées bancaires, contrat de travail, numéro de sécurité sociale, diplômes, congés, arrêts maladie, compte professionnel sur des outils informatiques (e-mail, etc.).
- Dans une relation B2B, il y a de la donnée à caractère personnel dans la mesure où derrière une entreprise se cache toujours une personne physique. Dans ce cas, la donnée personnelle sera relative à l'e-mail professionnel et l'identité de la personne physique représentant l'entreprise.
- Les données cryptées et pseudonymisées sont des données personnelles, car il suffit d'ajouter des informations supplémentaires pour réattribuer ces données à une personne. Dès qu'il est possible de réidentifier une personne, il s'agit de données à caractère personnel.

Le RGPD est l’affaire de tous

Au sein de votre entreprise, tous vos collaborateurs manipulent des données. À ce titre, ils ont un rôle à jouer dans leur protection.

Par exemple :

- L'équipe des ressources humaines est amenée à traiter toutes les informations relatives à la vie d'un collaborateur dans l'entreprise : depuis sa candidature lors du recrutement, en passant par son contrat de travail, ses évolutions et sa vie de salarié (demande de congés maternités ou autres), jusqu'à son départ.
- L'équipe marketing est amenée à traiter toutes les données relatives aux clients et prospects en utilisant des cookies sur le site internet ainsi que des traceurs ou des outils de mesure d'audience. Il existe également un sujet concernant le mailing avec les newsletters et tout type de communication marketing.
- L'équipe commerciale est amenée à traiter tout un tas de données relatives aux contacts de prospects.

La manipulation de ces données doit retenir votre attention car la prospection commerciale abusive entraîne souvent de nombreuses plaintes auprès de la CNIL, ce qui déclenche souvent un contrôle de sa part.

- L'équipe finance et comptabilité traite de toutes les données relatives à la facturation clients et fournisseurs qui recèlent beaucoup de données personnelles.
- L'équipe IT/Tech ou Data est au cœur de la manipulation des données, des systèmes de stockage et d'hébergement. Ces équipes sont particulièrement concernées notamment parce qu'ils mettent en place les systèmes de sécurité supportant la data de l'entreprise.

Vous l'aurez compris, aucune équipe au sein de votre entreprise n'est exclue des sujets RGPD. Les membres de ces équipes sont les mieux placés pour être les catalyseurs d'une mise en conformité réussie.

Les enjeux de la sensibilisation

Les enjeux éthiques

La protection des données personnelles est avant tout une question éthique. Chaque personne avec qui votre entreprise entre en contact vous fait confiance pour traiter ses informations personnelles avec respect et prudence.

Au contraire, la fuite ou l'utilisation non autorisée de données personnelles a des conséquences particulièrement préjudiciables : discrimination, harcèlement, usurpation d'identité, etc. Pour votre entreprise, elle entraîne la rupture du lien de confiance. Être transparent sur la manière dont votre entreprise s'efforce de garantir la sécurité des données est un gage de réassurance très fort auprès de vos interlocuteurs (clients, prospects, employés, fournisseurs et prestataires). Cela concerne non seulement votre image de marque, mais également le respect de la vie privée de vos interlocuteurs.

Les enjeux juridiques

Toute atteinte à l'intégrité des données engendre des conséquences négatives sur la vie des personnes, la réputation de votre entreprise, et fait peser sur elle un risque de sanction par les autorités (par exemple, la sanction de 1,5 million d'euros infligée à la société Dedalus Biologie, mentionnée en introduction).

Cependant, ces fuites de données peuvent être facilement évitées grâce à la mise en place de bonnes pratiques au sein de chaque équipe. La sensibilisation des collaborateurs est le meilleur moyen d'y parvenir. Cette méthode est même inscrite au sein du RGPD : la sensibilisation des membres de l'organisme fait partie des missions que doit obligatoirement remplir le DPO.

Pour rappel, le DPO (Data Protection Officer), ou délégué à la protection des données, est la personne chargée de mettre en œuvre la conformité au RGPD au sein d'un organisme qui l'a désigné. À ce titre, il a explicitement pour mission "la sensibilisation et la formation du personnel participant aux opérations de traitements" (article 39 RGPD). Cela signifie qu'il a la charge d'infuser une culture autour de la protection des données personnelles auprès des personnes opérant des traitements sur les données, c’est-à-dire tous vos collaborateurs.

La CNIL l'a elle-même confirmé dans son guide à l'intention des délégués à la protection des données : le DPO a avant tout pour mission d'informer l'ensemble des collaborateurs sur ces sujets. En cas de contrôle, vous devez être en mesure de démontrer à la CNIL que vos employés ont reçu une formation ou ont été sensibilisés à ces sujets. Cela signifie qu'il convient de documenter ces campagnes de sensibilisation ou, du moins, d'en garder une trace afin de pouvoir démontrer votre volonté de mise en conformité aux autorités.

Les enjeux business

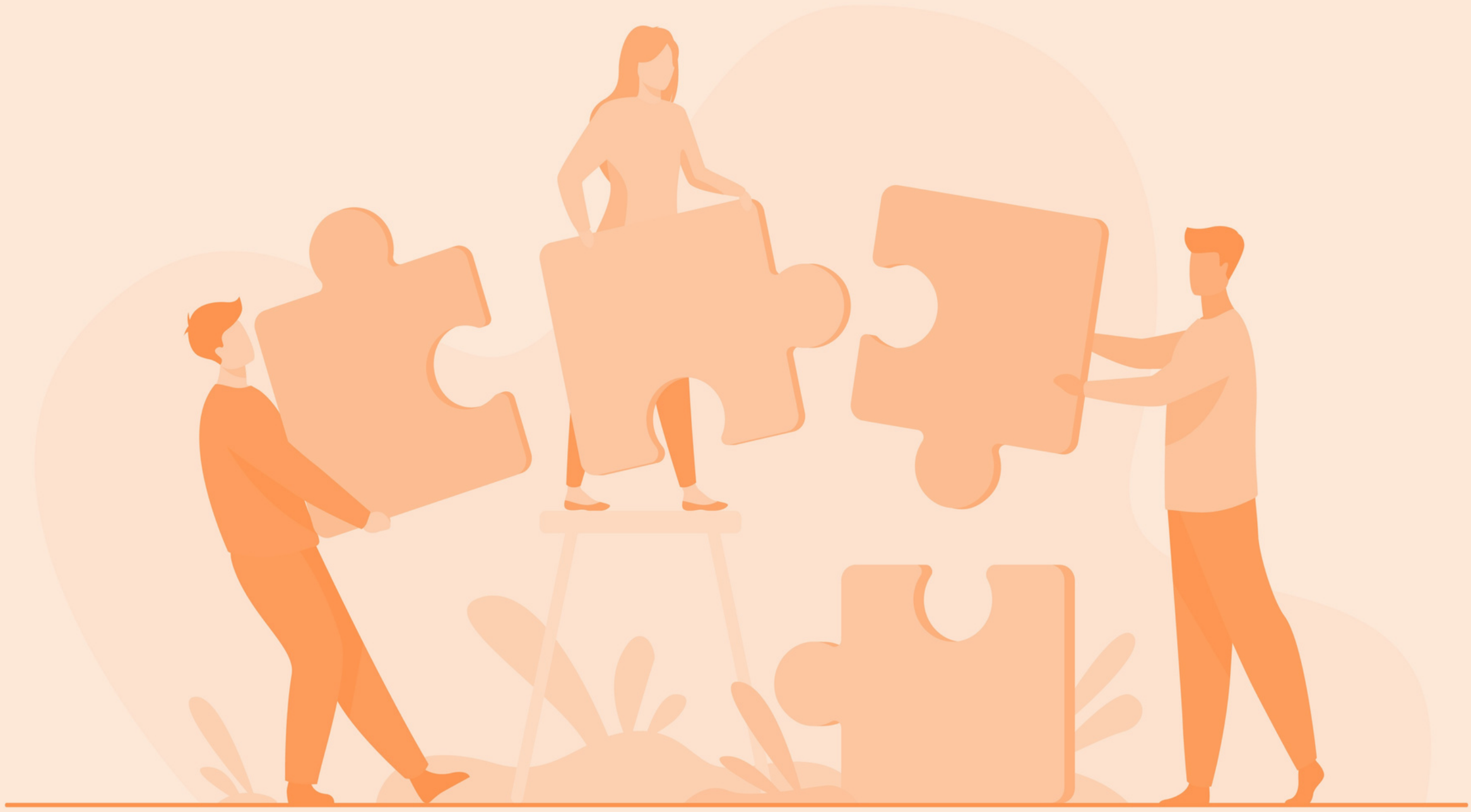
Une bonne gestion des données permet également d'améliorer votre efficacité interne et votre compétitivité sur le marché.

En interne, avoir une vue d'ensemble sur la manière dont les données sont stockées, sécurisées et gérées permet de gagner beaucoup de temps et de capacité de rendement. Vous ne cherchez plus vos données, vos mots de passe, vous ne résolvez plus de bugs ni ne comblez les brèches. Savoir qui a accès à quoi et pour quelles raisons vous permet d'adopter une organisation plus rigoureuse en interne et vous fait gagner du temps.

D'un point de vue purement commercial, les enjeux sont considérables. Depuis l'entrée en vigueur du RGPD en 2018, il est clair que la démonstration de la conformité au RGPD est un atout concurrentiel sur le marché. Les grandes entreprises ont l'habitude d'auditer leurs partenaires, y compris sur la partie Privacy. La plupart de ces audits consistent en une liste de questions sur la conformité au RGPD, dont un certain nombre concerne la manière dont vos collaborateurs sont sensibilisés au RGPD.

Ainsi, la sensibilisation de l'ensemble des équipes et la mise en œuvre opérationnelle de la protection des données personnelles sont des éléments très importants pour vos partenaires commerciaux. Cela fera la différence entre une entreprise avec laquelle ils souhaitent s'associer ou non.

En fin de compte, qu'elle soit l'expression d'une obligation légale ou d'une volonté de monter en maturité sur ces sujets, la sensibilisation est votre meilleur atout.



3. COMMENT SENSIBILISER SES COLLABORATEURS AU RGPD

Les méthodes

COMMENT SENSIBILISER SES ÉQUIPES AU RGPD : MÉTHODES

Comment sensibiliser efficacement ses collaborateurs à la protection des données personnelles ? Quelle est la **bonne méthode ?**

La tâche peut sembler ardue au regard des défis soulevés par la sensibilisation :

- Sensibiliser les bonnes personnes au sein des équipes,
- Obtenir efficacement des résultats dans la durée,
- Concilier la formation des collaborateurs avec les arrivées et les départs réguliers dans l'entreprise,
- Sensibiliser ses équipes sans un coût financier et humain important,
- Adapter la sensibilisation à votre activité et aux problématiques rencontrées par vos équipes au quotidien,
- Mesurer le niveau de maturité de vos équipes à ces sujets,
- Déclencher un fort engagement de vos équipes.

Quelle est la meilleure méthode pour atteindre l’ensemble de ces objectifs ?

Il existe beaucoup d’offres de formations diverses sur le marché et il n’est pas toujours aisé de s’y retrouver.

Avant de vous lancer, il faut avoir en tête les insuffisances des méthodes classiques. Basée sur notre expertise, nous préconisons une approche par le microlearning et vous proposons de partager avec vous un échantillon exclusif de notre module.

L’insuffisance des méthodes classiques

Les méthodes classiques de formation pour sensibiliser les collaborateurs à la protection des données personnelles présentent plusieurs inconvénients.

Formations en présentiel et conférences

Sous la forme de cours magistraux animés par des experts, ces formations sont souvent organisées à l'arrivée de chaque collaborateur ou par session (tous les 2 ans, par exemple). À l'issue de ces formations, vos employés sont généralement invités à signer une charte ou un document attestant de leur participation.

Si elles ont l'avantage de pouvoir démontrer que vous avez officiellement accompli votre devoir de sensibilisation de vos employés, elles comportent beaucoup d'inconvénients.

Elles prennent la forme de cours théoriques et entraînent assez peu d'engagements de la part de vos collaborateurs. Surtout, ces formations ne procurent aucun effet dans le temps : à l'issue de ces formations, très peu d'information reste en mémoire, et rien ne permet véritablement de changer les habitudes de vos collaborateurs.

E-learning

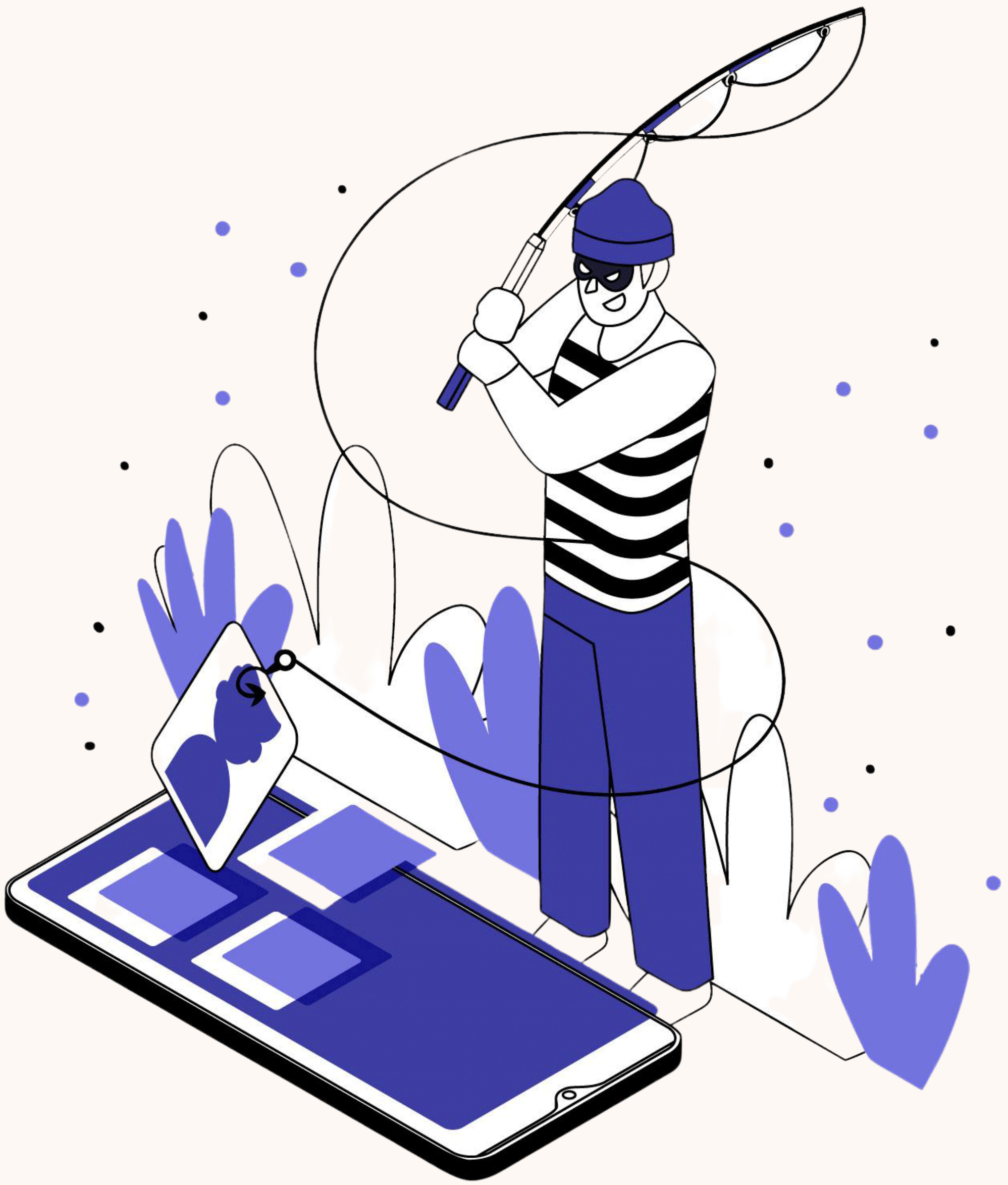
Il s'agit d'une méthode similaire aux formations en présentiel avec l'avantage de pouvoir s'adapter plus facilement aux agendas de vos collaborateurs.

Pour autant, ce type de formation a les mêmes inconvénients : à l'issue d'un certain nombre d'ateliers, vos collaborateurs auront tout oublié, elles n'engendrent que très peu d'engagements de leur part et surtout elles manquent cruellement de personnalisation.

À l'issue de ces ateliers, rien ne permet de s'assurer que vos collaborateurs ont acquis de nouveaux réflexes.

Jeux de simulation

Enfin, une dernière méthode a vu le jour plus récemment. Elle consiste à simuler des failles de sécurité ou de fuite de données personnelles. Si cette méthode présente l'avantage d'être plus amusante et moins théorique, elle manque de personnalisation par équipe et par secteur d'activité. De plus, aucun moyen ne permet de mesurer l'efficacité de la formation pour le collaborateur, si bien qu'il est impossible de savoir si elle a été utile ou non.



En définitive, l'ensemble de ces méthodes classiques présente les inconvénients suivants :

- Un manque d'engagement des équipes avec peu d'attention lors des formations qui peuvent s'avérer ennuyeuses.
- Un oubli rapide des informations délivrées lors des formations dû à la quantité d'informations théoriques et à l'absence de répétition.
- Un coût élevé financièrement, que ce coût soit direct (le prix de la formation) ou indirect (le temps passé par vos employés).
- Un manque de personnalisation lié à l'activité de votre organisme et surtout lié aux problématiques rencontrées par vos différentes équipes.
- L'absence de mesure sur l'efficacité de la formation. Aucun moyen n'est mis à votre disposition pour mesurer l'utilité de la formation, le niveau de maturité de vos collaborateurs et les sujets les moins maîtrisés par vos équipes.

Pour pallier à l'insuffisance de ces méthodes classiques, nous préconisons une approche par microlearning permettant d'atteindre l'ensemble de vos objectifs.

L’approche par microlearning

De quoi s’agit-il ?

Le microlearning est une approche de formation qui consiste à diffuser régulièrement des microapprentissages ou des parties d'information. Elle prend généralement la forme de minicours interactifs, tels qu'un quiz ou un rappel d'information. L'idée du microlearning est que chaque module dure moins de 5 minutes, mais se répète dans le temps.

L'avantage de ce format est qu'il permet d'apprendre sur la durée des éléments pratiques de manière digeste et facile à retenir. Cette approche est particulièrement adaptée pour sensibiliser les collaborateurs aux sujets de sécurité et de protection des données.

En effet, la plupart des études statistiques sur les méthodes d'apprentissage ont montré qu'une plus grande quantité d'information est retenue durablement lorsqu'elle est délivrée par microlearning.

Le format court de ce type de formation permet une meilleure attention de l'individu et un meilleur taux d'engagement.

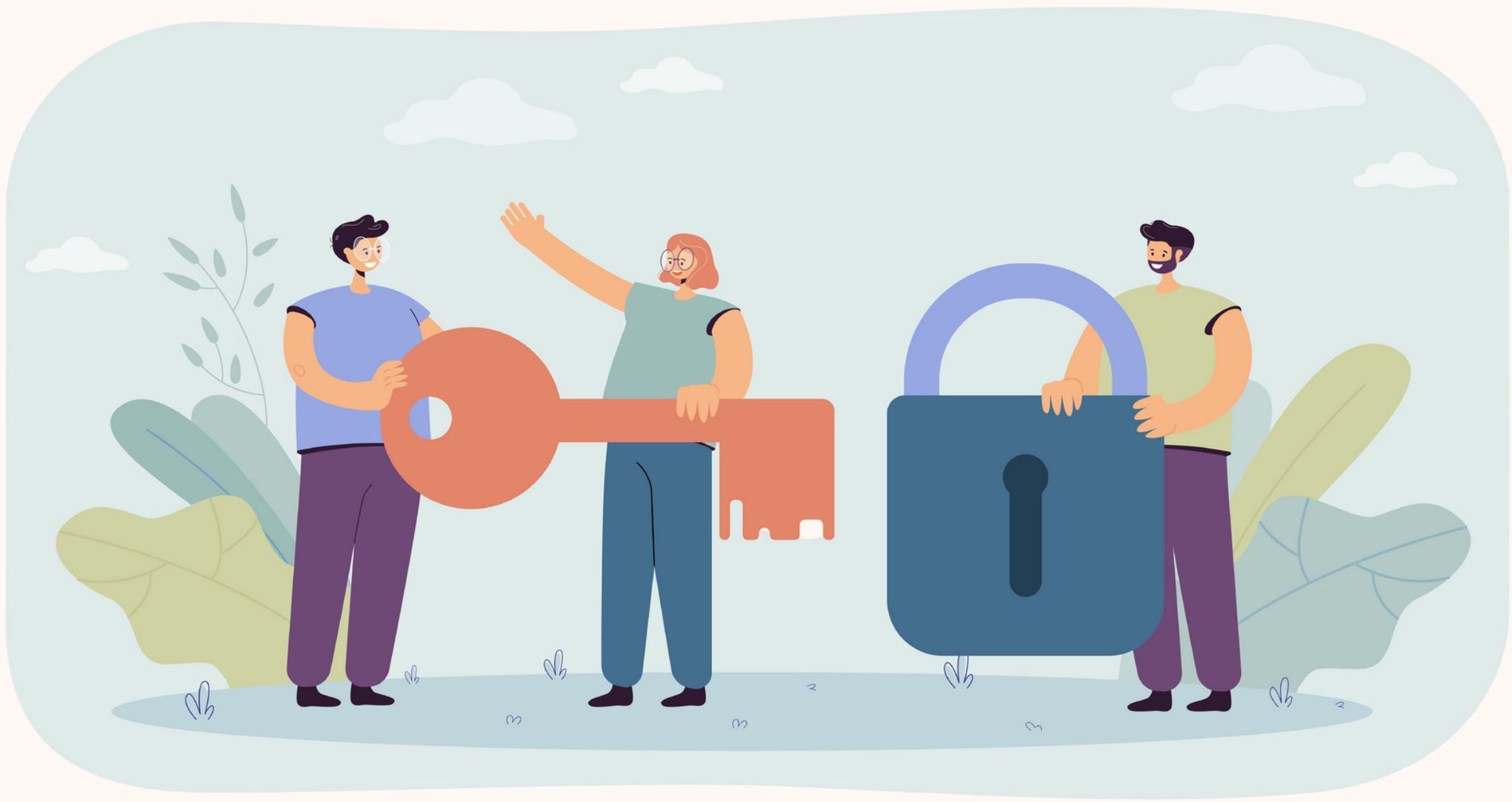
Notre module de sensibilisation par le microlearning

Méthode

Notre approche ne consiste pas à délivrer un cours magistral sur les définitions des données personnelles, le consentement, les cookies, les données sensibles et les mesures de sécurité, mais plutôt à déclencher une prise de conscience.

Ces sujets ont un impact réel dans votre quotidien.

Pour cette raison, nos questions sont conçues pour correspondre à des situations concrètes que vivent vos équipes. Ils peuvent alors directement se sentir concernés par le sujet et disposer d’une bonne pratique associée.



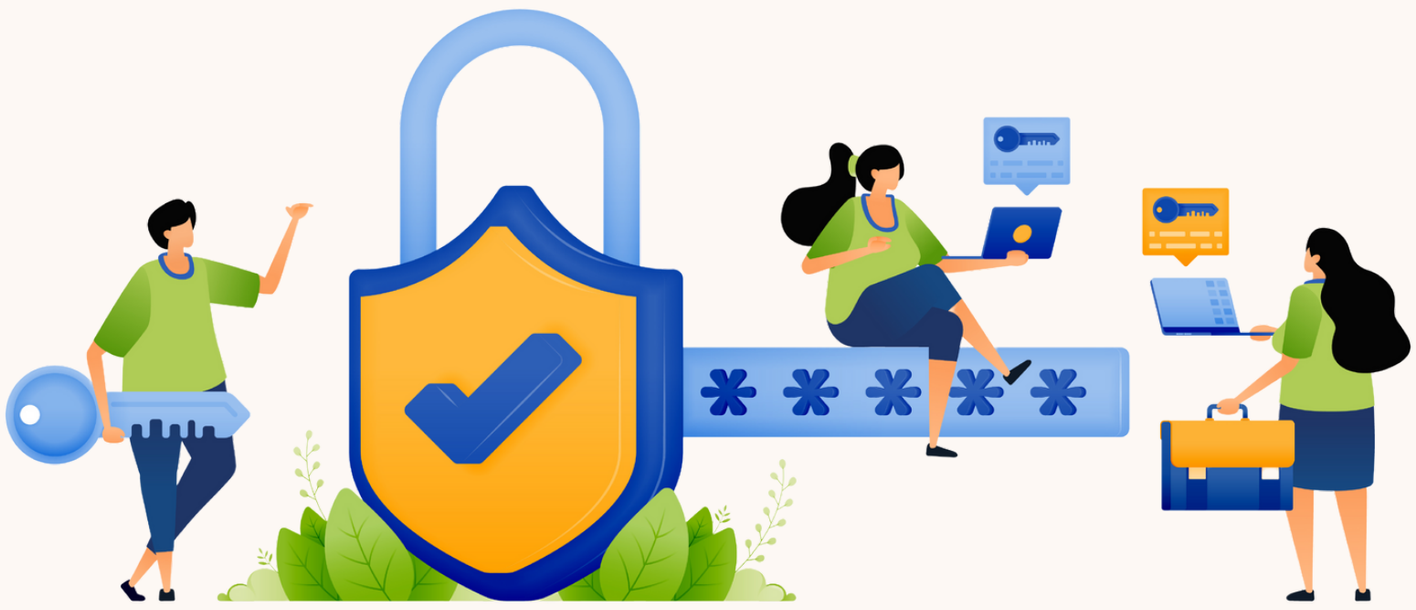
Notre outil vous permet également de créer vos propres questions, en plus de la banque de questions complétées chaque semaine. Imaginez vouloir challenger votre équipe Tech & Produits sur anonymisation des données en rapport avec un cas métier que vous avez rencontré dans le passé.

Nos équipes se tiennent à votre disposition pour coconstruire avec vous un nouvel ensemble de questions ou vous pouvez directement créer vos questions en toute autonomie depuis la plateforme.

Format

Sans avoir besoin de créer de compte (nous évitant ainsi de récolter vos data), vos collaborateurs reçoivent la question du jour (ou de la semaine) directement dans leur outil de messagerie préféré (e-mail, Slack ou Teams). Ils peuvent directement y répondre en cliquant sur le lien envoyé.

Résultat : il faut moins de 2 min à votre collaborateur pour ouvrir la question, y répondre et consulter la réponse. Un contenu vidéo, audio ou rédigé est toujours associé à la réponse afin de permettre à ceux qu'ils le souhaitent, d'aller plus loin.



Résultat et pilotage

Notre outil met à votre disposition un dashboard complet. Vous avez à votre disposition toutes les données dont vous avez besoin pour mesurer :

- le niveau d’avancement de la campagne,
- le niveau de participation par personne,
- le taux de réussite par question et par personne.

L’ensemble de ces données vous permettent de moduler la fréquence des questions, le taux d’engagement et le niveau de maturité de chaque collaborateur. Ces métrics ont beaucoup de valeur, car elles vous permettent de dresser un état des lieux et d’identifier les sujets les moins maîtrisés et les personnes qui ont le plus de difficultés.

Notre module de sensibilisation vous permet de piloter entièrement la sensibilisation de vos collaborateurs.

Plusieurs de nos clients l’ont testé et voici pourquoi ils l’ont adopté :

- L’ensemble des collaborateurs ont accueilli positivement le microlearning qui a été perçu comme une forme de jeux entre collaborateurs.
- Le module a soulevé des discussions lors des déjeuners et des pauses lorsque certaines des réponses les ont surpris.
- L’entreprise a une vue macro et micro de son niveau de maturité par équipes, par collaborateur et en fonction des sujets (cybersécurité, prospection commerciale, campagne marketing, etc.).

4. BONUS

Échantillon de 30 questions issues de notre module de sensibilisation

BONUS : ÉCHANTILLON DE 30 QUESTIONS DE MICROLEARNING ISSUES DE NOTRE MODULE

Question n°1 - Marketing

Un utilisateur vient de nous écrire pour qu'on supprime toutes les données qu'on a sur lui. Je le désabonne de la newsletter, puis c'est bon, c'est ça ?

Question n°2 - Marketing

On a désormais plusieurs milliers d'abonnés particuliers dans notre base. L'équipe marketing lance une campagne de retargeting sur Facebook à partir de ces e-mails, notamment pour promouvoir notre activité auprès de cette audience et auprès d'internautes qui ressemble à nos abonnés (le fameux "Look a like"). Qu'en penses-tu ?

Question n°3 - Marketing

On décide de mettre à jour le bandeau de cookies du site de l'entreprise. Pour avoir un maximum d'acceptation de cookies, on décide de mettre un bouton "Accepter" en gros, et un lien "Continuer sans accepter" en haut à droite, en petit. Qu'en penses-tu ?

Question n°4 - Marketing

À partir du moment où on utilise des cookies sur le site, il faut obligatoirement mettre un bandeau de consentement. Qu’en penses-tu ?

Question n°5 - Marketing

On lance un nouveau site, et il nous faut un outil d’analyses statistiques. L’équipe choisit le leader et en plus, il est gratuit : Google Analytics. Qu’en penses-tu ?

Question n°6 - Ressources humaines

Avec le travail hybride, la direction ne s’y retrouve plus : doit-on conserver les bureaux ? Pour avoir une idée du nombre de collaborateurs qui viennent au bureau, on décide d’installer des caméras de surveillance dans les bureaux. Est-ce possible ?

Question n°7 - Ressources humaines

À la suite d’un débat sur le don du sang au déjeuner, notre manager décide dans son coin de mettre dans un fichier partagé le groupe sanguin de chaque collaborateur. Sait-on jamais s’il y avait un accident au bureau et qu’il fallait faire une perfusion en urgence ! Qu’en penses-tu ?

Question n°8 - Ressources humaines

Je démissionne et j’aimerais que mon futur ex-employeur supprime toutes les données qui me concernent. Est-ce possible ?

Question n°9 - Ressources humaines

Les RH me demandent de fournir mon RIB. Pourtant, elles ne me demandent pas mon consentement pour s’en servir. C’est normal ?

Question n°10 - Ressources humaines

Ai-je le droit de poser la question suivante en entretien d’embauche : “Que font vos parents dans la vie ?”

Question n°11 - Tech

J’aperçois dans les logs une adresse IP en provenance de l’Azerbaïdjan. En creusant un peu plus, je remarque qu’il y a eu une lecture des données bancaires de certains de nos clients. Qu’est-ce que je dois faire ?

Question n°12 - Tech

Notre entreprise stocke le frontend et le backend sur deux outils américains. J’avertis alors mon équipe que les serveurs américains ne sont pas autorisés, car le droit américain n’est pas conforme au RGPD. Je propose de prendre une option à 400 euros par mois qui nous permet d’héberger les données sur des serveurs en Allemagne. Est-ce que ça suffit ?

Question n°13 - Tech

À quoi permet de “hasher” une donnée ?

Ex. : “Elon Musk” -(Hash)?

“21951C0B895D7B4B8C63E392D2E8C8AE”

Question n°14 - Tech

On doit supprimer les données personnelles d'un utilisateur suite à une demande de suppression. L'équipe a donc supprimé toutes les informations qui permettent de l'identifier. Il reste simplement l'identifiant lui correspondant en base. Est-ce suffisant ?

Question n°15 - Tech

Nous venons de migrer notre data center de Nextcloud, qui est français, pour tout héberger sur AWS qui appartient à Amazon (US). Est-ce que c'est possible même si c'est un serveur américain ?

Question n°16 - Finances/ comptabilité

Un ancien client demande la suppression de toutes ses données personnelles. À la compta, il y a notamment des factures de l'an dernier de ce client. Pour être conforme, on les supprime aussi ?

Question n°17 - Finances/ comptabilité

Un client mécontent m'envoie un e-mail m'indiquant qu'il ne paiera pas sa facture et qu'il souhaite que l'on supprime l'ensemble de ses données personnelles. Que dois-je faire ?

Question n°18 - Cybersécurité

J’ai toujours entendu nos clients se plaindre de la taille et la complexité de leurs mots de passe sur la plateforme. Je pense qu’un mot de passe composé de 6 caractères avec des lettres et des chiffres ça suffit niveau sécurité. Qu’en penses-tu ?

Question n°19 - Cybersécurité

Mon collègue est devant la porte d’embarquement de l’avion et décide de s’avancer sur son travail. Pour cela, il se connecte au réseau wifi de l’aéroport pour accéder à nos bases de données internes. Qu’en penses-tu ?

Question n°20 - Cybersécurité

Mon stagiaire de 3ème, Alexis, a publié une longue story Instagram de lui au travail. On y voit l’intégralité de nos contacts clients (nom, prénom, entreprise, email). Est-ce une violation de donnée personnelle ?

Question n°21 - Data

Le siège demande à l'ensemble des équipes, et notamment l'équipe technique d'anonymiser ou de supprimer les données "dès que nécessaire". Mais quand est-ce que je dois procéder à l'anonymisation des données ?

Question n°22 - Data

Je travaille dans une entreprise d'édition de jeux vidéo sur application. Lors d'une discussion avec un Product Manager, il m'indique qu'il souhaite qu'on ajoute des champs dans le formulaire d'inscription d'utilisateur (adresse postale, date de naissance, lieu de naissance). Or, moi en tant que Data Engineer je sais pertinemment que je n'aurai pas besoin d'autant de données. Qu'est-ce que je fais ?

Question n°23 - Data

Le nouveau Data Analyst nous donne accès à un jeu de données récupéré à son ancien job. Il contient des données très précieuses sur des centaines d'utilisateurs. Pouvons-nous exploiter ces données ?

Question n°24 - Data

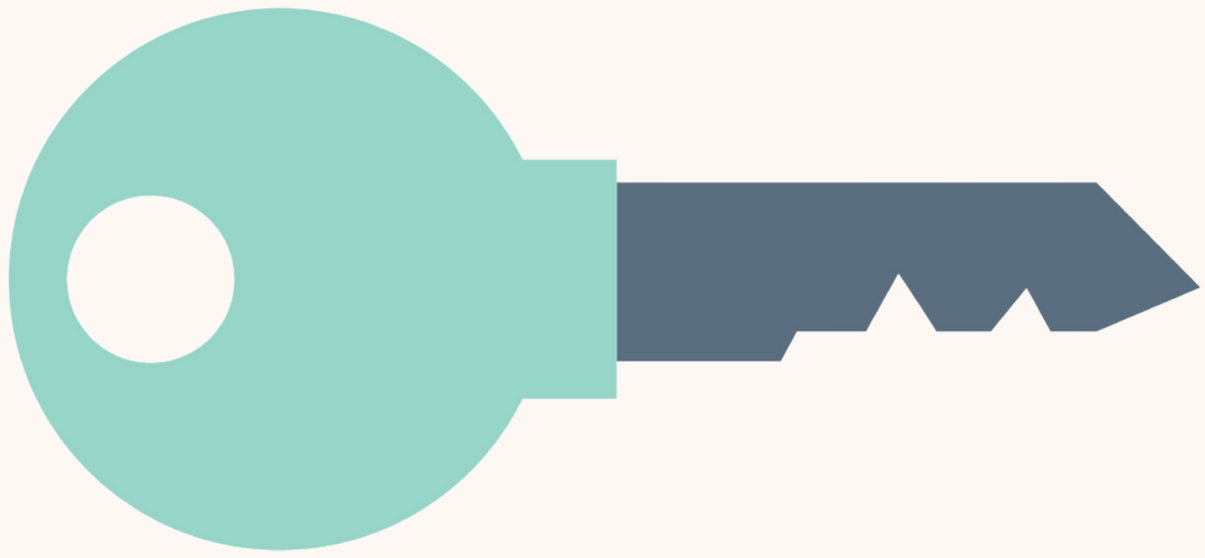
Dans l’équipe Data, je dois créer du reporting interne via notre Data Warehouse. En amont, j’ai fait en sorte de ne pas stocker les identifiants de base de données, mais de les transformer en hash (md5, SHA-1, etc.). Est-ce que c’est de la donnée personnelle ?

Question n°25 - Data

Je souhaite rapprocher les données clients depuis le CRM avec des données en open data pour mon reporting auprès de l’équipe Marketing.
Est-ce que je peux le faire ?

Question n°26 - Commercial

Lors de mes calls avec des prospects, j’ai l’habitude de tout noter dans mon CRM pour mieux cibler mon discours au prochain rendez-vous : nom, prénom, poste, âge, sexe, origine ethnique, appartenance syndicale ou non, habitudes religieuses, etc. Est-ce possible ?

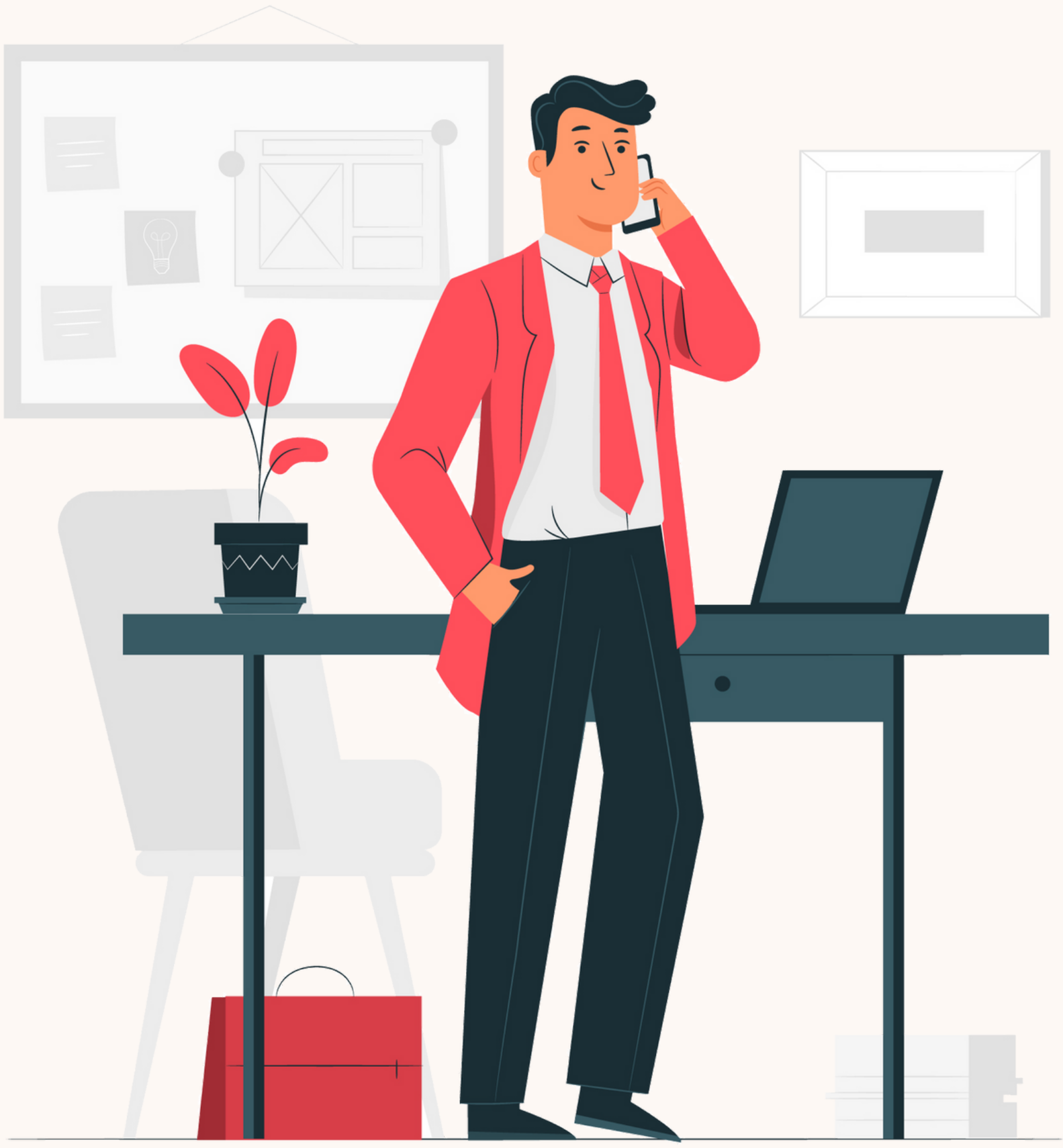


Question n°27 - Commercial

En discutant avec le secrétariat, j’apprends que l’entreprise conserve depuis une vingtaine d’années tous les numéros de téléphone et le nom des entreprises avec qui elle a établi une relation commerciale dans un fichier Excel accessible à tous. Qu’en penses-tu ?

Question n°28 - Commercial

De manière générale, il vaut mieux collecter un maximum de données sur les utilisateurs pour être sûrs d’avoir tout ce qu’il faut que l’inverse. Qu’en penses-tu ?



Question n°29 - Commercial

Un site propose la vente de bases de données marketing à un prix très attractif. Mon collègue m’avertit que l’achat de fichier client est interdit par le RGPD. Qu’en penses-tu ?

Question n°30 - Commercial

Ma société dont le siège est établi en France ne vend ses produits qu’en dehors de l’Union européenne et notamment en Asie. Le RGPD et le droit de la protection des données personnelles s’appliquent-ils à la société ?

5. À PROPOS DE LETO

Une solution automatise votre mise en conformité au RGPD

À PROPOS DE LETO

Comment mettre en œuvre le RGPD dans une entreprise de manière efficace ? Comment transformer cette contrainte réglementaire en opportunité de développement de son activité ?

C’est en partant de ces enjeux rencontrés dans leurs expériences entrepreneuriales que Benjamin et Édouard ont créé Leto.

Leto est une solution Saas dont l’ambition est d’automatiser la mise en conformité au RGPD et d’en faire une réalité opérationnelle au quotidien dans l’entreprise.

Leto vous permet notamment de :

- **gagner du temps au quotidien :** Leto réalise et maintient automatiquement l’inventaire des types de données personnelles traitées par l’organisation et toute la documentation de conformité,
- **raccourcir votre cycle de vente :** Leto aide vos équipes (commerciale, compliance, etc.) à répondre aux audits et questionnaires conformité de vos prospects,
- **réduire votre risque réputationnel :** Leto simplifie les procédures de demandes d’exercices de droits des citoyens (salariés, clients, candidats, etc.),
- **améliorer la maturité des équipes :** Leto sensibilise l’ensemble vos collaborateurs à la protection des données personnelles grâce une technologie unique de microlearning ultra-personnalisé.

LETO.LEGAL

ENVIE D'EN SAVOIR DAVANTAGE ?

N'HÉSITEZ PAS À NOUS CONTACTER.

NOTRE E-MAIL :
contact@leto.legal

NOTRE SITE WEB :
leto.legal

NOTRE NEWSLETTER :
leto.legal/newsletter-rgpd

NOTRE CHAINE YOUTUBE :
youtube.com/@letolegal

NOS LIVRES BLANCS :
leto.legal/livre-blanc/rgpd