3M Science. Applied to Life.™

Règlement européen sur la protection des données personnelles - RGPD

2017

Règlement européen sur la protection des données personnelles - RGPD

- En mai 2018, la RGPD (Règlement Général sur la Protection des Données), loi européenne (pas de possibilité de « contre-loi » nationale) et contraignante (donnant lieu à amendes) entrera en vigueur dans l'ensemble des 28 pays états membres

- Toutes entités (entreprises et collectivités) qui collectent, stockent ou traitent des données personnelles de citoyens européens y seront soumises
- Certaines violations seront passibles d'amendes pouvant atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

- « la responsabilité des organismes sera renforcée. Ils devront en effet **assurer une protection optimale des données à chaque instant** et **être en mesure de la démontrer** **en documentant leur conformité**. »

Obligation à partir de mai 2018 de mettre en place les mesures de protection des données appropriées

Attention, une violation de données est une atteinte à la réputation et à l'image de marque de votre entreprise

Source CNIL

Se préparer en 6 étapes

Etapes		
Désigner délégué à la protection des données	Obligatoire en 2018 si : • Vous êtes un organisme publique • Vous êtes une entreprise amenée au suivi régulier des personnes à grandes échelles ou au traitement de données dites sensibles	**Rôle du délégué à la protection des données :** • informer sur le contenu des nouvelles obligations, • sensibiliser les décideurs sur l'impact de ces nouvelles règles, • réaliser l'inventaire des traitements de données de votre organisme, • concevoir des actions de sensibilisation, • piloter la conformité en continu.
Cartographier vos traitements de données personnelles	Pour mesurer concrètement l'impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en oeuvre. Dans le cadre du futur règlement, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales.	**Recenser précisément :** • les différents traitements de données personnelles, • les catégories de données personnelles traitées, • les objectifs poursuivis par les opérations de traitement de données, • les acteurs (internes ou externes) qui traitent ces données ; vous devrez notamment clairement identifier les prestataires sous-traitants, • les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.
Prioriser les actions	Après avoir identifié les traitements de données personnelles mis en œuvre au sein de votre organisme, vous devez, pour chacun d'eux, identifier les actions à mener pour vous conformer aux obligations actuelles et à venir. Cette priorisation peut être menée au regard des risques que font peser vos traitements sur les libertés des personnes concernées. Certaines tâches seront faciles à mettre en œuvre et vous permettront de progresser rapidement.	**Points d'attention quels que soient les traitements de données** • Assurez-vous que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées. • Identifiez la base juridique sur laquelle se fonde votre traitement (par ex : consentement de la personne, intérêt légitime, contrat, obligation légale). • Révisez vos mentions d'information afin qu'elles soient conformes aux exigences du règlement. • Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées. • Prévoyez les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...). • Vérifiez les mesures de sécurité mises en place.

Source CNIL

Se préparer en 6 étapes

Gérer les risques	Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données (en anglais, Privacy Impact Assessment ou PIA). L'étude d'impact sur la protection des données permet : • de bâtir un traitement de données personnelles ou un produit respectueux de la vie privée, • d'apprécier les impacts sur la vie privée des personnes concernées, • de démontrer que les principes fondamentaux du règlement sont respectés.	**Quand mener une étude d'impact sur la protection des données (PIA) ?** • avant de collecter des données et de mettre en œuvre le traitement, • sur tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques. **Que contient une étude d'impact sur la protection des données (PIA) ?** • une description du traitement et de ses finalités, • une évaluation de la nécessité et de la proportionnalité du traitement, • une appréciation des risques sur les droits et libertés des personnes concernées, • les mesures envisagées pour traiter ces risques et se conformer au règlement.
Organiser les processus internes	Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement de données personnelles (par exemple : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire etc.).	Organiser les processus implique notamment de : • prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement • sensibiliser et d'organiser la remontée d'information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs, • traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités • anticiper les violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.
Documenter la conformité	Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu. Afin de prouver votre conformité, vous devez constituer un dossier documentaire permettant de démontrer que le traitement de données personnelles est conforme au règlement. Les mesures organisationnelles et techniques sont réexaminées et actualisées si nécessaire.	Votre dossier devra notamment comporter les éléments suivants • La documentation sur vos traitements de données personnelles • Information des personnes • Les contrats qui définissent les rôles et les responsabilités des acteurs

Les espaces et les habitudes de travail changent !

Les bureaux fermés ont laissé la place à des zones de travail plus ouvertes :

- Bureau semi-ouverts
- Bureau ouvert
- Bureaux partagés / free-sitting
- Co-working
- Travail en mobilité
- Travail à domicile

Les écrans sont exposés en permanence

- Prestataires
- Service de maintenance
- Fournisseur
- Visiteur
- Clients
- Etc.…

Histoire vraie !

Un journaliste voyage en avion à côté d'un homme d'affaire qui travaille sur son PC. En sortant de l'avion, il l'interpelle et lui dit : « j'ai pu voir tout ce que vous faisiez sur votre écran pendant le voyage »
L'homme d'affaire ne réagit pas.
Le lendemain, son business plan à 5 ans est publié dans le New York times.

On expose nos écrans

On ne sait jamais à côté de qui on se trouve

On travaille n'importe où avec un degrés de concentration qui nous fait oublier notre environnement

Un journaliste peut se trouver juste à côté de nous

Un concurrent peut se trouver à côté de nous

Une personne mal intentionnée peut voir notre écran

On vit dans un monde ultra connecté

On consulte des données personnelles n'importe où

On traite des données qui ne nous appartiennent pas

On passe 1h30 par jour sur les réseaux sociaux et on expose nos données personnelles et celle des autres

Etc …

La place de filtres de confidentialité

	Etapes	Le rôle du filtre de confidentialité	
	Désigner un délégué à la protection des données		
	Cartographier vos traitements de données personnelles	Les zones de travail « sensibles » et les travailleurs mobiles doivent être identifiés afin de vous prémunir contre le piratage visuel.	
	Prioriser les actions	Les filtres de confidentialité peuvent s'intégrer dans la phase finale de la protection des données. C'est la dernière étape du processus.	
	Gérer les risques	Le piratage visuel se produit rapidement, sur des informations sensibles. La plupart du temps, le pirate passe inaperçu. Le pirate peut être n'importe qui !	
	Organiser les processus internes	Intégrer le piratage visuel dans les processus interne est important. La mise en œuvre d'un protocole de sécurité dans les bureaux et pour les employés mobiles est de rigueur.	
	Documenter la conformité	La mise en place des filtres de confidentialité démontre que vous avez été au bout du processus de protection des données personnelles.	

La réalité : un pirate visual n’a besoin que d’une seule information pour lui permettre d’organiser un vol de données à grande echelle.

Si un pirate visual capture ces informations …

…les conséquences peuvent être les suivantes

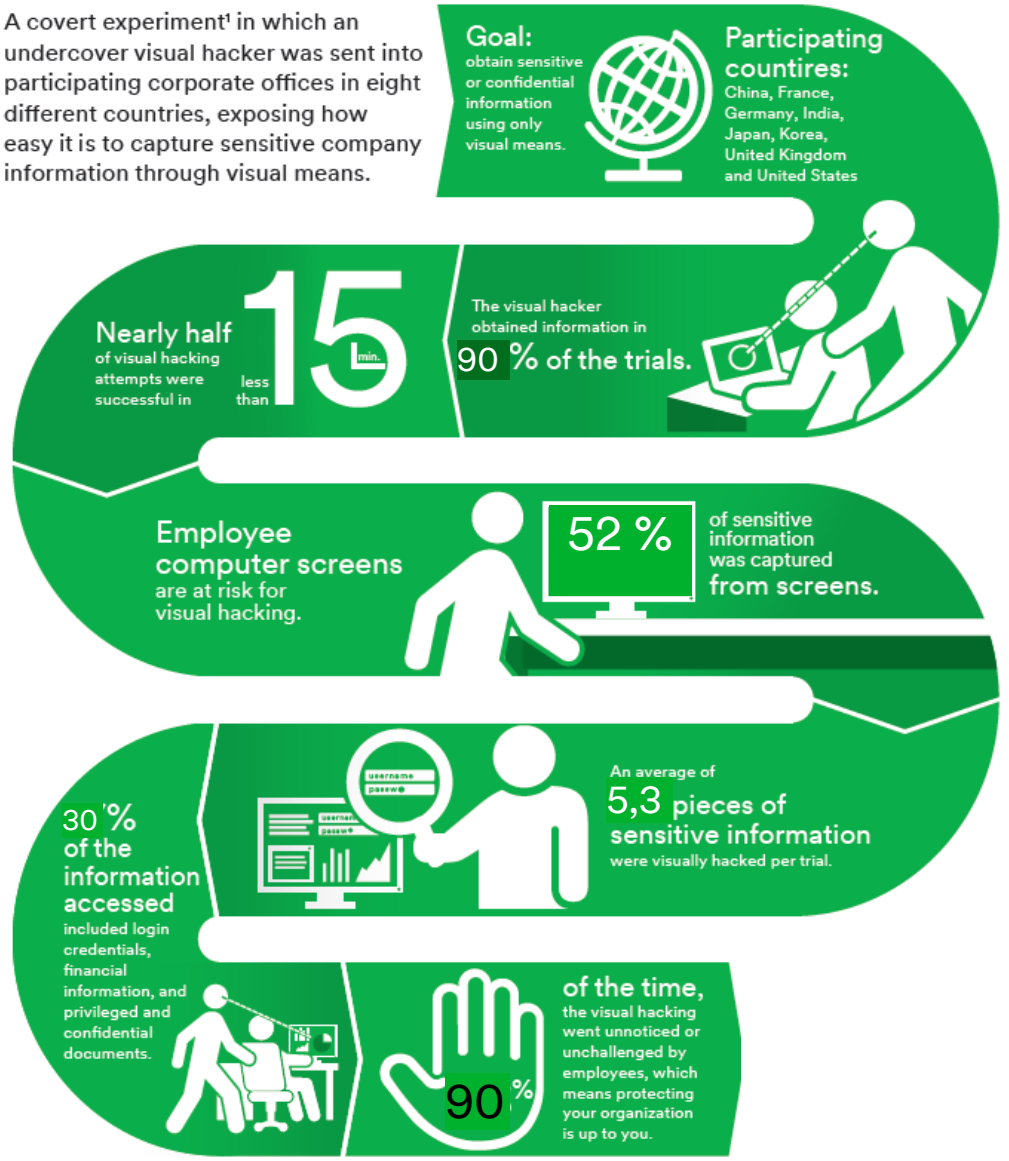
… perte de données

* 3M Visual Hacking Experiment from the Ponemon Institute, Sponsored by 3M Company.

Le piratage visuel
Conclusion

- Le piratage visuel se produit **rapidement**, sur des informations **sensibles.**
- La plupart du temps, le “pirate” passe **inaperçu.**
- Les “pirates” peuvent être **n’importe qui** !

- Les entreprises doivent :
  - Mettre en œuvre un protocole de sécurité contre le piratage visuel dans les bureaux mais également à l’extérieur du bureau.
  - Sensibiliser ses employés aux risques : le filtre est un bon moyen de faire visualiser la réalité du besoin de confidentialité.



Pourquoi investir des milliers d'Euros dans l'infra et ne pas aller au bout de la démarche en protégeant les données personnelles contre le piratage visuel ?