Se conformer au RGPD en utilisant une approche basée sur le risque

RGPD, une situation très particulière

50%

50%

International Association of Privacy Professionals (IAPP)

EY
Building a better working world

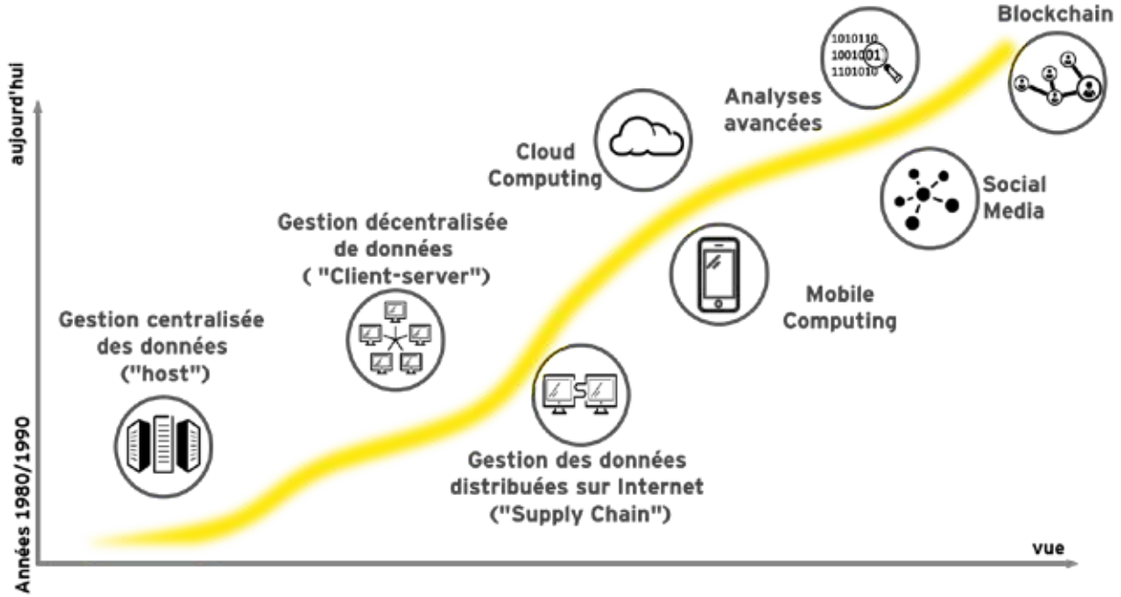
Sommaire

- **Pourquoi ce nouveau règlement ?**
- Quels sont les avantages pour votre PME ?
- Données personnelles
- Comment passer à l’action ? utilisant une approche basée sur le risque
- Conclusion

Pourquoi ce nouveau règlement ?

- L’acronyme RGPD signifie: « Règlement Général sur la Protection des Données ».
- Le RGPD encadre le traitement des données personnelles sur le territoire de l’Union européenne

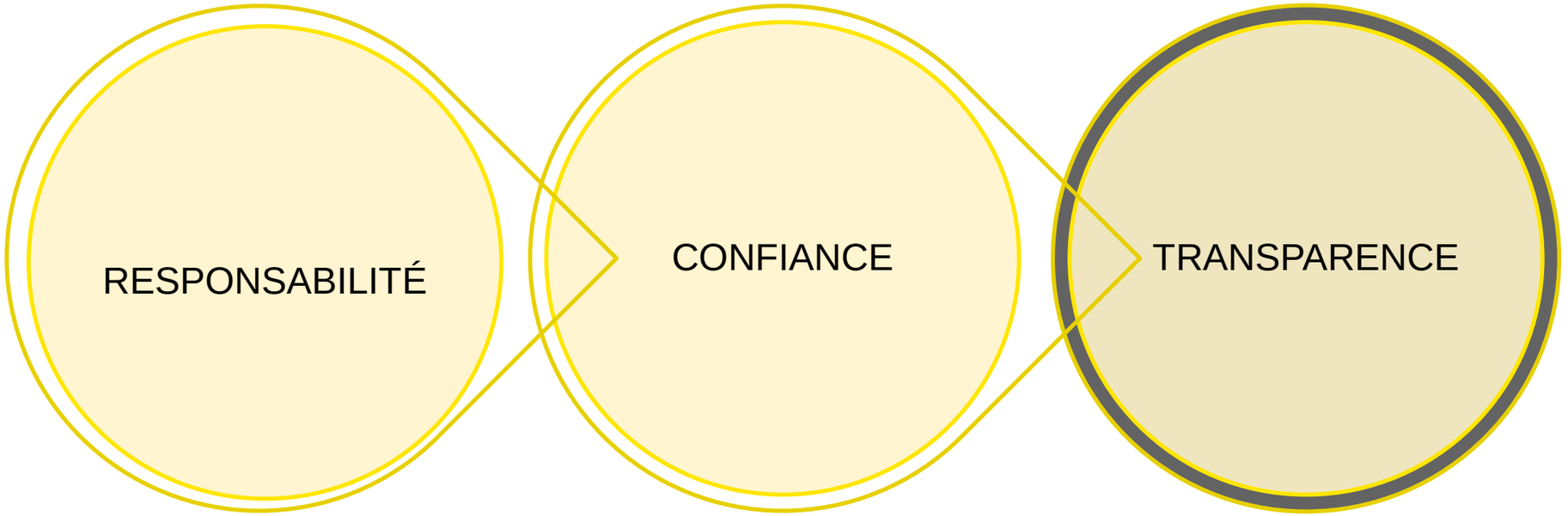
Évolution numérique:



Tout organisme quels que soient sa taille, son pays d’implantation et son activité, peut être concerné.

EY
Building a better working world

Le RGPD



Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.

Qu’est ce que le RGPD

le RGPD est le point final de plusieurs années de travail de l’UE pour reformer les lois de protection des données dans un Framework global au lieu d’un panel de législations spécifiques à chaque pays.

active au

Qui est impacté par le RGPD ?

Toutes les entreprises faisant du business avec des citoyens européens, sans distinction de l’emplacement de base de l’entreprise.

Pénalités sévères

Amendes jusqu’à

4% des revenus globaux annuels

ou

20 Million d’Euros

en comptant le plus grand des deux

La definition d’une donnée personnelle est maintenant plus large et inclut :

Les sujets des données ont un Droit à être oublié et efface des sauvegardes,
Les utilisateurs peuvent demander une copie de leurs données dans un format portable

Toutes données stockées devrait être obtenue par consentement

Donné librement, de manière informée, et sans ambiguité

Toute Fuite de Données doit être rapportée à l’autorité de tutelle dans les **72 Heures**

La designation de Responsable de la Protection des Données sera obligatoire pour les entreprises traitant de grandes quantités de données personnelles, et des bonnes pratiques pour les autres.

La cartographie des flux de données et les évaluations des facteurs relatifs à la vie privée deviennent obligatoires pour les organisations.

Les produits, systèmes et processus doivent prendre en compte les concepts de confidentialité dès la conception lors du développement

Building a better working world

Post 25ème, perspectives internationales

GOOGLE
$57 million

La collecte par consentement ne doit être ni spécifique ni ambigue.

Février 2019: *Plus de 59 000 fuites de données personnelles ont été rapportées à travers l'Europe depuis l'introduction de le RGPD*

€5.000 pour un système de surveillance excessif

€20.000 pour ne pas hasher les mots de passes des employés

L'autorité de Protection des Données Allemande a reçue une amende de €80.000 pour avoir publié des données de santé sur internet

Malgré tout, il est attendu que 2019 verra plus d'amendes pour des dizaines et potentiellement même des centaines de millions d'euros, dûs au fait que les régulateurs revoient les archives de le RGPD concernant les fuites de données.

*DLA Piper GDPR data breach survey

EY
Building a better working world

Sommaire

- Pourquoi ce nouveau règlement ?
- **Quels sont les avantages pour votre PME ?**
- Données personnelles
- Comment passer à l’action ? utilisant une approche basée sur le risque
- Conclusion

Quels sont les avantages pour votre PME ?

1. Renforcer la confiance
2. Améliorer votre efficacité commerciale
3. Mieux gérer votre entreprise
4. Améliorer la sécurité des données de votre entreprise
5. Rassurer vos clients et donneurs d'ordre et ainsi développer votre activité
6. Créer de nouveaux services

La mise en œuvre de le GDPR pleinement mature ne concerne pas seulement le respect de la réglementation, elle constitue un avantage concurrentiel sur un marché de plus en plus consommateur de données.

EY
Building a better working world

Sommaire

- Pourquoi ce nouveau règlement ?
- Quels sont les avantages pour votre PME ?
- **Données personnelles**
- Comment passer à l'action ? utilisant une approche basée sur le risque
- Conclusion

Données personnelles
Qu'est-ce que c'est ?

Références Légales :
- 4, 9 RGPD
- 4 n-LPD

Définition des informations personnelles

Les informations personnelles sont toute information physique ou numérique relative à une personne identifiée ou identifiable.

Informations personnelles

- Informations personnelles directes ou indirectes
- Informations sensibles

Informations non-personnelles

- Informations non personnellement identifiables (non-PII) - (par exemple, prénom ou nom de famille seul, pays ou état de résidence, etc.)
- Informations « désidentifiés » ou anonymisées - (par exemple - femme blanche de 25 ans travaillant dans l'entreprise ABC)

Catégories spéciales de données / Informations personnelles sensibles

- Concerne l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance à un syndicat, les données concernant la santé ou la vie sexuelle et les données relatives aux infractions ou aux condamnations pénales.

Éléments de données personnelles

Informations relatives aux **prospects**

Informations relatives aux **employés**

Informations relatives aux **tiers**

Informations relatives aux **clients**

EY
Building a better working world

Données personnelles
Comment les identifier ?

Données personnelles physiques ou numériques

Données structures

Les données structurées désignent les informations présentant un degré d'organisation élevé.
Les données structurées ont l'avantage d'être facilement saisies, stockées, interrogées et analysées.

Données non structurées

Habituellement, la plus grande partie des données détenues par les organisations.
Fichiers tels que les e-mails et les images qui ne sont pas hébergés dans un format de données traditionnels aux bases de données.

Description	Périmètre
Données en mouvement	► E-Mail ► Transferts de fichiers ► Web ► Autres canaux
Données au repos	► Disques durs d'ordinateurs ► Serveurs / NAS ► Logiciel de collaboration ► SGBD
Données utilisées	► Périphériques de communication ► Supports de stockage ► Logiciel de communication ► Autres actions
Data in the Cloud	► Services de stockage cloud ► Services basés sur le cloud

Cadre de gestion de la maturité des données

Évaluation des processus et des politiques

- Politiques
- Parties prenantes
- Classification des données
- Systèmes informatiques

Évaluations des Systèmes Informatiques

EY
Building a better working world

Sommaire

- Pourquoi ce nouveau règlement ?
- Quels sont les avantages pour votre PME ?
- Données personnelles
- **Comment passer à l’action ? utilisant une approche basée sur le risque**
- Conclusion

Comment passer à l'action ?

Changez la mentalité!!!

- Habituellement, nous pensons à l'approche du risque pour notre entreprise
- Mais dans le RGPDPD, vous devez vous assurer de la conformité, en prenant les domaines présentant le risque le plus élevé pour les personnes concernées…

Constituez un registre de vos traitements de données

Faites le tri dans vos données

Respectez le droits des personnes

Sécurisez vos données

Utilisant une approche basée sur le risque

Les données personnelles sont au cœur de votre modèle économique, vous mettez en place des services innovants, vous traitez des données sensibles ?

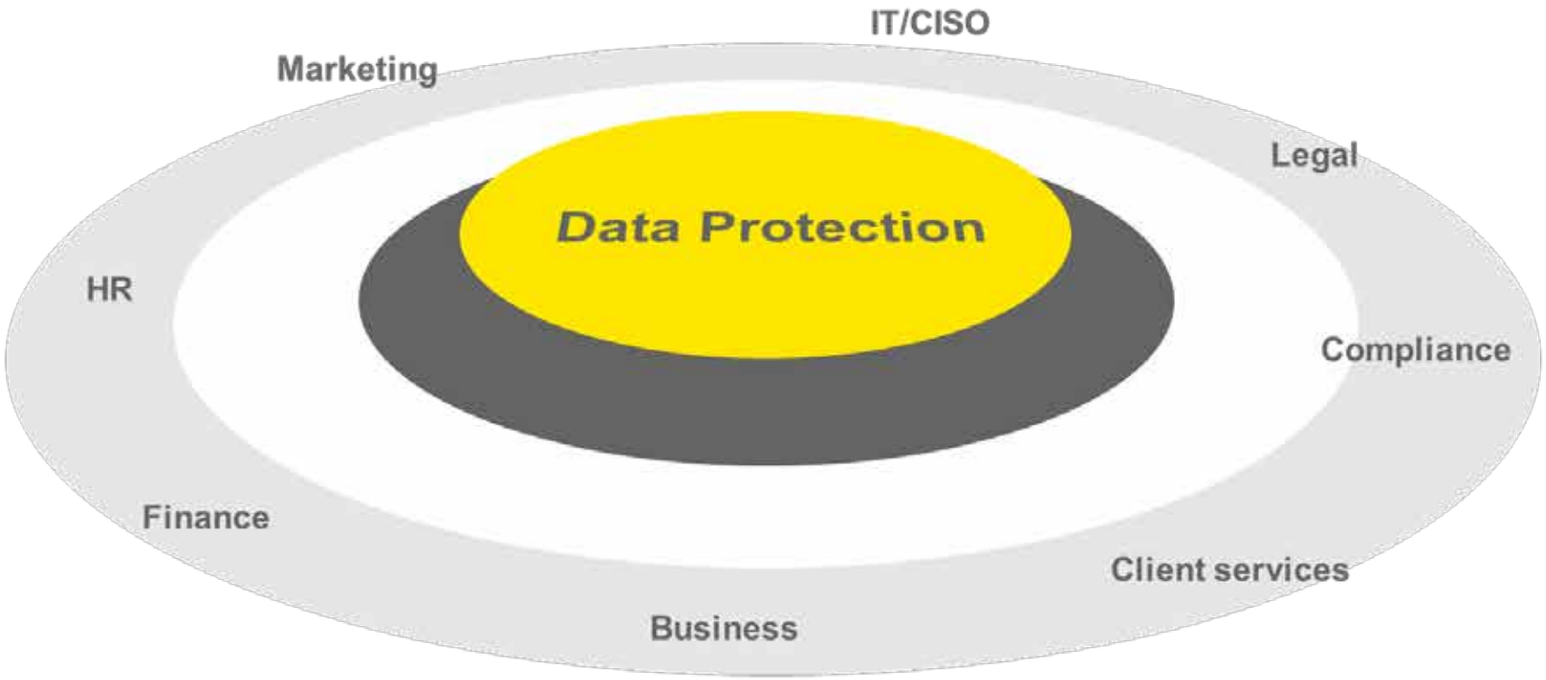
Une analyse approfondie de la règlementation est nécessaire pour déterminer les mesures à mettre en œuvre.

Certaines données ou certains types de traitements nécessitent une vigilance particulière

EY
Building a better working world

Utilisant une approche basée sur le risque

Le GDPR concerne toute l'organisation



EY
Building a better working world

Sommaire

- Pourquoi ce nouveau règlement ?
- Quels sont les avantages pour votre PME ?
- Données personnelles
- Comment passer à l’action ? utilisant une approche basée sur le risque
- **Conclusion**

Ne réinventez pas la roue

Il y a beaucoup à faire. Construire des systèmes et des processus entièrement nouveaux à partir de zéro peut être coûteux en temps et en argent.

Les meilleures pratiques basées sur la solution logicielle GDPR prête à l'emploi et l'apprentissage GDPR permettent une **approche de la conformité GDPR basée sur les risques, qui peut être mise en œuvre rapidement et facilement**.

https://www.cnil.fr/cnil-direct/attachement/1326/1366

EY
Building a better working world

Thank you

Nous vous remercions…

RGPD
Etapes clés

Stratégie de confidentialité et de protection des données

Développer une stratégie globale alignée avec la stratégie commerciale et les améliorations de processus identifiées.

Politique, normes et lignes directrices

Développer les politiques et les normes suivantes:

- Politique de confidentialité
- Mettre à jour la politique de sécurité de l'information relative à la protection des données
- Classification des données
- Politique de rétention des données (y compris la médecine légale)
- Normes et directives de protection des données

Modèle de gouvernance et Délégué à la Protection des Données

(Re-) Définir le modèle de gouvernance, y compris une description détaillée des rôles et responsabilités et la gestion des relations externes, y compris les régulateurs.

Cartographie du flux de données

Vue d'ensemble des flux de données (sensibles) au sein de l'organisation. Commencer par un inventaire de tous les processus et types de données liés à l'organisation. Sur la base d'une évaluation des risques, des priorités seront établies afin d'effectuer des évaluations des facteurs relatifs à la vie privée (ÉFVP) et de définir une feuille de route.

Responsabilité

Mettre en œuvre des mesures garantissant que les règles de protection des données personnelles sont respectées et rédiger une documentation prouvant aux personnes concernées et aux autorités quelles mesures ont été prises pour se conformer à la législation relative à la protection de la vie privée.

Protection des données

Développer et mettre en œuvre:

- Sécurité informatique
- La conservation des données
- Technologies d'amélioration de la confidentialité (PET)
- Confidentialité par design (PbD)
- Fonctionnalité de confidentialité spécifique

Droits de la personne concernée

Intégrer les droits d'accès utilisateur, notamment:

- Accès logique aux systèmes et applications
- Droit d'être oublié
- La portabilité des données

L'utilisation de données

Développer un modèle d'utilisation des données basé sur:

- Une utilisation légitime et consentie
- Un enregistrement durable

Évaluation de l'impact sur la vie privée et protection des renseignements personnels

Intégrez la confidentialité dans la conception de tous les nouveaux livrables organisationnels, par exemple:

- Les systèmes informatiques
- Processus
- Contrats

Gestion des fournisseurs et des partenaires

Définir un cadre qui gérera et guidera l'échange et le traitement des données par les fournisseurs, y compris:

- Gestion des risques
- Accords de tiers
- Surveillance de la conformité et rapports

Applications et processus existants

Intégrez la confidentialité dans vos applications et processus existants.

Surveillance et traitement des incidents

L'implémentation de:

- La surveillance de base
- La surveillance des fuites de données
- La gestion des incidents
- Reporting " Meldplicht datalekken " et autres obligations de déclaration

Sensibilisation et communication

La culture d'entreprise prenant en charge le traitement des données de l'organisation et la communication est importante. Par conséquent, l'organisation sera mise au courant pour gérer les attentes, mesurer et surveiller l'adoption.

Métriques, rapports et tableaux de bord

Définir des métriques de protection des données pertinentes, en validant les exigences avec les parties prenantes.
Implémenter une solution de tableau de bord dynamique pour gérer la mise en œuvre de la politique de protection des données.