
let's
oversee#
concordia

Les risques liés à la gestion des données: comment s'assurer?

De risico's van databeheer: hoe zich er tegen verzekeren?

André Van Varenberg

03/02/2018

CONCORDIA
Risk Management & Benefits

Sommaire

- Contexte du GDPR
- Intervention des institutions européennes
- Le RGPD en pratique:
- - le comsommateur
- - le professionnel
- Le RGPD nouvelle source de “risque”?
  - l’accountability
- Violation de données à caractère personnel
- Les solutions assurantielles
  - warning / public cible
  - où trouver les réponses
    - la responsabilité civile professionnelle
      - les clignotants / réserves

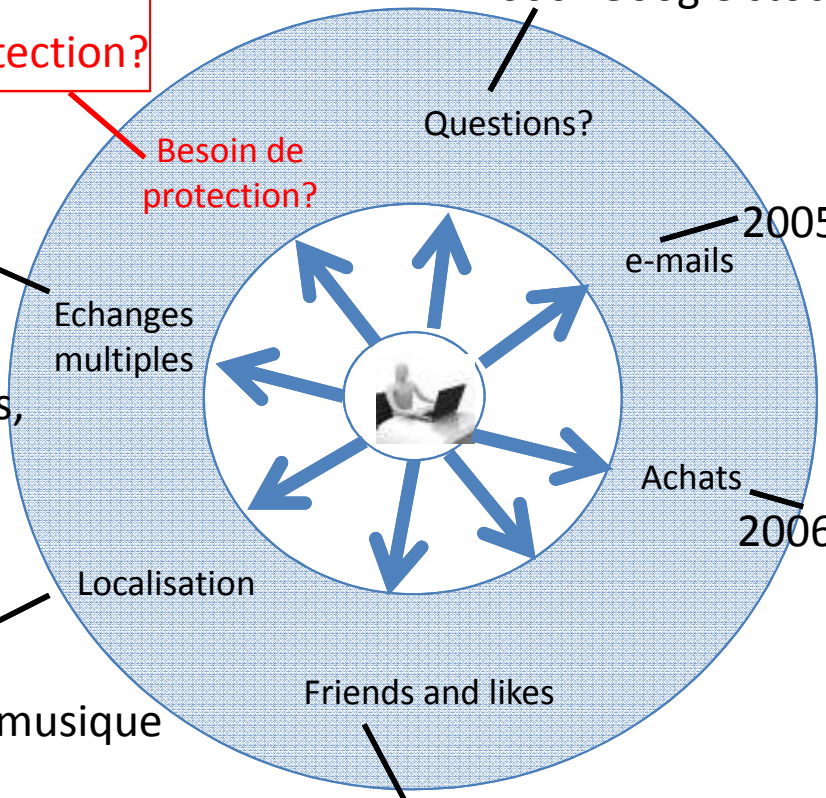
Sommaire

- l’assurance cyber risks
  - pourquoi ?
  - son rôle
  - trois axes d’intervention
- La panacée?
- L’assurance responsabilité civile des mandataires sociaux
- Conclusions

Contexte du GDPR

Qui va traiter
les besoins de protection?

2000- Google stocke mes questions



2005- Google stocke mes e-mails

2017- Google, Facebook et Apple stockent les échanges en ligne, la localisation, les photos, les videos, …

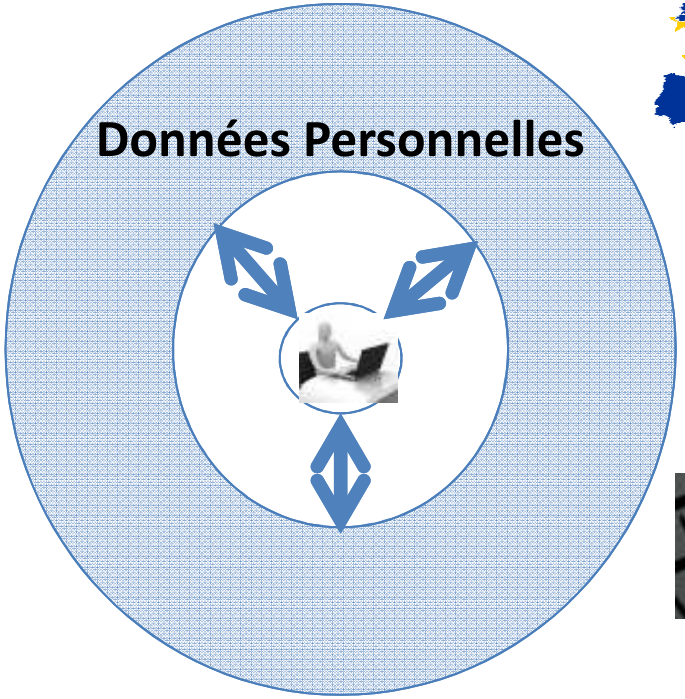
2006- Amazon stocke mes achats et mes livres

2010- Apple stocke ma localisation … et ma musique

2008- Facebook stocke mes amis et mes goûts (“like”)

Source: Portima

L'Europe veut protéger les données personnels



Règlement Général Pour la Protection des Données

Principales dispositions

- Informations à fournir sur les données et les traitements
- Consentement explicite
- Droit à la rectification, à l'oubli
- Portabilité des données
- Protection des données et Sécurité "par design"
- Notification en cas de "breach"
- Applicable hors UE

Source: Portima

Le RGPD en pratique

Comme consommateur	Comme entreprise
• Qui collecte mes données? →	• Responsable du traitement et sous-traitant
• Quelles données? →	• Registre des données + consentement/contrat
• Pour quoi faire? →	• Registre des traitements
• Qui a accès à mes données? →	• Sécurité – controle d'accès
• Comment mes données sont-elles protégées? →	• Politique de sécurité de l'information
• Comment puis-je contrôler ou adapter mes données? →	• Accès pour le client
• Combien de temps conservez-vous mes données? →	• A définir … en assurances?...
• Quelles données puis-je récupérer et comment? →	• A définir … en assurances?... • Réaction en cas de faille de sécurité

Source: Portima

Le RGPD (GDPR) nouvelle source de risque?

- Principes semblables à la directive 95/46/CE mais…
- Un nouveau principe de responsabilité (accountability) impose aux responsables du traitement la charge de démontrer qu'ils se conforment aux principes relatifs à la protection des données

Le RGPD (GDPR) nouvelle source de risque?

- Ce principe est développé

1) Au “considérant” 146
2) Au chapitre VIII

   2.1 article 82: droit de toute personne à la réparation du préjudice (matériel ou moral) subi suite à une violation du réglement

   2.2 article 83: conditions d’application des amendes administratives

   (en complément ou à la place des mesures imposables par l’autorité de controle selon l’article 58 “pouvoirs”

Violation de données à caractère personnel

Violation de données à caractère personnel (article 4/12)

Une violation de la sécurité entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données.

Les solutions du secteur de l'assurance

Warning:	le présent exposé ne s'adresse pas aux institutions hospitalières relevant des marchés publics (cahier des charges)
Public-cible:	les médecins pratiquant en tout ou partie en cabinet privé, en polyclinique…

Les solutions assurantielles

Où trouver les réponses du secteur des assurance?

- L’assurance responsabilité civile professionnelle
- L’assurance cyber-risque
- L’assurance responsabilité des mandataires sociaux (D&O)

Les solutions assurantielles

L’assurance responsabilité civile professionnelle:

Son rôle: indemniser les préjudices subis par les tiers suite à une faute professionnelle commise lors de l’exercice de votre art

Les solutions assurantielles

Les clignotants / Nos réserves

- La formulation de la définition de l'activité assurée ne prête-t-elle pas le flanc à pinaillerie?
- Les dommages immatériels purs sont-ils couverts?

  (cfr. - dommages corporels & immatériels consécutifs

  - dommages matériels & immatériels consécutifs)
- Dans l'affirmative pour quel montant?
- Les amendes administratives sont-elles assurées ou excluent (comme c'est généralement le cas)
- Dans l'affirmative jusqu'à quel plafond?
- Les cyber-risques sont-ils exclus en tout ou partie (la divulgation de données personnelles? Les dommages aux tiers engendrées par un virus? …)

Les solutions assurantielles

La solution la plus appropriée = une assurance cyber-risk

- Pourquoi? Les données à caractère personnel valent (beaucoup) d'argent
- Le RGDP va (de facto et involontairement) booster la cyber criminalité (les tentatives d'appropriation illicite de données à caractère personnel)
- Les préjudices seront de deux natures:
  - Ceux issus de la mise en cause de votre responsabilité en tant que responsable du traitement
  - Ceux affectant directement votre patrimoine
- Une assurance RC Pro c'est bien mais insuffisant

Les solutions assurantielles

Le rôle de l'assurance cyber risks

- Être l'allié de la continuité de vos activités professionnelles
- Permettre votre cyber résilience

Les solutions assurantielles

- **Trois axes d'intervention**, mais

  un seul montant assuré par sinistre et par an

  -> la responsabilité civile, RGPD inclus (les frais de défence en cas d'enquête de l'autorité de controle, les amendes administratives, l'indemnisation des tiers)

  -> les pertes financières dues à l'interruption ou la diminution de votre activité professionnelle (perte d'honoraires)

  -> les "first response" les mesures d'urgence lors des premières 48h (IT spécialiste, avis juridique, consultant de crise – réputation)

La panacée?

NON

Points d’attention:

- Le montant assuré
- La portée des garanties
- Les exclusions

L’assurance de la responsabilité civile des mandatires sociaux (D&O)

- Le GDPR prévoit des dispostions concernant la gouvernance des données

- En tant qu’administrateur ou dirigeant, il est envisageable que vous soyez tenu personnellement responsable (engageant dès lors vos biens propres) d’un cyber incident résultant de votre mauvaise gestion

Conclusions

- Le GBS met une “solution” cyber risks à disposition de ses membres
- Des réponses au RGDP se trouvent dans vos contrats
  - RC professionnelle
  - Cyber risks
  - RC mandataires sociaux
- Il est indispensable d’acquérir ces couvertures d’assurance
- L’assurance n’est pas la panacée

CONCORDIA
Risk Management & Benefits

CONCORDIA
Risk Management & Benefits