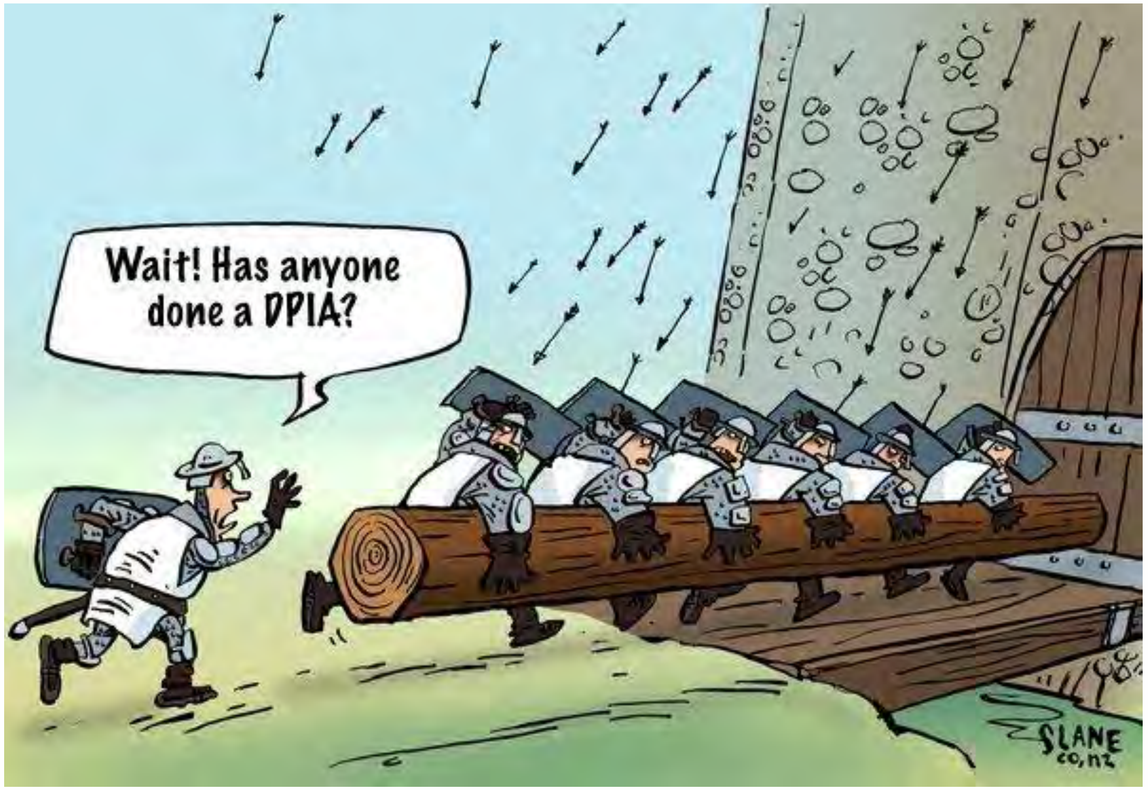
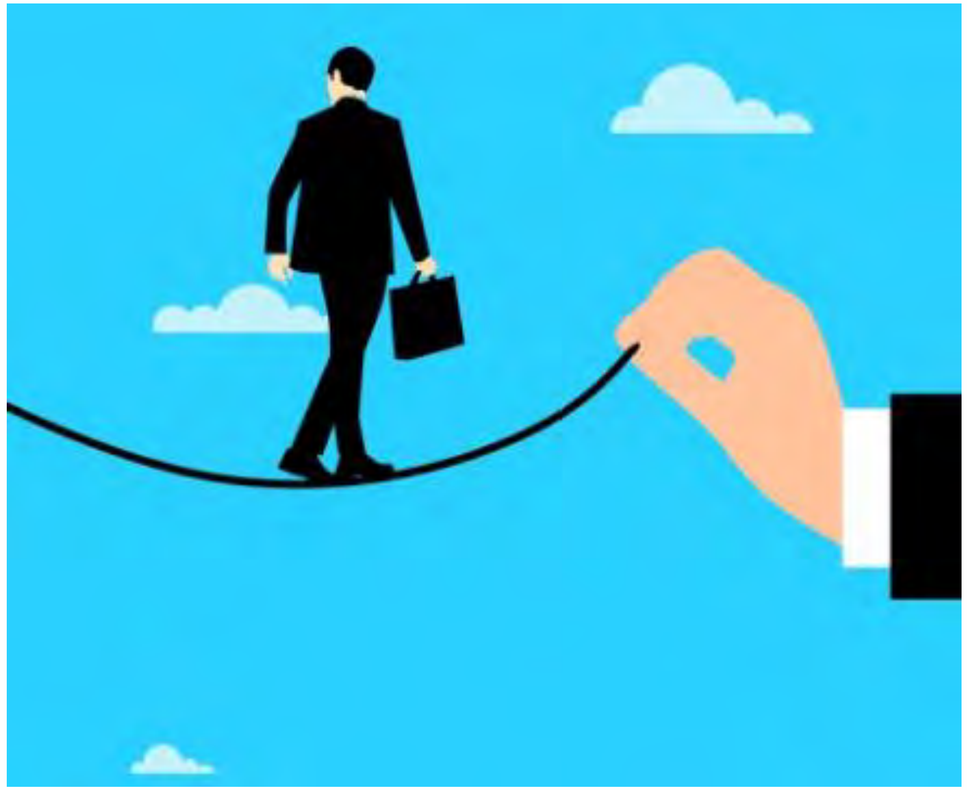
Data Privacy Information Security

PRESENTED BY: QUENTIN RANDAXHE

Bisoft

"Regis(tre) et DPO sont sur un bateau..."





Registre comme outil de pilotage/ gouvernance

"Regis(tre) et DPO sont sur un bateau..."

Le RGPD est perçu comme une charge administrative et une contrainte légale de plus.

-> Le rôle du DPO est d'informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés (art.39). Le DPO tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement (art.39).

-> Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Le registre des activités de traitements est « obligatoire » ou « recommandé » (art. 30).

-> Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (art.32).

Registre comme outil de pilotage

Pistes de réflexions:

- Utiliser le registre pour piloter/gouverner le projet de mise en conformité
- Utiliser le registre pour la gouvernance des données
- Utiliser le registre pour s’assurer des mesures de protection techniques et organisationnelles appropriées (par traitement) et ces mesures ont été appliquées aux données à caractère personnel
- Utiliser le registre pour prioriser les actions et gérer les risques
- Utiliser le registre pour définir des KPI du DPO (reporting)

Registre des activités de traitement

Art. 30

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;

g) dans la mesure du possible , une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

le nom et les coordonnées du responsable du traitement (responsable conjoint, représentant).	Nom du délégué à la protection des données

Description du traitement	Finalité(s) du traitement effectué	(Base légale)	Catégories de données personnelles concernées	Catégories de personnes concernées	Destinataires	Transferts hors UE	(Durées de conservation)	(Mesures de sécurité)

Registre comme outil de pilotage

Cas vécu dans une A.S.B.L

Registre « RGPD »	Exemple
Description du traitement	Enquête de satisfaction après une séance de formation
Finalité(s) du traitement effectué	- Gestion de la clientèle - Statistiques
Base légale	Intérêt légitime
Catégories de données personnelles concernées	Données d'identification, Données d'identification électroniques, Détails personnels, Habitudes Style de vie, Qualifications professionnelles Expérience professionnelle
Catégories de personnes concernées	Participants aux sessions de formation Formateur
Destinataires	Interne
Transferts hors UE	Non
Durée de conservation	1 an
Mesures de sécurité	Gestion d'accès, clause de confidentialité du personnel, protection du PC (login, mot de passe, antivirus,…), politique de confidentialité,… mesures de l'ASBL

"Regis(tre) et DPO sont sur un bateau..."

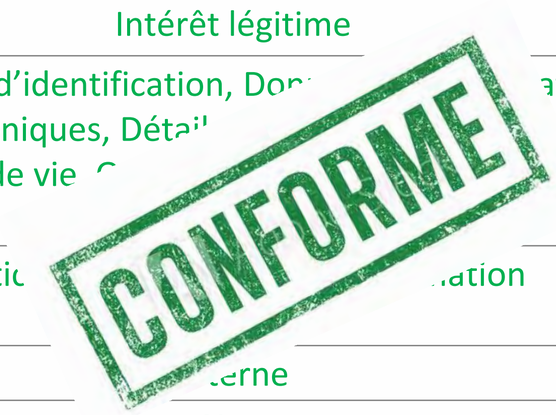
Article 39: Missions du délégué à la protection des données

1. Les missions du délégué à la protection des données sont au moins les suivantes:

a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;

2. Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Traitement
Enquête de satisfaction après une séance de formation
- Gestion de la clientèle - Statistiques
Intérêt légitime
Données d'identification, Don ation électroniques, Détai s Style de vie C
Partic iation
terne
Non
1 an
Gestion d'accès, clause de confidentialité du personnel, protection du PC (login, mot de passe, antivirus,…), politique de confidentialité,… mesures de l'ASBL



Registre comme outil de pilotage

Registre « RGPD »	Points de contrôles supplémentaires du DPO
Description du traitement	Processus défini et documenté
Finalité(s) du traitement effectué	Sous-finalités
Base légale	Vérification (procédure d'évaluation d'intérêt légitime)
Catégories de données personnelles concernées	Catégories de données sensibles
Catégories de personnes concernées	Nombres de personnes concernées
	Lieux de stockage (applicatifs et support, réseaux, personnes,…)
Destinataires	Internes (qui?) et externes (qui?)
Transferts hors UE	Identifier les Sous-traitants et destinataires
Durées de conservation	Archivage et destruction
Mesures de sécurité	- Mesures de sécurité techniques - Mesures de sécurité organisationnelles - Evaluation des risques (CIA) - Objectifs: Financiers, juridiques, organisationnelles, réputation,… - Appétence aux risques

Registre comme outil de pilotage

Cas vécu dans une A.S.B.L

Registre « RGPD »	Points de contrôles supplémentaires du DPO	Traitement de l'ASBL
Description du traitement	Processus défini et documenté	Chaque formateur utilise sa méthodologie sans formalisation
Finalité(s) du traitement effectué	Sous-finalités	Suivi individuel des participants et réutilisation des informations
Catégories de données personnelles concernées	Catégories de données sensibles	« Champs libre » ->Affiliation à un groupe d'intérêts/des organisations militantes, Données relatives au comportement sexuel, Données concernant l'état de santé psychique
Base légale	Vérification (procédure d'évaluation d'intérêt légitime)	Intérêt légitime ?
Catégories de personnes concernées	Nombres de personnes concernées	1-1000
	Lieux de stockage (applicatifs et support, réseaux, personnes,…)	Google forms (Environnement O365)
Destinataires	Internes et externes	Internes ?
Transferts hors UE	Sous-traitants	Google (hors EU)
Durées de conservation	Archivage et destruction	Papier – 1 an Digital –> Google > NEVER -> XLS -> NEVER -> BACK UP -> NEVER
Mesures de sécurité	- Mesures de sécurité techniques - Mesures de sécurité organisationnelles - Evaluation des risques (CIA) Financiers, juridiques, organisationnelles, réputation,…	60% d'adresses mail dans des brèches Appétence aux risques ++ Confidentialité – Intégrité - Disponibilité

Registre comme outil de pilotage

Registre des activités de traitement comme outil de pilotage:

- Processus défini et documenté et gouvernance des données
- Shadow IT – CISO as a friend
- Gestion des sous-traitants et transferts hors EU
- Mesures de sécurité - Evaluation des risques

Processus défini et documenté et gouvernance des données

Par analogie, la gouvernance des données peut parfaitement jouer le rôle à la fois d'orchestrateur et de garant du respect des mesures de sécurité techniques et organisationnelles prédéfinies pour chaque activité de traitement de données à caractère personnel

L'accountability sera prouvée à la fois par ***les modèles d'exécution des processus prédéfinis*** en amont et la ***traçabilité***, en aval, via les traces laissées par leur exécution sur les données.

De plus, la mise en place d'une stratégie efficace de gouvernance des données permet de ***réduire le risque de violation de données*** en limitant l'accès aux données.

Elle permet de créer un cadre qui assure ***l'exactitude, la complétude et la cohérence*** des données à caractère personnel. Elle assure également la création de cartographies de données qui facilitent la gestion transversale des données à caractère personnel et l'exercice des droits des personnes concernées (consentement, oubli, …).

COBIT-GDPR :http://www.ab-consulting.fr/blog/gdpr/rgpd/cobit-vous-aide-a-devenir-conforme-au-rgpd

Shadow IT – CISO as a friend

Au sein d'une entreprise, le terme « Shadow IT » désigne l'utilisation de systèmes informatiques, d'appareils, de logiciels, d'application et de service **sans l'approbation explicite du département informatique**.

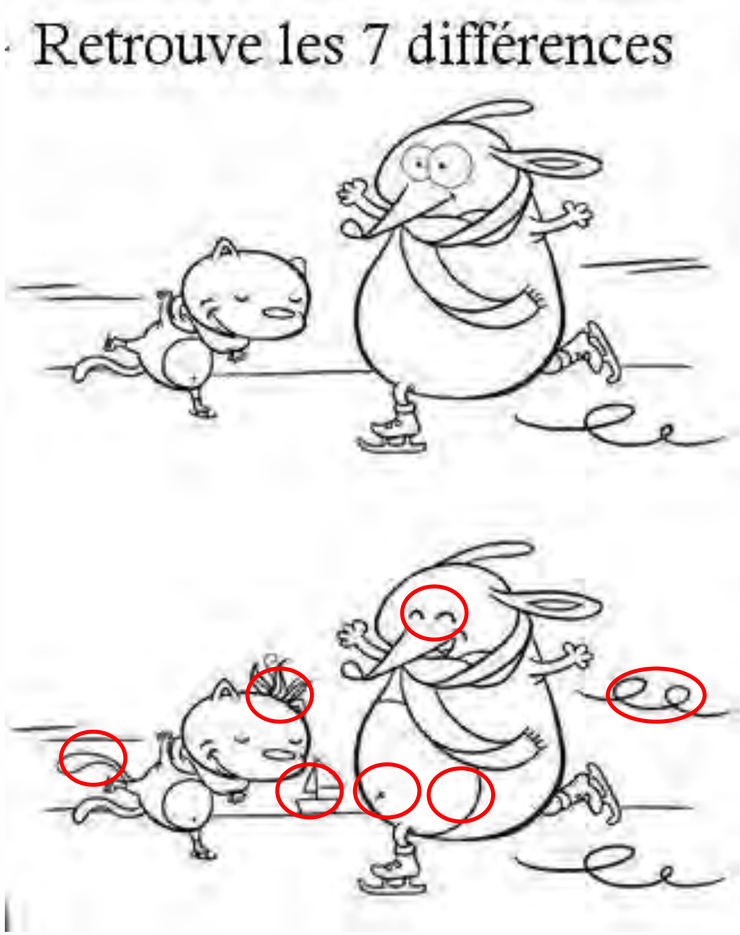
La plupart des organisations sont confrontées à une augmentation du Shadow IT. Plusieurs tendances peuvent être identifiées :

- l'essor du Cloud et la facilité d'utilisation de plateformes d'échange de fichiers. Cisco a notamment souligné le fait qu'en moyenne **98% des services Cloud** utilisés par les grandes entreprises **font partie du Shadow IT** .En 2017, une étude réalisée par le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) révèle que lorsque les DSI des entreprises interrogées répertorient en moyenne entre **30 à 40 applications Cloud, 1700 applications** sont en réalité utilisées par leurs employés.
- La transformation digitale dépasse le département IT. Désormais, des **applications comme Google Docs, Trello, Slack ou Dropbox** peuvent être téléchargés en un clic et l'intérêt d'avertir le département informatique de leur utilisation peut sembler superflu. Google dépasse déjà les 2 milliards d'utilisateurs actifs par mois. Le CA de Zoom en hausse de 355% depuis l'année passée.
- Le « Bring Your Own Device » – une pratique encourageant l'utilisation d'équipements informatiques personnels (smartphone, ordinateur personnel…) à des fins professionnelles.
- Avec la COVID -> continuité des activités (utilisation de PC privés, confinement et Netflix, CCB,…)

Gestion des sous-traitants et transferts hors EU

Comparer :

- la liste des sous-traitants (Département des achats - service marchés publics)
- Fournisseurs SI
- Inventaire applicatifs / Provider
- Registre des activités de traitement



Mesures de sécurité - Evaluation des risques

Confidentialité
Intégrité
Disponibilité

Risques Juridique
Risques Informatique
Risque Réputation
…

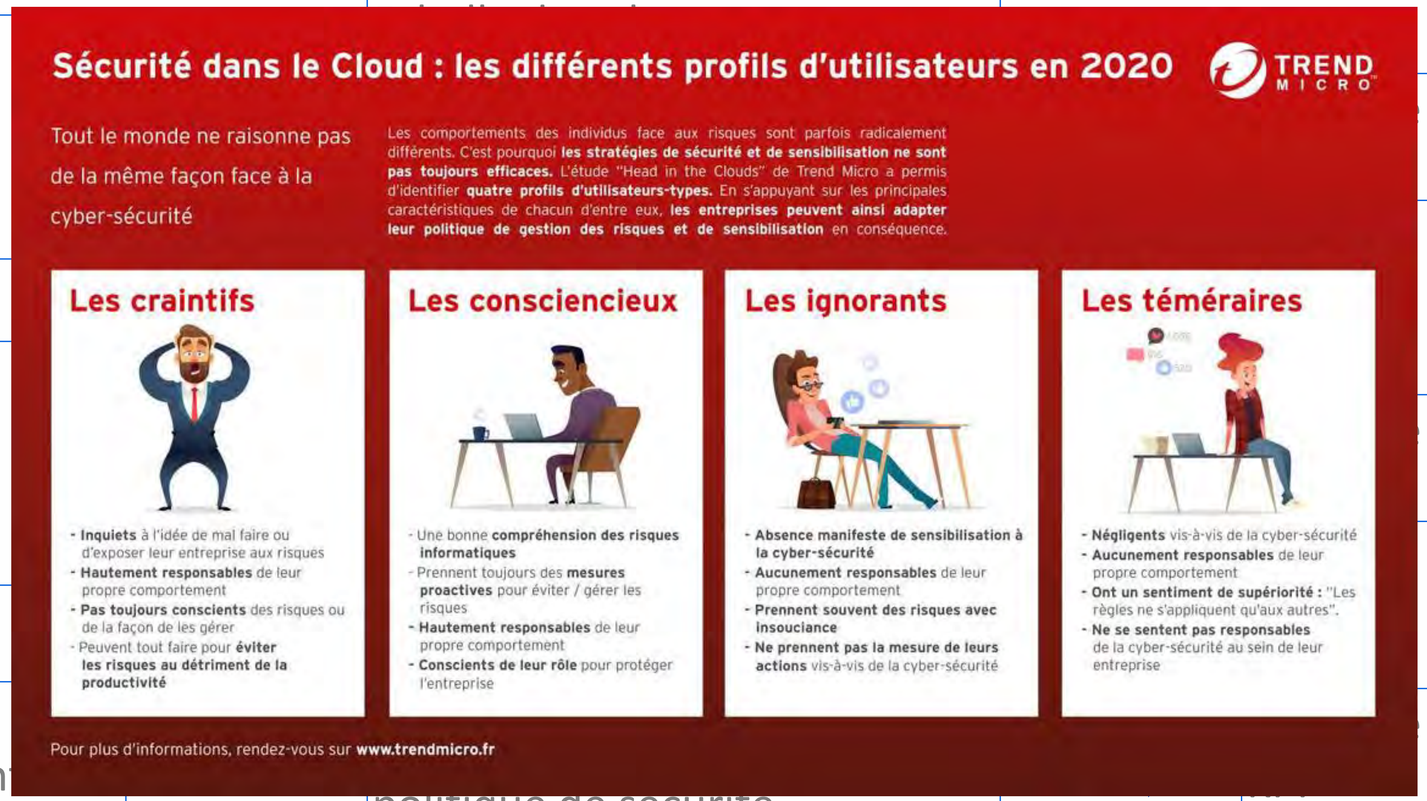
Appétence au risque du gestionnaire de traitemen

priorité

priorité

priorité

politique de sécurité…



Quelques conseils et astuces

1. Créez un sentiment d'urgence et de criticité au niveau du top management (fixez le niveau de maturité et vos objectifs en fonction de ceux-ci)
2. Inventoriez les pratiques et les référentiels utilisés actuellement
3. Considérez le RGPD comme une opportunité de créer davantage de valeur (gouvernance des données)
4. Utilisez des référentiels existant (ISO 2700X, ISO 27701, COBIT, Prosci,…)
5. Go to gemba (Lean Six Sigma – Toyota)
6. Déterminez vos KPI et fixez vos priorités (convaincre le leadership - Data)
7. CISO as a friend - gestionnaire des traitements as ambassador -> ~~GENDARME~~
8. Faire appel à des profils expérimentés, certifiés, diplomates et orientés solution

   –> solution externalisée et personnalisée avec une équipe pluridisciplinaire

Merci et prenez soin de vous

Des questions?

N’hésitez pas à nous contacter

privacy@bde-group.be

0032 2 880 12 00

A bientôt