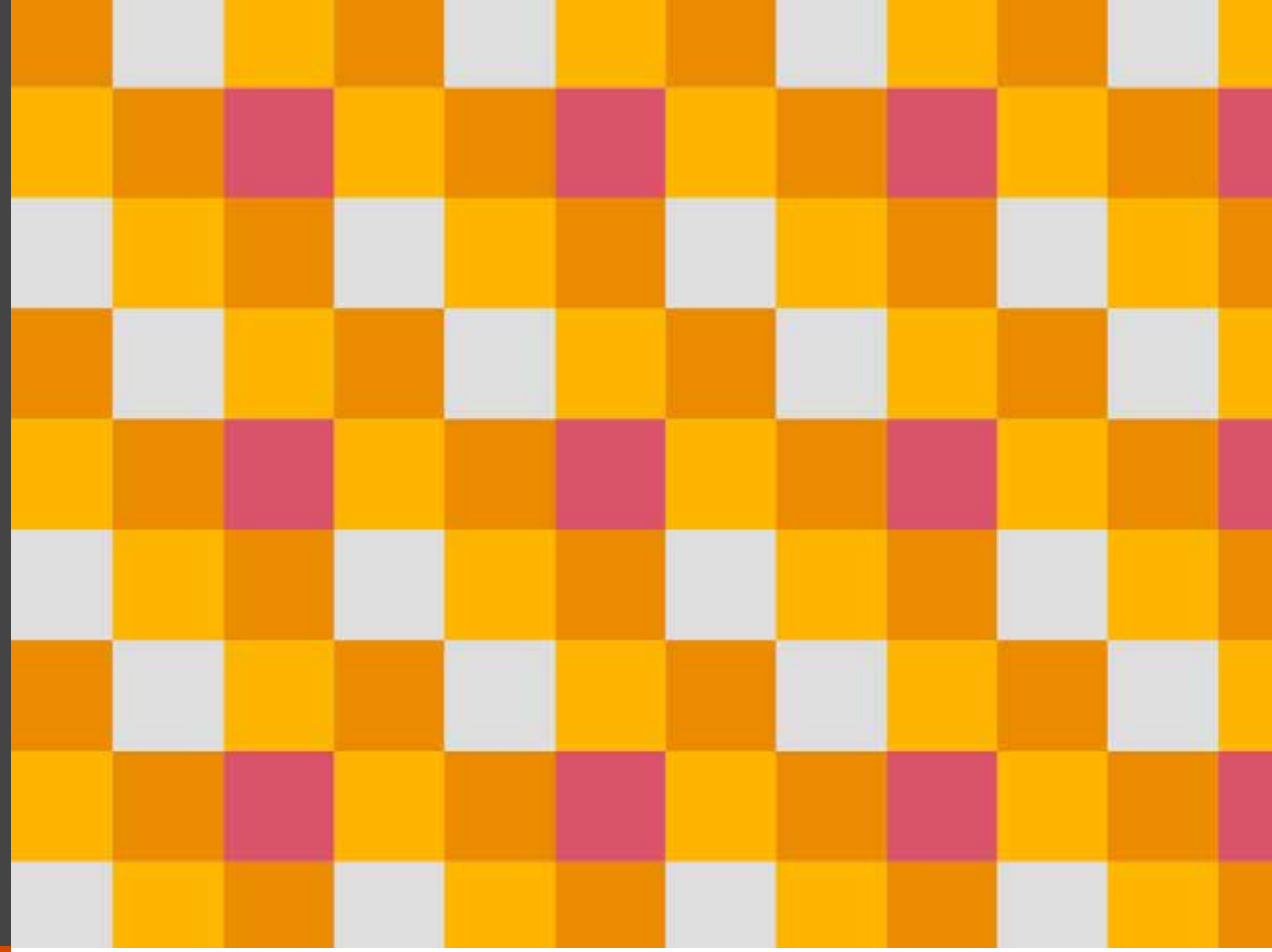
Principe de responsabilité : comment démontrer que mon entreprise respecte les exigences du RGPD ?



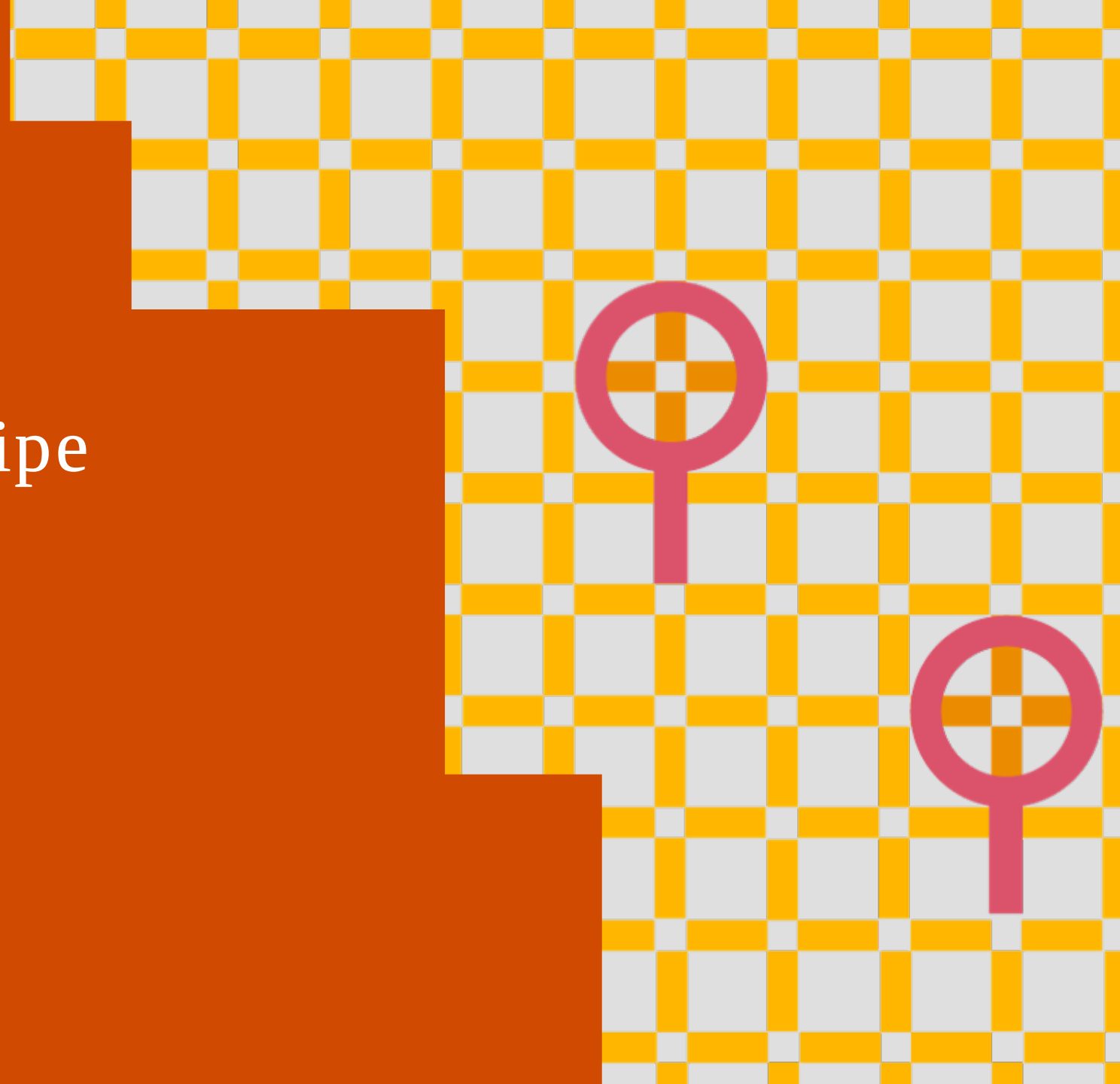
Présentation par **Vincent Colonna**
1er mars 2019

pwc

Ordre du jour

1

Qu’est-ce que le principe de responsabilité ?



Les organisations sont l'objet d'une attention croissante quant à leurs pratiques en matière de protection des données

Direction

« A quels risques de réputation, financiers et de conformité faisons-nous face ? »

« Devrions-nous reconcevoir les services que nous proposons ? »

Autorité de protection des données

« Peuvent-ils démontrer leur responsabilité et conformité au regard du RGPD ? »

Partenaires commerciaux

« Est-ce que je fais face à des risques de réputation s'ils ne respectent pas notre accord sur le traitement des données ? »

Société & Individus

« Mes données personnelles sont-elles en sécurité entre leurs mains ? »

Les exigences de responsabilité sont considérablement renforcées avec le RGPD

> L'organisation est responsable du respect des principes de protection des données définis dans le RGPD et est en mesure de démontrer qu'ils sont respectés
>
> **RGPD**
> Article 5 – par 2

Lorsqu'un traitement doit être effectué pour le compte d’une organisation, celle-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée

RGPD
Article 28 – par 1

Le principe de responsabilité implique la mise en œuvre d'actions concrètes de la part des organisations

Mettre en œuvre une approche de protection des données proactive et organisée

Être capable de montrer les actions mises en œuvre pour se conformer

Principe de responsabilité

- Sensibiliser le personnel à la protection des données
- Développer des politiques et des procédures pour gérer les données personnelles
- Conserver des traces de ce qui est fait et dans quel but

2

Comment mettre en œuvre le principe de responsabilité ?

1. Nommer un délégué à la protection des données

Obligatoire dans certains cas, encouragé pour toutes les organisations

Nomination obligatoire

- Pour les autorités et organismes publics
- Lorsque les activités de base consistent en un suivi régulier et systématique des personnes à grande échelle
- Lorsque les activités de base consistent en un traitement à grande échelle de données « sensibles »

Tâches

- Contrôle le respect du règlement
- Informe et conseille sur les obligations de protection des données
- Dispense des conseils sur les analyses d'impact vie privée
- Est le point de contact pour les individus et les autorités

Profil

- Indépendant
- Rapporte au niveau le plus élevé de la direction
- Expert en protection des données
- Dispose des ressources nécessaires
- Peut être un employé existant, une création de poste ou une prestation externe à l'organisation

Responsabilité

- Joue un rôle crucial pour aider l'organisation à être conforme au RGPD
- Ne peut pas être tenu personnellement responsable d'éventuels manquements

2. Développer et faire appliquer des politiques, standards et procédures de protection des données

Une politique de protection des données liste les exigences minimales relatives aux thèmes suivants *(liste non exhaustive)* :

- Protection des données dès la conception
- Protection des données par défaut
- Licéité de la collecte, du traitement, du transfert et de la conservation des données
- Informations à fournir aux individus
- Sécurité
- Exactitude et intégrité des données
- Droits des individus
- Registre des activités de traitement
- Gestion des violations de données

D'autres standards et procédures peuvent compléter la politique

Ces documents fournissent des lignes directrices sur une thématique précise (par exemple : traitement des données sensibles, gestion des requêtes d'individus, notification en cas de violation de données)

3. Effectuer des analyses d'impact relatives à la protection des données

Processus visant à identifier les risques d'un projet sur les droits des individus

Périmètre

- Activités de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes

Contenu

- Nature, périmètre, contexte et finalité du traitement
- Analyse de la nécessité et de la proportionnalité du traitement
- Identification et analyse des risques pour les individus (probabilité d'occurrence, sévérité de l'impact)
- Identification des mesures de réduction du risque

Consultation

- Délégué à la protection des données, si existant
- Experts et sous-traitants, si nécessaire
- Autorité de contrôle compétente, en cas d'identification d'un risque élevé qui ne peut être atténué

4. Réviser les contrats avec les tiers

Le traitement des données personnelles par un sous-traitant doit être régi par un contrat ou un autre acte juridique, de façon à ce que les deux parties comprennent leurs responsabilités

Un tel contrat doit contenir des clauses relatives aux sujets suivants :

- Objet et durée du traitement, nature et finalité du traitement, types de données et catégories de personnes concernées
- Traitement sur instructions documentées uniquement
- Obligation de confidentialité
- Mesures de sécurité appropriées
- Recours à un autre sous-traitant
- Traitement des demandes des individus
- Assistance dans la garantie du respect des obligations
- Terme de la prestation
- Audits et inspections

5. Maintenir un registre des activités de traitement et la documentation nécessaire

Le registre des activités de traitement documente pour toutes les activités de traitement :

- La finalité des traitements
- La description des catégories d'individus et de données
- Les catégories de destinataires
- Les transferts vers les pays tiers
- La durée de conservation des données
- Les mesures de sécurité organisationnelles et techniques

Exception : pour les entreprises de moins de 250 employés, seules les activités qui ne sont pas occasionnelles, qui peuvent comporter un risque pour les droits des individus ou qui portent sur des données sensibles doivent être documentées.

La documentation suivante démontre la conformité au RGPD *(liste non exhaustive)* :

- Informations requises pour les avis de confidentialité / mentions de traitement des données
- Preuves des consentements
- Enregistrements des requêtes des individus et preuves de leur traitement
- Contrats signés avec les sous-traitants
- Rapports des analyses d'impact relatives à la protection des données
- Enregistrements des violations de données
- Informations requises pour traiter des données sensibles

6. Mettre en œuvre les mesures de sécurité organisationnelles et techniques appropriées

1

Évaluation des risques et des menaces

2

Mise en œuvre des mesures de sécurité incontournables

- Pare-feu et passerelle internet
- Configuration sécurisée
- Contrôle d'accès
- Protection contre les logiciels malveillants
- Gestion des mises à jour et des correctifs

3

Protection des données stockées et en transit

- Sécurité physique
- Chiffrement
- Sauvegarde
- Désactivation ou effacement à distance
- Identification des données dans le cloud
- Authentification multi-facteur pour les accès distants

4

Sensibilisation et formation

5

Revue des logs et des alertes

6

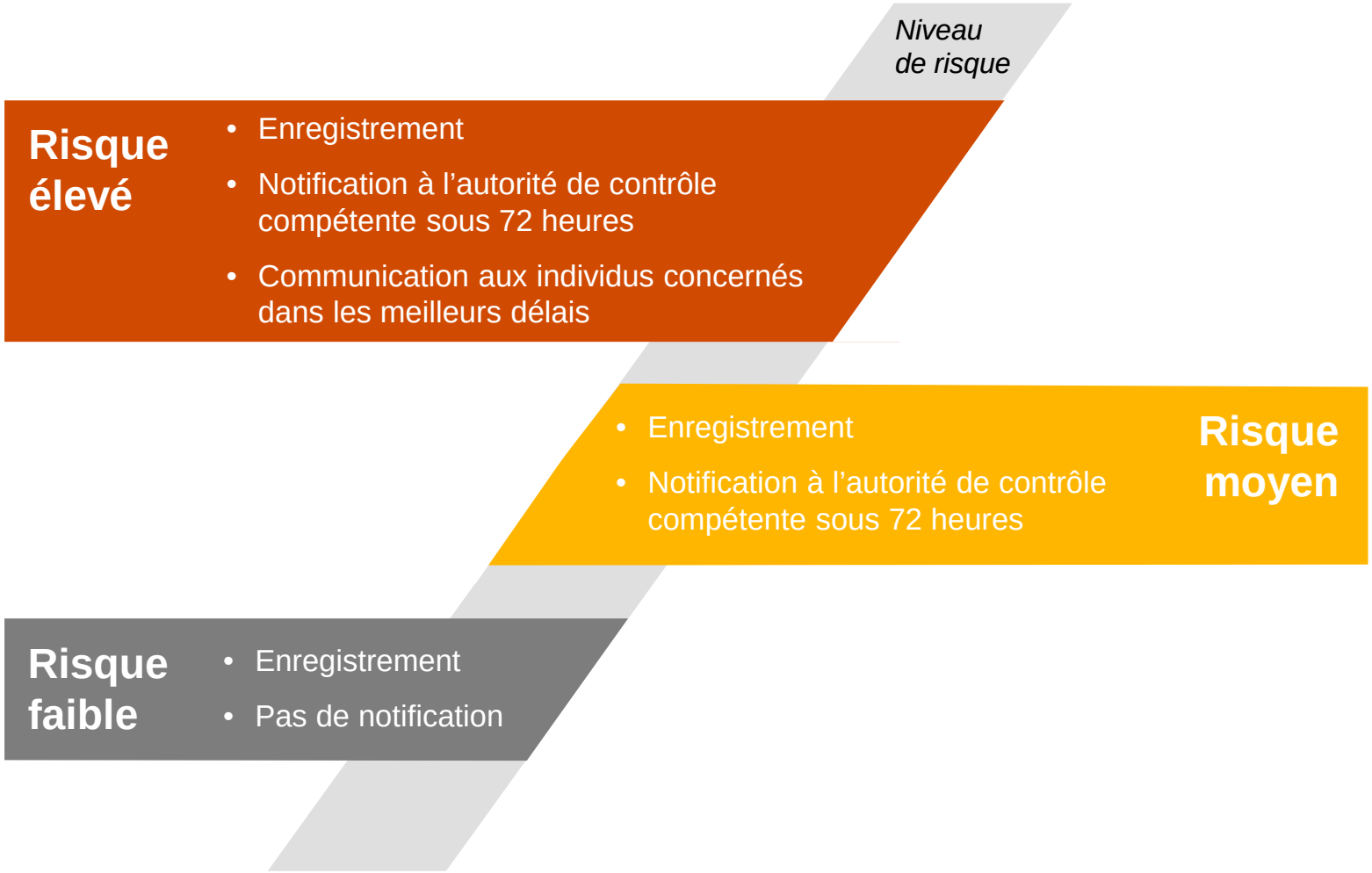
Minimisation des données, effacement et archivage sécurisés

7

Surveillance des prestataires de services IT

- Audit sécurité
- Revue des analyses de risque du fournisseur
- Revue des contrats
- Effacement des données et mise au rebut des équipements

7. Enregistrer les violations de données et communiquer avec les autorités et les individus



Recommandations

- Revoir les procédures de détection, investigation et reporting interne pour faciliter la classification des incidents en moins de 72 heures
- Maintenir un registre de toutes les violations de données, indépendamment du niveau de risqué associé

3

Comment démontrer la conformité avec le RGPD ?

Le RGPD prévoit des codes de conduite et des mécanismes de certification, encore peu répandus

Codes de conduite

Un code de conduite traduit une application concrète du RGPD à un secteur donné et se compose de bonnes pratiques

Les organisations professionnelles peuvent créer des codes de conduite pour aider le secteur qu'elles représentent

Certifications

Une certification est une assurance écrite, donnée par un tiers certificateur, qu'un processus ou un service est en conformité avec les exigences données dans un référentiel

L'adhésion à un code de conduite ou l'obtention d'une certification est volontaire, mais facilite la mise en œuvre du principe de responsabilité et aide à démontrer la conformité d'une organisation aux autorités de contrôle, aux partenaires commerciaux et au grand public

D’autres solutions pragmatiques existent pour renforcer la confiance dans les pratiques de protection des données

Auto-évaluation ou analyse d’écarts

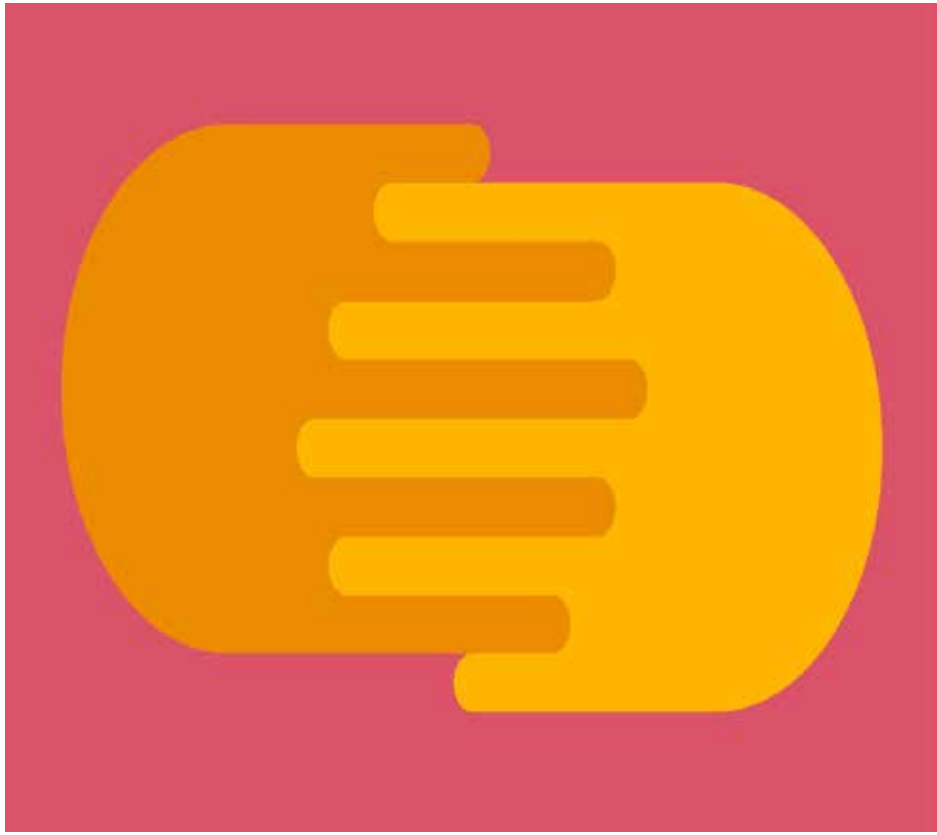
Ø Donne une indication du niveau de maturité et des écarts avec le RGPD

Certification existante (de type ISO 27XXX)

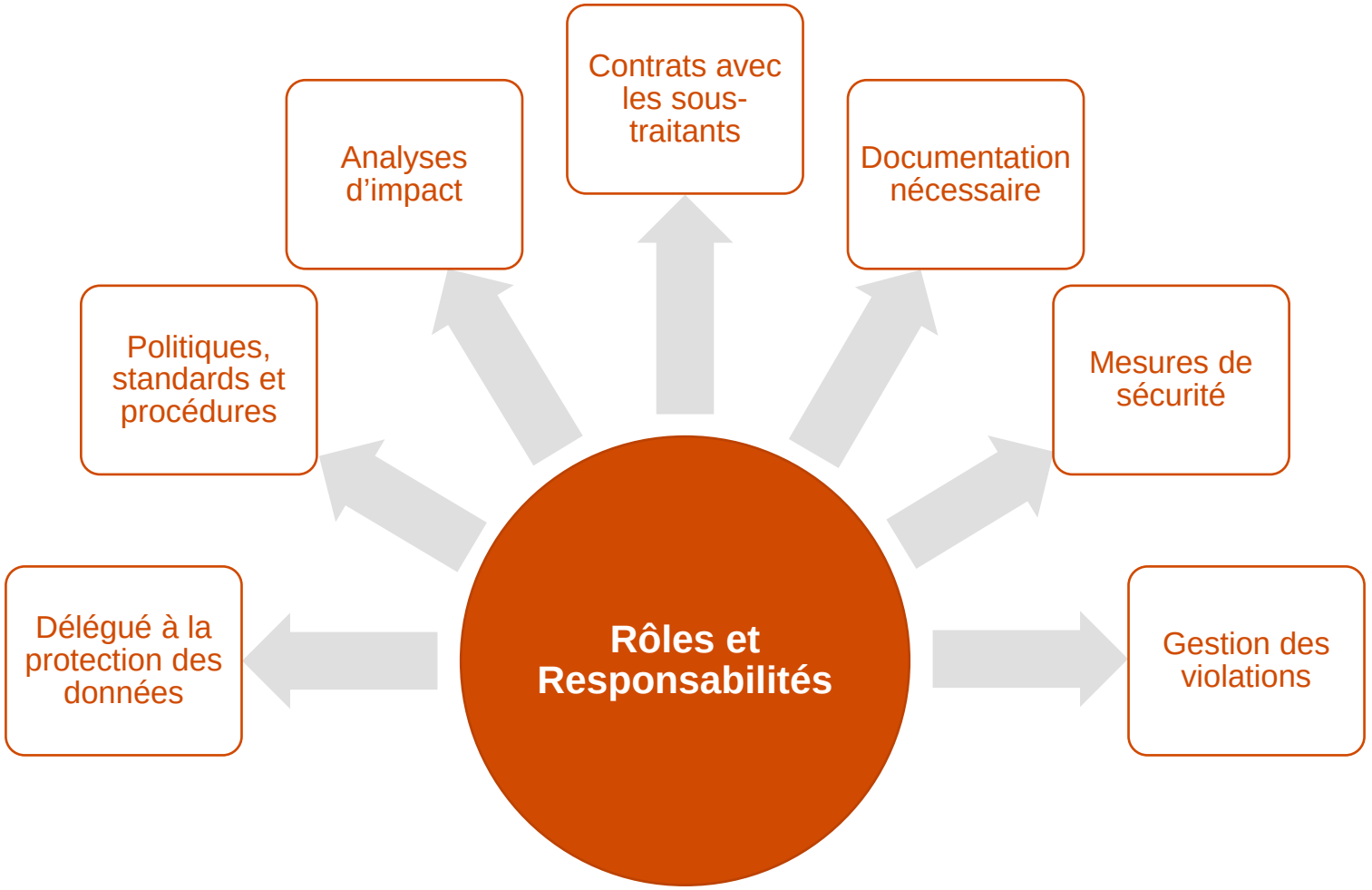
Ø Démontre qu’un système de management est établi, mis en œuvre, maintenu et amélioré de façon continue pour sécuriser / protéger les données

Rapport de contrôle incluant des contrôles relatifs à la protection des données

Ø Atteste que les contrôles relatifs à la protection des données sont définis, effectivement mis en œuvre et contribuent à l’efficacité de l’approche de protection des données



Conclusion



attesté par

- Code de conduite
- Certification
- Autre sceau de confiance

Merci pour votre attention !

Vincent Colonna

Senior Manager

Cybersecurité & Protection des données personnelles

+41 79 257 8840

vincent.colonna@ch.pwc.com

pwc.ch/cybersecurity

Le présent document est protégé par la loi suisse relative au droit d'auteur. Il contient des informations qui sont la propriété de PwC. Toute duplication, utilisation ou divulgation à des tiers de ces informations, que ce soit en tout ou en partie, sans le consentement de PwC, est interdite.

© 2019 PwC. Tous droits réservés. Dans ce document, « PwC » se réfère à PricewaterhouseCoopers SA, qui est une société membre de PricewaterhouseCoopers International Limited, chaque société membre étant une entité légale séparée et indépendante.