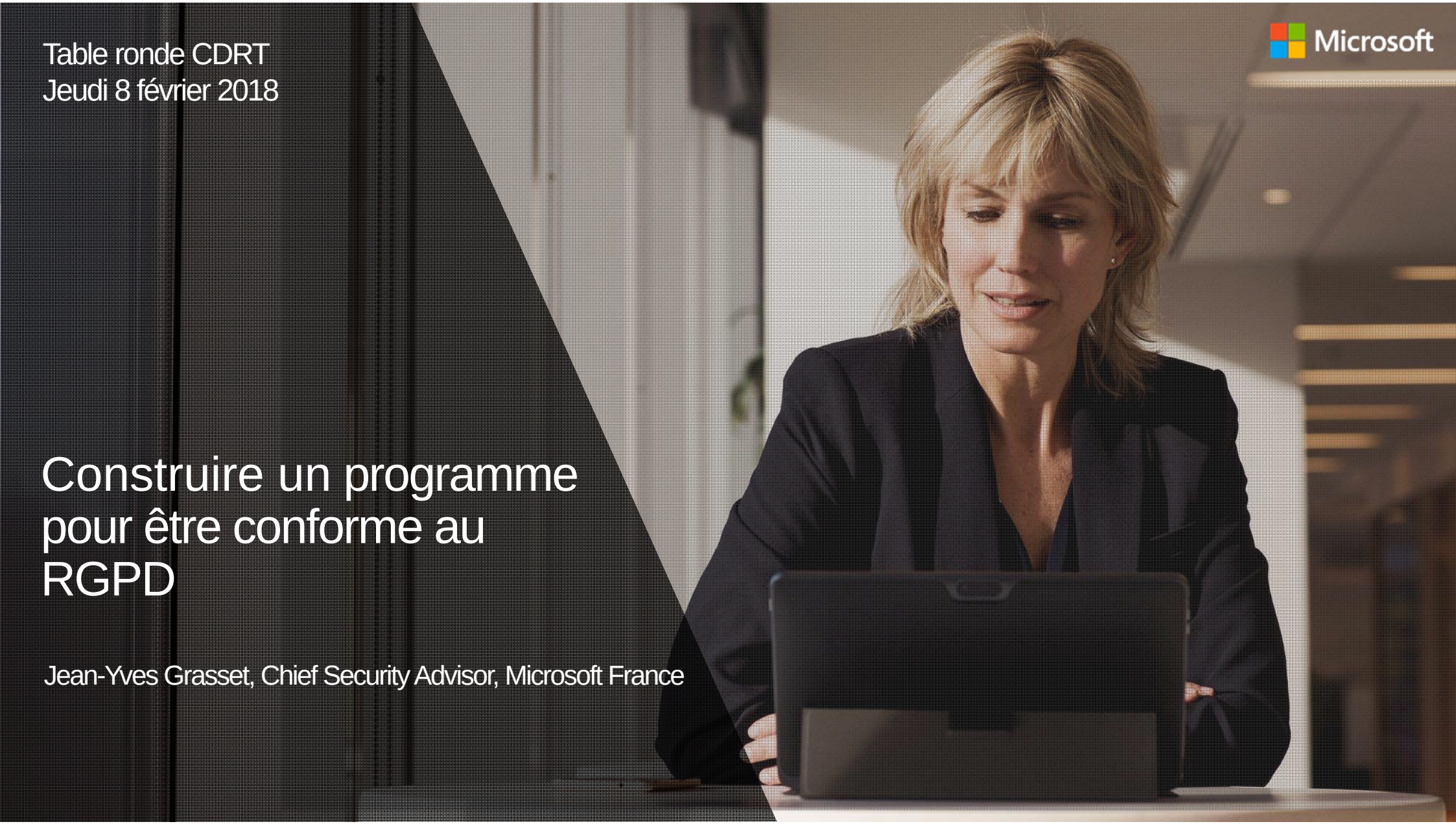
Table ronde CDRT
Jeudi 8 février 2018

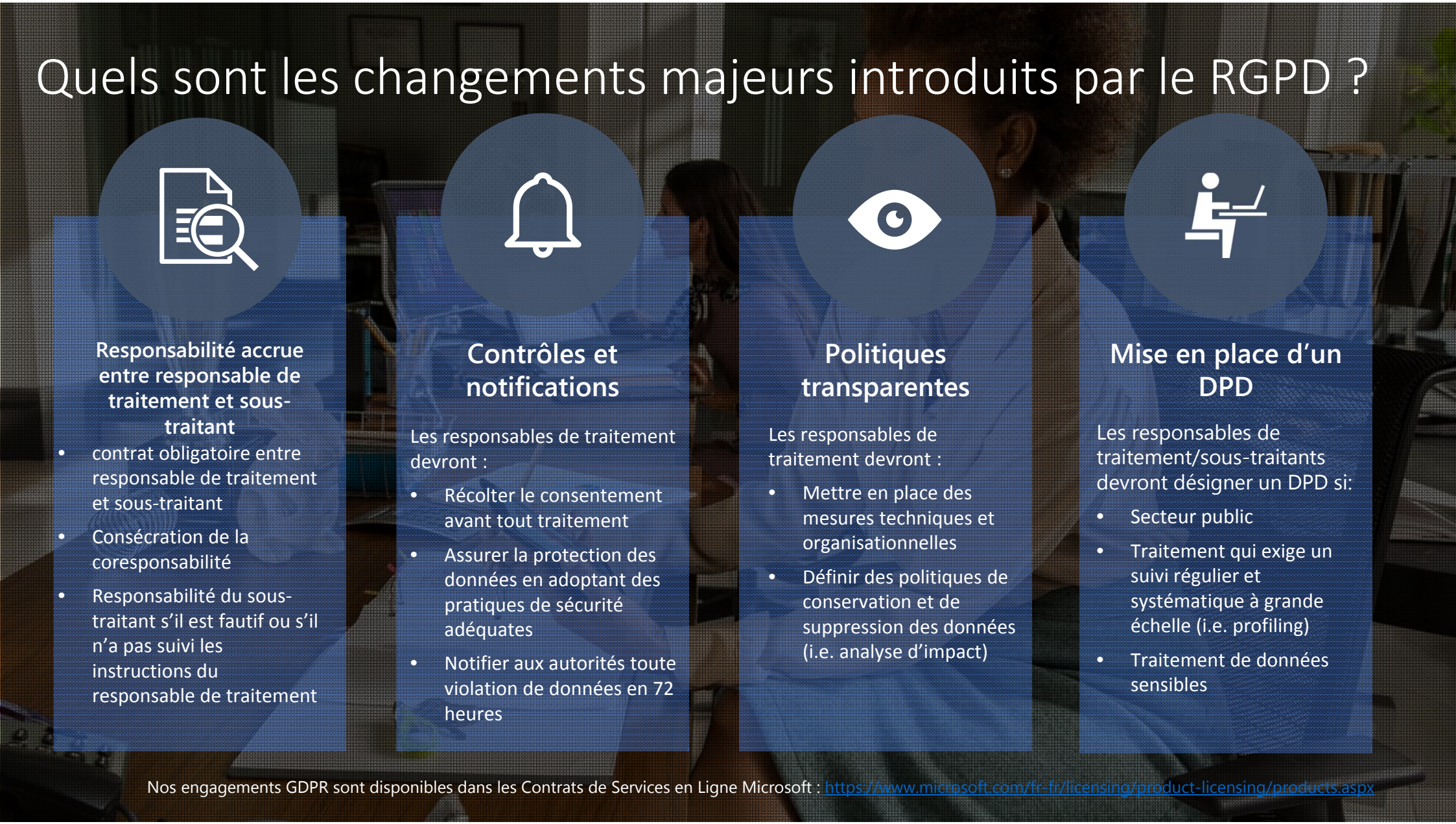
Construire un programme pour être conforme au RGPD

Jean-Yves Grasset, Chief Security Advisor, Microsoft France




Le 25 mai 2018, le règlement européen sur la protection des données personnelles RGPD (GDPR) sera applicable…
…C'est déjà demain !
http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

Quels sont les changements majeurs introduits par le RGPD ?



Responsabilité accrue entre responsable de traitement et sous-traitant

- contrat obligatoire entre responsable de traitement et sous-traitant
- Consécration de la coresponsabilité
- Responsabilité du sous-traitant s'il est fautif ou s'il n'a pas suivi les instructions du responsable de traitement

Contrôles et notifications

Les responsables de traitement devront :

- Récolter le consentement avant tout traitement
- Assurer la protection des données en adoptant des pratiques de sécurité adéquates
- Notifier aux autorités toute violation de données en 72 heures

Politiques transparentes

Les responsables de traitement devront :

- Mettre en place des mesures techniques et organisationnelles
- Définir des politiques de conservation et de suppression des données (i.e. analyse d'impact)

Mise en place d'un DPD

Les responsables de traitement/sous-traitants devront désigner un DPD si:

- Secteur public
- Traitement qui exige un suivi régulier et systématique à grande échelle (i.e. profiling)
- Traitement de données sensibles

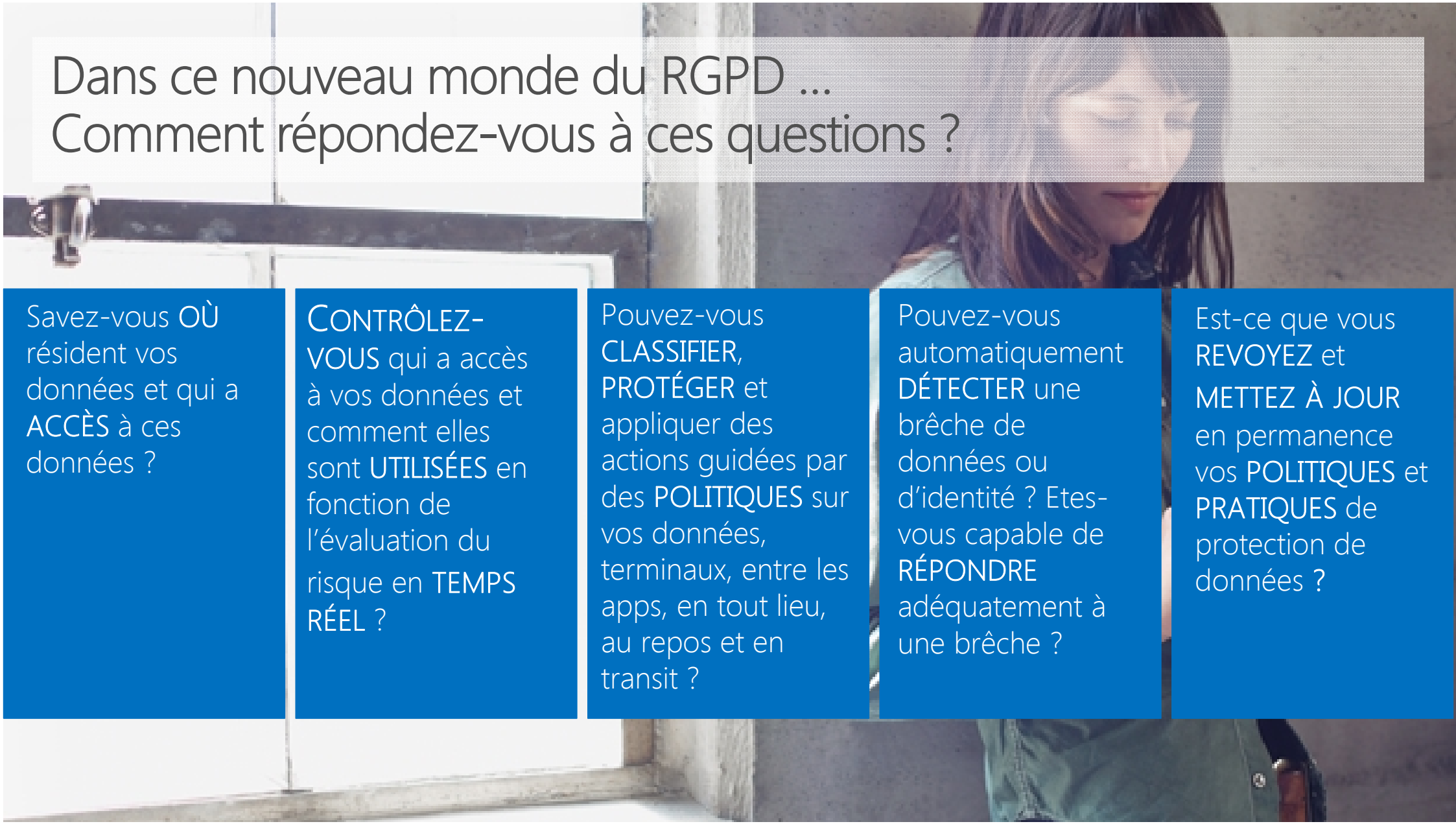
Nos engagements GDPR sont disponibles dans les Contrats de Services en Ligne Microsoft : https://www.microsoft.com/fr-fr/licensing/product-licensing/products.aspx

Notre engagement envers vous

Pour simplifier votre démarche de conformité, nous nous engageons à **être conformes au RGPD sur nos services Cloud** lorsque la loi s'appliquera dès le 25 mai 2018.

Nous **partagerons notre expérience** autour du respect de règlements complexes tels que le RGPD.

Ensemble avec nos partenaires, nous sommes prêts à vous **aider à respecter vos objectifs** en termes de politique, de personnes, de processus et de technologie dans votre démarche de conformité au RGPD.



Dans ce nouveau monde du RGPD …
Comment répondez-vous à ces questions ?

Savez-vous **OÙ** résident vos données et qui a **ACCÈS** à ces données ?

CONTRÔLEZ-VOUS qui a accès à vos données et comment elles sont **UTILISÉES** en fonction de l'évaluation du risque en **TEMPS RÉEL** ?

Pouvez-vous **CLASSIFIER**, **PROTÉGER** et appliquer des actions guidées par des **POLITIQUES** sur vos données, terminaux, entre les apps, en tout lieu, au repos et en transit ?

Pouvez-vous automatiquement **DÉTECTER** une brêche de données ou d'identité ? Etes-vous capable de **RÉPONDRE** adéquatement à une brêche ?

Est-ce que vous **REVOYEZ** et **METTEZ À JOUR** en permanence vos **POLITIQUES** et **PRATIQUES** de protection de données ?

Slide 5

A1 Shoud we add this question to one of the 'pillars in this slide, of leave it out? or add it to block 2?
Author; 13/04/2017

Une approche structurée autour de 4 piliers

Découvrir

Identifier les données personnelles dont vous disposez et où celles-ci résident.

Gérer

Gérer l'accès et l'utilisation de vos données personnelles.

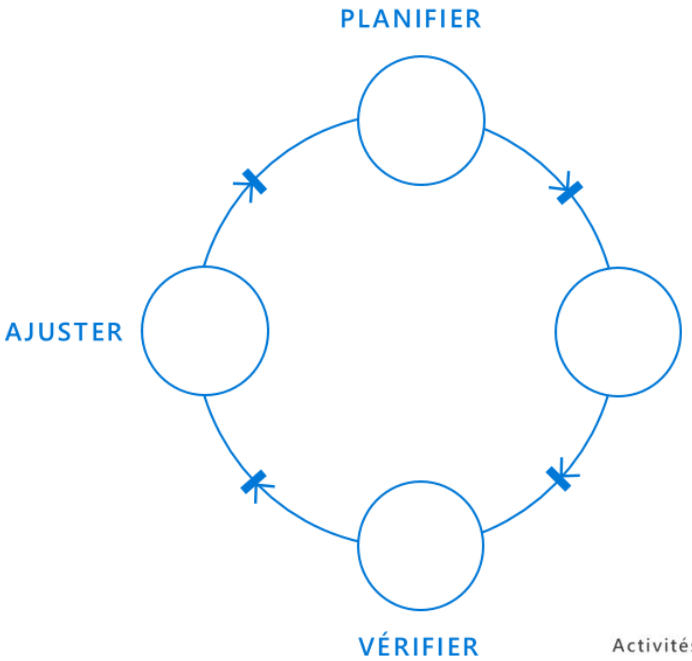
Protéger

Mettre en œuvre les contrôles de sécurité pour prévenir, détecter et répondre aux vulnérabilités et aux violations de données personnelles.

Rapporter

Maintenir la documentation requise, et gérer les demandes relatives aux données personnelles et les notifications de violation.

S’appuyer sur une approche multicycle



Activités principales

- Recruter/désigner un Délégué à la Protection des Données
- Définir la structure organisationnelle pour conduire le programme GDPR
- Estimer le périmètre du programme GDPR en matière de traitements de données personnelles
- Définir l’outillage et les divers modèles, définitions, etc. nécessaires au programme GDPR
- Définir un Framework d’analyse d’impact relative à la protection des données pour le programme GDPR
- Cartographier les traitements de données personnelles
- Procéder à une étude préalable du niveau de risque de chaque traitement de données personnelles
- Gérer les risques pour les traitements de données personnelles à risque élevé

Catégorie d’activités

DÉCOUVRIR — Identifier les données personnelles dont vous disposez et où celles-ci résident

Activités principales

- Gouverner la façon dont les données personnelles sont accédées et utilisées
- Classifier les données personnelles
- Améliorer la sécurité des traitements et des données personnelles
- Mettre en place un processus de notification de violation des données personnelles
- Améliorer la prise de conscience et la collaboration en interne

Catégories d’activités

GÉRER — Gouverner comment les données personnelles sont accédées et utilisées

Gestion du consentement et des droits des personnes concernées, conservation des données personnelles, (encadrement du) transfert de données, etc.

PROTÉGER — Prévenir, détecter et répondre aux vulnérabilités et aux violations de données personnelles

Protection des données personnelles, détection des violations et réponse appropriées

RAPPORTER — Maintenir la documentation requise, et gérer les demandes relatives aux données personnelles et les notifications de violation

Activités principales

- Suivre les traitements de données à risque élevé
- Vérifier la (trajectoire de mise en) conformité avec GDPR
- Maintenir la documentation requise pour la mise en conformité GDPR

Catégorie d’activités

RAPPORTER — Maintenir la documentation requise, et gérer les demandes relatives aux données personnelles et les notifications de violation

POUR ALLER PLUS LOIN…

→ Parcours de démos GDPR : aka.ms/mtc-securite

→ Compliance Manager : aka.ms/cmpr

→ Livre blanc « S'organiser et mettre en place les bons processus » : aka.ms/GDPRprocess

→ Livre Blanc « Aider à devenir et rester conforme » : aka.ms/GDPRinpractice

→ microsoft.com/GDPR (en 7 langues)

→ Toutes les ressources sur le Microsoft Trust Center : aka.ms/trust-center