Université IBM i 2017

17 et 18 mai – IBM Client Center de Bois-Colombes

S7 – Préparer la GDPR

Les premiers pas vers la mise en conformité

Mercredi 17 mai – 14h00-14h40

Julian Gouez – Helpsystems

Julian Gouez, Regional Sales Manager

HelpSystems, EMEA (from Tango/04 business unit)

Rejoint Tango/04 en 2006.
Ex Directeur Avant-ventes de Tango/04.
Responsable Commercial France
En charge des partenariats EMEA

Contact: julian.Gouez@helpsystems.com
+34 637 456 130

L’agenda

- Qu’est ce que le GDPR et quel est son but?
- Vos droits selon le GDPR
- GDPR: implications pour l’entreprise?
- Comment se preparer?
- Helpsystems peut vous aider
- Offre gratuite d’évaluation aux participants de l’Université
- Q&R

Qu’est ce que le GDPR?

GENERAL **D**ATA **P**ROTECTION **R**EGULATION

(**R**égulation **G**énérale pour la **P**rotection des **D**onnées)

Un nouveau cadre legal de l’Union Européenne, remplaçant l’actuelle *“Directive de Protection des données 95/46/EC”*.

Adopté par le Conseil puis voté par le Parlement européen le 14 avril 2016

GDPR entrera en application en **Mai 2018**

Règlement vs. Directive

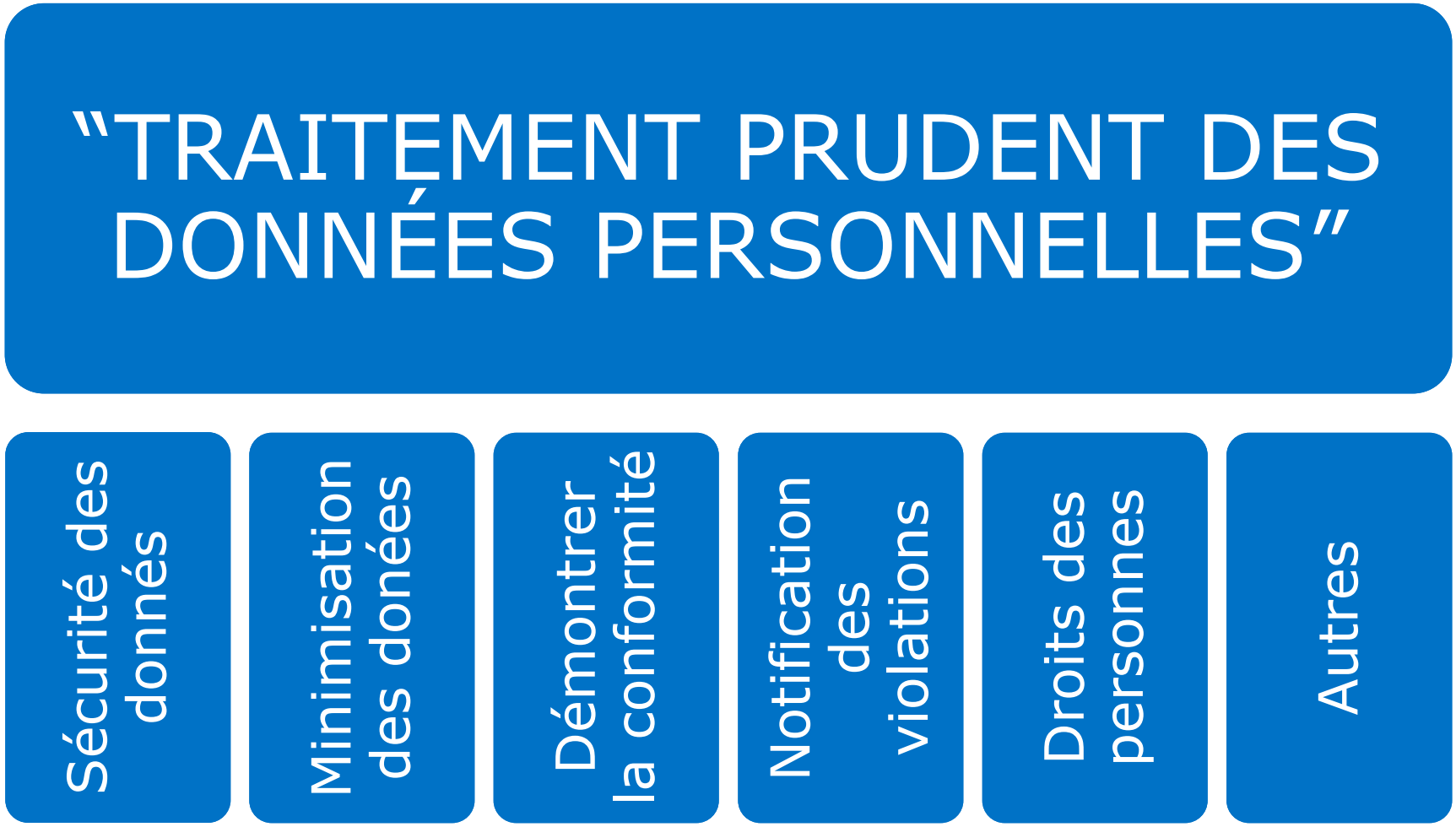
Qu’est ce que le GDPR?

- Objectifs:
  - la protection de **vos** données personnelles
  - la définition de comment les organisations peuvent/doivent stoker puis détruire les informations une fois devenues inutiles.

- Périmètre:
  - Transfert de données entre membres de l’UE
  - Transfert vers l’extérieur de l’UE

- Actions:
  - Gestion des cas de violation de données personnelles
  - Capacité de sanctions aux organisations impliquées

Qu’est ce que le GDPR?



La GDPR c’est pas pour nous!

Qu’est ce qu’une donnée personnelle?

- Nom, prénom, mail, tel, date de naissance, nº de CB, IP etc.

Mais aussi:

- *“Donnée identifiée ou identifiable d’une personne physique permettant une identification directe* ***ou indirecte****.”*

Qu’est ce qu’un traitement des données?

- *“Collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication, transmition ou diffusion”* de données à caractère personnel.

Les droits du GDPR

Les droits du GDPR (1/2)

1. **Droit à l'information**
   - Transparence sur l'utilisation faite de vos données

2. **Droit d'accès**
   - Fournir un accès à vos propres données E
   - Expliquer l'utilisation qui en est faite
   - Toute autre information associée à vos données personnelles (gout, habitudes etc.)

3. **Droit de rectification**
   - Droit de voir vos données rectifiées si elles sont incomplètes ou inexactes

Les droits du GDPR (2/2)

1. **Droit à l'oubli**
   - Droit de voir vos données supprimèes quand il n'existe plus de raison valable de les conserver. (Fin de la relation commerciale)

2. **Droit de restriction ou d'opposition au traitement et son automatisation**
   - Vous pouvez autoriser le stockage des vos données et pas leur traitement (pas d'analyse comportemental, pas de tri etc)

3. **Droits de portabilité**
   - Vous pouvez exiger une copie des informations vous concernant et les reutiliser à votre convenance.

helpsystems
Tech solutions. Human support.

GDPR et l’entreprise

helpsystems
Tech solutions. Human support.

Le saviez-vous?

87%

des entreprises considèrent les failles de sécurité comme le principal facteur de risque.

MAIS

Seuls 5% des CxO estiment disposer de l'expertise suffisante à sa bonne gestion

Les notification de violation de données sont en constante augmentation.

Quelques cas récents

TalkTalk

TESCO

YAHOO!

Quelles conséquenses?

Des amendes

1. **2% du total du chiffre d'affaire mondial**
   - En cas de non obtension du consentement
   - Echec à l'implantation des mesures de protection des données
   - Non definition écrite de procédure
   - Non declaration de violation à l'EDPB (European Data Protection Board) quand celle-ci est obligatoire

2. **4% du chiffre d'affaire mondial**
   - Non respect des consignes de l'autorité de supervision
   - Non adhésion aux règles internationals de la GDPR pour le transfer de données
   - Echec à se soumettre aux principes basiques de traitement de données impliquant un consentement

Comment s’en prévenir?

Responsabilité et bonne gouvernance

Vous devez veiller à ce que des mesures **techniques** et **organisationnelles** appropriées soient mises en place pour assurer conformité et transparence sur l’utilisation faite de vos données

Comment se préparer?

Mesures Organisationnelles

1. **Operateur**
   - Traite des données au nom du contrôleur. C'est l'organisme ou personne traitant les données personnelles (employé, développeur, fournisseur externe, société d'hébergement cloud etc)

2. **Controleur**
   - Contrôle et assure la conformité quant à la manière dont vos données sont traitées (par exemple le CIO, le CISO)

3. **Data Protection Officer**
   - Obligatoire si:
     - Organisme public
     - Traitement de données de caractère "sensible" ou pénal
     - toutes les entreprises qui procèdent à des « ***opérations de traitement*** »
     - lorsque le droit national d'un Etat membre de l'UE l'impose (Pas la France … pour l'instant)

Mesures Techniques

Mise en place de

1. **Politiques et procédures**
2. **Audit**
3. **Formulaires de consentement**
4. **Révision des clauses légales**
5. **Utilisation de certificats**
6. **Cryptage des données**
7. **“Pseudonimisation” – “Anonymisation”**

Focus sur Pseudonimisation/Anonymisation

Pseudonymisation: Il existe une clé. Processus réversible

Anonymisation: Aucun lien possible à la personne

Evidemment inutile pour une utilisation en Prod.

Utile pour le BI par exemple, pour des études de marché, étude produit etc.

ENJEU

Aucune donnée ne doit sortir de la prod sans être anonymisée ET vous devez protéger la prod.

Préparez-vous au GDPR

- Indentifiez les données concernées
- Créez un cadre de gestion
- Actualisez les procedures
- Préparez-vous à une faille

Identifier les données concernées

- Assurez-vous de **connaitre les données** que vous conservez (peut-être traitez vous plus de données personnelles que vous ne le pensez)
- Révisez **pourquoi** vous conservez ces données.
- Déterminez quelles sont les données personnelles et quelle est la part des **identifiants uniques**. (GDPR considère les ID et la géolocalisation comme des données personnelles). Sont-elles utiles?
- **Pseudonymisation** des données: utilisez le cryptage pour render les données personnelles non-identifiables
- Identifier les **documents** d'ou proviennent ces données
- Documentez tous les **échanges de données** avec des tiers

Créez un cadre de gestion

- Documentez un **organigramme** désignant une structure de gouvernance
- Nommez ou embauchez des employés pour assumer de **nouvelles tâches**
    - Agent de protection des données
    - CSO ou administrateur de la sécurité
- Sensibilisez vos équipes en **interne**
- Exécutez un plan de **formation** des employés

Actualisez les procédures

- Révisez les **politiques existantes** et évaluez leur pertinance
- **Communiquez** sur les données privées conformément à la GDPR, en particulier:
  - Le droit d'accès
  - Les périodes de conservation
  - Le droit à la rectification
- Assurez-vous que les consignes soient **facilement accesibles**
- Identifiez les **risques non couverts**
- **Minimisez** les données. De quelles données avons-nous réellement besoin?

Préparez-vous à une violation de sécurité

- Comment doit-on communiquer une violation de données?
  - **En 72h** contre “un délai raisonnable” aujourd’hui…
- Testez les **procedures de notification** de faille
- Mise en place de **procedures internes d’alerte**. Faites de vos emplyés des partenaires.
- **Contention**: ´Comment stopper une violation au plus vite?
- **Actions correctives**: comment prévenir une nouvelle faille?
- Mise en place d’un plan d’amélioration continue

Helpsystems peut vous aider

helpsystems
Tech solutions. Human support.

Qui sommes nous?

Powertech: une suite dédiée à la sécurité IBMi

3…2…1… Go!

Demandez votre consultation gratuire *GDPR Ready?*

- Une session de 30 minutes avec notre équipe
- Lancez une évaluation gratuite du niveau de sécurité de votre IBM i

www.helpsystems.com/gdpr-ready