Université IBM i 2018

16 et 17 mai

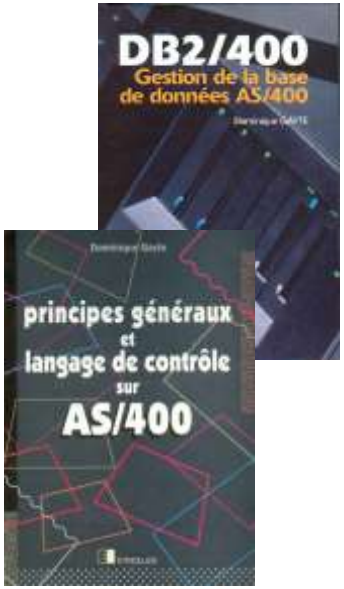
IBM Client Center Paris

S04 - GDPR et IBM i : retour d'expérience

Dominique GAYTE
NoToS
dgayte@notos.fr – www.notos.fr

NoToS

- Expertise autour de l'IBM i
  - Regard moderne
  - Sécurité
  - Service
    - Formation, audit, développement…
- PHP sur IBM i avec Zend
  - Modernisation
  - Web Services…
- Développement de progiciels
  - Modernisation à valeur ajoutée des IBM i



Plan de la présentation

- Rappels
- Etendue
- Audit de Sécurité
- Mise en conformité site Web
- Le registre de traitement
- Traçabilité

Rappels

- Il y a un an, je vous présentais « Les atouts de l'IBM i pour répondre aux contraintes du GDPR »
- A télécharger
  - Sur le site d'IBM
  - Sur le site de NoToS
- L'objet de ce séminaire est de faire un point sur plus d'une année d'accompagnement à la mise en conformité

Qu’est-ce que le GDPR ?

- GDPR: *General Data Protection Regulation*
- En français RGPD : Règlement Général sur la Protection des Données
- Règlement européen applicable à partir du 25 mai 2018
  - Obligatoire
  - Pour tous États membres de l'Union Européenne

> *Les personnes physiques doivent avoir le contrôle de leurs données à caractère personnel !*

  - Pour en savoir plus, voir la présentation de l’an dernier !
- Est en train de devenir une législation de référence au niveau mondial
  - Le Congrès des États-Unis l’a cité à plusieurs reprises à propos de l’affaire *Cambridge Analytica* lors de l’audition du dirigeant de Facebook

Projet de loi relatif à la protection des données personnelles

- Adopté par le Sénat en deuxième lecture le 19 avril 2018
- Renforcement des pouvoirs de la CNIL qui devient l'organisme de contrôle
- Il n'y a plus de déclaration préalable mais un contrôle à posteriori
  - Sauf pour les traitements des données les plus sensibles
    - Données biométriques
    - Numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR)
- Plus de protection pour les mineurs
  - 15 ans : âge à partir duquel un mineur peut consentir seul au traitement de ses données personnelles
- Education : sensibilisation du corps enseignant et des élèves aux problématiques liées à la protection des DCP

Le GDPR : pour qui ?

- Tous les professionnels
- Toutes les structures que nous avons étudiées étaient concernées
  - PME/PMI (TPE)
  - Associations, caisses, assurances
  - Collectivités
  - …
- Même si elle n’ont pas de rapports avec les particuliers
- Même si elle n’ont pas de site Web

Les principaux domaines concernés

- Les Ressources Humaines
  - A partir du moment où vous avez un collaborateur, vous êtes concernés
  - Même si la paie est externalisée
  - Contrats de travail, bulletins de salaires…
  - Attention aux données « sensibles » : médical, notamment
  - Attention au papier !
- La gestion commerciale, l'ERP
  - Souvent des adresses mails, des contacts nominatifs
- Tout ce qui est relation avec le particulier
  - BtoC
  - Mutuelles, caisses, assurances…
- Sites Web non statiques

Le 25 mai 2018

- Ce n’est pas la fin du projet
- Au contraire, c’est là que tout commence !
- Le GDPR doit s’envisager dans le temps
- Il faut s’habituer à vivre avec et c’est justement l’objectif de ce règlement
- Tout nouveau projet Informatique devra se faire dans le contexte du GDPR
  - Protection des Données à Caractère Personnel (DCP) dès la conception
  - Sécurisation des DCP par défaut
  - Tenue du registre des traitements
  - Protection des communications (voir session 52 sur SSL/TLS)

La mise en conformité est porteuse de valeur

La mise en conformité doit être vue comme une chance et non comme une charge!

- Prise de conscience de défauts dans l'organisation
- C'est l'occasion de redéfinir certains processus
- Conduit à une meilleure sécurisation du SI
- Permet de mieux connaitre son SI
  - Cartographie des DCP
  - Données structurées (bases de données) : relativement maitrisées
  - Données non structurées : non maitrisées
    - Varonis DatAdvantage orienté Active Directory
    - IBM StoreIQ dispose de nombreux connecteurs
      - 75 sources de données et 450 types de fichiers

Droits de la personne concernée

- Durée de rétention
  - Problématique car généralement non géré
  - Il faut mettre en place des processus pour l'acquisition (consentement explicite) et la suppression des DCP
- Droit à l'oubli
  - Ne s'applique pas s'il y a une obligation légale
  - Pendant la durée de la contrainte
- Portabilité
  - « *On verra bien si on a une demande….* »

Données sensibles

- Les données sensibles sont définies par le GDPR
  - Données génétiques, biométriques
  - Relatives à la santé, à la vie ou à l'orientation sexuelle
  - Révélant l'origine raciale ou ethnique, les opinions politiques les convictions religieuses ou philosophiques, l'appartenance syndicale
- Par défaut, interdiction de les traiter !
- Il ne faut pas les confondre avec celles qui font courir un risque important à la personne physique
  - Numéro de CB
  - Il faut leur prêter une attention particulière (sécurisation, cryptage, archivage…)

Le site web

- Le site web doit être mis en conformité
  - Sauf s'il est purement statique
- Les cookies
  - Souvent utilisés simplement pour tracer les actions sur le site (Google Analytics)
  - Il faut demander le consentement explicite de l'utilisateur s'il y a un lien possible avec la personne physique (adresse IP, par exemple !)
  - Attention dans ce cas, la durée de conservation de ces données est limitée à 13 mois
    - Suppression au-delà
    - Donc nouvelle demande de consentement en cas de nouvelle visite du site

Le site web (2)

- Pour les données recueillies par des formulaires divers
  - Information sur les finalités des traitements
  - Durée de conservation de ces données
  - Consentement explicite
- Utiliser des pages Web indiquant la politique de protection des DCP
- Privilégier HTTPS pour préserver la confidentialité
  - Surtout s'il y a des DCP sur le site
    - Documents officiels, factures…

Les collaborateurs

- Charte d’utilisation du SI
- Sensibilisation et formation
- Attention aux exports « sauvages » de données
  - Excel
  - Non maitrisés par le service Informatique
  - Envoyés par mail ou sur une clé USB non protégée

DPO

- Délégué à la Protection des Données (DPD ou en anglais DPO pour *Data Protection Officer*)
- Précisé par le G29 (13 décembre 2016)
  - Obligatoire seulement
    - Pour Organismes publics
    - Si traitements réguliers à grande échelle de données personnelles
    - Si traitement de données sensibles
      - Médicales, génétiques, biométriques…
- Doit être « indépendant »
  - Attention aux conflits d'intérêts
- Peut être l'ancien Correspondant Informatique et Libertés
  - Pas (forcément) le RSSI qui a des intérêts divergents
- Possibilité d'un DPO en temps partagé

Registre de traitements

- C’est le (seul) moyen de prouver votre conformité !

> Afin de démontrer qu'il respecte le présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des registres pour les activités de traitement relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à la disposition de celle-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement.

- Sous forme
  - Papier
  - Excel
  - Logiciels spécialisés

Registre de traitements

- Description des traitements et des occurrences
- Les sous traitants
  - Sont ils conformes ?
- Le DPO
- Et tous documents prouvant vos actions de mise en conformité
  - Audit et mise en œuvre des préconisations
  - Formations
  - Analyses lors des phases de conceptions

Traçabilité

- Indispensable afin :
  - De comprendre ce qui s'est passé en cas de violation
  - Répondre aux besoins d'un contrôle
  - D'anticiper
- Connexion au SI
  - Au travers de points d'exit
  - A permis de comprendre/constater certaines connexions
    - Tentatives de pénétration à partir d'Internet
    - Accès en production à des données de serveurs de test/développement
    - Utilisation de « vieux » profils
    - Détail des requêtes SQL ODBC/JDBC

Traçabilité (2)

- Audit système
  - Tentative d’accès à des objets interdits
  - Utilisation de commandes
- Historique du système (QHSTxxx)
  - Connexions à des heures étonnantes
- Journalisation des objets
  - Qui a modifié quoi et quand

Conclusions

- Envisagez la mise en conformité comme une chance pas comme une charge
- Ne relâchez pas vos efforts après le 25 mai
- Tenez un registre des traitements

Merci de votre attention !

Dominique GAYTE - NoToS
dgayte@notos.fr – www.notos.fr