Université IBM i 2017

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

S22 - Les atouts de l'IBM i pour répondre aux contraintes du GDPR

Jeudi 18 mai – 11h00-12h30

Dominique GAYTE
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

php.spool lorena monitor i distant.backup

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
  - Modalités d’application de certains aspects sont encore à transcrire en droit français

Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant.

Qu’est-ce que le GDPR ? (2)

- Concerne les entreprises qui traitent des données personnelles des ressortissants de l’UE
  - Même en dehors de l’UE
- Sanctions lourdes en cas de manquement

> Les violations des dispositions … font l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu

- Des dispositions particulières sont prises pour les données sensibles
  - Santé
  - Opinions, préférences
  - Origines

Quelques grands principes

- Les citoyens ont plus de contrôle sur leurs données personnelles
  - Consentement explicite
  - Droit à l'oubli et à la portabilité
- Notification en cas de fuites de données
  - 72 heures au plus tard après la découverte de la fuite
  - À l'autorité de contrôle (CNIL)
- Protection des données dès la conception
  - On doit prendre en compte les exigences relatives à la protection des données personnelles dès la conception des produits, services et systèmes utilisant des données à caractère personnel

Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut.

Quelques grands principes (2)

- Sécurité des traitements

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 y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement

Quelques grands principes (3)

- Tenue d'un registre des activités de traitement

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.

Pour tenir compte de la situation particulière des micro, petites et moyennes entreprises, le présent règlement comporte une dérogation pour les organisations occupant moins de 250 employés en ce qui concerne la tenue de registres

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.

Quelques grands principes (4)

- Nomination d'un délégué à la protection des données ou DPO (*Data Protection Officer*)
- Assiste les Responsables de traitement
- Précisé par le G29 (13 décembre 2016)
- Obligatoire seulement
  - Pour Organismes publics
  - Si traitements réguliers à grande échelles de données personnelles
  - Si traitement de données sensibles
    - Médicales, génétiques, biométriques…

Autrement dit, il faut :

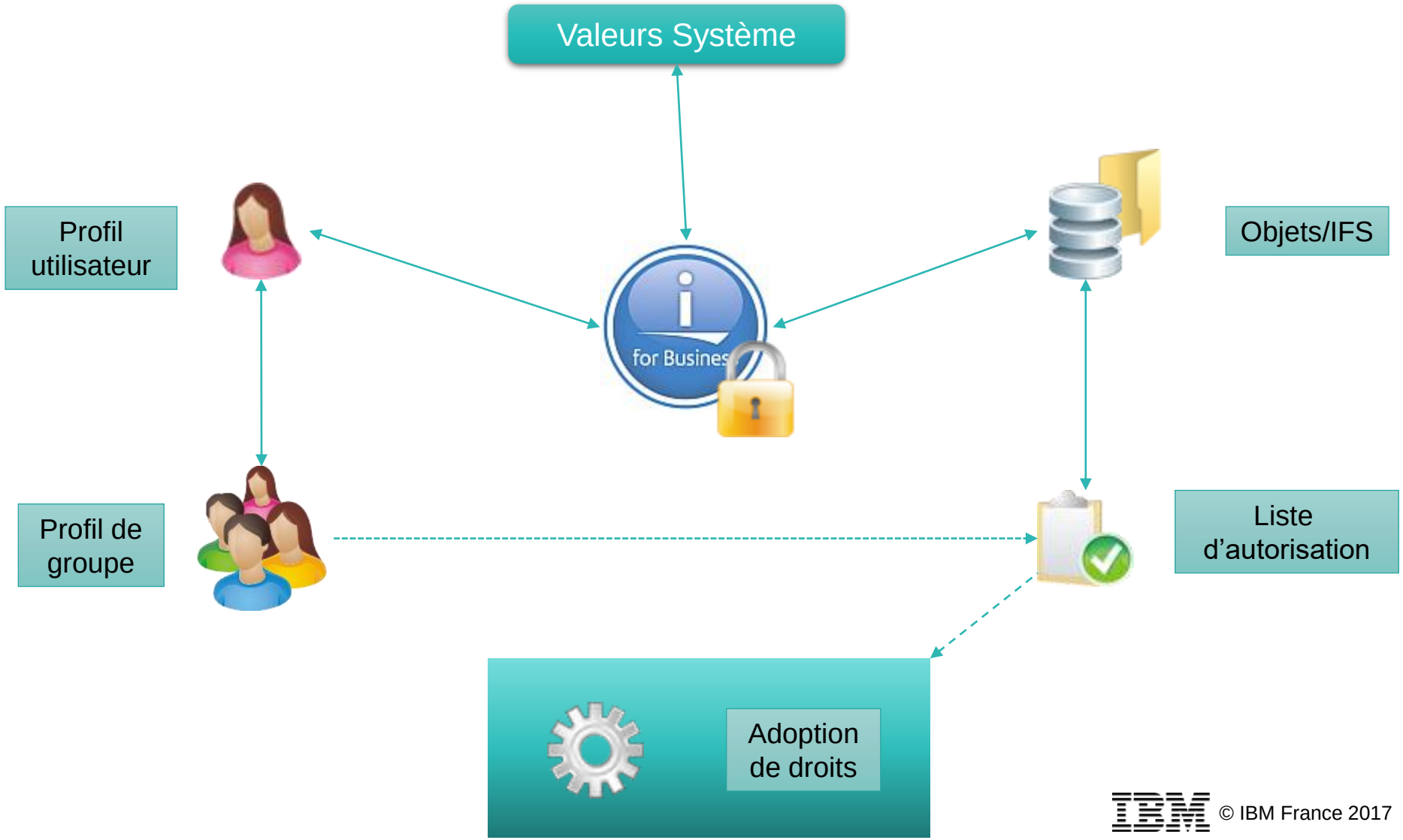
- Protéger les données à caractères personnel
- Tracer ce qui s'est passé afin d'identifier et de comprendre une éventuelle fuite
- Permettre à la personne concernée de les contrôler

Protéger les données

Protection des données

- Droits d'accès
- Chiffrement de l'information
  - Disque
  - Base de données
    - Field Procedure
    - RCAC
  - Réseau SSL
- Anonymiser/pseudonymiser

Organisation de base de la Sécurité



Droits d'accès

- L'IBM i est un des systèmes les plus robustes en termes de Sécurité des droits d'accès
- Mais souvent très mal configuré…
- Il faut revoir
  - Les droits spéciaux accordés aux utilisateurs
    - Faire la chasse aux *ALLOBJ
  - Les objets/fichiers sensibles contenant des données personnelles
    - Lister les données, traitements et les flux concernés
    - Identifier les utilisateurs autorisés (et les sous-traitants)
    - Gérer les droits : attention aux droits publics !

Droits publics

- Droits par défaut d'accès à l'objet ou au fichier
- Par défaut *CHANGE
  - Tous les droits sur les données
- Préoccupant pour tout ce qui est accès hors applications métier
- Devrait être à *EXCLUDE

Droits permanents

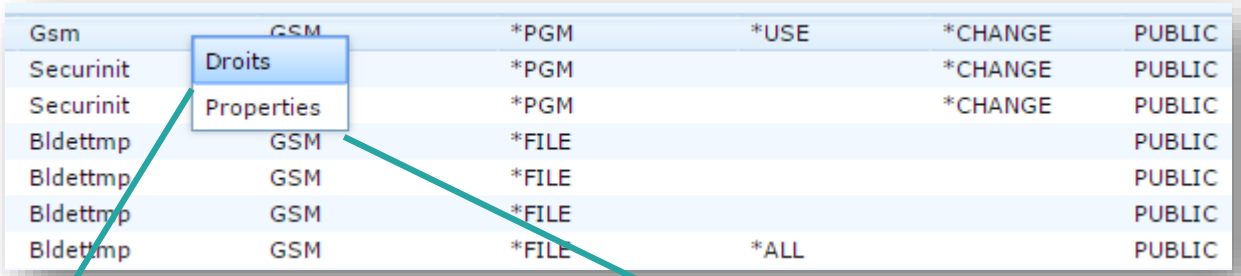
- Droits accordés aux objets/fichiers en dehors des applications métier
  - Donc utilisés en ODBC/JDBC, FTP…
- Proviennent
  - Du droit spécial *ALLOBJ du profil
  - Des droits privés sur l'objet
  - Des droits issus du (ou des groupes) auquel appartient le profil
  - Des droits publics
- Authority Collection
  - Pour connaitre les droits réellement nécessaires

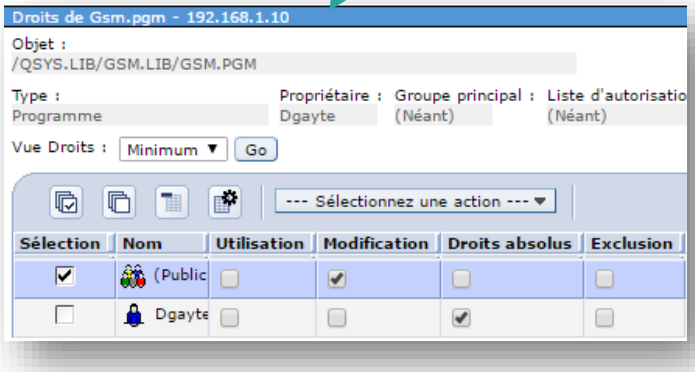
Authority Collection

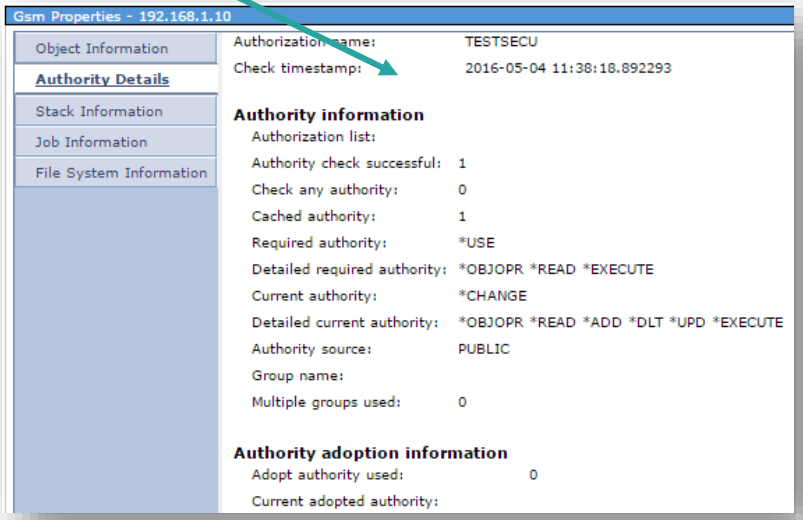
- Fonction qui permet à l'administrateur de la Sécurité de mieux comprendre les mécanismes d'attributions des droits réellement mis en œuvre dans le cadre d'une application
- Utile pour n'octroyer que les droits nécessaires aux utilisateurs
- Intégré à l'IBM i (V7R3) (et au microcode)
- Capture d'informations lors de l'exécution des programmes par un profil utilisateur
- Affichage et analyse des données
- Déduction des plus petits droits nécessaires au bon fonctionnement des applications pour ce profil

Affichage d'une collection

- Visualisation des droits utilisés pour accéder à l'objet







Chiffrement

- L'IBM i dispose de toutes les technologies de chiffrement !
- Disques
  - Cryptage des ASP (pas l'ASP système !)
  - SS1 Option 45 - Encrypted ASP Enablement
- Base de données
  - Field Procedure
    - Permet le cryptage de zones au niveau disque
  - RCAC
    - C'est le résultat qui peut être crypté, pas la zone au niveau disque
    - Possibilité d'obfuscation totale ou partielle
    - Restitution différente selon le contexte (par utilisateur, par exemple)
    - Option 47 de SS1 (IBM Advanced Data Security for i)

Chiffrement (2)

- Réseau
  - SSL
    - Telnet, FTPS, HTTPS…
    - Voir présentation S28 de 2013
  - SSH/SFTP
- Développement
  - API de cryptage
  - QSHELL avec le produit 5733SC1
- Sauvegarde
  - BRMS : BRMS Advanced feature (BR1 option 2)
  - SS1 option 44 - IBM i Encrypted Backup Enablement

Exemple RCAC Ligne

```
CREATE PERMISSION dgayte.Client_Inf_1000
ON dgayte.entete
FOR ROWS WHERE
    SESSION_USER = 'DGAYTE'
OR client < 1000
ENFORCED FOR ALL ACCESS ENABLE
Instruction CREATE PERMISSION terminée pour CLIENT_INF_1000 de DGAYT
ALTER TABLE dgayte.entete ACTIVATE ROW ACCESS CONTROL
L'exécution de l'instruction ALTER est terminée pour la table ENTETE
```

```
SELECT * FROM dgayte.entete ORDER BY CLIENT  desc
```

DGAYTE

CLIENT	TOTAL
29.483	2.264,2536
29.482	2.264,2536
29.481	3.729,3640
29.480	2.698,4432
29.479	2.264,2536
29.478	2.649,8453
29.477	2.682,9953
29.476	3.756,9890

QSECOFR

CLIENT	TOTAL
701	7.775,7170
701	275,7448
701	22,1760
701	2.730,7313
701	892,8369
701	3.043,2769
700	40.868,0960
700	28.918,4417

Exemple colonne

```
CREATE OR REPLACE MASK dgayte.masquecpt ON dgayte.entete
FOR COLUMN compte RETURN
  CASE
    WHEN SESSION_USER = 'DGAYTE'  THEN compte
  ELSE
    'XX-XXXX' CONCAT SUBSTR(compte, 8, 7)
  END
ENABLE ;
ALTER TABLE dgayte.entete ACTIVATE COLUMN ACCESS CONTROL;
```

```
SELECT CLIENT, TOTAL, COMPTE FROM dgayte.entete ORDER BY CLIENT desc
```

DGAYTE

CLIENT	TOTAL	COMPTE
29.483	2.264,2536	10-4030-029483
29.482	2.264,2536	10-4030-029482
29.481	3.729,3640	10-4030-029481
29.480	2.698,4432	10-4030-029480
29.479	2.264,2536	10-4030-029479
29.478	2.649,8453	10-4030-029478

QSECOFR

CLIENT	TOTAL	COMPTE
701	7.775,7170	XX-XXXX0-00070
701	275,7448	XX-XXXX0-00070
701	22,1760	XX-XXXX0-00070
701	2.730,7313	XX-XXXX0-00070
701	892,8369	XX-XXXX0-00070
701	3.043,2769	XX-XXXX0-00070

Pseudonymisation & anonymisation

- Pseudonymisation
  - Réversible
  - Les données qui permettent la réversibilité sont conservées séparément des données pseudonymisées

Le traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable

- Anonymisation
  - Non réversible
  - Deviennent donc des données non personnelles !
  - Hors du scope du GDPR…

Pseudonymisation & anonymisation (2)

- A utiliser pour toutes les données personnelles dont la valeur réelle n'est pas nécessaire au traitement
  - On change le nom et le prénom d'une personne
  - On masque une partie du numéro de Sécurité Sociale
    - RCAC (obfuscation)
- Concerne les données des environnements/partitions
  - De test, de recette
  - De développement
  - Et même dans certains cas de DataWarehouse/Infocentre

Traçabilité

Traçabilité

- Journal d'audit (QAUDJRN)
- Les journaux de la base de données
  - Utilisés par les outils de réplication
- Historique du système
  - Fichiers QHSTxxx
- Traces internes
  - Applications
  - Triggers
  - Points d'exit
- Je recommande une politique de rétention/sauvegarde adaptée aux traces diverses
- Exploitation via des outils tierces (CSI de Trader's)

Contrôle des données personnelles

Droits de la personne concernée

- Droit d'accès
  - La personne concernée doit pouvoir accéder aux données la concernant
- Rectification et effacement
  - Modification des données
  - Droit à l'oubli

ne s'appliquent pas dans la mesure où ce traitement est nécessaire:
a) à l'exercice du droit à la liberté d'expression et d'information;
b) pour respecter une obligation légale …;
c) pour des motifs d'intérêt public dans le domaine de la santé publique
d) à des fins archivistiques
e) à la constatation, à l'exercice ou à la défense de droits en justice.

- Communication d'une violation de ses données

Droits de la personne concernée (2)

- Droit à la portabilité des données

Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies …, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement

- L'IBM i permet de travailler en XML et CSV
  - Et autres formats
- Transmission
  - FTP, FTPS, SFTP, e-mail

Elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible

Le contrôle de ses données personnelles

- La possibilité offerte à une personne de modifier/gérer ses données personnelles contenu dans votre SI dépasse le cadre de ce séminaire mais :
- Les Web Services répondent bien à ce type de besoin
  - Environnement hétérogène
    - Multi-système
    - Multi-langage
  - Sécurité
    - Seul le frontal est exposé, pas l'IBM i
- Les WS sont bien intégrés à l'IBM i
  - SOAP, REST
  - Serveur ou client
  - En RPG IV, PHP, SQL…

Conclusions

- L'IBM i est bien armé pour répondre aux contraintes du GDPR
- Mais vos applications et votre SI sont-ils prêts ?
- Il est temps de mettre la Sécurité à un niveau correct
- Une année sera vite passée…

Définitions

- Données à caractère personnel
  - Toute information se rapportant à une personne physique identifiée ou identifiable … est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale
- Traitement
  - Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

Définitions (2)

- Pseudonymisation
  - Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable
  - Est réversible, par opposition à l'anonymisation qui ne l'est pas
- Violation de données à caractère personnel
  - Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données

Quelques liens

- Le règlement
  - HTML : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679
  - PDF : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR
- Version commentée
  - https://www.afcdp.net/IMG/pdf/rgpd_annote_et_indexe_afcdp_v3.pdf