Les myhtes sur le RGPD

https://twitter.com/MonsieurRelou/status/1358731470588825600

“Oui, mais c'est conforme #RGPD, cet outil, au moins ?” ➡ debunking point par point de quelques idées reçues trop souvent répétées. Un thread #MythesRGPD #enseignement .

✖ La conformité n’est pas celle d’un outil, mais celle d’un traitement de DCP lié à une tâche (administrative ou pédagogique). Un même outil peut engendrer des traitements très différents, selon les finalités recherchées ou le régime contractuel privilégié, par exemple.

 L’entrée par outil n’est pas pertinente, car centrée sur les usages visibles et non sur les conditions (souvent invisibles pour l’enseignant) auxquelles les traitements de DCP sont opérés. Or, c’est précisément là que se joue cette fameuse conformité.

✖ La conformité n’est pas “constatable sur pièces”. Elle doit pouvoir être démontrée : respect de standards techniques (par l’opérateur), souscription d’un régime contractuel protecteur (par le RT), mise en place de dispositions locales spécifiques (CGU, registre, info public).

 La conformité RGPD ne peut pas faire l’économie de sa propre démonstration. Les textes imposent qu’elle soit construite, documentée et assumée par le responsable de traitement, au nom du principe de “redevabilité” (accountability).

✖ La conformité n’est pas “déclarative”, au sens d’annoncée par le prestataire et réputée démontrée (hop pouf). C’est le résultat d’un process interne (et actif !) de responsabilisation, au sein de la structure souhaitant contractualiser avec le sous-traitant.

 Trop de “solutions” font commerce d’une conformité trompeuse. Elles laissent entendre qu’un régime de validation automatique pourrait exister pour leur produit, dispensant par là les RT de la mise en place de process de validation : c’est tout à fait faux.

✖ La conformité n’est pas “absolue”. Les décisions de conformité dépendent d’une évaluation des risques liés aux traitements. Chaque RT a le devoir de la diligenter, en appui sur des expertises locales : ce que l’un acceptera, l’autre le refusera peut-être… c’est ainsi.

 Les décisions de conformité ont une portée locale, limitée à la structure pilotée par le RT ayant validé le déploiement. La décision d’une académie (par exemple) ne peut pas préjuger de celle des autres.

✖ Il n’existe pas, pour cette même raison, de “protocole d’accord” national entre le MEN et un fournisseur, avec à terme une prescription valable dans tous les établissements. C’est impossible, car contraire à l’autonomie conférée aux RT par le RGPD.

 Attendre de l’autorité centrale qu’elle substitue son pouvoir décisionnel à celui des RT locaux est illusoire et contre-productif. Cela contribue à entretenir la confusion autour de l’application du RGPD en milieu scolaire.

Monsieur Relou

+ Your Authors | Archive

@MonsieurRelou

Relou du RGPD. Certifié opiniâtre ©.

Feb. 08, 2021 · 2 min read

"Oui, mais c'est conforme #RGPD, cet outil, au moins ?" ➞ debunking point par point de quelques idées reçues trop souvent répétées. Un thread #MythesRGPD #enseignement .

✕ La conformité n'est pas celle d'un outil, mais celle d'un traitement de DCP lié à une tâche (administrative ou pédagogique). Un même outil peut engendrer des traitements très différents, selon les finalités recherchées ou le régime contractuel privilégié, par exemple.

👉 L'entrée par outil n'est pas pertinente, car centrée sur les usages visibles et non sur les conditions (souvent invisibles pour l'enseignant) auxquelles les traitements de DCP sont opérés. Or, c'est précisément là que se joue cette fameuse conformité.

✕ La conformité n'est pas "constatable sur pièces". Elle doit pouvoir être démontrée : respect de standards techniques (par l'opérateur), souscription d'un régime contractuel protecteur (par le RT), mise en place de dispositions locales spécifiques (CGU, registre, info public).

👉 La conformité RGPD ne peut pas faire l'économie de sa propre démonstration. Les textes imposent qu'elle soit construite, documentée et assumée par le responsable de traitement, au nom du principe de "redevabilité" (accountability).

✕ La conformité n'est pas "déclarative", au sens d'annoncée par le prestataire et réputée démontrée (hop pouf). C'est le résultat d'un process interne (et actif !) de responsabilisation, au sein de la structure souhaitant contractualiser avec le sous-traitant.

👉 Trop de "solutions" font commerce d'une conformité trompeuse. Elles laissent entendre qu'un régime de validation automatique pourrait exister pour leur produit, dispensant par là les RT de la mise en place de process de validation : c'est tout à fait faux.

✕ La conformité n'est pas "absolue". Les décisions de conformité dépendent d'une évaluation des risques liés aux traitements. Chaque RT a le devoir de la diligenter, en appui sur des expertises locales : ce que l'un acceptera, l'autre le refusera peut-être... c'est ainsi.

👉 Les décisions de conformité ont une portée locale, limitée à la structure pilotée par le RT ayant validé le déploiement. La décision d'une académie (par exemple) ne peut pas préjuger de celle des autres.

✕ Il n'existe pas, pour cette même raison, de "protocole d'accord" national entre le MEN et un fournisseur, avec à terme une prescription valable dans tous les établissements. C'est impossible, car contraire à l'autonomie conférée aux RT par le RGPD.

👉 Attendre de l'autorité centrale qu'elle substitue son pouvoir décisionnel à celui des RT locaux est illusoire et contre-productif. Cela contribue à entretenir la confusion autour de l'application du RGPD en milieu scolaire.