le cnam

Conservatoire national des arts et métiers

Le RGPD et la nouvelle loi française sur la protection des données personnelles

Quels enjeux pour les professionnels ?

Guillaume DESGENS-PASANAU
Magistrat
Maitre de conférences associé au CNAM

CGE – avril 2018

Introduction

Quelles sont les conséquences opérationnelles liées à la modification de la réglementation « informatique et libertés » à compter du 25 mai 2018 ?

- Nouvelles obligations en termes de gestion de la conformité
- Nouveaux risques de non-conformité

Textes applicables

Avant le 25 mai 2018 :

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Loi n° 2004-801 du 6 août 2004

Textes applicables

Après le 25 mai 2018 :

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) a été adopté par le Parlement européen et Conseil (*JOUE n° L 119, 4 mai 2016)*

- Projet de loi sur la protection des données personnelles

- Proposition de règlement européen « e-privacy »

En synthèse

- **Les grands principes de protection des données ne sont pas modifiés par le RGPD, mais les modalités de gestion de la conformité sont significativement modifiées**
  - Plus de formalités préalables auprès de la CNIL, remplacées par l'obligation de documenter sa conformité
  - Nouvelle dimension européenne de la protection des données
- **Les droits des personnes concernées sont renforcés**
- **Les pouvoirs de sanction de la CNIL sont renforcés**

Risques de non-conformité

- Risque d'image
- Risque de contentieux judiciaire
- Risque de sanction administrative prononcée par la CNIL

Focus : les pouvoirs de contrôle et de sanction de la CNIL

- Nouveaux art. 44 et s. du projet de loi sur la protection des données personnelles
- Pouvoirs de contrôle globalement inchangés
- Pouvoirs de sanction administrative renforcés :
  - Plus de mise en demeure préalable obligatoire
  - Sanctions pécuniaires jusqu'à 20 millions d'euros ou 4% du CA mondial d'une entreprise

Elargissement de certains concepts

- Nouvelle possibilité de co-responsabilité sur un traitement
- Renforcement de la responsabilité des sous-traitants
- Le RGPD s'applique aux opérateurs hors UE

Mise en œuvre d'une politique de documentation de la conformité

- **Obligation de documenter sa conformité**
- Principe de l'approche par les risques (art. 24 RGPD)

Contenu de l'obligation de documentation (accountability)

- Registre des traitements (art. 30 RGPD)
- Rédaction d'études d'impact (art. 35 RGPD)
- Désignation d'un délégué à la protection des données (art. 37 RGPD)

- Prise en compte du principe de « privacy by design » (art. 25 RGPD)
- Rédaction de procédures et clausiers
- Organisation d'opérations d'audit
- Formation et sensibilisation des personnels

Focus : rédaction d'un PIA

Art. 35 règlement UE

- Rédaction obligatoire pour les traitements ayant pour finalité:
  - l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
  - le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ;
  - la surveillance systématique à grande échelle d'une zone accessible au public »

Vérifier le respect des principes-clé de la réglementation

- La collecte des données du traitement est-elle **licite, loyale et transparente** ? (art. 5 RGPD)
- Le principe de **proportionnalité** est-il respecté ? (art. 5 RGPD)
- Une **durée de conservation des données** a-t-elle été définie ? Des modalités d'archivage des données ont-elles été définies ? (art. 17 RGPD)
- Une **politique de sécurité** et de confidentialité des données est-elle définie ? (art. 32 RGPD)
- Y a-t-il des **transferts de données en dehors de l'Union européenne ?** Si oui, ceux-ci font-ils l'objet d'un encadrement juridique adapté ? (art. 44 RGPD)

Focus : généralisation de l'obligation de notifier les violations de données personnelles

Art. 33 règlement UE

- « En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard»

Attention à la nouvelle loi nationale

- **Est-il procédé à la collecte ou au traitement :**
  - De données sensibles (art. 9 RGPD)
  - De données d'infractions (art. 10 RGPD)
  - Du numéro de sécurité sociale

Dans l'affirmative, des précautions particulières sont-elles bien prises ?

Droits des personnes fichées

- **Des procédures sont-elles définies afin de respecter les droits des personnes fichées ? (chapitre 3 RGDP)**
  - Question relative au consentement préalable
  - Information préalable
  - Droit d'accès et de rectification
  - Droit à la portabilité
  - Droit à l'effacement et droit d'opposition
  - Droit à la limitation des données
  - Droits spécifiques concernant les internautes

Le délégué à la protection des données

- **Désignation obligatoire dans 3 cas :**
  - le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;
  - les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou
  - Les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Statut et missions du DPD

- Missions de conseil et de contrôle du DPD
- Des règles statutaires globalement inchangées
  - DPD externe / DPD mutualisé
  - Qualifications professionnelles
  - Conflits d'intérêts
  - Responsabilité
  - Indépendance

Accueil · Tous les cours · Protection des données personnelles : le nouveau droit

Protection des données personnelles : le nouveau droit

Les thématiques Droit et juridique Numérique, technologie

le cnam

S'inscrire

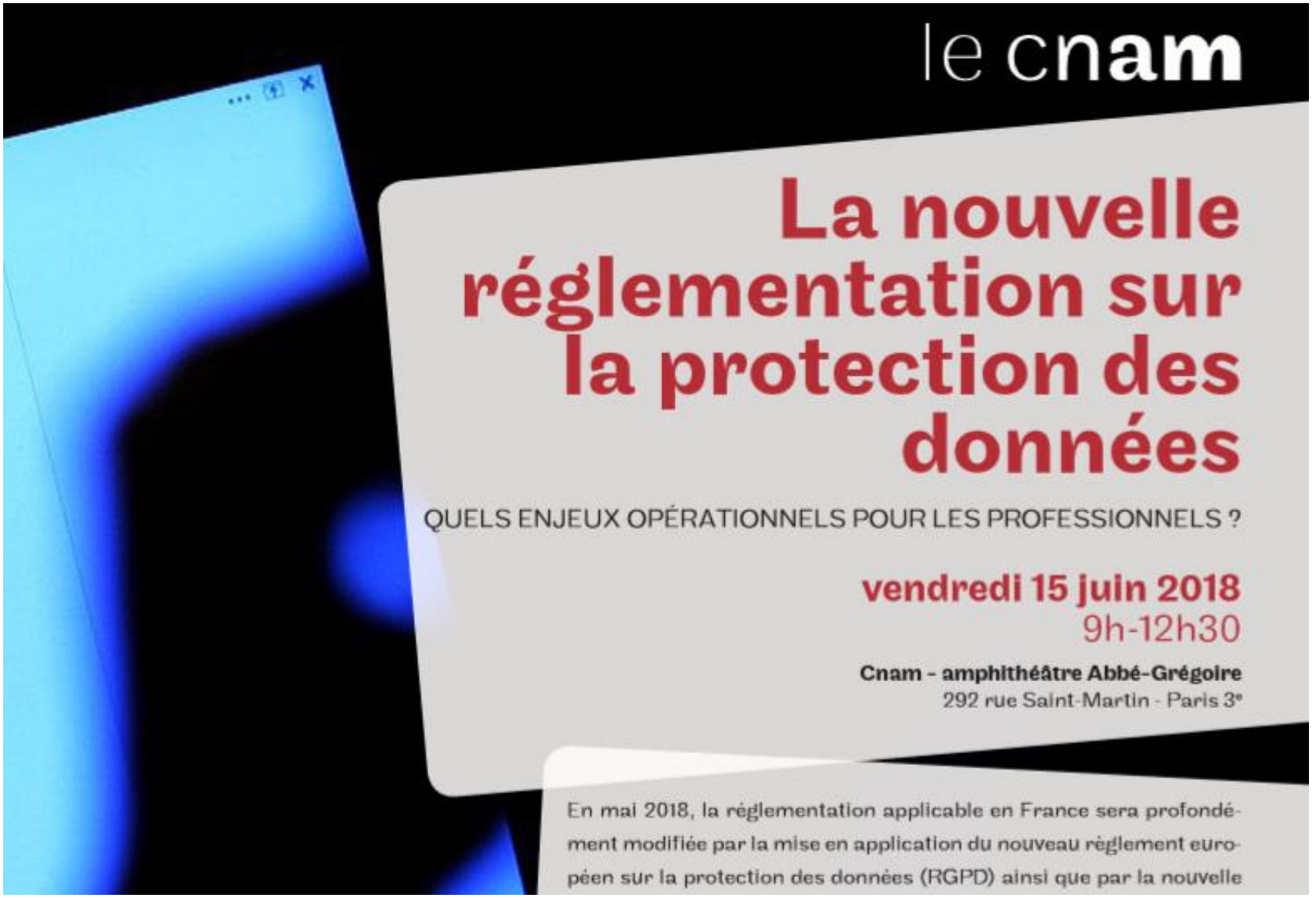
Fin d'inscription
03 jui 2018

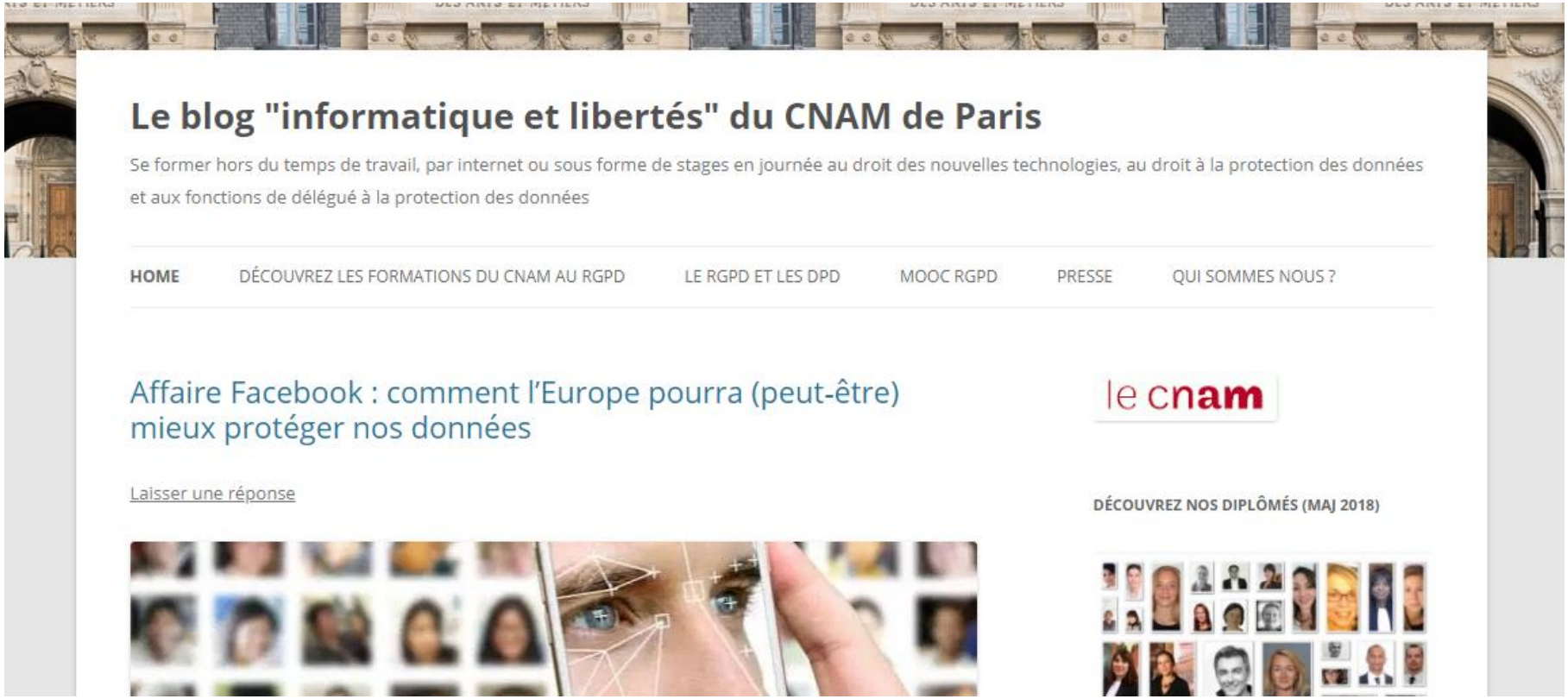
Début du Cours
23 avr 2018

Fin du cours
03 jui 2018

Effort estimé
02:30 h/semaine

https://www.fun-mooc.fr/courses/course-v1:CNAM+01032+session01/about


le cnam
La nouvelle réglementation sur la protection des données
QUELS ENJEUX OPÉRATIONNELS POUR LES PROFESSIONNELS ?
vendredi 15 juin 2018
9h-12h30
Cnam - amphithéâtre Abbé-Grégoire
292 rue Saint-Martin - Paris 3e
En mai 2018, la réglementation applicable en France sera profondément modifiée par la mise en application du nouveau règlement européen sur la protection des données (RGPD) ainsi que par la nouvelle



https://cnamcil.wordpress.com/

CONTACT

CNAM
METIERS DU DROIT
2, rue Conté
75141 Paris cedex 03

guillaume.desgens@lecnam.net

Association des diplômés (AJES-DIT)
https://cnamcil.wordpress.com