CONFERENCE

amue
MUTUALISATION + SOLUTIONS

Le RGPD dans l'Enseignement supérieur et la Recherche : impacts et promesses

Maison des Universités
Salle de conférences
4ème étage
103 boulevard Saint-Michel
75005 PARIS

MERCREDI 21 MARS 2018

amue
MUTUALISATION + SOLUTIONS

Le RGPD dans l'enseignement supérieur et la recherche: Impacts et Promesses

MERCREDI 21 MARS 2018

14h00 *Ouverture*

Stéphane ATHANASE, directeur de l'Amue

Emmanuel Roux, Président de la commission Juridique de la CPU

14h15 **La CNIL soutient l'ESR**

Sophie VULLIET-TAVERNIER, directrice des relations avec les publics et la recherche, *CNIL*

14h40 **Décryptage stratégique du RGPD**

Florence CELEN, animatrice du réseau SUPCIL, *université Toulouse III Paul Sabatier*

15h00 **Sur la trajectoire du 25 mai 2018**

+ Règlement européen sur la protection des données - Les étapes conseillées par la CNIL pour s'y préparer,
Victor LARGER, animateur du réseau SUPCIL, *université Paris Descartes*

+ Conformité de l'Amue au RGPD,
Frantz GOURDET, DPO, *Amue*

Le RGPD dans l'enseignement supérieur et la recherche: Impacts et Promesses

15h00 **Sur la trajectoire du 25 mai 2018**

+ Règlement européen sur la protection des données - Les étapes conseillées par la CNIL pour s'y préparer,
Victor LARGER, animateur du réseau SUPCIL, *université Paris Descartes*

+ Conformité de l'Amue au RGPD,
Frantz GOURDET, DPO, *Amue*

15h40 **Impacts du RGPD sur les DSI**
Serge PORTELLA, président de l'A-DSI

16h00 **La transition CIL-DPO**
Anne FONTANILLE, juriste au service des CIL, *CNIL*

16h20 *Mot de clôture*

Mise en conformité des traitements au RGPD à l'Amue

Phase préparatoire	Phase organisationnelle	Phase opérationnelle
		
L'ascension	La contemplation	La descente

Pour parallèle : Rappel des étapes de mise en conformité conseillés par la CNIL

La conformité en trois phases… et 6 étapes Amue (mises en regard des 6 étapes CNIL)


L'ascension

Phase préparatoire ou « pré-organisationnelle » (anticipative)

- Mise en place de l'organisation générale et des procédures de gouvernance


La contemplation

Phase organisationnelle

- Étape 1 : Inventaire des traitements
- Étape 2 : Estimation de la charge de diagnostic des traitements
- Étape 3 : Choix d'une stratégie de priorisation


La descente

Phase opérationnelle

- Étape 1 : Diagnostic
- Étape 2 : Maintien ou mise en conformité effective


L'ascension

Phase anticipative, préparatoire ou préorganisationnelle : Mise en place de l'organisation générale et des procédures de gouvernance

- Le Cil assure le pilotage global de la mise en conformité de l'Amue au RGPD
- Décision prise dès 2015 : Anticiper le RGPD en exploitant le référentiel de gouvernance Informatique et Libertés de la CNIL comme fil conducteur et support d'*accountability*

- Elaborer la *Procédure générale de gouvernance Informatique et Libertés* de l'Amue anticipant l'application du RGPD
- Livrable : Dossier complet de gouvernance labélisé par la CNIL le 30 juin 2016
- Action en cours (bouclage fin mars) : Réactualisation du label de gouvernance dans le cadre de l'application du RGPD


La contemplation

Un pilotage décentralisé de la mise et du maintien en conformité des traitements…

+ La Procédure de gouvernance Informatique et Libertés de l'Amue comporte des ***référentiels*** qui décrivent la cible de la conformité totale
+ Ces ***référentiels*** sont mis en vigueur par le directeur de l'Amue avec force exécutive (feuille de route) afin d'analyser nos traitements et d'y apporter des mesures correctives chaque fois que nécessaire
+ Le témoin est ainsi passé à un réseau de **relais Informatique et Libertés (RIL)** composé des **responsables hiérarchiques des principales unités** (Pôles, services, départements ou équipe produit)

+ Au sein de l'unité qu'il représente, chaque RIL pilote la suite de la phase organisationnelle puis la phase opérationnelle de mise en conformité
+ Chaque RIL a pour mission d'appliquer et de faire appliquer les ***référentiels*** correspondant aux traitements se situant dans son périmètre
+ Un inventaire de ces traitements s'avère donc nécessaire


La contemplation

Un pilotage décentralisé de la mise et du maintien en conformité des traitements…

+ Certains de ces ***référentiels*** sont destinés aux agents chargés de la mise en œuvre des traitements internes :
  - Fondamentaux en exploitation
  - Fondamentaux protection *by design* interne
  - Sécurité en exploitation
    - Modèle générique de PIA
    - Logiciel libre de PIA de la CNIL

+ Un autre ***référentiel*** est conçu pour les agents s'occupant de la conception ou de la maintenance des produits de l'offre SI Amue (produits utilisés par les établissements pour traiter leurs données à caractère personnel) :
  - Fondamentaux protection *by design* externe

+ Le ***référentiel*** qui chapeaute l'ensemble est bien entendu le référentiel de gouvernance décliné en procédures

+ *La suite de la présentation porte uniquement sur le référentiel Protection by design externe (point d'intérêt de nos adhérents)*

Les référentiels couvrent les 3 phases

La contemplation

Étape 1 — Phase organisationnelle

- Étape 1 : Inventaire des traitements
- Étape 2 : Estimation de la charge de diagnostic des traitements
- Étape 3 : Choix d'une stratégie de priorisation

Étape 3

Cartographier — Prioriser

Étape 2

Étape 1 — Désigner un pilote

Étape 5 — Organiser

Pré-diagnostic		
Charge estimée (j.h)	Chargés du contrôle	Echéance

Phase préparatoire ou « pré-organisationnelle » (anticipative)

- Mise en place de l'organisation générale et des procédures de gouvernance

L'ascension

Phase opérationnelle

- Étape 1 : Diagnostic
- Étape 2 : Maintien ou mise en conformité effective

La descente

Point de contrôle		Mesure	Pré-diagnostic			Diagnostic				Moyen à mettre en œuvre (mesures correctives)	Mise en conformité		Moyens mis en œuvre (500 caractères maximum)	Eléments justificatifs
			Charge estimée (j.h)	Chargés du contrôle	Echéance	Charge consommée (j.h)	Chargés du contrôle	Finalisé le	Conformité		Coûts	Délais		
1	Finalité : finalité déterminée, explicite et légitime	Énoncer les finalités de manière détaillée et compréhensible par les personnes dont les données vont être traitées												
		Ne pas aller au-delà des finalités déclarées ou effectuer une nouvelle analyse complète pour tout souhait d'ajout de nouvelle finalité												
		(Permettre de) Recueillir des données (que) pour un usage précis et bien défini (éviter par exemple les zones de commentaires libres)												
		Ne pas aller à l'encontre de la loi, ni des droits ou des libertés fondamentales des personnes												


La descente

Les référentiels en Phase opérationnelle

Phase opérationnelle

- Étape 1 : Diagnostic
- Étape 2 : Maintien ou mise en conformité effective

Diagnostic			Conformité	Moyen à mettre en œuvre (mesures correctives)
Charge consomée (j.h)	Chargés du contrôle	Finalisé le		

Etape 5

Organiser

Etape 6

Documenter


La descente

Les référentiels en Phase opérationnelle

Phase opérationnelle

- Étape 1 : Diagnostic
- Étape 2 : Maintien ou mise en conformité effective

Mise en conformité				
Coûts	Délais	Etape 1 Désigner un pilote Etape 5 Organiser	Moyens mis en œuvre (500 caractères maximum) Etape 6 Documenter	Eléments justificatifs Etape 6 Documenter

Le référentiel « Fondamentaux de la protection by design/default externe » : Matrice de conformité (13 points de contrôle)

Terme
Court
Moyen
Long

✓	1	Finalité : finalité déterminée, explicite et légitime
✓	2	Minimisation : réduction des données à celles strictement nécessaires
●	3	Durées de conservation : durée nécessaire à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue
●	4	Information : respect du droit à l'information des personnes concernées
●	5	Consentement : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement
●	6	Droit d'opposition, effacement (droit à l'oubli), limitation du traitement, portabilité et gestion post mortem
●	7	Droit d'accès : respect du droit des personnes concernées d'accéder à leurs données
✓	8	Droit de rectification : respect du droit des personnes concernées de corriger leurs données et de les effacer
✓	9	Formalités : définition et accomplissement des formalités préalables applicables au traitement
●	10	En cas de sous-traitance
✓	11	Renseignement fiche traitement
✓	12	Sécurité
●	13	Etude d'impact sur la vie privée (EIVP/PIA)

En résumé

- 10 des 13 points de contrôle de conformité RGPD sont satisfaits par les applications de l'offre SI Amue. Les travaux restant à finaliser concernent :
  - L'analyse des durées de conservation et des processus d'archivage qui permettent notamment de mettre en œuvre les procédures d'effacement nécessaires au droit à l'oubli
  - L'analyse de la totalité de nos nombreuses conventions et marchés (en particulier de TMA) afin d'aligner le partage de responsabilités quand c'est nécessaire
  - Quelques compléments destinés aux CCI lorsque nécessaires pour faciliter les PIA (en présence de données sensibles)
  - L'établissement ou la mise à jour des fiches de traitements types (notamment pour les nouveaux produits). Ces fiches ainsi que les procédures d'extraction pour la portabilité seront mises à disposition des établissements

- L'Amue introduit les exigences du RGPD dans son DAQ pour couvrir les applications en construction ainsi que les évolutions touchant aux données à caractère personnel des applications déployées (en application du *privacy by design/default*)
- Nous publierons bientôt régulièrement sur le site de l'Amue dans la rubrique « Conformité RGPD » les informations permettant aux établissements de suivre l'avancement de nos travaux.

Mise en conformité au RGPD des traitements à l'Amue – Synthèse, impacts et promesses

THÉORIE		PRATIQUE
DPO		RIL & Agents (Contrôle: DPO)
Phase anticipative	Phase organisationnelle	Phase opérationnelle

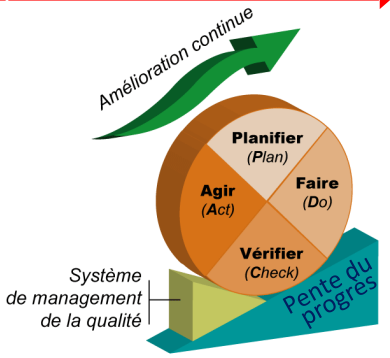
L'ascension	La contemplation	La descente

14 mois

14 mois

7 mois | 2 mois | Processus permanent

Qualité + Accompagnement



Merci de votre attention

Contact

frantz.gourdet@amue.fr


La descente

Le référentiel « Fondamentaux de la protection by design/default externe »

Point de Contrôle		Mesure conforme	
1	Finalité : finalité déterminée, explicite et légitime	Finalités connues et énoncées de manière détaillée et compréhensible par les personnes dont les données vont être traitées	☐
		Ne pas aller au-delà des finalités déclarées ou effectuer une nouvelle analyse complète pour tout souhait d'ajout de nouvelle finalité	☐
		Ne permettre de recueillir des données que pour un usage précis et bien défini (éviter par exemple les zones de commentaires libres)	☐
		Ne pas aller à l'encontre de la loi, ni des droits ou des libertés fondamentales des personnes (mesure triviale et générale)	☐


La descente

Le référentiel « Fondamentaux de la protection by design/default externe »

Point de Contrôle		Mesure conforme	
2	Minimisation : réduction des données à celles strictement nécessaires	Données traitées décrite avec précision notamment de l'origine de la collecte, des catégories de personnes concernées et des destinataires	☐
		Veiller à ce que les données à collecter soient pertinentes, adéquates et non excessives c'est-à-dire strictement nécessaires à la finalité déclarée	☐
		Ne permettre l'enregistrement que d'informations personnelles pertinentes et en relation avec la finalité déclarée du traitement	☐
		Ne pas procéder à des traitements d'information qui, du fait de leur nature, de leur portée ou de leurs finalités, excluent des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire (sauf analyse préalable poussée effectuée avec le DPO de l'Amue)	☐
		Éviter de traiter le numéro de sécurité sociale (sauf analyse préalable poussée effectuée avec le DPO de l'Amue)	☐
		Eviter de traiter (sauf analyse préalable poussée effectuée avec le DPO de l'Amue) des informations relatives à des infractions, condamnations, mesures de sûreté, biométriques ou subjectives, ou des données sensibles[1] qu'il est interdit de collecter sauf autorisation ou avis spécifique de la CNIL nécessitant des démarches à anticiper plusieurs mois à l'avance	☐


La descente

Le référentiel « Fondamentaux de la protection by design/default externe »

Point de Contrôle		Mesure conforme	
3	Durées de conservation : durée nécessaire à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue	Déterminer les durées de conservation par défaut. Ces durées pourront dans un premier temps être issues du document de référence mis à disposition des équipes de conception sur l'intranet de l'Amue	
		Implémenter un mécanisme permettant de basculer les données à caractère personnel de leur archive/base active à leur archive intermédiaire	
		Prévoir la possibilité d'appliquer à cette occasion les restrictions d'accès ou d'habilitation qui s'imposeront, ainsi que la possibilité de transférer ces archives intermédiaires aux personnes/services chargés de leur destruction ou de leur archivage définitif	
		Paramétrer les durées pour anticiper les évolutions règlementaires/légales ou prendre en compte des situations variées intermédiaires aux personnes/services chargés de leur destruction ou de leur archivage définitif	
4	Information : respect du droit à l'information des personnes concernées	Paramétrer l'affichage de mention d'information afin de permettre à l'exploitant de l'outil conçu de fournir un lien Internet vers sa propre mention d'information (ou de personnaliser l'affichage d'une mention type en en renseignant les éléments paramétrés)	
5	Consentement : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement	Déterminer lesquels des traitements et des données à caractère personnel à traiter exigent un consentement des personnes concernées en mode opt-in et/ou opt-out	
		Prévoir en conséquence du point précédent des mécanismes de recueil de consentement : case à cocher (opt-in) ou à décocher (opt-out), par exemple	


La descente

Le référentiel « Fondamentaux de la protection by design/default externe »

6	Droit d'opposition et autres droits entrant dans le cadre des articles 12 à 23 du RGPD : effacement (droit à l'oubli), limitation du traitement, portabilité et gestion post mortem : respect des droits des personnes concernées	Prévoir des mécanismes de suppression des données à caractère personnel relatives à un traitement donné et à une personne concernée et/ou prévoir des indicateurs/ marques/ témoins permettant d'exclure une personne donnée d'un traitement	□
		Prévoir tout mécanisme facilitant l'exercice des droits d'opposition, effacement (droit à l'oubli), limitation du traitement, portabilité et gestion post mortem	□
7	Droit d'accès : respect du droit des personnes concernées d'accéder à leurs données	Prévoir une fonctionnalité d'extraction de l'ensemble des données à caractère personnel d'une personne donnée	□
		Prévoir les mécanismes facilitant l'exercice du droit d'accès pour les scénarios moins larges	□
8	Droit de rectification : respect du droit des personnes concernées de corriger leurs données et de les effacer	Permettre la rectification - si justifiée - des données personnelles collectées (mesure triviale)	□
9	Formalités : définition et accomplissement des formalités préalables applicables au traitement	Effectuer l'analyse du régime juridique et des formalités applicables au traitement en fonction de ses finalités et des catégories de données traitées avec l'aide du DPO, en amont du déploiement du traitement dans les établissements	□

La descente

Le référentiel « Fondamentaux de la protection by design/default externe »

	Point de Contrôle	Mesure conforme	
	10 En cas de sous-traitance	Insérer dans les contrats les clauses contractuelles de sous-traitance proposées par la CNIL après les avoir adaptées et précisées avec l'aide du DPO	☐
		En particulier pour les besoins de bases de formation ou de tests de masse (tests de performance sur données issues des établissements) : Prévoir de *contractualiser à l'avance la récupération des données d'un établissement*, non sur la base d'une « convention de confidentialité » entre l'Amue, le titulaire et les établissements qui voudraient bien coopérer, mais en prévoyant que le titulaire du marché leur fournisse un outil d'anonymisation adapté à appliquer par que l'établissement lui-même avant de transmettre à l'Amue ses données. La transmission des données au prestataire pour tests se fera ensuite sous forme déjà anonymisée.	☐
		Les mécanismes d'anonymisation proposés par le titulaire devront être correctement explicités et préalablement évaluables par l'Amue. Ces mécanismes devront être tels que l'établissement devra pouvoir, en toute autonomie, l'appliquer à ses propres données. Les mises à jour de la base (ou des bases) de formation ou de tests seront à réaliser par ré-applications successives de l'outil d'anonymisation sur les nouvelles données en établissement	☐
		Prévoir la mise à jour de l'outil d'anonymisation lui-même en cas de changement de structure, ou en cas de tout autre possible impact de versions évolutives du produit de l'offre SI Amue sur cet outil	☐
		Prévoir une clause générale impliquant une application du principe de protection *by design* propre à garantir qu'aucune déficience attachée à la conception même du produit ne puisse, lors de son exploitation, rendre impossible la vérification avec succès des points de contrôle de PIA (notamment concernant les mesures de nature juridique)	☐
		Prévoir une clause de « devoir de conseil » du prestataire en matière d'Informatique et Libertés (RGPD) et exigeant le respect par ce dernier du principe de protection *by design/default* à toutes les étapes du cycle de vie du produit de l'offre SI Amue	☐


La descente

Le référentiel « Fondamentaux de la protection by design/default externe »

	Point de Contrôle	Mesure
11	Renseignement fiche taitement	Renseigner la fiche (cf. feuille suivante)
12	Sécurité	Fournir aux établissements exploitant l'offre SI Amue les informations et moyens (liés aux logiciels) de prendre effectivement des mesures en fonction des risques pour garantir l'intégrité, la disponibilité et la confidentialité des données à caractère personnel
13	Etude d'impact sur la vie privée (EIVP/PIA)	En présence de données sensibles, fournir aux établissements exploitant l'offre SI Amue les informations et moyens (liés aux logiciels) de mener correctement le volet gestion des risques de l'étude d'impact sur la vie privée exigée par le règlement