

## LES INDICATEURS DE MATURITE RGPD DANS LES ETABLISSEMENTS D'ENSEIGNEMENT SUPERIEUR ET DE RECHERCHE



### Synthèse :

Le réseau SupDPO propose une grille d'auto-évaluation à destination des établissements de l'enseignement supérieur et de la recherche (ESR). Elle permet **d'apprécier le niveau de sa maturité organisationnelle** au Règlement général sur la protection des données (RGPD)<sup>1</sup>, sans préjuger de la conformité effective des traitements mis en œuvre avec ce Règlement.

Cette grille se base notamment sur le référentiel du label « Gouvernance » de la Commission nationale de l'informatique et des libertés (CNIL)<sup>2</sup> modifié en 2017<sup>3</sup>, ainsi que sur la *checklist* « Evaluer le niveau de sécurité des données personnelles de votre organisme »<sup>4</sup>.

Ces indicateurs ont vocation à être renseignés par l'agent en charge de la protection des données (le Délégué à la protection des données (DPO) de l'organisme, s'il existe), et à être validés par le responsable des traitements. Associés à un bilan d'activité, ils peuvent permettre de **constater un niveau de conformité**, de **tracer un plan d'action** et d'en constater les effets, ainsi que de préparer une candidature à une reconnaissance des mesures prises (labellisation, certification,...).

L'élaboration de cette grille a été proposée dans le cadre du comité de pilotage de la convention signée entre la CNIL, la CPU et le réseau SupDPO<sup>5</sup>, pour favoriser l'amélioration continue du niveau de protection des données à caractère personnel dans les établissements de l'ESR.

Elle pourrait utilement être complétée d'indicateurs issus de la grille d'évaluation de la Politique de sécurité des systèmes d'information de l'Etat (PSSIE), des critères du Référentiel général de sécurité (RGS), ainsi que d'une analyse liée aux exigences archivistiques et d'accès aux documents administratifs.

A renseigner selon le principe suivant :



0 : Mesure non appliquée - 1 : Mesure appliquée  
2 : Mesure appliquée et documentée - 3 : Mesure appliquée, documentée et auditée

*Les indicateurs apparaissant en rouge sont critiques : une note inférieure à 2 sera rédhibitoire pour considérer une quelconque maturité.*

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679>

<sup>2</sup> Délibération n°2014-500 du 11 décembre 2014 publiée au JO du 10 janvier 2015 a porté adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance « Informatique et libertés »

<sup>3</sup> Délibération n°2017-219 du 13 juillet 2017 portant modification du référentiel pour la délivrance de labels en matière de procédures de gouvernance tendant à assurer la protection des données

<sup>4</sup> [https://www.cnil.fr/sites/default/files/atoms/files/check\\_list.pdf](https://www.cnil.fr/sites/default/files/atoms/files/check_list.pdf)

<sup>5</sup> <https://www.cnil.fr/fr/la-cnil-et-la-conference-des-presidents-duniversity-cpu-renouvellent-leur-convention-de-partenariat>

Indicateurs relatifs à la gouvernance des données	
Un délégué à la protection des données a été désigné pour l'ensemble des traitements mis en œuvre par l'organisme.	0 1 2 3 ■ ■ □ □
Un archiviste est en poste au sein de la structure.	0 1 2 3 □ □ □ □
Un Responsable de la sécurité des systèmes d'information (RSSI) est en poste au sein de l'organisme.	0 1 2 3 □ □ □ □
Le délégué est en capacité de travailler en étroite coopération avec le Responsable de la sécurité des systèmes d'information (RSSI).	0 1 2 3 □ □ □ □
Indicateurs relatifs à la politique de protection des données	
Il existe une politique écrite ou "charte" en matière de protection des données personnelles.	0 1 2 3 □ □ □ □
Celle-ci a été approuvée au plus haut niveau de l'organisation (ex. Conseil d'administration pour une université).	0 1 2 3 □ □ □ □
Celle-ci a été portée à la connaissance des personnes concernées dans un format concis, transparent, compréhensible et aisément accessible.	0 1 2 3 □ □ □ □
Cette politique est réexaminée et actualisée si nécessaire, <i>a minima</i> tous les trois ans	0 1 2 3 □ □ □ □
Indicateurs relatifs au délégué à la protection des données	
Le délégué fait rapport directement au niveau le plus élevé de la gouvernance de l'organisme.	0 1 2 3 □ □ □ □
L'étendue des missions du délégué est clairement précisée dans une lettre de mission ou dans un contrat.	0 1 2 3 □ □ □ □
Le délégué peut entretenir et développer ses connaissances spécialisées.	0 1 2 3 ■ ■ □ □
Le délégué dispose des ressources et moyens nécessaires à l'exercice de ses missions.	0 1 2 3 □ □ □ □
Le délégué sensibilise à la protection des données à caractère personnel les différents niveaux de personnels et usagers (étudiants) de l'organisme.	0 1 2 3 □ □ □ □
Le délégué à la protection des données est associé systématiquement et en amont des réflexions sur toutes les questions relatives à la protection des données.	0 1 2 3 □ □ □ □
Le délégué a les moyens d'informer et de conseiller les personnels mettant en œuvre les traitements.	0 1 2 3 ■ ■ □ □
Indicateurs relatifs à l'analyse de la conformité	
Les traitements nécessitant une analyse d'impact ont été identifiés.	0 1 2 3 □ □ □ □
Les analyses d'impact nécessaires sont réalisées.	0 1 2 3 □ □ □ □
Le délégué est consulté pour toute analyse d'impact et vérifie son exécution.	0 1 2 3 □ □ □ □
Dans le cadre des analyses d'impact, il est prévu la possibilité de demander l'avis des personnes concernées.	0 1 2 3 □ □ □ □
Les opérations de sous-traitance sont encadrées par des actes juridiques prévoyant les clauses appropriées en matière de protection des données personnelles.	0 1 2 3 ■ ■ □ □
L'organisme tient à jour un registre des activités de traitement.	0 1 2 3 ■ ■ □ □

Les traitements sont documentés, notamment sur les aspects liés à la sécurité.	0 1 2 3 □ □ □ □
Il existe une cartographie des traitements mis en œuvre.	0 1 2 3 □ □ □ □
<b>Indicateurs relatifs à l'analyse de la conformité dans le temps</b>	
Les procédures mises en place sont régulièrement testées, analysées et évaluées, afin de vérifier leur efficacité.	0 1 2 3 □ □ □ □
Des mesures correctives sont adoptées en cas de manquement constaté lors de l'examen de conformité.	0 1 2 3 □ □ □ □
Ces mesures sont documentées et régulièrement mises à jour.	0 1 2 3 □ □ □ □
<b>Indicateurs relatifs à la gestion des réclamations et à l'exercice des droits des personnes</b>	
Une procédure encadrant l'exercice des droits des personnes est mise en place.	0 1 2 3 ■ ■ □ □
Le délégué pilote la gestion des demandes des personnes concernées relatives au traitement de leurs données et à l'exercice de leurs droits.	0 1 2 3 □ □ □ □
<b>Indicateurs relatifs à la gestion des violations de données</b>	
Une procédure de notification d'une violation de données à caractère personnel est mise en place.	0 1 2 3 ■ ■ □ □
<b>Indicateurs relatifs à la sécurité informatique</b>	
Une charte informatique est mise en place dans l'organisme.	0 1 2 3 □ □ □ □
Une politique de sécurité des systèmes d'information (PSSI) est mise en place.	0 1 2 3 □ □ □ □
Les utilisateurs accèdent au système d'information à l'aide d'un identifiant individuel.	0 1 2 3 ■ ■ □ □
Une gestion des habilitations (profils, révision, et suppression) est mise en place.	0 1 2 3 □ □ □ □
Les accès distants sont sécurisés par des mesures techniques (filtrage IP, VPN,...).	0 1 2 3 □ □ □ □
Le déploiement des mises à jour de sécurité est organisé.	0 1 2 3 □ □ □ □
Des audits de sécurité (internes, et auprès des sous-traitants) sont organisés.	0 1 2 3 □ □ □ □