université PARIS-SACLAY

RGPD

Pack de conformité à destination des informaticiens

Contenu

Ce pack de conformité à destination des informaticiens est une synthèse du « Pack de conformité des Universités et Grandes Ecoles au RGPD » rédigé à l'initiative du CSIESR (www.csiesr.eu), association professionnelle ayant pour objectif de contribuer au développement du numérique pour l'éducation, la culture et la recherche. Sa rédaction a été confiée à Me Eric Barbry et l'équipe IP/IT/DATA protection du cabinet Racine, avocats spécialisés dans le droit des nouvelles technologies et des données à caractère personnel.

1. RGPD - Présentation

1.1. Définitions

RGPD : Règlement Général sur la Protection des Données

Règlement européen sur la protection des données personnelles qui s'ajoute à la « loi Informatique et Libertés » (adaptée depuis), et ce, à partir du 25 mai 2018. Le RGPD définit la donnée à caractère personnel (DCP) comme toute information se rapportant à une personne physique identifiée ou identifiable, c'est-à-dire qui peut être identifiée directement ou indirectement grâce à celle-ci, ou au croisement de plusieurs données.

Le traitement désigne quant à lui toute opération ou tout ensemble d'opérations susceptible d'être effectué sur des données à caractère personnel, que ce soit ou non grâce à des procédures automatisées. Une liste non exhaustive d'opérations peut être proposée : collecte, enregistrement, structuration, conservation, extraction, consultation, utilisation, diffusion, etc.

1.2. Innovation majeure du RGPD : Le principe d'Accountability

« … The controller shall be responsible for, and be able to demonstrate compliance with, paragraphe 1 (accountability) »

La nécessité pour le responsable du traitement de démontrer sa conformité aux dispositions du RGPD apparaît de façon récurrente dans le corps du texte, où revient à plusieurs reprises la phrase aux termes de laquelle « ***le responsable du traitement doit s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement*** ». La démonstration de la conformité s'opère auprès des personnes concernées et de la Cnil, qui peut à tout moment effectuer un contrôle des traitements effectués par ce dernier.

⇨ **Renversement de la charge : Régime de preuve a priori devient a posteriori**

Avant RGPD, la personne doit démontrer que les DCP ne sont pas protégées
Après RGPD, le responsable du traitement doit prouver que les DCP sont protégées

1.3. Statuts des personnes en lien avec un traitement de données

- ***Personne concernée*** : Personne dont les données sont collectées et traitées, ce qui permet soit de l'identifier, soit de la rendre identifiable par recoupements avec d'autres données.
- ***Responsable du traitement*** : Personne physique ou morale, autorité publique, service ou tout organisme qui détermine les finalités et moyens d'un traitement.
- ***Sous-traitant*** : Personne physique ou morale, autorité publique, service ou tout organisme qui traite des DCP pour le compte du responsable du traitement.
- ***Destinataires de données*** : Personne physique ou morale, autorité publique, service ou tout autre organisme qui reçoit communication des données à caractère personnel.
- ***Délégué à la Protection des Données (DPD)*** : Personne physique désignée sur la base de ses compétences par un responsable du traitement afin d'être associée à toutes les questions relatives à la protection des DCP. Le DPD est titulaire des missions de conseil, de contrôle du respect du RGPD et de coopération avec la CNIL.

1.4. Autres définitions

- ***Collecte directe*** : fait de recueillir des données directement par l'intermédiaire de la personne concernée (envoi ou remise de données par la personne concernée).
- ***Collecte indirecte*** : fait de recueillir les données de la personne concernée par l'intermédiaire qui les communique au responsable du traitement.
- ***Données sensibles*** : données relatives à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la santé, ou des données concernant la vie sexuelle d'une personne physique.
- ***Données de connexion*** : données de nature à permettre l'identification de quiconque a contribué à la création d'un contenu en ligne (adresse IP, identifiant, date et heures de connexion, logs de connexion, etc).
- ***Profilage*** : traitement de données consistant à utiliser celles-ci pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire divers éléments.

2. Analyse thématique des essentiels du RGPD

- Principes directeurs
  - ✓ Le principe de minimisation
  - ✓ La durée de conservation
  - ✓ La licéité du traitement
  - ✓ La notion de consentement
- Droits de la personne concernée
  - ✓ L'obligation de transparence
  - ✓ Le droit d'accès et de copie
  - ✓ Le droit de rectification
  - ✓ Le droit à l'effacement
  - ✓ Le droit à la limitation du traitement
  - ✓ Le droit à la portabilité des données
  - ✓ Le droit d'opposition
  - ✓ Décision individuelle automatisée
- Statuts et responsabilité
  - ✓ Sous-traitance
  - ✓ Registre des traitements
  - ✓ Responsabilité conjointe
  - ✓ Le DPD
  - ✓ Transferts de données hors UE
- Protection et sécurisation
  - ✓ Protection by design/default
  - ✓ Obligation de sécurité
  - ✓ Violation de sécurité
  - ✓ Analyse d'impact

2.1. RGPD – Principes directeurs

2.1.1. Le principe de minimisation

Les données à caractère personnel doivent être :

- Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)

- Exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les DCP qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude).

⇨ Il s'avérerait opportun que l'établissement ESR déploie une cartographie des traitements mis en œuvre par lui en tant que responsable du traitement. La cartographie se définit comme un outil d'inventaire permettant d'identifier les différents traitements mis en œuvre par le responsable du traitement. Cette cartographie peut être réalisée par le DPD dans le cadre de la tenue du registre de l'établissement.

⇨ Cette cartographie est réalisée sous le prisme tant des métiers que des technologies et de renseigner quant à leurs principales caractéristiques. Parmi celles-ci figurent les finalités du traitement, qui doivent être énumérées, ainsi que la typologie des données traitées. (DPD)

2.1.2. La durée de conservation des données

La conservation des données à caractère personnel doit être limitée et proportionnée aux finalités du traitement.

- Données relatives aux étudiants

  - ✓ Droits d'inscription : 10 ans (prescription d'éventuelles dettes);
  - ✓ Gestion administrative : durée de l'inscription augmentée d'une période de 2 ans ;
  - ✓ Espace numérique de travail (ENT) : subordonnée à la signature par l'étudiant d'un accord des données, et ce jusqu'à ce que l'étudiant demande la suppression de celles-ci.

- Données relatives aux personnels

  - ✓ Gestion du personnel : 5 ans à compter du départ du salarié ;
  - ✓ Gestion de la paie : 5 ans à compter du dernier versement de la paie ;
  - ✓ Données de candidature : destruction immédiate du CV du candidat s'il n'a pas été retenu, mais possibilité de le conserver 2 ans pendant 2 ans après le dernier contact avec le candidat à condition que celui-ci soit informé ;
  - ✓ Annuaire du personnel : suppression des données une fois la période d'emploi de la personne concernée achevée ;
  - ✓ Données de connexion du salarié : 6 mois pour l'historique de connexion avec information préalable du salarié.

⇨ Il s'avérerait opportun d'adopter une politique de conservation des données, soit un document exclusivement consacré à cette thématique qui recenserait dans un tableau le point de départ du délai et la durée de conservation de chacun des traitements et la source permettant d'en justifier si elle existe. (DPD)

Il est à noter que les délais de conservation ne font pas obstacle aux impératifs d'archivage prévus par le Code du Patrimoine et les circulaires d'application.

2.1.3. La licéité des traitements

Pour être valable, un traitement à caractère personnel doit être licite.

Compte tenu de la grande diversité des traitements mis en œuvre par les établissements ESR, plusieurs bases légales permettent de justifier ces derniers.

- Traitements fondés sur le consentement ;
- Traitements fondés sur l'exécution d'un contrat entre la personne concernée et l'université ou la personne concernée et un autre organisme (ex : relation entre l'étudiant et le Crous pour la restauration universitaire) ;
- Traitements fondés sur une mission d'intérêt public (ex : formation initiale qui justifie les traitements mis en œuvre à des fins de gestion de la vie universitaire de l'étudiant ou du personnel salarié des établissements ESR) ;
- Traitements fondés sur une obligation légale (ex : allocation de bourses, médecine du travail).

2.1.4. Le consentement de la personne concernée

Dans le cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de DCP la concernant. La personne a le droit de retirer son consentement à tout moment. Il est aussi simple de retirer que de donner son consentement.

Le traitement des DCP relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 15 ans. Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur.

2.2. RGPD – Droits de la personne concernée

2.2.1. L'obligation de transparence

Le RGPD met à la charge du responsable de traitement une obligation générale de transparence vis-à-vis de la personne concernée, qui se matérialise par l'obligation de lui délivrer un certain nombre d'informations concernant le traitement et ses propriétés ainsi que les droits dont elle dispose et la façon de les mettre en œuvre. Il est nécessaire de communiquer à la personne concernée les 11 informations suivantes :

- Information à fournir en cas de collecte « directe »
- Information à fournir en cas de collecte « indirecte »
- Droit d'accès
- Droit de rectification
- Droit à l'effacement (droit à l'oubli)
- Droit à la limitation du traitement
- Obligation de notification aux destinataires des données
- Droit à la portabilité
- Droit d'opposition
- Décision individuelle automatisée (y compris le profilage)
- Communication à la personne concernée des violations

Les informations à fournir en cas de collecte sont par exemple, l'identité et les coordonnées du responsable de traitement, les coordonnées du DPD, les finalités et la base juridique du traitement, les destinataires du traitement, la durée de conservation des données, …

⇨ Il est recommandé la rédaction d'une politique Informatique et Libertés dont le principal objectif est de communiquer l'ensemble des informations exigées aux personnes concernées.

La sollicitation du DPD dans le cadre de la rédaction de ces mentions doit être systèmatique.

2.2.2. Le droit d'accès et de copie

Le droit d'accès est renforcé dans le cadre duRGPD en l'assortissant désormais d'un droit de copie, qui consiste en la fourniture par le responsable du traitement, à la demande de la personne concernée, d'une copie de l'ensemble des données à caractère personnel le concernant.

Incidence de la disposition sur l'établissement ESR par un exemple :

Dans un avenir proche, le nombre de demandes de droits d'accès pourrait toutefois croître de façon considérable du fait du recours à Parcoursup, la plateforme nationale d'admission des lycéens et étudiants dans les établissements qui remplace Admissions Post-Bac (APB) qui prévalait jusqu'alors. En effet, le candidat y effectue une préinscription en renseignant un grand nombre de données à caractère personnel (données d'identification, adresse email, numéro INE, relevés de notes du lycée et du baccalauréat, avis d'imposition des parents en cas de demande de bourse). Par la suite, le candidat formule des vœux d'affectation dans les établissements de son choix conformément à son souhait de poursuite d'études. Les éléments de préinscription précités sont par la suite communiqués aux établissements ESR concernés, lesquels formulent ensuite leur réponse au candidat. S'il est vrai que la plateforme est présentée comme étant « simple et transparente » et que les étudiants n'ont pas à classer leurs vœux contrairement à ce qui prévalait antérieurement sur APB, il est à craindre que certains candidats déçus de leur affectation cherchent à comprendre les raisons pour lesquelles ils n'ont pas été retenus dans la formation de leur choix. Dans une telle hypothèse, ils se tourneront davantage vers l'établissement ESR concerné que vers la plateforme Parcoursup, c'est pourquoi il conviendrait à titre préventif de prévoir des modalités d'exercice du droit d'accès des candidats et étudiants.

L'établissement ESR doit prévoir dans ses politiques Informatique et libertés une disposition spécifique à la mise en œuvre du droit d'accès et de copie, qui devra préciser les éléments suivants :

1. L'existence de ce droit et en quoi il consiste ;
2. Modalité d'exercice de ce droit ;
3. Contact pour exercer ce droit.

2.2.3. Le droit de rectification

La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des DCP la concernant qui sont inexactes. Compte tenu de la finalité du traitement, la personne concernée a le droit d'obtenir que les DCP incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

2.2.4. Le droit à l'effacement

La personne concernée a le droit de solliciter l'effacement des DCP la concernant, à condition de se situer dans l'une des hypothèses ci-dessous ;

- Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
- La personne concernée retire son consentement sur lequel est fondé le traitement ;
- Les DCP ont fait l'objet d'un traitement illicite.

Si le responsable du traitement n'a pas l'intention de donner suite à une demande d'effacement de la personne concernée, il devra informer la personne concernée des motifs de son refus, étant précisé qu'il dispose d'un délai d'un mois pour ce faire.
Ces réponses devront être éditées par le DPD et signées par le responsable du traitement.

2.2.5. Le droit à la limitation du traitement

Ce droit signifie concrètement la possibilité conférée à la personne d'obtenir la suspension temporaire du traitement de ses données, par exemple lorsqu'elle a formulé une demande d'effacement et quelques soit l'issue de cette dernière.

2.2.6. Le droit à la portabilité des données

Il s'agit du droit de la personne concernée de solliciter et d'obtenir la restitution des données la concernant auprès d'un responsable du traitement et/ou leur transmission auprès d'un autre responsable du traitement dans un format structuré, couramment utilisé et lisible par machine.

Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Le droit à la portabilité ne peut être mis en œuvre que si trois conditions cumulatives sont réunies :

- Les données sont communiquées par la personne concernée elle-même dans le cadre d'une collecte directe par le responsable du traitement ;
- Le traitement est fondé sur le consentement de la personne concernée ou sur l'exécution d'un contrat ou de mesures précontractuelles ;
- Le traitement est effectué à l'aide de procédés automatisés.

Le droit à la portabilité ne pourra être mis en œuvre s'agissant des données traitées par les établissements ESR que dans l'hypothèse des traitements reposant sur le consentement de la personne concernée.

2.2.7. Le droit d'opposition

Le droit d'opposition permet à la personne concernée d'obtenir que ses données ne soient plus traitées pour l'avenir par le responsable du traitement.

2.2.8. Décision individuelle automatisée (et profilage)

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, hormis pour les cas suivant :

- Nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
- Autorisé par le droit de l'Union ou le droit de l'Etat membre auquel le responsable de traitements est soumis ;
- Fondé sur le consentement explicite de la personne concernée.

Incidence de la disposition sur l'établissement ESR par un exemple :

Parcoursup étant autorisée par le droit français et notamment par l'article L.612-3 du Code de l'éducation, la personne n'est pas pourvue du droit d'exiger de ne pas faire l'objet d'une décision fondée sur une décision individuelle automatisée s'agissant de son affectation à l'université. S'agissant de la transparence, les établissements ESR doivent impérativement fournir aux candidats une information aussi exhaustive que possible sur les techniques de sélection auxquelles ils recourent dans la politique Informatique et liberté élaborée à leur destination.

D'après le Conseil constitutionnel (CC, 12 juin 2018, Loi relative à la protection des données personnelles, déc. N°2018-765DC), le seul recours à un algorithme pour fonder une décision administrative individuelle est subordonné au respect de trois conditions :

- D'une part, conformément à l'article L. 311-3-1 du code des relations entre le public et l'administration, la décision administrative individuelle doit mentionner explicitement qu'elle a été adoptée sur le fondement d'un algorithme et les principales caractéristiques de mise en œuvre de ce dernier doivent être communiquées à la personne intéressée, à sa demande.
- D'autre part, la décision administrative individuelle doit pouvoir faire l'objet de recours administratifs, conformément au chapitre premier du titre premier du livre quatrième du code des relations entre le public et l'administration. L'administration sollicitée à l'occasion de ces recours est alors tenue de se prononcer sans pouvoir se fonder exclusivement sur l'algorithme.
- Enfin, le recours exclusif à un algorithme est exclu si ce traitement porte sur l'une des données sensibles.

En dernier lieu, le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions, ce qui interdit l'usage d'algorithmes auto-apprenants.

2.3. RGPD – Statuts et responsabilité

2.3.1. Sous-traitance

La relation entre le responsable du traitement et le sous-traitant est le contrat ou l'acte juridique qui les lie, qui doit être établi par écrit.

Ce contrat ou acte juridique doit obligatoirement incorporer les affirmations suivantes :

- Le sous-traitant présente des garanties appropriées s'agissant de la mise en œuvre de mesures techniques et organisationnelles lui permettant de se conformer à ses obligations ;
- Le sous-traitant s'engage à respecter une obligation spécifique de confidentialité ;
- Le sous-traitant aide le responsable du traitement afin de donner suite aux demandes d'exercice des droits dont la personne concernée est investie ;
- Le sous-traitant, aux termes du contrat, s'engage soit à supprimer toutes les données, soit à les renvoyer au responsable du traitement.

Des clauses-types, disponibles sur le site internet de la Cnil, peuvent être jointes aux contrats pour s'assurer de la conformité du sous-traitant.

Le RGPD rompt avec la philosophie de la loi de 1978 (ancienne version), en ce qu'elle ne concevait que la responsabilité du responsable du traitement. Désormais, il existe une co-responsabilité entre le responsable du traitement et son sous-traitant.

2.3.2. Le registre des traitements

Le RGPD modifie profondément la philosophie applicable à la protection des DCP par la création d'un principe d'*accountability*. Alors que la loi Informatique et libertés exigeait jusqu'à présent l'accomplissement par le responsable du traitement de démarches et formalités auprès de la Cnil (déclarations ou autorisations), tel n'est plus le cas. Il doit désormais veiller et démontrer seul sa conformité aux règles de protection érigée par le RGPD.

Chaque responsable de traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

- Le nom et coordonnées du responsable du traitement ;
- Les finalités du traitement ;
- Une description des catégories de personnes concernées et des catégories de DCP ;
- Les catégories des destinataires.

En pratique, c'est le DPD qui tient le registre des traitements. Tous les traitements devant y être consignés, il est important de se référer systématiquement au DPD lors de la mise en place de tout traitement.

2.3.3. Responsabilité conjointe

Le RGPD crée la notion de responsabilité conjointe d'un traitement de DCP, qui a vocation à s'appliquer lorsque plusieurs responsables du traitement agissent conjointement s'agissant d'un même traitement, en déterminant ensemble ses moyens et finalités.

2.3.4. Le Délégué à la Protection des Données (DPD)

Le RGPD institue la notion de « Data Protection Officer (DPO) », traduite comme « Délégué à la Protection des Données (DPD) », qui remplace l'ancien Correspondant Informatique et Libertés (CIL) de la loi du 6 janvier 1978.

Le DPD est obligatoire si le responsable du traitement est un organisme ou une autorité publique.

Pour l'Université Paris-Saclay, le contact est dpd@universite-paris-saclay.fr

2.3.5. Transferts de données hors UE

Il est nécessaire de prendre en considération l'existence ou non d'une décision d'adéquation du niveau de protection du destinataire de transfert, qui se définit comme une décision d'adéquation de la Commission constatant que le pays concerné assure un niveau de protection adéquat au regard de la réglementation applicable à la protection des DCP.

Si tel est le cas, le transfert des données est libre, aucune formalité n'est à accomplir ni aucune autorisation particulière à recueillir. A l'inverse, en l'absence de décision d'adéquation, le transfert de données est interdit sauf si le destinataire des données met en œuvre des garanties appropriées.

2.4. RGPD – Protection et sécurisation

2.4.1. Protection by design et by default

Le responsable du traitement a une obligation de protection qui se décline en deux obligations distinctes, une obligation de protection des données dès la conception (« privacy by design ») et une obligation de protection des données par défaut (« privacy by defaults »).

La protection des données dès la conception suppose que le responsable du traitement, en amont de la mise en œuvre d'un traitement et ultérieurement une fois celui-ci effectif, envisage tous les moyens permettant de protéger les données et appliquer les principes relatifs à cette protection. Il doit à ce titre mettre en œuvre des mesures à la fois techniques (chiffrement, pseudonymisation, …) et organisationnelles (règles de minimisation).

La protection des données par défaut suppose que le responsable du traitement ne traite que les DCP strictement nécessaires au regard des finalités du traitement et limite l'accès à celles-ci aux seules personnes habilitées.

En pratique, pour être accompagné dans la mise en œuvre du principe de protection dès la conception, il est nécessaire de solliciter le DPD, de manière systématique, et ce, dès l'origine du projet de mise en place d'un traitement de données. Celui-ci accompagnera alors les acteurs dans la mise en place d'une conformité, qu'il pourra par ailleurs documenter en cas de contrôle.

2.4.2. Obligation de sécurité

Le responsable du traitement a une obligation de sécurisation des traitements des DCP mis en œuvre rédigée comme suit selon les besoins :

- La pseudonymisation et le chiffrement des DCP ;
- Des moyens permettant de garantir la confidentialité, l'intégrité et la disponibilité des systèmes et des services de traitement ;
- Des moyens permettant de rétablir la disponibilité des DCP et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2.4.3. Violation de sécurité

Compte tenu de l'ampleur des failles de sécurité et des conséquences très préjudiciables qu'elles sont susceptibles d'emporter, tant pour les personnes concernées que pour le responsable du traitement (préjudice d'image), la notification de la faille à la Cnil doit intervenir dans un délai de 72 heures après prise de connaissance et doit comporter les informations ci-dessous :

- Nature de la violation de DCP ;
- Communiquer le nom et les coordonnées du DPD ;
- Conséquences probables de la violation des DCP ;
- Décrire les mesures ou que le responsable du traitement propose de prendre pour remédier à la violation des DCP.

La seconde obligation consiste à la communication à la personne concernée de la faille et de ses conséquences réelles ou supposées lorsque celle-ci est susceptible de porter atteinte à ses droits et libertés. L'établissement ESR doit établir une procédure destinée à la fois à juguler la faille et ses conséquences le plus rapidement possible et à s'acquitter de ses obligations vis-à-vis de la Cnil et, le cas échéant, des personnes concernées par la faille. La procédure devra respecter les étapes suivantes :

- Identifier et corriger la faille dans un premier temps afin de limiter au maximum les conséquences sur les DCP ;
- Constituer un dossier de preuves (description de la faille identifiée, conséquences réelles ou supposées, mesures prises pour la corriger) ;
- S'interroger sur la qualification juridique (dépôt d'une plainte pénale) ;
- Notifier à la Cnil la violation de sécurité ;
- Si la faille de sécurité emporte des conséquences sur des DCP, communiquer aux personnes concernées.

2.4.4. Analyse d'impact

La Cnil considère que les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact :

- Evaluation, soit traitements de données mis en œuvre afin d'affecter une note à une personne ;
- Décision automatique avec effet légal ou similaire ;
- Collecte de données sensibles ;
- Collecte de données personnelles à grande échelle ;
- Traitement de données d'une personne considérée comme vulnérable (patients, personnes âgées, enfants) ;
- Exclusion du bénéfice d'un droit ou d'un contrat par le traitement de données lui-même.

Exemple sur l'établissement ESR :

Parcoursup est susceptible de nécessité la mise en œuvre d'une analyse d'impact. En effet, les établissements ESR sont libres du choix de la méthode mise en œuvre pour sélectionner les étudiants. Certains recourent à des dispositifs de « décision individuelle automatisée » qui rassemblent plusieurs des critères précités : évaluation des candidatures, décision automatique avec effet légal, peut concerner une personne vulnérable (mineur), susceptible d'exclure un candidat.

Là encore, cette obligation impose au service métier de solliciter le DPD dès l'origine pour qu'il participe ou réalise l'étude d'impact nécessaire, le cas échéant.

Annexe : Acronymes

CNIL : Commission Nationale Informatique et Libertés

DCP : Donnée à Caractère personnel

DPD : Délégué à la Protection des Données

ENT : Espace numérique de travail

ESR : Enseignement Supérieur et Recherche

RGPD : Règlement Général sur la Protection des Données

UE : Union Européenne