racine
AVOCATS

CSIESR
Association Loi 1901

# Pack de conformité des Universités et Grandes Ecoles au RGPD

## Information aux lecteurs

Le présent pack de conformité RGPD a été 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.

Ce pack de conformité est destiné à aider les établissements d'enseignement supérieur et de recherche dans leur démarche de mise en conformité au RGPD.

Le document est constitué de fiches pratiques et documents types.

Le CSIESR attire cependant votre attention sur le fait qu'il ne s'agit là que de modèles ou d'exemples de documents qu'il vous appartient ou non d'utiliser et dans tous les cas de personnaliser.

La mise en conformité est une démarche propre à chaque établissement et doit tenir compte de votre environnement technique, votre organisation et vos usages.

Nous vous invitons dans tous les cas à vous faire assister par un conseil interne ou externe dans le cadre de la mise en œuvre du RGPD.

Le présent pack tient compte de la règlementation au 25 mai 2018 et ne saurait préjuger des évolutions règlementaires ou futures recommandations de la Cnil.

Le présent document ne saurait engager ni le CSIESR ni le cabinet Racine.

## SOMMAIRE

# 1. PRESENTATION

Le présent pack de conformité a vocation à présenter aux établissements d'enseignement supérieur et de recherche (ci-après désignés « les établissements ESR ») la démarche à accomplir pour se conformer aux obligations auxquelles ils sont assujettis en vertu des dispositions du RGPD et pour assurer leur conformité à l'ensemble de ses dispositions.

Après une présentation générale du RGPD et des évolutions qu'il emporte ainsi que de ses incidences sur les établissements ESR, le présent document envisagera les différentes thématiques qui doivent attirer l'attention de celles-ci dans le cadre de leur mise en conformité à ce nouveau règlement.

# 2. ÉLEMENTS CONTEXTUELS : RGPD, UNIVERSITES ET GRANDES ECOLES

## 2.1. QU'EST-CE QUE LE RGPD ?

La protection des données à caractère personnel a connu ces dernières années un essor considérable compte tenu des nouveaux usages faits des données et de la prise de conscience par les personnes concernées de l'utilisation faite de celles-ci. Cet essor, couplé à la fragmentation importante des règles applicables au sein de des différents États membres, a rapidement entraîné la nécessité d'une réforme de la directive du 24 octobre 1995[1] *(Annexe n°1 : présentation du RGPD)*.

En janvier 2012, une réforme globale de la règlementation applicable a été proposée par la Commission européenne, avec pour problématique générale l'encadrement des hypothèses d'utilisation des données dans l'optique de renforcer et protéger les droits des personnes concernées, ce qui répondait à une véritable demande de la société, sans pour autant empêcher le développement économique en freinant l'économie florissante de la donnée.

Le 27 avril 2016, les instances européennes, grâce à la participation active du G29, sont parvenues à un règlement dit « règlement général sur la protection des données » (ci-après appelé « RGPD »)[2]. Le texte, bien que doté d'une vocation pédagogique indéniable, accroit considérablement les obligations à la charge des responsables de traitement et sous-traitants et renforce les droits des personnes concernées. Composé de 99 articles, ses 173 considérants de principe explicitent certaines notions et confèrent leur légitimité à ces nouvelles dispositions.

Le RGPD représente un enjeu d'envergure pour la quasi-totalité des structures quels que soient leur secteur d'activité, leur taille et leur statut. En effet, il fait peser sur les responsables de traitement et sous-traitants d'importants risques, qui s'observent à quatre niveaux distincts :

- Risque financier : le RGPD prévoit la possibilité d'être condamné à la plus élevée des deux sommes entre 10 à 20 millions d'euros ou jusqu'à 2 à 4% du chiffre d'affaires annuel mondial. Par ailleurs, il consacre la réparation du préjudice de chaque personne lésée par un manquement à ses dispositions ainsi que la possibilité de mettre en œuvre une action de groupe pour avoir de meilleures chances d'obtenir réparation ;

[1] 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

[2] 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)

- Risque pénal dans la mesure où de nombreux manquements aux dispositions du RGPD constituent des infractions pénales ;
- Risque sur le système d'information et la continuité de l'activité dans la mesure où le RGPD rend possible la suspension, l'arrêt ou la limitation du traitement litigieux.
- Risque en termes d'image dans la mesure où certaines décisions de condamnation sont susceptibles d'être rendues publiques par la Cnil.

Compte tenu des évolutions générées, un délai de mise en conformité de deux ans a été accordé aux États membres et aux acteurs concernés : les dispositions du RGPD deviendront applicables au 25 mai 2018. À cette date, les principaux textes alors en vigueur seront alors abrogées, tels que notamment la directive 95/46/CE du 24 octobre 1995 précitée et, pour la France, la loi Informatique et libertés du 6 janvier 1978[3] et ses décrets d'application[4].

Bien que le RGPD, contrairement à une directive, ne suppose pas de transposition dans le droit interne des États membres, les cinquante-sept renvois qu'il opère à la loi nationale ont nécessité l'adoption de textes à échelle nationale. En France, un projet de loi dit « LIL 3 » a été déposé devant l'Assemblée nationale le 13 décembre 2017[5] et a été adopté en lecture définitive devant cette même instance le 14 mai 2018[6], bien qu'il fasse l'objet d'un recours devant le Conseil constitutionnel.

Compte tenu de l'ensemble de ces bouleversements, le RGPD implique de la part de l'ensemble des acteurs concernés une mise en conformité à ses nouvelles dispositions. Cette mise en conformité constitue un véritable projet d'entreprise, avec une véritable impulsion politique, la constitution d'une équipe projet dédiée et enfin la mise à disposition de moyens techniques, financiers et matériels.

## 2.2. JARGONNEZ-VOUS RGPD ?

### 2.2.1. Définitions principales : données et traitements

Outre les considérants de principe qui permettent de définir un certain nombre de notions, l'article 4 du RGPD pose les définitions fondamentales. À ce titre, le RGPD repose sur deux notions clés largement appréhendées que sont la notion de donnée à caractère personnel et celle de traitement.

Le RGPD définit ainsi la donnée à caractère personnel 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. Ainsi, une information qui à première vue ne permettrait pas d'identifier une personne physique mais qui entraînerait son identification par recoupement avec d'autres informations est considérée comme une donnée à caractère personnel. Cette acception large englobe de nombreuses informations : outre les noms, prénoms, adresses, numéro de téléphone, etc., sont également concernés identifiant en ligne, numéro d'identification, adresse IP ou encore donnée biométrique, génétique ou physiologique.

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 procédés automatisés.

[3] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[4] Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978
[5] Projet de loi relatif à la protection des données personnelles, n°490, déposé le 13 décembre 2017
[6] Projet de loi relatif à la protection des données personnelles, adopté en Lecture définitive par l'Assemblée nationale le 14 mai 2018, TA n°113 (texte adopté provisoire avec liens vers les amendements)

L'article 4 cite une liste non exhaustive d'opérations : collecte, enregistrement, organisation, structuration, conservation, extraction, consultation, utilisation, diffusion, etc.

### 2.2.2. Statuts des personnes en lien avec un traitement de données

Par ailleurs, le RGPD appréhende plusieurs statuts susceptibles d'être revêtus par toute personne intervenant autour des données à caractère personnel :

| N° | Statut | Définition | Articles concernés |
|---|---|---|---|
| 1 | 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. | Considérants,<br>Article 4,<br>Articles 12 et s.,<br>Articles 77 et s. |
| 2 | Responsable de traitement | Personne physique ou morale, autorité publique, service ou tout organisme qui détermine les finalités et moyens d'un traitement. Le responsable du traitement est responsable de la mise en œuvre du traitement et des garanties que celui-ci doit présenter (licéité, droits et information de la personne concernée, sécurité, etc.). | Considérants,<br>Article 4,<br>Articles 24,<br>Article 82. |
| 3 | Sous-traitant | Personne physique ou morale, autorité publique, service ou tout organisme qui traite des données à caractère personnel pour le compte du responsable de traitement. Le sous-traitant doit présenter des garanties de fiabilité au sous-traitant et est assujetti à un certain nombre d'obligations, ce qui constitue une nouveauté par rapport à la directive 95/46/CE. | Considérants,<br>Article 4,<br>Article 28,<br>Article 82. |
| 4 | Destinataire de données | Personne physique ou morale, autorité publique, service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Contrairement au responsable de traitement et au sous-traitant, le destinataire ne traite pas les données. | Considérants,<br>Article 4,<br>Article 19. |
| 5 | Responsable conjoint de traitement | Responsable de traitement qui détermine les finalités et moyens d'un traitement de façon conjointe avec un autre responsable de traitement, étant précisé que les prérogatives peuvent être librement réparties entre les co-responsables de traitement. | Considérants,<br>Article 4,<br>Article 26,<br>Article 82. |
| 6 | Délégué à la protection des données (DPO) | Personne physique désigné sur la base de ses compétences, de façon facultative ou obligatoire, par un responsable de traitement ou un sous-traitant afin d'être associé à toutes les questions relatives à la protection des données à caractère personnel. Le DPO est titulaire de missions de conseil, de contrôle du respect du RGPD et de coopération avec la Cnil. | Articles 37-39 relatifs à sa désignation, ses missions et fonctions |

### 2.2.3. Autres définitions d'ordre technique

Au-delà des définitions précitées, le RGPD fait référence à un certain nombre de notions techniques, lesquelles ne sont pas systématiquement définies par le texte, même si l'article 4 ou certains considérants de principe les appréhendent. Afin de clarifier les développements ultérieurs, il convient ainsi de retenir les définitions suivantes :

- Collecte directe : fait de recueillir des données directement par l'intermédiaire de la personne concernée, c'est-à-dire soit par envoi ou remise des données au responsable de traitement par la personne concernée elle-même, soit par collecte de données techniques relatives aux actions accomplies par celle-ci sur un service de communication en ligne ;

- Collecte indirecte : fait de recueillir les données d'une personne concernée par l'intermédiaire d'un tiers qui les communique au responsable de traitement afin qu'elles soient ultérieurement traitées par lui ;

- Données sensibles : données relatives à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation 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, ce qui englobe notamment l'adresse IP, l'identifiant, les date et heures de connexion, les logs de connexion, le nom du serveur cache requis par l'utilisateur, etc. La notion de données de connexion est assimilable à celles de données de trafic ou de données techniques ;

- 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 (rendement au travail, situation économique, santé, préférences personnelles, intérêts, fiabilité, comportement localisation ou déplacements de la personne concernée) ;

- Décision individuelle automatisée : décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques sur la personne concernée ou l'affectant de manière significative de façon similaire ;

- Violation de données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

- Pseudonymisation : fait de traiter des données à caractère personnel de façon à ce qu'elles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces dernières soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données ne sont pas attribuées à une personne physique identifiée ou identifiable ;

- Chiffrement ou cryptage : procédé de cryptographie par lequel une donnée lisible en clair est convertie, par l'intermédiaire d'une clef de chiffrement, dans un format codé permettant sa lecture uniquement après déchiffrement.

## 2.3. UNE INNOVATION MAJEURE DU RGPD : LE PRINCIPE D'ACCOUNTABILITY

L'une des évolutions majeures du RGPD réside dans le changement de paradigme total qu'il engendre par rapport à la philosophie de la loi Informatique et libertés du 6 janvier 1978. Sous l'empire de cette loi, le responsable de traitement devait, préalablement à la mise en œuvre d'un traitement, accomplir un certain nombre de formalités auprès de la Cnil, telles que la déclaration d'un traitement ou une demande d'autorisation de celui-ci.

Désormais, le RGPD abandonne l'accomplissement de formalités auprès de l'autorité nationale de contrôle au profit du principe d'accountability, qui pourrait être défini comme un processus permanent et dynamique de mise en conformité d'un organisme à la règlementation applicable grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques correspondantes (ex : politique de protection des données, codes de bonne conduite, certifications, etc.).

Le terme d'accountability, qui se réfère ainsi à la proactivité du responsable de traitement dans la démonstration de sa conformité aux dispositions du RGPD, n'a pas de véritable traduction française, il provient de l'article 5 2) du RGPD dans sa version anglaise, aux termes duquel :

> *"(…) 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")".*

La nécessité pour le responsable de 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 de traitement doit s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* »[7]. 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.

Le principe d'accountability a également vocation à s'appliquer au sous-traitant, qui le met en œuvre vis-à-vis de la Cnil mais aussi et surtout vis-à-vis du responsable de traitement susceptible de faire appel à ses services ou déjà engagé auprès de lui.

## 2.4. L'IMPACT DU RGPD SUR LES ETABLISSEMENTS ESR

À l'heure actuelle, les établissements ESR se trouvent particulièrement impliqués et au cœur de la protection des données à caractère personnel, et donc de la mise en conformité aux dispositions du RGPD, pour plusieurs raisons telles que principalement :

- L'accroissement significatif de l'usage des nouvelles technologies dans les établissements ESR, qui revêt des formes très variables et concerne à la fois les apprenants, les enseignants

[7] Article 24, considérants (74), (78) et (81) du RGPD

et le personnel administratif. La généralisation des Espaces Numériques de Travail, la tendance émergente du Learning Analytics afin d'optimiser les apprentissages ou encore les MOOCs[8] permettant de suivre gratuitement une formation à distance constituent autant d'hypothèses nouvelles nécessitant le traitement de données à caractère personnel.

- Le fonctionnement d'un établissement ESR suppose la mise en œuvre de très nombreux traitements de données à caractère personnel, lesquels présentent des caractéristiques très variables. Ainsi, la liste des personnes concernées par les traitements mis en œuvre par l'établissement ESR est très étendue et concerne à la fois des personnes hébergées en son sein (personnel salarié et enseignant, apprenants, stagiaires étudiants, professeurs invités, etc.) ou extérieures à celui-ci (maîtres de stages, visiteurs, invités, prestataires, etc.). S'agissant des données traitées en tant que telles, certaines sont susceptibles d'être qualifiées de sensibles (données de santé, appartenance syndicale, données relatives à d'éventuelles infractions ou condamnations, etc.), et il existe plusieurs hypothèses de traitement de données de mineurs.

- Enfin, les établissements ESR sont des personnes publiques, ce qui à ce titre les assujettit à des obligations particulières prévues par le RGPD, telles que notamment l'obligation de désigner un délégué à la protection des données (DPO) figurant à l'article 37 du RGPD. Dans leur démarche de mise en conformité aux dispositions du règlement, les établissements ESR doivent donc avoir pleine connaissance des spécificités de leur statut.

S'agissant du statut des établissements ESR, ils sont a priori responsables de traitement dans la mesure où ils mettent en œuvre de nombreux traitements en interne, pour des finalités distinctes : traitements relatifs aux candidatures, aux examens et concours, aux laboratoires de recherche, aux Espaces Numériques de Travail, à la gestion des services de bibliothèques, etc.

En qualité de responsable de traitement, il existe plusieurs hypothèses dans lesquelles les établissements ESR externalisent les données traitées et recourent à des sous-traitants, que ce soit en mode SaaS ou en mode on-premise. Par ailleurs, les destinataires externes sont très nombreux : peuvent être cités le Cnous et les Crous, les bibliothèques universitaires, la CAF, les organismes de mutuelle étudiante, l'URSSAF pour le personnel salarié, etc.

Il convient également d'appréhender la problématique des composantes facultaires, anciennement dénommes UFR, qui sont dotées de la personnalité morale et agissent parfois de façon totalement indépendante de l'établissement ESR, ce qui peut les amener à mettre en œuvre leurs propres traitements de données à caractère personnel. Dans une telle perspective, les composantes facultaires pourraient être qualifiées de responsables de traitement, ce qui donnerait lieu à un cas de coresponsabilité de traitement avec l'établissement ESR concerné et nécessiterait le respect de plusieurs diligences, telles que notamment l'adoption d'un contrat de coresponsabilité.

L'ensemble des spécificités des établissements ESR du point de vue de la protection des données à caractère personnel justifie la mise en œuvre d'un tel pack de conformité exclusivement dédié à ces derniers afin de les accompagner dans leur démarche de mise en conformité aux dispositions du RGPD.

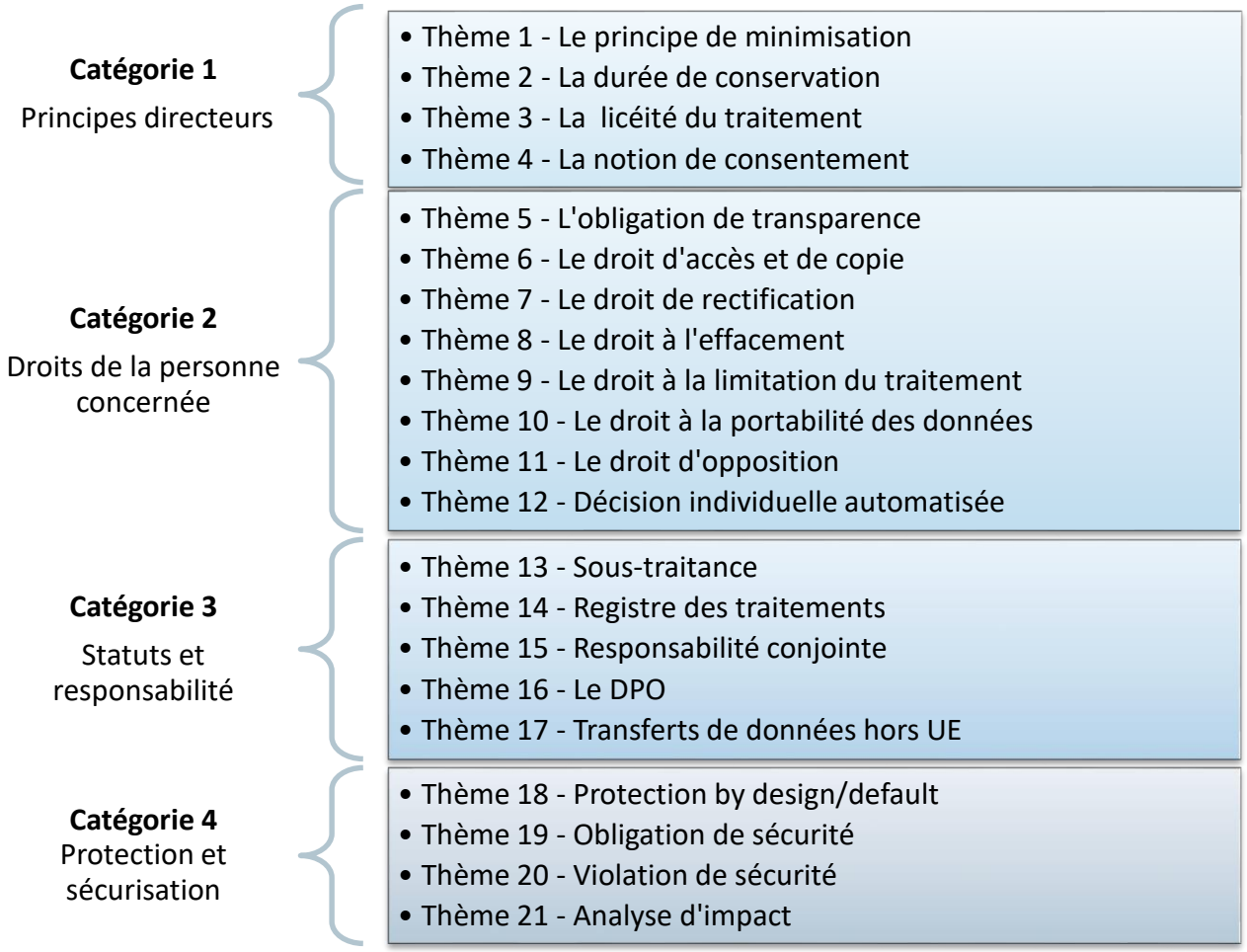
****

[8] Massive Open Online Courses, traduit en français par « cours en ligne ouverts à tous ». En France, peuvent être cités Coursera, OpenClassrooms, France Université Numérique (FUN), Udacity ou encore edX

## 3. ANALYSE THEMATIQUE DES ESSENTIELS DU RGPD

La présente analyse a pour objectif de cerner les principales thématiques dont les établissements ESR doivent prendre connaissance dans l'optique de leur mise en conformité au RGPD. La sélection desdites thématiques repose sur l'analyse des réponses fournies au questionnaire rempli par les dix établissements ESR ayant accepté de faire partie d'un échantillon représentatif.

L'analyse des réponses fournies à ce questionnaire a permis d'isoler les thématiques suivantes :




Chacune de ces thématiques sera envisagée de façon similaire en respectant le plan suivant :

- L'obligation telle que résultant du RGPD, avec la citation de l'article concerné et l'explicitation de ou des obligation(s) subséquente(s) ;

- L'incidence de la disposition concernée sur les établissements ESR et le degré d'exposition au risque en cas d'irrespect de celle-ci ;

- La mise en conformité, c'est-à-dire les démarches qu'il convient d'adopter et les documents et/ou procédures qu'il faut mettre en place dans les établissements ESR afin de se montrer conforme à la disposition concernée et de respecter la ou les obligation(s) qu'elle met à leur charge.

Le présent document incorporera également à titre d'annexes les modèles de livrables envisagé dans le présent guide, auquel il sera systématiquement renvoyé en temps utiles.

## 3.1. LE PRINCIPE DE MINIMISATION

### 3.1.1. Obligation

L'article 5 1) du RGPD envisage les six principes fondateurs qui gouvernent tout traitement de données à caractère personnel, et qui englobent notamment le principe dit de minimisation, envisagés au point c) en les termes suivants :

> *« 1. Les données à caractère personnel doivent être :*
> *(…) c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;*
> *d) exactes et, si nécessaires, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) (…) ».*

Le principe de minimisation signifie que, lors de la mise en œuvre d'un traitement de données, le responsable de traitement doit s'interroger sur les finalités de celui-ci, c'est-à-dire ses objectifs, afin de ne collecter et traiter que les données essentielles à l'accomplissement de celles-ci à l'exclusion de celles seulement susceptibles de présenter une utilité, qui ne serait que supposée et non avérée.

### 3.1.2. Incidence de la disposition sur l'établissement ESR

La particularité des établissements ESR réside dans le fait que pour fonctionner, ils mettent en œuvre une multitude de traitements de données à caractère personnel, lesquels se caractérisent par leur grande hétérogénéité à tout point de vue :

- la grande diversité de personnes concernées par ces différents traitements, qui peuvent être distinguées selon qu'il s'agit de personnel hébergé dans l'établissement ESR ou extérieur à celui-ci ;
- la grande diversité des finalités poursuivies par les différents traitements ;
- la présence de destinataires internes ou externes parfois multiples pour un même traitement ;
- la diversité des données susceptibles d'être traitées, qui peuvent dans certains cas être des données sensibles ou des données relatives à un enfant mineur ;
- le recours, en fonction des traitements, à des moyens de collecte directe ou indirecte, etc.

Cette hétérogénéité est susceptible de présenter certaines difficultés s'agissant des données collectées pour chacun des traitements. Pour autant, il ne s'avèrerait pas opportun d'exploiter les mêmes données pour chaque personne concernée et pour chacun des traitements mis en œuvre par lui et susceptible de la concerner, car cela ne respecterait pas le principe de minimisation.

### 3.1.3. Mise en conformité de l'établissement ESR

Afin de se conformer au principe de minimisation, il s'avèrerait opportun que l'établissement ESR déploie une cartographie des traitements mis en œuvre par lui en tant que responsable de traitement. La cartographie se définit comme un outil d'inventaire permettant d'identifier les différents traitements mis en œuvre par un responsable de traitement 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. Le fait de confronter ces deux caractéristiques permet de se renseigner quant à la nécessité de traiter certaines données conformément aux finalités du traitement et, le cas échéant, de suspendre la collecte des données qui s'avèreraient inutiles et compromettraient le respect du principe de minimisation *(Annexe n°2 – Modèle de cartographie des traitements)*.

## 3.2. LA DUREE DE CONSERVATION DES DONNEES

### 3.2.1. Obligation

L'article 5 1) e) du RGPD pose le principe selon lequel la conservation des données à caractère personnel doit être limitée et proportionnée aux finalités du traitement. Aux termes de cet article :

> *« 1. Les données à caractère personnel doivent être :*
> *(…) e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ».*

Ce principe n'est pas une innovation du RGPD : il existait déjà sous l'empire de la loi Informatique et libertés du 6 janvier 1978. La référence à un principe de proportionnalité a pour conséquence que très peu de durées de conservation sont légalement définies. En la matière, la Cnil délivre régulièrement des recommandations, notamment au travers de normes simplifiées, qui permettent de déterminer une durée maximale de conservation. En l'absence d'indication quant à une durée de conservation, il convient de s'interroger quant à une durée raisonnable au regard des finalités.

### 3.2.2. Incidence de la disposition sur les établissements ESR

L'appréhension de la thématique de la durée de conservation s'avère fondamentale dans l'enseignement supérieur dans la mesure où l'établissement ESR met en œuvre des traitements très diversifiés du point de vue de leurs finalités, ce qui justifie des durées de conservation différentes et souvent insusceptibles d'harmonisation dans la mesure où elles dépendent desdites finalités.

Par ailleurs, il existe des obligations d'archivage des documents produits par les établissements ESR et services de l'éducation nationale. En témoigne notamment une instruction ministérielle du 22 février 2005 relative au tri et à la conservation des archives reçues et produites par les services d'enseignement quels qu'ils soient[9].

Cette instruction élabore des tableaux d'archivage : pour chaque document, est précisé la durée d'utilisation administrative afférente (DUA), soit la durée au cours de laquelle il peut être conservé dans les locaux de l'établissement ESR en tant qu'archive nécessaire à la bonne marche de celui-ci, et le sort des documents à l'issue de la DUA (destruction ou versement aux archives départementales).

[9] Instruction n°2005-003 du 22 février 2005 de tri et de conservation pour les archives reçues et produites par les services et établissements concourant à l'éducation nationale (NOR : MENA0501142J)

Bien que cette instruction concerne les documents administratifs et non les données qu'ils incorporent, elle donne une orientation judicieuse sur les durées maximales de conservation qu'il convient de respecter, étant précisé que la loi et la Cnil ont prévu un certain nombre de durées de conservation s'agissant des données relatives à l'enseignement supérieur, telles que notamment :

- données relatives aux droits d'inscription : 10 ans (prescription d'éventuelles dettes) ;
- données relatives à la gestion administrative de l'étudiant : durée de l'inscription au sein de l'établissement ESR augmentée d'une période de 2 ans ;
- données traitées dans le cadre de l'Espace Numérique de Travail (ENT) : conservation subordonnée à la signature par l'étudiant d'un accord de conservation des données et ce jusqu'à ce que l'étudiant demande la suppression de celles-ci.

Au-delà des obligations de conservations propres aux données relatives à l'enseignement supérieur et aux apprenants, les établissements ESR doivent considérer les obligations de conservation applicables aux autres traitements mis en œuvre, tels que les traitements des données de leurs salariés. Le Code du travail et la Cnil prévoient notamment les durées de conservation suivantes :

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

### 3.2.3. Mise en conformité de l'établissement ESR

Les réponses obtenues au questionnaire de conformité au RGPD ont permis de constater que de nombreux établissements ESR, même les plus avancés s'agissant de l'appréhension du RGPD et de ses exigences, n'ont pas prévu de politique relative à la durée de conservation des données. De même, nombre d'entre eux n'ont pas circonscrit la durée de conservation des données, laquelle est illimitée, et n'ont prévu aucune politique de destruction de celles-ci aux termes d'une période définie.

Il pourrait dans un premier temps être recommandé de réaliser une cartographie des traitements, soit un descriptif de chaque traitement mis en œuvre par l'établissement ESR, ce qui permettrait, outre de multiples avantages dues à la décomposition des caractéristiques desdits traitements, d'isoler la problématique de la durée de conservation des données *(Annexe n°2 – Modèle de cartographie des traitements)*.

Une fois celle-ci établie, il s'avèrerait 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 des données de chacun des traitements et la source permettant d'en justifier si elle existe. Outre la simplification des procédures due à la synthèse de l'ensemble des informations dans un même document, l'adoption d'un tel document contribuerait largement à inscrire l'établissement ESR dans une démarche d'accountability.

## 3.3. LA LICEITE DU TRAITEMENT

### 3.3.1. Obligation

Pour être valable, un traitement de données à caractère personnel doit être licite, ce qui signifie qu'il doit reposer sur l'un des six fondements énoncés par l'article 6 du RGPD aux termes duquel :

> *« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :*
> *a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;*
> *b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;*
> *c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;*
> *d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;*
> *e) le traitement est 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 ;*
> *f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (…) ».*

### 3.3.2. Incidence de la disposition sur l'établissement ESR

Compte tenu de la grande diversité des traitements mis en œuvre par les établissements ESR, plusieurs bases légales permettent de justifier ces derniers, ce qui assujettit celles-ci à différentes obligations. Plusieurs exemples peuvent être cités pour chaque base légale :

- Traitements fondés sur le consentement : toute utilisation de la photographie de l'étudiant est soumise à l'obtention de son consentement (étant précisé que dans une telle hypothèse, sont mêlées les problématiques de protection des données à caractère personnel et de droit à l'image), de même que le traitement ayant pour effet le transfert de données à caractère personnel de l'étudiant vers le Cnous ;

- Traitements fondés sur l'exécution d'un contrat entre la personne concernée et l'université ou la personne concernée et un autre organisme : traitements effectués pour gérer les relations entre l'étudiant et le Crous pour la restauration universitaire ou encore traitements impliquant le recours à des prestataires tels que Digiposte afin que l'étudiant puisse se faire envoyer ses relevés de notes et bulletins en ligne sur sa boîte mail ;

- Traitements fondés sur une mission d'intérêt public : la formation initiale est une mission d'intérêt public, ce 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 (ex : traitement de données à caractère personnel permettant de faire fonctionner HARPEGE, logiciel de gestion des Ressources humaines dans les établissements ESR).

- Traitements fondés sur une obligation légale : traitements mis en œuvre à des fins de paiement des droits d'inscription et des cotisations sociales, traitement relatif à l'allocation de bourses, traitement relatif à la médecine du travail et à la médecine préventive, traitement relatif à la mise en œuvre d'un Espace Numérique de Travail (ENT), traitements relatifs à l'évaluation des enseignements et audits du ministère, etc.

- Traitement fondé sur l'intérêt légitime de l'établissement ESR : d'après la lettre du RGPD, ce fondement permet d'englober les hypothèses dans lesquelles le responsable de traitement doit mettre en œuvre un traitement insusceptible ou difficilement susceptible de reposer sur un autre fondement lorsque la personne concernée s'attend légitimement à ce que ses données soient traitées à une fin donnée. Toutefois, le RGPD précise que le législateur doit prévoir la base juridique de tout traitement mis en œuvre par une autorité publique : l'intérêt légitime ne devrait donc pas s'appliquer aux traitements mis en œuvre par les établissements ESR dans l'accomplissement de leurs missions.

### 3.3.3. Mise en conformité de l'établissement ESR

L'établissement d'une cartographie des traitements mis en œuvre par l'établissement ESR permet de réfléchir à l'ensemble des caractéristiques de ces derniers, parmi lesquelles leur fondement légal, afin d'en déduire leur licéité. La connaissance du fondement d'un traitement s'avère primordiale dans la mesure où certains d'entre eux mettent à la charge du responsable de traitement, en l'occurrence l'établissement ESR, un certain nombre d'obligations. Il en est ainsi s'agissant des traitements fondés sur le consentement de la personne concernée : l'article 7 du RGPD impose de respecter certaines conditions pour le recueillir *(Annexe n°2 – Modèle de cartographie des traitements)*.

## 3.4. LE CONSENTEMENT DE LA PERSONNE CONCERNEE

### 3.4.1. Obligation

L'article 6 du RGPD érige le consentement en l'un des six fondements conférant sa légitimité à un traitement de données à caractère personnel, ce qi ne constitue pas une nouveauté par rapport à la règlementation antérieure. Toutefois, alors qu'auparavant le consentement constituait la justification par défaut du traitement, tel n'est plus le cas aujourd'hui, où les six fondements présentent un caractère alternatif.

L'article 7 du RGPD envisage les conditions applicables au recueil du consentement de la personne concernée, et à ce titre, il prévoit les caractères que ce dernier doit revêtir. Cet article est rédigé en les termes suivants :

> *« 1. Dans les 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 données à caractère personnel la concernant.*
> *2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.*
> *3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement (…)».*

Les lignes directrices du G29 relatives au consentement, publiées le 28 novembre 2017[10], précisent utilement cet article en apportant des informations complémentaires sur ce qu'il faut entendre pour chacun des caractères du consentement et sur les modalités de recueil de celui-ci :

- Il doit impérativement être préalable à tout traitement de données ;
- Il peut être présenté soit à l'écrit soit à l'oral, via des messages audio ou vidéo ;
- Il peut se matérialiser de diverses façons dès lors qu'il implique un acte positif de la personne concernée : case à cocher (sachant qu'une case pré-cochée est invalide), *swipe* (passage du doigt sur un écran), acquiescement devant une caméra, mouvement du smartphone dans le sens des aiguilles une montre, dessin d'un huit, etc.
- Il doit être aisément accessible et isolé des autres informations mises à la disposition de la personne concernée ;
- Si le consentement est donnée par voie électronique, la demande doit être claire et concise ;
- Le langage utilisé doit être simple, clair et aisément compréhensible en référence à une « personne moyenne » non dotée de connaissances juridiques approfondies ;
- Il nécessite que des informations claires aient été communiquées sur le traitement et les finalités ainsi que sur l'identité du responsable de traitement ;
- Il ne doit pas être lié ou conditionné, la personne concernée ne doit subir aucune conséquence négative si elle refuse de le donner ;
- Si le traitement comporte plusieurs finalités, le consentement ne doit pas être général, la personne concernée doit pouvoir y consentir pour une ou certaines finalités uniquement ;
- La demande de consentement doit s'adapter au moyen utilisé pour obtenir celui-ci et ne doit pas perturber l'utilisation du service pour lequel le consentement est donné ;

[10] WP29, Guidelines on Consent under Regulation 2016/679, adopted on 28 November 2017

- La demande de consentement doit être distincte de toute autre (acceptation de conditions générales par exemple).

Par ailleurs, il convient de préciser que l'article 6 du RGPD confère à la personne concernée un nouveau droit, celui de retirer son consentement dès qu'il le souhaite à partir du moment où il l'a donné une première fois. La mention de ce droit de retrait doit lui être communiquée au même titre que celle des autres droits dont il dispose, et il doit pouvoir mettre ce droit en œuvre à tout moment et de façon simplifiée.

L'article 8 du RGPD est relatif à l'hypothèse du recueil du consentement des mineurs, que le RGPD cherche à protéger compte tenu de leur vulnérabilité. Il dispose :

> *« 1. Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.*
> *Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.*
> *2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles (…)».*

### 3.4.2. Incidence de la disposition sur l'établissement ESR

Bon nombre de traitements mis en œuvre par l'établissement ESR s'appuient sur le consentement de la personne concernée, tels que notamment les traitements relatifs à l'utilisation de l'image des apprenants ou encore le traitement ayant pour effet le transfert de données à caractère personnel de l'étudiant vers le Cnous.

De façon plus générale, dès lors qu'aucun autre fondement n'est applicable à un traitement de données à caractère personnel, il convient de solliciter le consentement de la personne concernée afin de le justifier. Ainsi, il conviendrait a priori de solliciter le consentement du candidat apprenant lorsque la plateforme Parcoursup le renverra, après l'avoir informé d'une possible pré-inscription dans un établissement ESR, vers le site internet de celui-ci afin qu'il puisse procéder à celle-ci en ligne.

L'hypothèse dans laquelle certains étudiants seraient encore mineurs au moment de l'inscription dans un établissement ESR ne pose aucune difficulté au regard de l'article 8 précité du RGPD dans la mesure où le projet de loi LIL 3 fixe à 15 ans l'âge auquel le mineur est considéré comme étant en mesure de donner seul son consentement : les dispositions de l'article 7 ont pleinement vocation à s'appliquer.

### 3.4.3. Mise en conformité de l'établissement ESR

Lorsque l'établissement ESR met en œuvre des traitements de données à caractère personnel fondés sur le consentement, et conformément aux réponses adressées aux questionnaires d'information, l'établissement ESR prévoit souvent une mention d'information assortie d'une case à cocher, méthode correspondant aux exigences de la loi Informatique et libertés.

Le RGPD ne prévoit pas de bouleversement majeur de ce formalisme : dans une telle hypothèse, chaque établissement ESR doit vérifier les éléments suivants :

- la pertinence et la cohérence de la mention d'information proposée, sa lisibilité,
- la précision obligatoire des finalités sur lesquelles repose le traitement en question,
- la mention ne porte que sur le consentement au traitement concerné, et pas sur l'acceptation de mentions d'information quelles qu'elles soient (ex : s'agissant de l'acceptation du contenu d'une politique Informatique et libertés, une autre case doit être prévue) ;
- le refus de la personne concernée de donner son consentement ne doit pas perturber ou empêcher l'utilisation du service concerné.

Il convient également de prévoir une mention relative à la possibilité pour la personne concernée d'exercer son droit de retrait du consentement et de mettre en mesure celle-ci de l'exercer de façon effective, par exemple via l'envoi d'un mail à une adresse dédiée à l'exercice de ce droit.

## 3.5. TRANSPARENCE

### 3.5.1. Obligation

L'article 12 du 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. Cette obligation est rédigée dans les termes suivants :

> *« 1. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.*
> *2. Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22. Dans les cas visés à l'article 11, paragraphe 2, le responsable du traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 15 à 22, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée (…) ».*

L'article précise ainsi la forme que doit revêtir l'information communiquée à la personne concernée, étant précisé que les caractères de simplicité, de concision et de clarté paraissent quelque peu contradictoires avec le nombre élevé d'informations à communiquer. En effet, l'article exige que soient communiquées les 11 informations suivantes :

| Article | Synthèse |
|---|---|
| 13 | Information à fournir en cas de collecte « directe » |
| 14 | Information à fournir en cas de collecte « indirecte » |
| 15 | Droit d'accès |
| 16 | Droit de rectification |
| 17 | Droit à l'effacement (droit à l'oubli) |
| 18 | Droit à la limitation du traitement |
| 19 | Obligation de notification aux destinataire des données |
| 20 | Droit à la portabilité |
| 21 | Droit d'opposition |
| 22 | Décision individuelle automatisée (y compris le profilage) |
| 34 | Communication à la personne concernée des violations |

Les articles 13 et 14 du RGPD énumèrent les différentes informations que le responsable de traitement doit communiquer à la personne concernée, étant précisé que le premier s'applique en cas de collecte directe de données, tandis que le second s'applique en cas de collecte indirecte, c'est-à-dire quand les données sont collectées par l'intermédiaire d'un tiers et pas de la personne concernée elle-même. En effet, malgré un tronc commun d'informations à communiquer, certains éléments diffèrent selon le mode de collecte, comme le montre le tableau synthétique suivant :

| Collecte directe auprès de la personne concernée | Collecte indirecte |
|---|---|
| - Identité et coordonnées du responsable de traitement ou de son représentant<br>- Coordonnées du DPO s'il existe<br>- Finalités et base juridique du traitement<br>- Destinataires ou catégories de destinataires (s'ils existent en cas de collecte directe)<br>- L'éventualité d'un transfert hors de l'UE<br>- Mention de l'intégralité des droits de la personne concernée<br>- **Mention du droit de retirer son consentement à tout moment**<br>- Mention du droit de faire une réclamation auprès d'une autorité nationale de contrôle<br>- **Durée de conservation des données ou critères pour la déterminer**<br>- **Existence d'une prise de décision automatisée y compris un profilage** | |
| - Obligation ou non pour la personne de fournir ses données, les conséquences en cas de non-fourniture<br>- Caractère règlementaire ou contractuel de la collecte des données à caractère personnel<br>- **Intérêts légitimes poursuivis par le responsable de traitement si nécessaire**<br>- Finalités envisagées dans la perspective éventuelle d'un traitement ultérieur | - Catégories de données concernées<br>- Source de provenance de ces données et le cas échéant, la mention selon laquelle elles proviennent d'une source accessible au public. |

### 3.5.2. Incidence de la disposition sur l'établissement ESR

La grande diversité des traitements mis en œuvre par les établissements ESR, l'hétérogénéité des personnes concernées et le recours à plusieurs sources de collecte des données constituent autant de facteurs susceptibles de complexifier la communication d'une information claire, exhaustive et complète à l'ensemble des destinataires de celle-ci.

En effet, les hypothèses de collecte directe auprès de la personne concernée sont nombreuses, même si elles sont parfois couplées avec des cas de collecte indirecte : inscription ou réinscription administrative de l'étudiant en ligne, présentation d'un dossier de candidature ou d'inscription à un concours, affectation d'un personnel titulaire à la suite de la réussite d'un concours ou d'une mutation, etc.

Dans de très nombreux cas, la collecte les données s'opère de façon indirecte : traitement de la paie, traitement relatif aux contrôles d'accès dans l'établissement ESR, traitement impliquant des échanges entre les bibliothèques universitaires, les Crous et les mutuelles étudiantes, la réalisation d'un annuaire ou encore la mutation d'un étudiant vers un nouvel établissement ESR.

Jusqu'à présent, plusieurs non-conformités sont susceptibles d'être relevées s'agissant de la thématique de l'information de la personne concernée, en premier lieu par rapport à la loi Informatique et libertés. En effet, il n'est pas rare que certaines opérations aient lieu sur les données à l'insu de la personne concernées ou que les demandes d'exercice des droits de ces dernières ne donnent lieu à aucune procédure spécifique et soient traitées comme toute autre demande de support, ce qui entraîne une absence d'homogénéité des processus au sein des établissements ESR.

Dans la mesure où le RGPD renforce considérablement l'obligation d'information du responsable de traitement, l'établissement ESR s'expose à des recours de la part des personnes concernées quelles qu'elles soient, c'est pourquoi il convient de prêter une attention particulière à cette thématique.

### 3.5.3. Mise en conformité de l'établissement ESR

Pour concilier l'impératif de transparence avec la densité des informations à communiquer, qui peuvent paraître contradictoires, est recommandée la rédaction d'une politique Informatique et libertés dont le principal objectif est de communiquer l'ensemble des informations exigées aux personnes concernées.

En effet, la politique peut être communiquée très facilement, à la fois sur support papier ou par voie électronique, étant précisé qu'elle peut demeurer en ligne et librement accessible sur une page internet, au même titre que les mentions légales et les conditions générales de vente. Une telle politique, au-delà du fait qu'elle permet de se ménager la preuve du respect de son obligation de transparence, s'avère constituer un excellent support pour diffuser de nombreuses informations de façon claire et concise.

Compte tenu de la grande diversité des traitements mis en œuvre par les établissements ESR, il conviendrait d'adopter plusieurs politiques Informatique et libertés distinctes et propres à chaque catégorie de personnes concernées. Pourraient ainsi être envisagées la mise en œuvre des politiques suivantes :

- la politique à destination des étudiants, candidats et prospects *(Annexe n°3 – Modèle de politique RGPD à destination des étudiants et candidats)*,
- la politique à destination des salariés et personnel enseignant *(Annexe n°4 – Modèle de politique à destination des salariés et agents publics)*,
- la politique à destination des partenaires, ce qui englobe de façon générale tous les tiers *(Annexe n°5 – Modèle de politique RGPD à destination des partenaires)*.

La politique doit être distinguée de la charte des systèmes d'information de l'établissements ESR, qui a vocation à recueillir l'engagement de son signataire de se conformer aux obligations qui s'imposent à lui s'agissant de l'usage des outils numériques mis à sa disposition par l'établissement ESR et de respecter les règles de bonne utilisation de ceux-ci. S'il est vrai que la charte peut incorporer une disposition relative aux données à caractère personnel, elle ne suffira pas à intégrer l'ensemble des informations exigées tout en respectant l'impératif de clarté et de simplicité requis par le RGPD.

## 3.6. DROIT D'ACCES ET DE COPIE

### 3.6.1. Obligation

Le droit d'accès existait déjà avant l'entrée en vigueur du RGPD, la loi Informatique et libertés le reconnaissait déjà au profit de la personne concernée. Le responsable de traitement était ainsi déjà assujetti à l'obligation de l'informer quant à l'existence de ce droit et aux modalités de son exercice.

L'évolution du RGPD en la matière est qu'il renforce ce droit d'accès 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.

L'article 15 du RGPD relatif au droit d'accès et de copie est rédigé comme suit :

> *« 1. La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations suivantes :*
> *a) les finalités du traitement ;*
> *b) les catégories de données à caractère personnel concernées ;*
> *c) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales*
> *d) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;*
> *e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement ;*
> *f) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;*
> *g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;*
> *h) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée (…) ;*
> *3. Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement. Le responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement ».*

### 3.6.2. Incidence de la disposition sur l'établissement ESR

Comme pour tous les droits dont est investie la personne concernée, il s'avère complexe pour les établissements ESR d'identifier la quantité et la régularité des demandes d'accès dans la mesure où elles ne déploient pas de procédure adaptée en cas de demande d'exercice de ses droits par celle-ci et ne tiennent pas de registre des demandes.

Dans un avenir proche, le nombre de demandes de droit d'accès pourrait toutefois croître de façon considérable du fait du recours à Parcoursup, la nouvelle plateforme nationale d'admission des lycéens et étudiants dans les établissements ESR qui remplace Admissions post bac 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.

### 3.6.3. Mise en conformité de l'établissement ESR

Afin de faciliter les demandes d'exercice du droit d'accès et de copie de toute personne concernée par un des traitements mis en œuvre par l'établissement ESR, chaque établissement ESR doit organiser la façon dont celui-ci peut être mis en œuvre avec une certaine latitude : il peut déployer une cellule « droit d'accès et de copie » comportant du personnel compétent pour administrer de telles demandes ou, pour les traitements qui s'y prêtent, prévoir une administration de ses données par la personne concernée elle-même (exemple : administration via l'espace personnel de l'étudiant sur l'ENT).

L'établissement ESR doit également prendre en considération l'exercice du droit de copie, et prévoir le cas échéant l'envoi à toute personne qui formulerait une telle demande la communication de ses données sur un document PDF par exemple.

Enfin, afin de se conformer à son obligation de transparence et de fournir à la personne concernée une information exhaustive, l'établissement ESR doit prévoir dans les différentes 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 :

- L'existence de ce droit et en quoi il consiste ;
- Les modalités d'exercice de ce droit (personne dont la demande émane, pièces à fournir…) ;
- Le contact compétent et ses coordonnées afin de pouvoir effectivement exercer ce droit ;
- Le droit pour la personne concernée de demander copie de ses données et les éventuels coûts à supporter en cas de demande de copie supplémentaire ;
- L'interdiction d'exercer ce droit de façon abusive pour déstabiliser le service concerné *(Annexes n°3, 4 et 5 – Modèles de politique à destination des étudiants et candidats, salariés et agents publics et partenaires).*

## 3.7. DROIT DE RECTIFICATION

### 3.7.1. Obligation

Comme le droit d'accès, le droit de rectification ne constitue pas une nouveauté propre au RGPD, il existait déjà sous l'empire de la loi Informatique et libertés. L'article 16 du RGPD énonce :

> *« La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire ».*

### 3.7.2. Incidence de la disposition sur l'établissement ESR

Comme pour le droit d'accès, il s'avère complexe pour les établissement ESR d'identifier avec précision l'ampleur des demandes d'exercice du droit de rectification des personnes concernées. Toutefois, le questionnaire adressé aux établissements ESR laisse apparaître que le nombre de ces demandes s'avère peu important et concerne a priori les hypothèses suivantes : correction d'une information erronée quelle qu'elle soit, changement d'état civil (mariage ou divorce) ou, plus rarement encore, changement de genre.

### 3.7.3. Mise en conformité de l'établissement ESR

De façon similaire au droit d'accès, il conviendra de prévoir une procédure spécifique permettant à l'établissement ESR de répondre aux demandes de droit de rectification qui lui seraient faites : cellule droit de rectification ou possibilité pour la personne concernée de rectifier et mettre à jour toutes les données inexactes, incohérentes ou obsolètes sur l'espace personnel mis à sa disposition sur le site internet de l'établissement ESR.

Là encore, il conviendra de modifier les différentes politiques Informatique et libertés afin de porter à la connaissance des différentes personnes concernées à la fois l'existence du droit de rectification et les modalités d'exercice de ce dernier, de telle sorte qu'elles puissent en faire usage en cas d'inexactitudes dans les données saisies *(Annexes n°3, 4 et 5 – Modèles de politique à destination des étudiants et candidats, salariés et agents publics et partenaires).*

## 3.8. DROIT A L'EFFACEMENT

### 3.8.1. Obligation

Le droit à l'effacement constitue une nouveauté prévue par le RGPD. Désormais, la personne concernée a le droit de solliciter l'effacement des données à caractère personnel la concernant, à condition de se situer dans l'une des hypothèses limitativement énumérées par l'article 17 aux termes duquel :

> *« 1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :*
> *a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;*
> *b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;*
> *c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;*
> *d) les données à caractère personnel ont fait l'objet d'un traitement illicite ;*
> *e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis (…).*
> *2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci ».*

Conformément au considérant 59 du RGPD, 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.

### 3.8.2. Incidence de la disposition sur l'établissement ESR

Aujourd'hui, les établissements ESR ne semblent pas avoir envisagé la mise en œuvre du droit à l'effacement, même si certaines d'entre elles commencent à prendre la mesure de ce nouveau droit. A priori, les seules hypothèses dans lesquelles le droit à l'effacement pourrait être mis en œuvre dans les établissements ESR sont les suivantes :

- S'agissant d'un traitement fondé sur le consentement si la personne concernée retire celui-ci conformément à la possibilité qui lui est accordée par l'article 7 du RGPD ;

- En cas de mise en œuvre par la personne concernée de son droit d'opposition s'agissant d'un traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique dont est investi le responsable du traitement.

La spécificité et la difficulté tenant à l'exercice de ce droit tient à l'obligation pour l'établissement ESR de prendre des mesures raisonnables pour prévenir d'autres responsables de traitement qui traiteraient également ces mêmes données, étant précisé que cette hypothèse est susceptible de survenir. Prenons par exemple le cas de la carte étudiant européenne, qui n'en est encore qu'au stade du projet : les établissements ESR et le Crous, qui diligente ce projet et centralise les données, mettent chacun en œuvre un traitement à partir des mêmes données de l'étudiant.

### 3.8.3. Mise en conformité de l'établissement ESR

La mise en œuvre par les établissements ESR d'une procédure visant à répondre aux demandes d'effacement de leurs données par les personnes concernées suppose au préalable de mener une réflexion sur les durées de conservation des données à caractère personnel : grâce à la politique relative à la conservation des données, les établissements ESR doivent s'assurer qu'aucune donnée n'est conservée plus longtemps qu'il n'est nécessaire.

Comme pour les autres droits dont bénéficie la personne concernée par les traitements mis en œuvre par l'établissement ESR, il convient d'adopter une procédure permettant la mise en œuvre de ce droit et de prévoir une clause relative à son exercice dans les différentes politiques Informatique et libertés.

En outre, il convient de mettre en œuvre une procédure permettant à l'établissement ESR de contrôler la diffusion des données à caractère personnel auprès d'autres responsables de traitement, comme par exemple de tenir un registre des différents destinataires des données qu'elle traite. Par la suite, il conviendra d'adopter une procédure permettant à l'établissement ESR d'informer efficacement ces autres responsables de traitement dans l'hypothèse de l'introduction d'une demande d'effacement *(Annexes n°3, 4 et 5 – Modèles de politique à destination des étudiants et candidats, salariés et agents publics et partenaires).*

## 3.9. DROIT A LA LIMITATION DU TRAITEMENT

### 3.9.1. Obligation

Le droit à la limitation constitue également une nouveauté prévue par le RGPD. L'article 4 du RGPD définit la limitation comme « *le marquage des données à caractère personnel conservées, en vue de limiter leur traitement futur* ». La limitation implique donc la suspension du traitement de ces données par le responsable de traitement : aucune opération ne peut être réalisée sur celles-ci.

Ce droit signifie concrètement la possibilité conférée à la personne concernée d'obtenir la suspension temporaire du traitement de ses données, par exemple lorsqu'elle a formulé une demande d'effacement et quelle que soit l'issue de cette dernière. La personne concernée évite de subir le délai d'attente d'un mois si le traitement de ses données s'avère préjudiciable pour quelque raison que ce soit.

Comme pour le droit à l'effacement, l'exercice de ce nouveau droit est subordonné à la caractérisation de l'une des hypothèses limitativement énumérées par l'article 18 du RGPD aux termes duquel :

> *« 1. La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :*
> *a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;*
> *b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;*
> *c) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;*
> *d) la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.*
> *2. Lorsque le traitement a été limité en vertu du paragraphe 1, ces données à caractère personnel ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre*
> *3. Une personne concernée qui a obtenu la limitation du traitement en vertu du paragraphe 1 est informée par le responsable du traitement avant que la limitation du traitement ne soit levée ».*

Le considérant 67 du RGPD expose différentes méthodes techniques permettant de limiter efficacement le traitement des données à caractère personnel de la personne ayant formulé une demande en ce sens :

> *« Les méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer temporairement les données sélectionnées vers un autre système de traitement, à rendre les données à caractère personnel sélectionnées inaccessibles aux utilisateurs, ou à retirer temporairement les données publiées d'un site internet. Dans les fichiers automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques de façon à ce que les données à caractère personnel ne fassent pas l'objet d'opérations de traitements ultérieures et ne puissent pas être modifiées. Le fait que le traitement des données à caractère personnel est limité devrait être indiqué de manière claire dans le fichier».*

### 3.9.2. Incidence de la disposition sur l'établissement ESR

La seule hypothèse dans laquelle une personne concernée par l'un des traitements mis en œuvre par l'établissement ESR pourrait mettre en œuvre son droit à la limitation serait la mise en œuvre du droit d'opposition et l'attente qu'il soit fait droit à cette demande. Dans les autres hypothèses, ce droit est susceptible d'être exclus par l'établissement ESR sous réserve d'en informer la personne concernée.

### 3.9.3. Mise en conformité de l'établissement ESR

Pour faire droit aux demandes de limitation du traitement, il convient que l'établissement ESR adopte les démarches suivantes :

- prévoir une procédure applicable au traitement des demandes de limitation des données,
- sélectionner des dispositifs techniques permettant de mettre en œuvre effectivement ce droit,
- inscrire dans les différentes politiques Informatique et libertés une disposition relative au droit à la limitation, qui précise l'existence de ce droit et en quoi il consiste, les modalités de son exercice, les coordonnées du contact compétent afin de pouvoir l'exercer effectivement. Il s'avère également envisageable, par référence aux conditions posées par l'article précité, de circonscrire l'application de ce droit à la seule hypothèse de la mise en œuvre du droit d'opposition *(Annexes n°3, 4 et 5 – Modèles de politique à destination des étudiants et candidats, salariés et agents publics et partenaires).*

## 3.10. DROIT A LA PORTABILITE DES DONNEES

### 3.10.1. Obligation

Le droit à la portabilité des données constitue lui aussi une innovation du RGPD ; il s'agit du droit de la personne concernée de solliciter et d'obtenir la restitution des données la concernant auprès d'un responsable de traitement et/ou leur transmission auprès d'un autre responsable de traitement. L'article 20 en définit les modalités comme suit :

> *« 1. Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque :*
> *a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); et*
> *b) traitement est effectué à l'aide de procédés automatisés.*
> *2. Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.*
> *3. L'exercice du droit, visé au paragraphe 1 du présent article s'entend sans préjudice de l'article 17. 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.*
> *4. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers ».*

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

- Les données ont été communiquées par la personne concernée elle-même dans le cadre d'une collecte directe par le responsable de 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.

### 3.10.2. Incidence de la disposition sur l'établissement ESR

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, qui survient de façon assez rare.

S'agissant de l'hypothèse du transfert d'un étudiant dans un autre établissement ESR, on ne peut pas parler de droit à la portabilité en tant que tel car le fondement n'est pas identique : les établissement ESR se communiquent les données de l'étudiant concerné afin d'assurer la continuité de la formation universitaire de ce dernier, qui constitue une mission de service public.

### 3.10.3. Mise en conformité de l'établissement ESR

La probabilité, même résiduelle, qu'une personne concernée formule une demande de portabilité de ses données auprès de l'établissement ESR qui les traite, nécessite que l'établissement ESR envisage les moyens techniques de restitution des données à celle-ci et prévoie une disposition relative à ce nouveau droit dans les politiques Informatique et libertés, laquelle devra englober les informations suivantes :

- L’existence de ce droit et en quoi il consiste ;
- Les conditions dans lesquelles il peut être exercé et, par conséquent, les hypothèses d’exclusion dans le cadre des traitements mis en œuvre par l’établissement ESR ;
- Les modalités d’exercice de ce droit (personne dont la demande émane, pièces à fournir…) ;
- Le contact compétent et ses coordonnées afin de pouvoir effectivement exercer ce droit *(Annexes n°3, 4 et 5 – Modèles de politique à destination des étudiants et candidats, salariés et agents publics et partenaires).*

## 3.11. DROIT D'OPPOSITION

### 3.11.1. Obligation

L'article 21 du RGPD envisage le droit d'opposition, qui permet à la personne concernée d'obtenir que ses données ne soient plus traitées pour l'avenir par le responsable de traitement. Une fois encore, la mise en œuvre de ce droit s'avère conditionnée, comme en témoigne la lettre du texte:

> *« 1. La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice (…).*
> *2. Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.*
> *3. Au plus tard au moment de la première communication avec la personne concernée, le droit visé aux paragraphes 1 et 2 est explicitement porté à l'attention de la personne concernée et est présenté clairement et séparément de toute autre information.*
> *4. Dans le cadre de l'utilisation de services de la société de l'information, et nonobstant la directive 2002/58/CE, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.*
> *5. Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques en application de l'article 89, paragraphe 1, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public ».*

Ce droit d'opposition ne peut être exercé que dans les circonstances suivantes :

- le traitement est fondé sur une mission d'intérêt public ou relevant de l'exercice de l'autorité publique du responsable du traitement,
- le traitement est fondé sur l'intérêt légitime du responsable du traitement,
- le traitement est élaboré à des fins de prospection commerciale,
- le traitement est élaboré à des fins de recherche scientifique ou historique.

### 3.11.2. Incidence de la disposition sur l'établissement ESR

Dans la mesure où un grand nombre de traitements mis en œuvre par les établissements ESR sont fondés sur une mission d'intérêt public, le droit d'opposition est susceptible d'être mis en œuvre notamment par les personnes concernées dans le cadre du traitement ayant pour finalité leur formation universitaire. Il en va de même s'agissant des traitements ayant pour finalité la recherche scientifique compte tenu de l'importance que revêt celle-ci dans certains établissements ESR.

### 3.11.3. Mise en conformité de l'établissement ESR

Comme pour l'ensemble des droits dont est titulaire la personne concernée, l'établissement ESR doit, dans l'optique de sa mise en conformité au RGPD, procéder en deux temps s'agissant du droit d'opposition de la personne concernée :

- Organiser la mise en œuvre effective de ce droit, c'est-à-dire sélectionner les procédés techniques permettant de répondre aux demandes, prévoir une cellule droit d'opposition avec la liste des personnes habilitées à traiter celles-ci et à informer la personne concernée des suites de ses demandes ;

- Inclure dans les politiques Informatique et libertés une disposition relative au droit d'opposition comportant, comme pour les autres droits, un descriptif de ce droit, les conditions dans lesquels il peut être exercé, les modalités de son exercice et les coordonnées du contact compétent pour répondre à une quelconque demande d'exercice de celui-ci *(Annexes n°3, 4 et 5 – Modèles de politique à destination des étudiants et candidats, salariés et agents publics et partenaires).*

## 3.12. DECISION INDIVIDUELLE AUTOMATISEE (ET PROFILAGE)

### 3.12.1. Obligation

Les décisions individuelles automatisées (DIA) sont susceptibles d'être définies comme des décisions fondées exclusivement sur un traitement automatisé, souvent un algorithme, produisant des effets juridiques sur la personne concernée ou l'affectant de manière significative de façon similaire. A priori, les DIA excluent toute intervention humaine, et ont souvent une incidence significative sur les droits légaux et contractuels de la personne concernée.

Compte tenu de la hausse significative du recours à de tels dispositifs et des conséquences préjudiciables susceptibles de survenir pour la personne concernée, le RGPD a prévu à son profit un droit de ne pas faire l'objet d'une décision fondée exclusivement sur un tel dispositif. L'article 22 du texte, utilement précisé par les lignes directrices du G29 relatives au profilage[11], dispose ainsi :

> *« 1. La personne concernée a le droit de pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.*
> *2. Le paragraphe 1 ne s'applique pas lorsque la décision :*
> *a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;*
> *b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou*
> *c) est fondée sur le consentement explicite de la personne concernée.*
> *3. Dans les cas visés au paragraphe 2, points a) et c), le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.*
> *4. Les décisions visées au paragraphe 2 ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, à moins que l'article 9, paragraphe 2, point a) ou g), ne s'applique et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place ».*

### 3.12.2. Incidence de la disposition sur l'établissement ESR

L'enseignement supérieur recourt à des dispositifs de décision automatisée s'agissant de la sélection des candidats dans les établissements ESR. Entre 2009 et 2017, le ministère de l'Enseignement supérieur et de la Recherche avait mis en place le télé-service Admission Post-Bac (APB), plateforme permettant aux candidats de formuler leurs vœux d'affectation dans les différents établissements ESR du territoire.

[11] W29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopter on October 2017

Après avoir essuyé de vives critiques et fait l'objet d'une mise en demeure de la Cnil[12] compte tenu de l'opacité de la procédure malgré l'obligation de transparence des algorithmes[13] créée par la loi pour une République numérique[14], cet outil a été remplacé le 15 janvier 2018 par Parcoursup, créé dans le cadre de la loi pour l'orientation et la réussite des étudiants du 8 mars 2018[15] dans un objectif d'accroissement de la transparence due aux candidats.

La mise en œuvre d'un tel dispositif, qui implique une sélection des étudiants par les établissements ESR, suscite deux questions du point de vue des traitements de données à caractère personnel mis en œuvre : la question de l'applicabilité de l'article 22 1) précité du RGPD et celle de la transparence et de l'information à délivrer aux candidats. En effet, l'article 12 relatif à l'obligation de transparence du responsable de traitement s'étend à l'hypothèse de la mise en œuvre d'un DIE mais le considérant 73 du RGPD permet de s'affranchir de certaines obligations parmi lesquelles l'obligation d'information si des intérêts supérieurs le justifient, ce qui pourrait être le cas ici.

La question de l'applicabilité de l'article 22 1) du RGPD se tranche assez aisément dans la mesure où Parcoursup est autorisée par le droit français et notamment par l'article L. 612-3 du Code de l'éducation tel que résultant de la loi précitée. Par conséquent, par application de l'article 22 2-b) du RGPD, la personne n'est pas en droit d'exiger de ne pas faire l'objet d'une décision fondée sur une DIE s'agissant de son affectation à l'université.

La question de la transparence s'avère d'autant plus importante que le système est complexe, car il fait intervenir à la fois Parcoursup et les établissements ESR eux-mêmes :

- dans un premier temps, les candidatures sont pré-classes via l'algorithme de la plateforme, qui repose sur l'attribution d'une note à chaque candidat au regard de ses éléments de candidature (bulletins, notes de français, appréciations de l'équipe éducative, etc.) ;

- dans un second temps, les critères de sélection des candidats sont laissés à l'entière appréciation des établissements ESR sans aucune harmonisation nationale. Certains recourent uniquement au classement automatique généré par un algorithme, d'autres se fondent à la fois sur l'algorithme et l'intervention d'une équipe de professeurs, quand d'autres privilégient l'analyse des dossiers de candidature par des professeurs.

L'examen du projet de loi a fait l'objet d'importantes controverses et n'a pas permis de lever le principe du secret des délibérations, qui permet aux établissements ESR de ne pas dévoiler les algorithmes locaux mis en œuvre pour sélectionner les candidats et de limiter aux seuls candidats qui en font la demande l'accès aux critères, modalités d'examen et motifs pédagogiques qui justifient leur admission ou leur refus d'admission[16].

[12] Décision n°MED-2017-053 du 30 août 2017 mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche de et l'Innovation et Délibération du bureau de la Commission nationale de l'informatique et des libertés n° 2017-233 du 7 septembre 2017 décidant de rendre publique la mise en demeure n° 2017-053 du 30 août 2017 prise à l'encontre le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation
[13] Art. L. 311-3-1 du Code des relations entre le public et l'administration (CRPA)
[14] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique
[15] Loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants
[16] Dossier législatif relatif à la loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants

Toutefois, cette problématique semble avoir été tranchée par la loi LIL 3 dans sa version telle qu'acceptée en lecture définitive par l'Assemblée nationale le 14 mai 2018[17]. En effet, l'article 21 de cette loi va dans le sens de la suppression du secret au profit d'une obligation de transparence et d'information, laquelle se manifeste par la rédaction d'un rapport annuel relatif au déroulement de cette procédure et aux modalités d'examen des candidatures par les établissements ESR.

### 3.12.3. Mise en conformité de l'établissement ESR

La question de l'applicabilité de l'article 22 1) du RGPD se tranche assez aisément dans la mesure où Parcoursup est autorisée par le droit français et notamment par l'article L. 612-3 du Code de l'éducation tel que résultant de la loi précitée. Par conséquent, par application de l'article 22 2-b) du RGPD, la personne n'est pas pourvue du droit d'exiger de ne pas faire l'objet d'une décision fondée sur une DIE s'agissant de son affectation à l'université.

S'agissant de la transparence assortissant les critères de sélection des établissements ESR, et malgré l'existence de thèses antinomiques s'agissant de l'obligation de transparence due aux étudiants, la loi LIL 3 a conclu dans le sens du respect d'une telle obligation. Par conséquent, 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 libertés élaborée à leur destination *(Annexes n°3, 4 et 5 – Modèles de politique à destination des étudiants et candidats, salariés et agents publics et partenaires).*

[17] Projet de loi relatif à la protection des données personnelles, adopté en Lecture définitive par l'Assemblée nationale le 14 mai 2018, TA n°113 (texte adopté provisoire avec liens vers les amendements)

## 3.13. SOUS-TRAITANCE

### 3.13.1. Obligation

Le RGPD renforce considérablement le rôle joué par le sous-traitant, soit celui qui traite des données à caractère personnel sous les instructions et pour le compte du responsable de traitement. Désormais, les rapports entre responsable de traitement et sous-traitant donnent lieu à d'importants enjeux en termes de responsabilité, ce qui n'était pas le cas auparavant, où le sous-traitant n'était susceptible d'engager sa responsabilité que dans de rares hypothèses.

L'article 28, relatif aux obligations réciproques de ces derniers et à l'organisation de leur relation contractuelle, est rédigé comme suit :

> *« 1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.*
> *2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.*
> *3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement (…).*
> *4. Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations (…).*
> *9. Le contrat ou l'autre acte juridique visé aux paragraphes 3 et 4 se présente sous une forme écrite, y compris en format électronique*
> *10. Sans préjudice des articles 82, 83 et 84, si, en violation du présent règlement, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement ».*

Le premier élément à appréhender s'agissant de la relation entre le responsable de traitement et le sous-traitant est le contrat ou l'acte juridique qui les lie, qui doit être établi par écrit. Au-delà d'être obligatoire, il va permettre de matérialiser les engagements réciproques de ces derniers et de démontrer que la conformité du sous-traitant à ses obligations a été envisagée de façon exhaustive. Ce contrat ou acte juridique doit obligatoirement incorporer les 8 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 traitement est opéré par le sous-traitant sous les instructions documentées du responsable de traitement ;
- le sous-traitant s'engage à respecter une obligation spécifique de confidentialité ;

- le sous-traitant s'engage à respecter les exigences prévues par l'article 32 du RGPD en matière de sécurité ;
- le sous-traitant aide le responsable du traitement afin de donner suite aux demandes d'exercice des droits dont les personnes concernées sont investies ;
- le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et notamment permettre la réalisation d'audits ;
- le sous-traitant s'engage à respecter les conditions prévues par le responsable de traitement pour recruter un sous-traitant ultérieur (autorisation générale ou spécifique) ;
- le sous-traitant, aux termes du contrat de sous-traitance, s'engage soit à supprimer toutes les données, soit à les renvoyer au responsable du traitement en ayant pris soin de détruire toutes les copies existantes.

L'article 82 du RGPD, après avoir posé un principe général de réparation du dommage subi par toute personne du fait d'un manquement à ses dispositions, organise la répartition de la responsabilité entre le responsable de traitement et son sous-traitant. Cet article, qui s'appuie sur les principes généraux du droit de la responsabilité (responsabilité en cascade, action récursoire, etc.), dispose :

> *« 1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.*
> *2. Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.*
> *3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.*
> *4. Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.*
> *5. Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2 (…). ».*

### 3.13.2. Incidence de la disposition sur l'établissement ESR

Les établissements ESR sont nombreux à faire appel à des sous-traitants pour externaliser certains traitements qu'ils mettent en œuvre, tels que par exemple et de façon non exhaustive :

- la gestion de la paie, qui peut être intégralement confiée à des prestataires spécialisés,
- le recrutement via le recours à des plateformes collaboratives (IAE Link par exemple),
- le recours à des prestataires d'hébergement ou de maintenance quels qu'ils soient,
- le recours à des prestataires d'emailing chargés d'envoyer des newsletters,
- le recours à des billetteries en ligne chargées d'éditer les billets et de gérer les inscriptions en cas d'organisation d'évènements, etc.

À l'heure de l'entrée en vigueur des dispositions du RGPD, certains établissements ESR rencontrent des difficultés avec leurs prestataires, qui leur sont préjudiciables à l'exécution de leur obligation de s'assurer de la conformité de ces derniers au RGPD :

- tous n'ont pas conclu de contrats relatifs à prestation de services effectuée,
- tous n'ont pas appréhendé la nécessaire mise en conformité aux dispositions du RGPD,
- le dialogue s'avère parfois complexe à mettre en œuvre sur la thématique du RGPD et de la mise en conformité du sous-traitant,
- certains prestataires n'hésitent pas à monétiser leur conformité au RGPD en faisant souscrire à leurs clients de nouveaux services « conformes au RGPD », comme si le respect des dispositions du RGPD constituait une faculté optionnelle alors qu'il s'agit d'une obligation règlementaire à laquelle tous sont assujettis...

### 3.13.3. Mise en conformité de l'établissement ESR

Afin de s'acquitter de son obligation de veiller à ce que ses sous-traitants présentent des garanties suffisantes s'agissant du respect des dispositions du RGPD, il est recommandé de mener les actions suivantes :

- élaborer une cartographie des différents sous-traitants, ce qui est très lié avec la cartographie juridique, qui pour chacun des traitements effectués par l'établissement ESR précise le recours éventuels à des sous-traitants, l'identité de ces derniers et l'existence ou non d'un contrat de sous-traitance. Cette cartographie permet à l'établissement ESR de savoir quelles démarches doivent être accomplies avec les sous-traitants existants ;

- adresser aux sous-traitants existants, qui comptent déjà l'établissement ESR parmi leurs clients, une lettre de demande de conformité destinée à entamer avec eux un dialogue sur les démarches accomplies par ces derniers pour agir en conformité avec les exigences du RGPD *(Annexe n°6 – Lettre type de demande de conformité aux sous-traitants)* ;

- selon le retour du sous-traitant, et s'il ne dispose pas d'un document contractuel convaincant, il convient de préparer un avenant au contrat de prestation de services qui le lie à l'établissement ESR, lequel renvoie vers une annexe RGPD comportant tous les éléments devant obligatoirement figurer dans l'acte juridique exigé par l'article 28 précité *(Annexe n°7 – Avenant RGPD à joindre au contrat de prestations de services ; Annexe n°8 – Annexe RGPD au contrat de prestations de services)* ;

- faire entrer la conformité aux RGPD dans le champ des négociations avec les sous-traitants nouveaux et en fonction de l'issue des discussions, leur proposer d'adjoindre l'annexe RGPD précitée à leur contrat et d'y insérer une clause permettant de renvoyer vers ce dernier *(Annexe n°9 – Modèle de clause « données à caractère personnel » à opposer au sous-traitant)* ;

- Faire signer au sous-traitant à un engagement de confidentialité, étant précisé que le RGPD impose à ce dernier d'agir dans le cadre d'une obligation spéciale de confidentialité afin qu'il respecte à la fois les données et les spécificités de l'activité du responsable de traitement *(Annexe n°10 – Modèle de lettre d'engagement de confidentialité)* ;

- prévoir une procédure d'audit des sous-traitants afin de se mettre en mesure de juger leur niveau de conformité aux exigences du RGPD, comme le prévoit le texte.

## 3.14. REGISTRE DES TRAITEMENTS

### 3.14.1. Obligation

Le RGPD modifie profondément la philosophie applicable à la protection des données à caractère personnel par la création d'un principe d'accountability. Alors que la loi Informatique et libertés exigeait

jusqu'à présent l'accomplissement par le responsable de traitement de démarches et formalités auprès de la Cnil (déclarations ou autorisations), tel n'est plus le cas, il doit désormais démontrer seul sa conformité aux règles de protection érigée par le RGPD.

Le registre des traitements constitue un outil permettant à ce dernier de témoigner de sa conformité. Il s'agit d'un document de synthèse de l'ensemble des traitements mis en œuvre au sein de l'organisme concerné. Contrairement à la cartographie qui a vocation à rester interne à celui-ci, le registre de traitement est établi dans l'optique de démontrer sa conformité dans l'hypothèse d'un contrôle de la Cnil. L'article 30 relatif au registre des traitements dispose :

> *« 1. Chaque responsable du 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 :*
> *a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;*
> *b) les finalités du traitement ;*
> *c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;*
> *d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;*
> *e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;*
> *f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;*
> *g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 ;*
> *2. Les registres (…) se présentent sous une forme écrite y compris la forme électronique.*
> *3. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.*
> *4. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».*

La mise en œuvre d'un registre des traitements n'est obligatoire que si la structure du responsable de traitement comporte plus de 250 salariés ou, le cas échéant, si le traitement concerné est susceptible de présenter un risque particulier pour les droits et libertés des personnes concernées, s'il n'est pas habituel ou s'il porte sur des catégories particulières de données.

Hors ces hypothèses, il est envisageable pour un responsable de traitement de prévoir un tel registre de façon à respecter le principe d'accountability, c'est-à-dire afin de démontrer sa conformité aux dispositions du RGPD.

D'un point de vue formel, il est seulement exigé que le registre des traitements soit écrit, ce qui permet de recourir à un tableau Excel relativement simplifié, lequel doit incorporer les informations mentionnées aux points a) à f) de l'article 30 précité.

### 3.14.2. Incidence de la disposition sur l'établissement ESR

En fonction de leur effectif, les établissements ESR sont susceptibles d'être assujettis à l'obligation de tenue d'un registre des traitements. Quand bien même tel ne serait pas le cas, il pourrait s'avérer opportun de mettre en œuvre un tel registre afin que l'établissement ESR se ménage la preuve de la démarche de conformité au RGPD qu'il aura adoptée.

### 3.14.3. Mise en conformité de l'établissement ESR

Que la tenue d'un registre des traitements soit obligatoire ou résulte d'une décision stratégique de la part de l'établissement ESR, il conviendra de se référer à la cartographie des traitements, dans la mesure où les informations à y faire figurer sont identiques *(Annexe n°2 – Modèle de cartographie des traitements)*.

Dès lors, le registre pourra soit être élaboré en interne (par exemple via un fichier Excel) avec si nécessaire une collaboration de la DSI, soit être élaboré grâce au recours à un outil externe, ce qui nécessiterait l'adoption de prérequis techniques et juridiques. L'idée est en effet de procéder à l'intégration au registre des données issues de la cartographie des traitements *(Annexe n°11 – Modèle de registre des traitements ; Annexe n°12 : Modèle de prérequis juridiques de développement)*.

Il conviendra ensuite, une fois le registre complété par les différentes informations requises, de s'interroger sur le maintien en conditions opérationnelles de ce dernier. En effet, il devra impérativement être tenu à jour, ce qui s'avère primordial en cas de communication du document à la Cnil dans l'hypothèse d'un contrôle de celle-ci. Pour ce faire, il pourra s'avérer opportun de déterminer des règles de gouvernance internes à l'établissement ESR concerné afin de déterminer la compétence de chacun dans la tenue à jour de registre.

## 3.15. RESPONSABILITE CONJOINTE

### 3.15.1. Obligation

Le RGPD crée la notion de responsabilité conjointe d'un traitement de données à caractère personnel, qui a vocation à s'appliquer lorsque plusieurs responsables de traitement agissent conjointement s'agissant d'un même traitement, en déterminant ensemble ses moyens et finalités. L'article 26 du RGPD envisage la responsabilité conjointe de la façon suivante :

> *« 1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.*
> *2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.*
> *3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement ».*

Cet article impose deux obligations fondamentales :

- La rédaction d'un contrat entre les responsables conjoints, qui a vocation à prévoir leurs obligations réciproques, car leurs fonctions ne se recoupent pas nécessairement ;

- La mise à disposition de ce contrat ou au moins de ses grandes lignes aux personnes concernées afin qu'elles bénéficient d'une information exhaustive sur les rapports entretenus entre les responsables conjoints du traitement.

### 3.15.2. Incidence de la disposition sur l'établissement ESR

Les traitements mis en œuvre par un établissement ESR supposent fréquemment des échanges de données avec d'autres organismes, lesquels sont très nombreux à intervenir et à traiter des données à caractère personnel afin de porter le service public de l'enseignement supérieur. Plusieurs exemples peuvent être cités, tels que notamment le Cnous via l'application IZLY ou dans un futur proche la carte étudiant européenne, les Crous régionaux, Parcoursup, le rectorat, la plateforme de cours en ligne Fun Mooc ou encore d'autres universités.

Pour chacune de ces situations, il convient d'analyser les prérogatives des parties et leur intervention sur les données à caractère personnel afin de déduire leur qualité au regard du RGPD. En effet, l'échange de données à caractère personnel entre plusieurs organismes n'emporte pas de façon systématique la qualification de responsabilité conjointe : selon le cas, il peut y avoir sous-traitance, communication de données entre deux responsables de traitement ou encore simple échange de données d'un responsable de traitement vers un destinataire.

Si l'on considère par exemple le projet de déploiement par le Cnous d'une carte étudiante européenne, l'analyse des rapports projetés entre les établissements ESR et le Cnous conduit à rejeter la qualification de sous-traitant et de responsables conjoints de traitement : chaque établissements ESR met en œuvre son propre traitement de données et communique au Cnous les données essentielles au traitement que ce dernier met en œuvre pour faire fonctionner la carte étudiant européenne. Dès lors, les deux interviennent respectivement en qualité de responsables de traitement indépendants, et le Cnous est destinataire des données qui lui sont communiquées par les établissements ESR.

### 3.15.3. Mise en conformité de l'établissement ESR

Dès lors qu'un rapport de responsabilité conjointe aura été identifié entre l'établissement ESR et un organisme partenaire quel qu'il soit, il conviendra de réfléchir à la contractualisation de la relation, étant précisé que l'existence d'un contrat n'est jusqu'à présent pas systématique dans un tel cas de figure.

Afin de rédiger ce contrat, il convient de formaliser en amont les obligations de chacun des responsables conjoints en isolant leurs compétences communes et propres, leurs moyens matériels, leurs dispositifs de sécurité, etc. *(Annexe n°13 : Modèle de contrat de responsabilité conjointe entre deux responsables de traitement)*.

## 3.16. DPO

### 3.16.1. Obligation

Le RGPD institue aux articles 37 à 39 du RGPD la notion de « Data protection officer », traduit comme « délégué à la protection des données » (DPO), qui remplace l'ancien Commissaire informatique et libertés (CIL) de la loi du 6 janvier 1978.

L'article 37 du RGPD est relatif à la désignation du DPO :

> *« 1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :*
> *a) 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 ;*
> *b) 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*
> *c) 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 (…).*
> *3. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille (…).*
> *5. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.*
> *6. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service (…) ». .*

La désignation du DPO est ainsi obligatoire dans trois cas de figure :

- le responsable de traitement est un organisme ou une autorité publique ;
- le traitement visé concerne des données particulières, c'est-à-dire des données sensibles ou relatives à des condamnations judiciaires ;
- le traitement exige le suivi systématique et à grande échelle des personnes concernées.

S'agissant de la désignation du DPO, trois critères de désignation doivent être respectés :

- Il peut être membre du personnel de l'organisme concerné ou prestataire de services externalisé, le choix étant susceptible d'être effectué de façon discrétionnaire. Par ailleurs, il peut être mutualisé et exercer sa fonction au profit de plusieurs autorités publiques ou plusieurs organismes appartenant à un groupe ;
- Il doit disposer de connaissances spécialisées en droit en notamment en matière de protection des données à caractère personnel afin qu'il maîtrise les sujets sur lesquels il sera amené à intervenir ;
- aucun conflit d'intérêt ne doit exister entre le DPO et la structure au profit de laquelle il agit. L'absence de conflit d'intérêt est interprétée par le G29 comme permettant à ce dernier d'agir de façon indépendante. Bien que les DPO puissent exercer d'autres fonctions au sein de

l'organisme concerné, ces fonctions ne doivent pas les mener à déterminer les finalités et moyens d'un traitement de données, auquel cas le conflit d'intérêt serait caractérisé[18].

Aux termes de l'article 39 du RGPD, les missions du DPO sont a minima les suivantes, ce qui suppose qu'il puisse accomplir d'autres actes en fonction des spécificités de l'organisme au sein duquel il intervient.

> *« Les missions du délégué à la protection des données sont au moins les suivantes :*
> *a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;*
> *b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;*
> *c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 ;*
> *d) coopérer avec l'autorité de contrôle ;*
> *e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet (…).*
> *2. Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement ».*

S'agissant des modalités d'exercice de ses missions et conformément à l'article 38 du RGPD, le DPO doit être associé en amont à toute problématique relative à la protection des données à caractère personnel et doit être équipé des ressources nécessaires à l'exercice de ses fonctions. Il accomplit ses missions en toute indépendance, ne reçoit aucune instruction et est soumis au secret professionnel ou à une obligation de confidentialité.

### 3.16.2. Incidence de la disposition sur l'établissement ESR

En tant qu'organismes publics et par application de l'article 37 précité, les établissements ESR sont tenus de désigner un DPO. Jusqu'à présent, il apparaît qu'ils étaient nombreux à avoir désigné un CIL, mais cela n'était pas systématique pour autant. Dans certaines universités, la fonction était ainsi vacante depuis un moment, dans l'hypothèse notamment du non-remplacement d'un CIL démissionnaire.

La fonction de CIL était parfois mutualisée, comme c'est le cas s'agissant de l'Université de Grenoble, où un seul CIL administre les données à caractère personnel au sein des 5 établissements ESR que comporte le site. La question de la mutualisation du DPO s'avère importante dans la mesure où celle-ci pourrait s'avérer avantageuse pour des raisons organisationnelles.

En général, quand un établissement ESR dispose déjà d'un CIL, ce dernier est pressenti pour devenir DPO pour des raisons évidentes de simplicité et de compétence, les rôles de CIL et de DPO étant similaires, exception faite de la fonction de contrôle par le DPO du respect par le responsable de

[18] WP29, Guidelines on Data Protection Officer ('DPOs'), adopted on 5 April 2017

traitement des dispositions du RGPD. Il semblerait par ailleurs que la plupart des établissements ESR envisagent de recourir à un membre de leur personnel plutôt qu'à un DPO externe.

### 3.16.3. Mise en conformité de l'établissement ESR

Les actions suivantes doivent être accomplies par l'établissement ESR s'agissant de la thématique du DPO, étant précisé qu'il n'y a pas lieu de s'interroger sur l'opportunité de sa désignation dans la mesure où celle-ci est obligatoire :

- Établir une stratégie s'agissant de la désignation du DPO : doit-il être l'ancien CIL ? Doit-il être mutualisé sur l'ensemble des sites de l'université ou est-il préférable de doter chaque site de son propre DPO ? Le conflit d'intérêt est-il totalement évincé ? Dispose-t-il des compétences nécessaires ?

- Mettre en œuvre une organisation adaptée lui permettant d'accomplir ses fonctions en toute indépendance, d'accéder à l'ensemble des données et ressources nécessaires et de respecter le secret professionnel ou une obligation de confidentialité ;

- Établir des règles de gouvernance, c'est-à-dire prévoir les règles applicables aux rapports entretenus avec ses différents interlocuteurs (Direction générale, DSI-RSSI, personnes concernées, Cnil, autres DPO susceptibles d'interagir avec lui ou encore sous-traitants) ;

- Sensibiliser le personnel à la désignation du DPO, ce qui se traduit par deux aspects : tout d'abord, prévoir une information interne sur la désignation du DPO, par l'intermédiaire notamment d'un mailing groupé du personnel ; puis prévoir des mesures de sensibilisation du personnel sur la protection des données à caractère personnel et le rôle joué par le DPO ;

- Prévoir la rédaction par le DPO d'un rapport annuel relatif à l'activité de l'établissement ESR du point de vue des données à caractère personnel, ce qui s'inscrit dans une démarche d'accountability, soit de démonstration de la conformité de l'établissement ESR à ses obligations du point de vue de la protection des données et des exigences du RGPD.

## 3.17. TRANSFERTS HORS UE

### 3.17.1. Obligation

Le chapitre V du RGPD est relatif aux transferts de données à caractère personnel vers des pays tiers, soit des pays situés hors de l'Union européenne, ou des organisations internationales. Son article 44 pose le principe selon lequel tout transfert de données vers des pays tiers doit respecter les dispositions dudit chapitre :

> *« Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis ».*

Les articles 45 et 46 exposent le régime applicable aux transferts de données hors de l'Union européenne. Ils invitent à prendre en considération l'existence ou non d'une décision d'adéquation du niveau de protection du destinataire du transfert, qui se définit comme une décision de la Commission constatant que le pays concerné assure un niveau de protection adéquat au regard de la règlementation applicable à la protection des données à caractère personnel.

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, définies par l'article 46 du RGPD aux termes duquel :

> *« (…) 2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par :*
> *a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics ;*
> *b) des règles d'entreprise contraignantes conformément à l'article 47 ;*
> *c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2 ;*
> *d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2 ;*
> *e) un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ; ou*
> *f) un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ».*
> *3. Sous réserve de l'autorisation de l'autorité de contrôle compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, par :*
> *a) des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale ; ou*
> *b) des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées ».*

L'article 49 du RGPD prévoit des exceptions dans lesquelles un transfert de données à caractère personnel hors de l'Union européenne peut avoir lieu, même en l'absence de décision d'adéquation ou de garanties appropriées :

> *« 1. En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes :*
> *a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ;*
> *b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;*
> *c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ;*
> *d) le transfert est nécessaire pour des motifs importants d'intérêt public ;*
> *e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;*
> *f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;*
> *g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce ».*

### 3.17.2. Incidence de la disposition sur l'établissement ESR

Le transfert de données en provenance d'un établissement ESR français vers un pays tiers à l'Union européenne est susceptible de concerner plusieurs hypothèses, telles que notamment la mobilité étudiante ou encore les échanges entre universités à des fins de recherche.

La mobilité étudiante constitue un objectif fondamental pour les établissements ESR européens, qui depuis plusieurs années cherchent à la développer afin que leurs étudiants bénéficient d'une expérience à l'étranger. Elle passe principalement par les réseaux Erasmus et Erasmus+, qui comportent des membres participants et des membres partenaires situés dans l'Union européenne et hors de celle-ci.

Il convient ainsi de prêter attention aux données échangées entre ces pays, étant précisé que l'inscription d'un étudiant à un programme de mobilité étudiante n'implique pas un transfert de ses données entre son établissement ESR d'origine et l'établissement ESR de destination mais une réinscription totale auprès de l'établissement ESR de destination.

### 3.17.3. Mise en conformité de l'établissement ESR

Afin que les transferts de données vers des pays tiers à l'Union européenne soient opérés conformément aux exigences du RGPD, il convient de respecter la méthodologie suivante :

- Identifier les hypothèses de flux transfrontières selon les traitements mis en œuvre ;
- Analyser la situation de chaque pays destinataire du point de vue de la Commission européenne : s'agit-il d'un pays présentant un niveau de protection adéquat ?
- Vérifier qu'aucune exception prévue à l'article 49 du RGPD n'a vocation à s'appliquer ;

- Le cas échéant, rédiger des clauses contractuelles standards ou mettre en œuvre d'une procédure de contrôle des clauses soumises par les pays concernés ;
- Rédiger des binding corporate rules afin d'accompagner les transferts de données hors de l'Union européenne.

## 3.18. PROTECTION BY DESIGN ET BY DEFAULT

### 3.18.1. Obligation

L'article 25 du RGPD met à la charge du responsable du traitement 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 default »). Aux termes de cet article :

> *« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.*
> *2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concerné (…)».*

La protection des données dès la conception (« privacy by design ») suppose que le responsable de 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 d'appliquer les principes relatifs à cette protection. Il doit à ce titre mettre en œuvre des mesures à la fois techniques (chiffrement, pseudonymisation, etc.) et organisationnelles (règles de minimisation, conformément au principe de minimisation précité).

La protection des données par défaut (« privacy by default ») suppose que le responsable de traitement ne traite que les données à caractère personnel strictement nécessaires au regard des finalités du traitement et limite l'accès à celles-ci aux seules personnes habilitées.

### 3.18.2. Incidence de la disposition sur l'établissement ESR

Dans le cadre de leur démarche de mise en conformité au RGPD, les établissements ESR, au même titre que tout responsable de traitement, doivent appréhender les thématiques fondamentales de la protection et de la sécurisation afin que tous les traitements actuels soient mis aux normes et que les nouveaux traitements soient envisagés sous cet angle dès leur mise en œuvre.

Or, la particularité des établissements ESR en leur qualité de responsable de traitement tient à la grande hétérogénéité des traitements qu'ils mettent en œuvre, qui s'analyse au niveau de la diversité des finalités, du type et de la quantité de données traitées, au grand nombre d'organismes tiers intervenant dans le traitement en diverses qualités (responsable de traitement, sous-traitant ou simple destinataire), etc. Ainsi, tous les traitements ne sont pas soumis au même degré de risque et ne supposent pas le déploiement des mêmes mesures et règles de gouvernance.

Il apparaît que nombre d'établissements ESR semblent avoir pris en considération la thématique de la protection des données en isolant les traitements les plus sensibles, en prévoyant une politique d'habilitation permettant à un nombre restreint de personnes d'accéder aux données ou encore en recourant à diverses techniques de protection (pseudonymisation, anonymisation, etc.).

### 3.18.3. Mise en conformité de l'établissement ESR

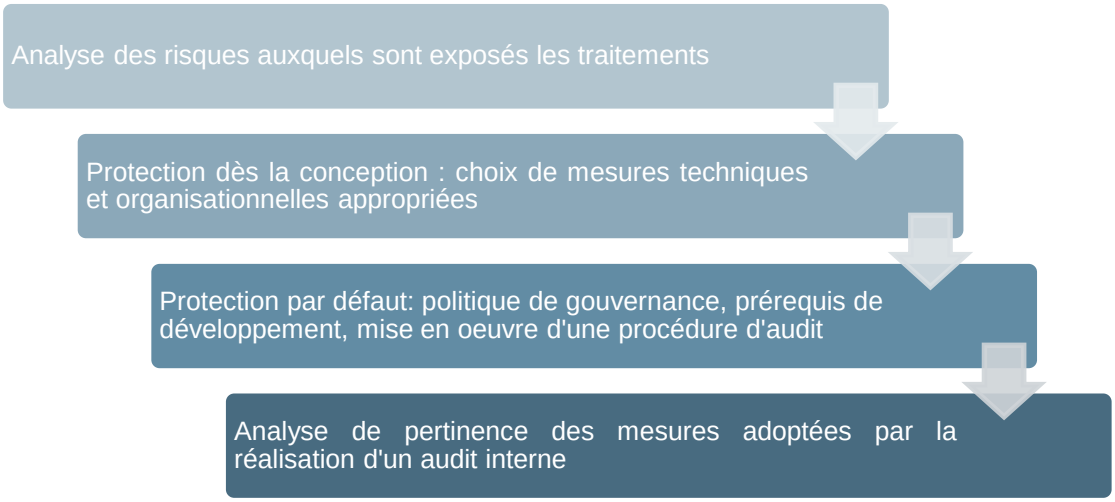
Avant de déployer les mesures requises, l'établissement ESR peut commencer par réaliser une analyse des risques générés sur la vie privée des personnes concernées par les traitements qu'il met en œuvre ou projette de mettre en œuvre[19]. À ce titre, la cartographie des traitements rassemble les informations requises pour déterminer le degré de risques auquel est exposé un traitement : nature des données traitées, personnes susceptibles d'y avoir accès, éventuel transfert à des destinataires, recours à des sous-traitants, etc.

Par la suite, il convient de déployer les mesures adéquates et proportionnées à ces risques :

- Mise en œuvre de mesures techniques appropriées, telles que par exemple le chiffrement, la pseudonymisation ou l'anonymisation ;
- Mise en œuvre de mesures organisationnelles appropriées, qui consistent en les procédures adoptées pour mettre en œuvre les principes de nécessité et de minimisation ;
- Adoption d'une politique de gouvernance des données afin de déterminer des règles de compétence en matière de protection des données à caractère personnel ;
- Adoption de prérequis de développement, soit la formalisation des actes à accomplir afin de se conformer aux exigences de chaque obligation du RGPD, qui permettent de démontrer sa bonne foi et d'organiser le déploiement de la mise en conformité *(Annexe n°12 : Modèle de prérequis juridiques de développement)* ;

Une fois l'ensemble de ces mesures déployées, l'analyse de leur pertinence peut s'avérer opportune afin que l'établissements ESR analyse leur proportionnalité et leur nécessité aux risques générés par le traitement. Pour ce faire, il peut s'avérer opportun de mettre en œuvre une procédure d'audit interne de de diligenter ledit audit avec pour objectif le test de l'ensemble de ces mesures pour prendre connaissance de leur adéquation aux spécificités des traitements mis en œuvre par l'établissement ESR.

[19] L'analyse des risques diffère de l'analyse d'impact imposée par l'article 35 du RGPD, et traitée ultérieurement dans le présent document.




## 3.19. SECURITE

### 3.19.1. Obligation

L'article 5 du RGPD érige la sécurité en principe fondateur relatif aux traitements de données à caractère personnel. Son article 32 met à la charge du responsable de traitement et de son sous-traitant une obligation de sécurisation des traitements de données à caractère personnel mis en œuvre, rédigée comme suit :

> *« 1. Compte tenu l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :*
> *a) la pseudonymisation et le chiffrement des données à caractère personnel ;*
> *b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
> *c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;*
> *d) 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. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite (…) ».*

### 3.19.2. Incidence de la disposition sur l'établissement ESR

Comme il a été observé précédemment, les caractéristiques des traitements mis en œuvre par un même établissement ESR sont susceptibles de les soumettre à des risques en matière de sécurité : traitement de données sensibles (données de santé et relatives à l'appartenance syndicale) ou de données dotées d'un caractère critique (données bancaires, données relatives au parcours scolaire et académique de l'étudiant, données de candidature, etc.), données de personnes mineurs, grande hétérogénéité des personnes concernées, etc.

### 3.19.3. Mise en conformité de l'établissement ESR

Les établissements ESR, compte tenu du caractère fondamental que revêt la thématique de la sécurité, peuvent décider d'adopter les démarches suivantes :

- Procéder à une analyse des risques que présentent les différents traitements mis en œuvre par l'établissement ESR afin de pouvoir adapter les mesures prises pour les juguler afin qu'elles ne soient ni insuffisantes ni trop contraignantes à mettre en œuvre. Une fois encore, la réalisation de la cartographie permet de renseigner utilement sur toutes les mesures déployées en termes de sécurité, car ces informations doivent y être recensées ;

- Adopter les mesures techniques requises, ce qui peut signifier recourir au chiffrement ou à tout autre moyen technique permettant d'assurer l'intégrité et la confidentialité des données, étant précisé que de nombreux établissements ESR recourent déjà à des techniques telles que la pseudonymisation. Afin d'assurer l'effectivité de telles mesures, un audit de vulnérabilité pourrait être diligenté pour tester la réponse apportée à une hypothétique faille de sécurité ;

- Adopter les mesures organisationnelles requises, ce qui concerne les procédures mises en œuvre par l'établissement ESR en matière de sécurité. À ce titre, il convient d'adopter un PSSI (plan de sécurité des systèmes d'information) ou, s'il existe déjà, de l'adapter pour tenir compte des exigences du RGPD et des spécificités des traitements mis en œuvre par l'établissement ESR. Il peut également s'avérer utile d'adopter un plan de reprise d'activité ou un plan de continuité d'activité et de mettre en œuvre une procédure d'audit.

## 3.20. VIOLATION DE SECURITE

### 3.20.1. Obligation

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 les responsables de traitement (préjudice d'image), le RGPD a prévu à leur charge deux obligations à mettre en œuvre en cas d'exposition à une faille.

La première de ces obligations, envisagées par l'article 33 du RGPD, consiste en la notification de la faille à la Cnil, laquelle doit intervenir dans un délai 72 heures après qu'il en a pris connaissance et comporter les informations énumérées audit article, rédigé comme suit :

> *« 1. 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 (…).*
> *3. La notification visée au paragraphe 1 doit, à tout le moins :*
> *a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;*
> *b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;*
> *c) décrire les conséquences probables de la violation de données à caractère personnel ;*
> *d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives ;*
> *4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.*
> *5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article ».*

La seconde obligation, prévue par l'article 34 du RGPD, consiste en 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. Cette obligation s'avère plus conditionnée que la précédente, elle ne doit être respectée que dans certaines hypothèses prévues par l'article précité :

> *« 1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.*
> *2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).*
> *3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :*
> *a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;*
> *b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;*

> *c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.*
> *4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie ».*

### 3.20.2. Incidence de la disposition sur l'établissement ESR

Dans la mesure où les établissements ESR concentrent de nombreuses données à caractère personnel, tels que des identifiants bancaires, des numéros de sécurité sociale ou encore des identifiants et leurs mots de passe, ils sont très régulièrement la cible d'actes de piratage informatique ou de failles de sécurité, dont les conséquences vont parfois jusqu'à des fuites de ces données.

Les actes de piratage informatique subis par les établissements ESR, parfois commis par des étudiants ou d'anciens étudiants, sont de plusieurs natures : compromission d'applications de gestion de contacts rendant accessibles les données y étant enregistrées, accès frauduleux de hackers dans les serveurs de l'établissement ESR, etc. Les conséquences peuvent être multiples : modification et altération de données sur le serveur du responsable de traitement, revente de données, piratage d'identifiants bancaires, usurpation d'identité, etc.

Certains programmes de piratage s'adressent d'ailleurs spécifiquement aux étudiants : sur le Darknet, des hackers leur proposent via certains programmes payants d'attaquer les bases de données de leur université afin de modifier les notes obtenues aux examens. Malgré la simplicité conférée par le recours à des hackers professionnels, de tels services nécessitent que l'étudiant soit formé à l'utilisation du Darknet, ce qui explique que de tels piratages soient encore rares.

L'hypothèse de la fuite de données peut également résulter d'une erreur ou mauvaise manipulation informatique effectuée par le personnel de l'établissement ESR, susceptible d'aboutir à la divulgation de données. Par exemple, une erreur de pièce jointe ou d'ensemble de destinataires d'un mail peut donner lieu à la divulgation de nombreuses données à des personnes non habilitées à y accéder.

### 3.20.3. Mise en conformité de l'établissement ESR

Compte tenu des importants risques de faille de sécurité et de divulgations de données à caractère personnel, il convient que l'établissement ESR établisse 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 qu'il conviendra de mettre en œuvre devra appréhender la nécessité, face à une faille de sécurité quelle qu'elle soit, de respecter les étapes suivantes :

- Identifier et corriger la faille dans un premier temps afin de limiter au maximum ses conséquences sur les données à caractère personnel des étudiants ;
- Constituer un dossier de preuve technique, c'est-à-dire rédiger un document comportant une description de la faille identifiée, de ses conséquences réelles ou supposées sur les données et des mesures prises pour la corriger ;
- S'interroger sur la qualification juridique éventuellement susceptible de s'appliquer ;
- Le cas échéant et selon les résultats de cette analyse, déposer une plainte pénale ;

- Notifier à la Cnil la violation de sécurité, si possible dans les 72 heures après avoir pris connaissance des faits ;
- Si la faille de sécurité emporte des conséquences sur des données à caractère personnel, communiquer aux personnes concernées à propos de celle-ci conformément aux dispositions de l'article 34 précité ;
- Prendre attache avec sa compagnie d'assurance, étant précisé qu'il existe des polices d'assurance couvrant spécifiquement les risques afférents à la protection des données à caractère personnel.

## 3.21. ANALYSE D'IMPACT

### 3.21.1. Obligation

Bien qu'une brève analyse des risques soit recommandée préalablement à la mise en œuvre d'un traitement de données à caractère personnel, le RGPD va plus loin en exigeant dans certaines situations que soit effectuée une analyse d'impact, définie comme une analyse de l'impact du traitement sur les droits des personnes concernées. L'article 25 du RGPD énonce :

> *« 1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires (…)*
> *3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants :*
> *a) 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 ;*
> *b) 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 c)*
> *c) la surveillance systématique à grande échelle d'une zone accessible au public ».*

D'après la lettre du texte, l'analyse d'impact concerne tous les traitements présentant des risques particuliers du point de vue de leur nature, de leur portée et de leur finalité, tels que notamment les traitements cités aux points a) à c).

De façon générale, la Cnil considère que les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact :

- évaluation / scoring, soit traitements de données mis en œuvre afin d'affecter une note à un client ou prospect, laquelle traduit fréquemment la probabilité qu'il réponde à une sollicitation commerciale ou appartienne à une cible recherchée (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique, ce qui se réfère à l'hypothèse de la géolocalisation permanente ;
- collecte de données sensibles ;
- collecte de données personnelles à grande échelle, ce qui se réfère à l'hypothèse du big data, défini comme l'analyse de données en masse via des outils spécifiques et permettant au public d'accéder en temps réel à des bases de données géantes ;
- croisement de données, c'est-à-dire recoupement de données à caractère personnel afin de parvenir aux conclusions recherchées par rapport à la personne concernée ;
- traitement des données d'une personne considérée comme vulnérable, ce qui se réfère aux patients, personnes âgées, enfants, etc. ;
- usage innovant, ce qui se réfère à toute hypothèse d'utilisation d'une nouvelle technologie ;
- exclusion du bénéfice d'un droit ou d'un contrat par le traitement de donnée lui-même.

### 3.21.2. Incidence de la disposition sur l'établissement ESR

Une brève analyse des traitements mis en œuvre par les établissements ESR permet d'entrevoir que le traitement par lequel la plupart d'entre eux sélectionnent les candidats bacheliers et étudiants en réorientation préinscrits sur la plateforme Parcousup est susceptible de nécessiter 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 : certaines recourent à des dispositifs de DIA, qui rassemblent plusieurs des critères précités :

- Cette technique est mise en œuvre aux fins d'évaluation des candidatures ;
- Cette technique est un procédé de décision automatique avec effet légal ou similaire ;
- Cette technique est susceptible de concerner une personne vulnérable, soit un mineur ;
- Cette technique est susceptible d'exclure un candidat du bénéfice de l'inscription au sein de l'établissement ESR concerné.

Par conséquent, si l'établissement ESR recourt à un dispositif de DIA pour sélectionner ses futurs étudiants, il conviendra, d'après la grille d'analyse précitée de la Cnil, de réaliser une étude d'impact afin de s'assurer de l'absence d'atteinte de ce dernier aux droits et libertés des candidats concernés.

### 3.21.3. Mise en conformité

Dans un premier temps l'identification des traitements soumis à analyse d'impact s'avère fondamentale : il conviendra de mener la même réflexion que précédemment avec le traitement ayant pour finalité la sélection des candidats à l'établissement ESR pour chacun des traitements mis en œuvre par l'établissement ESR.

Si tel est le cas, l'établissement ESR pourra recueillir l'assistance du sous-traitant s'il existe et solliciter l'aide et les conseils de son DPO afin de parvenir à l'analyse d'impact, laquelle doit comporter, dans l'ordre, les éléments suivants :

- Description générale du traitement envisagé et de ses finalités ;
- Évaluation des caractères de nécessité et de proportionnalité de ce traitement ;
- Évaluation des risques pour les droits et libertés des personnes concernées ;
- Explication des moyens envisagés pour faire face à ces risques.

## TABLEAU SYNTHETIQUE DE LA DEMARCHE DE MISE EN CONFORMITE RGPD

| N° | Thème concerné | Énoncé de la démarche | Personnel de l'établissement ESR impliqué | Liste des livrables à élaborer |
|---|---|---|---|---|
| **1** | Principe de minimisation | Déploiement d'une cartographie des traitements mis en œuvre afin d'identifier toutes les données traitées. En fonction des résultats, analyse de l'opportunité du traitement de certaines données et, le cas échéant réajustement de la liste des données traitées. | Tous les services qui traitent des données à caractère personnel au sein de l'établissement ESR doivent contribuer à la création de la cartographie et envisager le réajustement des données traitées. | - Annexe 2 : Modèle de cartographie des traitements |
| **2** | Durée de conservation | Cartographie des traitements indispensable pour prendre connaissance des durées de conservation actuelles des données. Puis réflexion et éventuels réajustements, formalisés dans une politique de conservation des données. | - Services concernés pour réfléchir à la durée de conservation selon chaque traitement<br>- DSI pour la suppression des données à l'expiration du délai | - Annexe 2 : Modèle de cartographie des traitements |
| **3** | Licéité du traitement | Cartographie des traitements indispensable pour envisager le fondement sur lequel repose un traitement et pour pouvoir en justifier. | Services concernés pour réfléchir à la justification de la licéité du traitement qu'ils mettent en œuvre. | - Annexe 2 : Modèle de cartographie des traitements |
| **4** | Consentement | Mention de recueil du consentement pertinente, lisible, qui permette un acte positif de la personne concernée (case à cocher) et distincte des mentions d'acceptation de conditions générales ou politiques diverses. | Service juridique | - Mention de recueil du consentement de la personne concernée à un traitement de données<br>- Annexe 14 : Modèle de clause de recueil du consentement lors de l'inscription à une newsletter |

| | | | | |
|---|---|---|---|---|
| **5** | Transparence | Élaboration de politiques sur la thématique de la protection des données à caractère personnel, qui diffèrent selon les catégories de personnes concernées et donc selon les traitements mis en œuvre. | Service juridique | - Annexe 3 : Modèle de politique RGPD à destination des étudiants et candidats<br>- Annexe 4 : Modèle de politique RGPD à destination des salariés<br>- Annexe 5 : Modèle de politique RGPD à destination des partenaires |
| **6** | Droit d'accès et de copie | - Organisation de la procédure destinée à répondre aux demandes d'exercice du droit d'accès<br>- Rédaction d'une disposition relative au droit d'accès dans les différentes politiques RGPD | Service juridique | - Disposition spécifique dans les politiques RGPD concernées |
| **7** | Droit de rectification | - Analyse de dispositifs techniques permettant de procéder à la rectification de données inexactes ou obsolètes<br>- Organisation de la procédure destinée à répondre aux demandes d'exercice du droit d'accès<br>- Rédaction d'une disposition propre au droit d'accès dans les différentes politiques RGPD | Service juridique | - Disposition spécifique dans les politiques RGPD concernées |

| | | | | |
|---|---|---|---|---|
| **8** | Droit à l'effacement | - Identification des cas d'usage<br>- Analyse de dispositifs techniques pour procéder à l'effacement de données ;<br>- Organisation de la procédure destinée à répondre aux demandes d'exercice du droit à l'effacement<br>- Rédaction d'une disposition propre au droit à l'effacement dans les politiques RGPD (précision des conditions) | Service juridique | - Disposition spécifique dans les politiques RGPD concernées |
| **9** | Droit à la limitation | - Identification des cas d'usage<br>- Analyse de dispositifs techniques pour procéder à la limitation des données ;<br>- Organisation de la procédure destinée à répondre aux demandes d'exercice du droit à la limitation des données<br>- Rédaction d'une disposition propre au droit à la limitation dans les politiques RGPD (précision des conditions) | Service juridique | - Disposition spécifique dans les politiques RGPD concernées |
| **10** | Droit à la portabilité | - Identification des cas d'usage<br>- Analyse de dispositifs techniques pour assurer la portabilité des données ;<br>- Organisation de la procédure destinée à répondre aux demandes d'exercice du droit à la portabilité<br>- Rédaction d'une disposition propre au droit à la portabilité dans les politiques RGPD (précision des conditions) | Service juridique | - Disposition spécifique dans les politiques RGPD concernées |

| | | | | |
|---|---|---|---|---|
| **11** | Droit d'opposition | - Identification des cas d'usage<br>- Analyse de dispositifs techniques pour répondre aux demandes d'exercice du droit d'opposition ;<br>- Organisation de la procédure destinée à répondre aux demandes d'exercice du droit d'opposition<br>- Rédaction d'une disposition propre au droit d'opposition dans les politiques RGPD (précision des conditions) | Service juridique | - Disposition spécifique dans les politiques RGPD concernées |
| **12** | Décision individuelle automatisée | Rédaction dans la politique relative aux étudiants et candidats d'une disposition relative aux moyens employés pour sélectionner les candidats dans le cadre de la procédure d'affectation de ces derniers via Parcoursup. | Service juridique | - Disposition spécifique dans les politiques RGPD concernées |
| **13** | Sous-traitance | - À partir de la cartographie des traitements, établir une cartographie des sous-traitants pour identifier les traitements existants.<br>- Sous-traitants actuels : adresser une lettre de demande de conformité. Selon leur réponse, prévoir un avenant au contrat de prestation de services qui renvoie vers l'annexe RGPD.<br>- Sous-traitants futurs : proposer d'insérer dans leur contrat une clause renvoyant vers l'annexe RGPD. | Membre du personnel ou de la direction chargé des relations avec les prestataires externes. | - Annexe 6 : Lettre type de demande de conformité au sous-traitant<br>- Annexe 7 : Modèle d'avenant au contrat de prestations de services<br>- Annexe 8 : Annexe RGPD au contrat de prestations de services<br>- Annexe 9 : Clause RGPD et sous-traitance à incorporer au contrat de prestations de services<br>- Annexe 10 : Modèle de lettre d'engagement de confidentialité |

| | | | | |
|---|---|---|---|---|
| **14** | Registre des traitements | Une fois la cartographie achevée, intégration de ses données dans le registre des traitements, document qui synthétise l'ensemble des caractéristiques des traitements mis en œuvre par l'établissement ESR. | - Soit chaque service pour les traitements qu'il administre ;<br>- Soit la DSI ou toute autre personne compétente pour incorporer les données des cartographies dans le registre. | - Annexe 11 : Modèle de registre des traitements du responsable de traitement<br>- Annexe 12 : Modèle de prérequis juridiques de développement |
| **15** | Responsabilité conjointe | - Analyse des rapports entretenus avec les différents interlocuteurs de l'établissement ESR avec lesquels sont échangés des données à caractère personnel<br>- Rédaction de contrats de responsabilité conjointe pour encadrer | Service juridique | - Annexe 13 : Modèle de contrat de responsabilité conjointe entre deux responsables de traitement |
| **16** | DPO | - Établissement d'une stratégie de désignation du DPO s'il n'a pas encore été désigné<br>- Établissement d'une procédure afin que le DPO puisse exercer sa mission<br>- Adoption de règles de gouvernance pour régir les relations entre le DPO et ses différents interlocuteurs<br>- Actions de sensibilisation du personnel | Instances en charge de la désignation du DPO | - |
| **17** | Transferts hors UE | - Identification des hypothèses de flux transfrontières<br>- Analyse de la situation de chaque pays destinataire : présente-t-il un degré de protection adéquat ?<br>- Vérification de l'absence d'exception aux principes de degré de protection adéquat<br>- Le cas échéant, rédaction de binding corporate rules (BCR) | Service juridique | - |

| | | | | |
|---|---|---|---|---|
| **18** | Protection | - Analyse des risques générés par les différents traitements mis en œuvre<br>- Déploiement des différentes mesures techniques et organisationnelles appropriées pour mettre en œuvre les principes de nécessité et minimisation<br>- Adoption d'une politique de gouvernance<br>- Adoption de prérequis juridiques de développement | DSI et services à l'initiative de la mise en œuvre d'un traitement afin de décider des mesures qui s'imposent en amont | - Annexe 12 : Modèle de prérequis juridiques de développement |
| **19** | Sécurité | - Analyse des risques générés par les différents traitements mis en œuvre<br>- Déploiement des différentes mesures techniques appropriées ;<br>- Déploiement des différentes mesures organisationnelles appropriées : PSSI, PRA, PCA, procédure d'audit interne<br>- Le cas échéant, analyse de pertinence de l'ensemble de ces mesures grâce à divers tests (audit de vulnérabilité, etc.) | DSI et services à l'initiative de la mise en œuvre d'un traitement afin de décider des mesures qui s'imposent en amont | - Annexe 12 : Modèle de prérequis juridiques de développement<br>- PSSI<br>- Plan de reprise d'activité<br>- Plan de continuité d'activité |
| **20** | Violation de sécurité | Établissement d'une procédure destinée à juguler toute faille et ses conséquences et permettant de s'acquitter de ses obligations vis-à-vis de la Cnil et des personnes concernées. | DSI | - |
| **21** | Analyse d'impact | - Identification des traitements soumis à analyse d'impact<br>- Le cas échéant, réalisation d'une analyse d'impact documentée par apport à chaque traitement qui le requiert | DSI | - |

## 4. ANNEXES : LIVRABLES DE MISE EN CONFORMITÉ AU RGPD

Liste des annexes

- Annexe n°1 : Présentation du RGPD
- Annexe n°2 : Modèle de cartographie des traitements
- Annexe n°3 : Modèle de politique RGPD à destination des étudiants et candidats
- Annexe n°4 : Modèle de politique RGPD à destination des salariés
- Annexe n°5 : Modèle de politique RGPD à destination des partenaires
- Annexe n°6 : Lettre type de demande de conformité au RGPD à adresser aux sous-traitants
- Annexe n°7 : Avenant au contrat conclu entre responsable de traitement et sous-traitant
- Annexe n°8 : Annexe RGPD opposée par le responsable de traitement au sous-traitant
- Annexe n°9 : Modèle de clause données à caractère personnel à opposer au sous-traitant
- Annexe n°10 : Modèle de lettre d'engagement de confidentialité
- Annexe n°11 : Modèle de registre des traitements du responsable de traitement
- Annexe n°12 : Modèle de prérequis juridiques de développement
- Annexe n°13 : Modèle de contrat de responsabilité conjointe
- Annexe n°14 : Modèle de clause relative à l'inscription à une newsletter

## ANNEXE N°1 – PRÉSENTATION DU RGPD

Le règlement général sur la protection des données (« RGPD »)[20], entré en vigueur le 24 mai 2016, sera applicable à compter du 25 mai 2018.

Le RGPD modifie le droit des données à caractère personnel tel que nous le connaissons aujourd'hui.

En effet, le RGPD allège une partie des formalités préalables des entreprises mais :

- renforce les droits des personnes ;
- accroit les obligations du responsable de traitement ;
- responsabilise les sous-traitants bien plus qu'aujourd'hui.

L'incidence du RGPD est d'autant plus grande qu'il met en œuvre un nouveau principe intitulé l'« accountability »[21] qui renverse la charge de la preuve et oblige les entreprises et les acteurs publics à démontrer leur conformité auprès de l'autorité de contrôle (la « Cnil »).

En outre, les risques en cas de non-conformité au RGPD sont très importants :

- risque financier, avec un risque d'amende administrative pouvant atteindre jusqu'à 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires annuel mondial. De plus, toute entreprise ou acteur public pourra être tenu de réparer le préjudice subi par les personnes concernées ;
  - atteinte à l'image, qui sera d'autant plus importante dans le cadre des premières condamnations prises sous l'empire du RGPD ;
  - risque de suspension ou de limitation d'un traitement considéré comme non-conforme ;
- risque de condamnation pénale dans des situations extrêmes.

Face à de tels risques, toutes les entreprises et acteurs publics, en tant que responsables de traitement, quels que soient leur taille ou leur statut, se doivent de mettre en œuvre une politique RGPD.

Cette politique passe par 10 actions prioritaires que sont :

**Action 1** – Cartographie juridique des traitements afin d'identifier le nombre et la nature des traitements à prendre en charge dans le cadre du programme de mise en conformité RGPD ;

**Action 2** – Élaboration du registre des traitements pour les entreprises qui y sont astreintes (plus de 250 employés et autres cas spécifiques), registre qui reste conseillé même en dessous de ces seuils et conditions ;

**Action 3** – Identification des cas de sous-traitance et adoption de règles spécifiques pour traiter la relation entre le responsable de traitement et ses sous-traitants. Le RGPD impose en effet qu'un contrat

[20] 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
[21] Cf. article 5 du RGPD

soit établi entre le responsable de traitement et le sous-traitant, contrat dans lequel doivent impérativement figurer 8 dispositions précises elles aussi imposées par le RGPD ;

**Action 4** – Obligation d'information et transparence qui passe nécessairement par l'adoption de la politique RGPD salariés/agents qui définit les conditions dans lesquelles sont traitées les données des salariés ou des agents et la politique RGPD clients/prospects qui, elle, permet de traiter les cas des données relatives aux clients et aux prospects pour une entreprise. Cette deuxième politique doit être adaptée aux cas d'espèce. Pour les collectivités territoriales, il s'agira plutôt d'une Politique des données citoyens, pour les écoles et universités, d'une charte des données des élèves et/ou des étudiants, etc. ;

**Action 5** – Mise en œuvre de l'obligation de protection par défaut et de la protection dès la conception qui imposent l'adoption de règles de gouvernance précises sur « qui fait quoi » en termes de données personnelles et de « guidelines » pour tout nouveau traitement ;

**Action 6** – Sécurisation des traitements qui passe par un double travail : d'une part, un travail technique servant à implémenter les outils de sécurité appropriés et, d'autre part, un travail juridique comme la refonte de la PSSI ou de la charte des systèmes d'information ;

**Action 7** – Identification des flux effectués en dehors de l'Union européenne qui sont traités soit par le déploiement de clauses contractuelles types, établies par la Commission européenne, soit par l'adoption de Binding Corporate Rules (« BCR ») au sein des groupes internationaux ;

**Action 8** – La formation et la sensibilisation des personnels ne figurent pas dans le RGPD en tant que telles mais elles sont nécessaires dans le cadre de la politique d'accountability et de gestion du risque (perte de données accidentelle principalement). Ce besoin de former le personnel est d'ailleurs régulièrement rappelé par la Cnil (notamment dans son dernier Guide de la sécurité) ;

**Action 9** – Désignation d'un délégué à la protection des données (« DPO »), obligatoire dans trois cas (notamment pour les acteurs publics) mais vivement conseillée dans tous les autres cas ;

**Action 10** – Mise en œuvre d'une analyse d'impact et consultation préalable de la Cnil lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Ces 10 actions sont prioritaires. Ceci étant précisé, il y a bien d'autres sujets à aborder notamment autour des concepts nouveaux tels que la minimisation ou la portabilité ; ou encore des réflexions autour de la licéité des traitements (consentement v. intérêt légitime), la certification ou le recours à des codes de conduite, etc.

# ANNEXE N°2 – MODÈLE DE CARTOGRAPHIE DES TRAITEMENTS

## 1. CONTEXTE ET OBJECTIFS

Le règlement général sur la protection des données[22][23] (« RGPD »), entré en vigueur depuis le [24] mai 2016, va prochainement modifier le droit des données à caractère personnel tel que nous le connaissons aujourd'hui.

Compte tenu des modifications profondes que cette réforme implique, le règlement n'entrera en application que le 25 mai 2018, soit deux ans après son entrée en vigueur, afin de laisser aux acteurs publics et privés le temps de se préparer et de s'adapter aux nouvelles obligations pesant sur eux.

Le point clé de cette nouvelle règlementation est le montant très élevé des sanctions que risquent les acteurs privés et publics en cas de manquement à ces nouvelles obligations.

Afin de prévenir tout risque de sanction, il est indispensable d'être en conformité avec la règlementation applicable.

La présente cartographie de traitement est un outil mis à votre disposition par le cabinet Racine pour facilement identifier les traitements mise en œuvre dans le cadre de votre activité.

L'objectif est de répondre aux exigences de l'article 30 du RGPD relatif à la tenue d'un registre des activités de traitement qui doit nécessairement contenir les informations recensées par cette cartographie.

Le cabinet Racine reste à votre disposition pour toutes questions ou tout doute concernant le contenu de cette cartographie.

| | |
|---|---|
| Date | |
| Version | |
| Rédacteur[23] | |
| Personne interviewée[24] | |

[22] 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

[23] Nom et fonction du rédacteur de la fiche ou de l'interviewer s'il y a lieu

[24] Uniquement dans le cas où le cabinet Racine réalise l'interview

## 2. IDENTIFICATION DU TRAITEMENT

| | |
|---|---|
| Nom du traitement en interne[25] | |
| Dénomination commerciale de l'éditeur et nom de l'application | |
| Versioning[26] | |
| Date de mise en service | |
| Editeur[27] | |
| Maintenance | |

## 3. DESCRIPTIF SYNTHÉTIQUE DU TRAITEMENT [28]

[25] Acronyme à détailler
[26] Version de l'application utilisée
[27] En cas de développement interne, mettre le service concerné
[28] Cette partie doit décrire de manière synthétique le traitement mis en œuvre (personne concernée, finalités, durée de conservation, etc.)

## 4. RESPONSABLE DU TRAITEMENT & CONTACTS

Rappel – Le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Le responsable du traitement est donc celui qui identifie les objectifs principaux du traitement et les moyens utilisés pour mettre en œuvre ce traitement.

| | |
|---|---|
| Nom et coordonnées du responsable du traitement | |
| Co-responsable de traitement [29] | Non ☐<br>Oui ☐<br>Si oui, préciser le nom et les coordonnées : |
| Nom et coordonnées du service ou de la personne en charge du traitement s'il est différent du responsable du traitement | |

[29] Dans le cas où un ou plusieurs responsables de traitement déterminent conjointement les finalités et les moyens du traitement

## 5. FINALITÉS DU TRAITEMENT

Rappel – La finalité d'un traitement est définie comme étant les « objectifs principaux assignés au traitement et aux fonctions substantielles mises en œuvre » par le responsable de traitement ou le sous-traitant.

Exemple de finalités : la gestion des comptes utilisateurs et des espaces personnalisés sur une plateforme internet, la mise en œuvre de la comptabilité, l'utilisation de cookies, la mise à disposition d'une newsletter, la gestion des ressources humaines, la mesure de l'audience d'un site internet, le traitement des dossiers de candidats, etc.

| Finalités | Description |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| N | |

## 6. PERSONNES CONCERNÉES

Rappel – Les personnes concernées sont « les personnes physiques identifiables ou identifiées dont les données à caractère personnel sont collectées et intégrées dans le traitement de données à caractère personnel ».

Salariés /agents ☐

Intérimaire ☐

Stagiaire ☐

Étudiants /auditeur ☐

Visiteurs ☐

Client ☐

Prospects ☐

Adhérents ☐

Fournisseur ☐

Partenaires ☐

Prestataires ☐

Autres ☐

- Préciser :

## 7. CATÉGORIES DE DONNÉES COLLECTÉES

Rappel – La notion de données personnelles s'entend de « toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

La notion de catégorie de données à caractère personnel s'entend d'un ensemble de données pouvant être regroupé au sein d'une même famille.

Identité[30] ☐

Préciser :

Identification[31] ☐

Préciser :

État civil[32] ☐

Préciser :

Coordonnées[33] ☐

Préciser :

Images[34] ☐

Préciser :

[30] Nom, prénoms
[31] Pseudo, numéro, NIR, immatriculation, etc.
[32] Marié, pacsé, célibataire, filiation, etc.
[33] Tel, adresse postale et électronique, etc.
[34] Image d'une personne concernées (ex : vidéo-surveillance, trombinoscope, annuaire, organigramme).

Vie personnelle[35] ☐

Préciser :

Vie professionnelle[36] ☐

Préciser :

Informations d'ordre économique et financier[37] ☐

Préciser :

Données de connexion[38] ☐

Préciser :

Données de localisation[39] ☐

Préciser :

Autres ☐

- Si autres, préciser :

[35] Habitudes de vie, enfants à charge, etc.
[36] CV, scolarité, formation professionnelle, distinctions, adresse email professionnelle, etc.
[37] Revenu, situation financière, situation fiscale, RIB, coordonnées bancaires, etc.
[38] Adresse IP, logs, etc.
[39] Déplacements, données GPS, GSM, etc.

## 8. COLLECTE DE DONNÉES SENSIBLES

Rappel – La notion de données sensibles s'entend de « toutes données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que toutes données génétiques, toutes données biométriques aux fins d'identifier une personne physique de manière unique, et toutes données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

Il faut intégrer dans les données sensibles le numéro de carte vitale ainsi que les données relatives aux condamnations pénales et aux infractions (exemple : infraction au code de la route pour les voitures de fonction).

Les sanctions internes ne sont pas considérées comme faisant partie des infractions au sens du RGPD.

Non : ☐

Oui : ☐

- origine raciale ☐
- origine raciale ☐
- opinion politique ☐
- convictions religieuses ☐
- convictions philosophiques ☐
- appartenance syndicale ☐
- données génériques ☐
- données biométriques aux fins d'identification d'une personne de manière unique ☐
- données concernant la santé ☐
- données concernant la vie sexuelle ☐
- données concernant les préférences sexuelles ☐

## 9. LICÉITÉ DE LA COLLECTE DES DONNÉES

Rappel – La licéité du traitement signifie que le responsable de traitement traite les données de manière licite, loyale et transparente.

Pour cela, le traitement doit être effectué en se fondant sur l'un des fondements suivants.

Consentement de la personne ☐

Exécution d'un contrat[40] ☐

Respect d'une obligation légale[41] ☐

Sauvegarde des intérêts vitaux de la personne[42] ☐

Réponse à une mission d'intérêt public[42] ☐

Intérêt légitime du responsable de traitement[43] ☐

Collecte indirecte[44] ☐

- Préciser :

[40] Données nécessaires pour assurer la bonne exécution du contrat

[41] Données fiscales pour l'administration fiscale, données de connexion dans le cadre de la lutte contre le terrorisme, etc. [42] Données traitées par un établissement hospitalier, maison de retraite, etc.

[42] Données scolaires, prestations sociales, etc.

[43] Intérêt légitime du responsable de traitement (ex : gestion du personnel pour les données RH)

[44] Données non-collectées directement par le responsable de traitement auprès des personnes concernées

## 10. DURÉE DE CONSERVATION DES DONNÉES

Rappel – La notion de données durée s'entend par le fait que « les données sont conservées par le responsable de traitement sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

| Catégorie de données concernées | Durée de conservation | Justification |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## 11. SOUS-TRAITANCE

Rappel – La notion de de sous-traitance « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

Attention, il ne s'agit pas de sous-traitance au sens technique du terme mais au sens du RGPD.

☐ Non, le traitement ne fait pas l'objet d'une sous-traitance

☐ Oui, le traitement fait l'objet d'une sous-traitance dans les conditions suivantes :

| | |
|---|---|
| Nom et coordonnées du sous-traitant | |
| Type(s) d'intervention(s) | |
| Existe-t-il un contrat ?[45] | Oui ☐<br>Non ☐<br>- Si non, justifier : |
| Existe-t-il des flux de données hors de l'Union européenne[46] ? | Oui ☐<br>Non ☐<br>- Si oui, vers quels pays ? Détailler : |
| Le sous-traitant a-t-il désigné un DPO ? | Oui ☐<br>Non ☐ |

[45] Le contrat est obligatoire mais il importe de savoir en l'occurrence si, en pratique, vous avez effectivement conclu un contrat de sous-traitance au sens du RGPD

[46] Les flux en dehors de l'UE doivent être clairement identifiés

| | |
|---|---|
| Le sous-traitant dispose-t-il d'un registre des traitements sous-traitant ? | Oui ☐<br><br>Non ☐ |

## 12. DESTINATAIRES DES DONNÉES

Rappel – les destinataires des données s'entendent de toute « personne physique ou morale, l'autorité publique, service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. »

Exemple de destinataires : une filiale, un établissement partenaire, un sous-traitant, etc.

| | |
|---|---|
| Destinataires internes | |
| Destinataires externes | |

## 13. SÉCURITÉ

L'article 34 de la loi du 6 janvier 1978 dispose que « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

L'article 32 du RGPD renforce cette obligation en imposant que « le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».

| | |
|---|---|
| Mesures organisationnelles de protection | PSSI ☐<br>PRA ☐<br>PCA ☐<br>Audit de sécurité ☐<br>Politique de minimisation ☐<br>Politique d'habilitation ☐<br>Politique Rebut ☐<br>Sensibilisation ☐ |

| | |
|---|---|
| Mesures techniques de protection | Identification ☐<br><br>Pseudonymisation ☐<br><br>Chiffrement ☐<br><br>Traçabilité ☐ |

Un audit de vulnérabilité a-t-il été réalisé ?

Oui ☐
- Préciser :

Non ☐

Un test intrusif a-t-il été réalisé ?

Oui ☐
- Préciser :

Non ☐

Disposez-vous d'une certification en matière de sécurité ?

Oui ☐
- Préciser :

Non ☐

## 14. ANALYSE D'IMPACT

Rappel - L'article 35 du RGPD considère que « *lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel* ».

Ainsi, la Cnil considère que les traitements qui remplissent au moins **deux des critères suivants** doivent faire l'objet d'une analyse d'impact.

| | |
|---|---|
| Évaluation / scoring (y compris le profilage) | ☐ |
| Décision automatique avec effet légal ou similaire | ☐ |
| Surveillance systématique | ☐ |
| Collecte de données sensibles | ☐ |
| Collecte de données personnelles à large échelle | ☐ |
| Croisement de données | ☐ |
| Personnes vulnérables (patients, personnes âgées, enfants, etc.) | ☐ |
| Usage innovant (utilisation d'une nouvelle technologie) | ☐ |
| Exclusion du bénéfice d'un droit/contrat | ☐ |

## 15. PORTABILITÉ

Rappel - L'article 20 du RGPD instaure le droit à la portabilité des personnes concernées par le traitement de leurs données à caractère personnel.

Trois règles **cumulatives** sont fixées afin de permettre à la personne concernée l'exercice de ce droit.

Données fournies par la personne concernée elle-même ☐

Le traitement est fondé soit sur la base du consentement (article 6.1.a) ou article 9.2.a)), soit sur un contrat (article 6.1.b)). ☐

Le traitement est automatisé ☐

## 16. INFORMATIONS COMPLÉMENTAIRES

### 16.1. ZONE COMMENTAIRE

Existe-t-il une « zone commentaire » ou un « champ libre »[47] :

Non : ☐

Oui : ☐

### 16.2. MENTIONS D'INFORMATIONS

Existe-t-il des mentions d'information telles que :

Mentions formulaire ☐

Note de service ☐

Affichage ☐

Notice d'informations ☐

Déclaration ☐

### 16.3. MINEURS

Le traitement porte-t-il sur des données de personnes de moins de 16 ans ?

Exclusivement ☐

En partie ☐

Jamais ☐

[47] Une zone de commentaire ou de champs libre permet à l'utilisateur de soumettre des observations sur la personne concernée. Ces zones ou champs peuvent faire l'objet d'un commentaire subjectif comme : « candidat ennuyeux, bavard, sérieux, agaçant, etc. ».

# ANNEXE N°3 – MODÈLE DE POLITIQUE RGPD À DESTINATION DES ÉTUDIANTS ET CANDIDATS

## 1. PRÉAMBULE

Le Règlement (EU) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personne et à la libre circulation de ces données, autrement appelé le Règlement général sur la protection des données (ci-après RGPD) fixe le cadre juridique applicable aux traitements de données à caractère personnel.

Le RGPD renforce les droits et les obligations des responsables de traitements, des sous-traitants, des personnes concernées et des destinataires des données.

Pour une bonne compréhension de la présente politique il est précisé que :

- le « responsable du traitement » s'entend de la personne physique ou morale, qui détermine les finalités et les moyens d'un traitement de données à caractère personnel. Au titre de la présente politique, le responsable du traitement est [nom de l'établissement ESR] ;

- le « sous-traitant » s'entend de toute personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable du traitement. Il s'agit donc en pratique des prestataires avec lesquels [nom de l'établissement ESR] travaille et qui interviennent sur les données à caractère personnel de [nom de l'établissement ESR] ;

- les « personnes concernées » sont les personnes qui peuvent être identifiées, directement ou indirectement et leurs données à caractère personnel font l'objet d'une collecte par le responsable du traitement, c'est-à-dire l'ensemble des apprenants de [nom de l'établissement ESR] ;

- les « destinataires » des données s'entendent des personnes physiques ou morales qui reçoivent communication des données à caractère personnel. Les destinataires des données peuvent donc être aussi bien des salariés de [nom de l'établissement ESR] que des organismes extérieurs (établissements, organismes sociaux, Crous, etc.).

Le RGPD, en son article 12, impose que les personnes concernées soient informées de leurs droits de manière concise, transparente, compréhensible et aisément accessible.

## 2. OBJET

Pour satisfaire à son bon fonctionnement, [nom de l'établissement ESR] est tenu de mettre en œuvre et d'exploiter des traitements de données à caractère personnel relatifs à ses étudiants et aux candidats qui postulent auprès de ce dernier.

La présente politique a pour objet de satisfaire à l'obligation d'information de [nom de l'établissement ESR] et ainsi de formaliser les droits et les obligations des étudiants et candidats au regard du traitement de leurs données à caractère personnel.

## 3. PORTÉE

La présente politique de protection des données à caractère personnel a vocation à s'appliquer dans le cadre de la mise en place des différents traitements des données à caractère personnel des étudiants de [nom de l'établissement ESR] et des candidats auprès de cette dernière.

La présente politique ne porte que sur les traitements dont [nom de l'établissement ESR] est responsable du traitement et ne vise donc pas les traitements qui ne seraient pas créés ou exploités par [nom de l'établissement ESR] elle-même (traitement dit « sauvages »).

Le traitement de données à caractère personnel peut être géré directement par [nom de l'établissement ESR] ou par le biais d'un sous-traitant spécifiquement désigné par [nom de l'établissement ESR].

Cette politique est indépendante de tout autre document pouvant s'appliquer au sein de [nom de l'établissement ESR], notamment les chartes des systèmes d'information, charte des étudiants ou les chartes administrateur par exemple.

## 4. INFORMATIONS GÉNÉRALES

Responsable des traitements :

[nom de l'établissement ESR]

[adresse de l'établissement ESR]

## 5. OPPOSABILITÉ

Le présent document est opposable :

- à [nom de l'établissement ESR] en sa qualité de « responsable du traitement » au sens du RGPD ;
- aux étudiants de [nom de l'établissement ESR] c'est-à-dire à toute personne auprès de [nom de l'établissement ESR] en cette qualité ;
- aux candidats auprès de [nom de l'établissement ESR] via la plateforme Parcoursup ou par d'autres intermédiaires ;
- aux personnes à qui [nom de l'établissement ESR] communique ces données (ci-après « destinataire des données ») ;
- aux prestataires de [nom de l'établissement ESR] qui traitent des données pour son compte (ci-après les « sous-traitants »).

## 6. PRINCIPES GÉNÉRAUX

Aucun traitement n'est mis en œuvre par [nom de l'établissement ESR] concernant des données à caractère personnel des étudiants et candidats s'il n'a pas été préalablement approuvé par la Direction de l'Université et s'il ne répond pas aux principes généraux du RGPD.

Tout nouveau traitement, modification ou suppression d'un traitement existant sera porté à la connaissance des étudiants.

Une liste des traitements de données à caractère personnel existants est jointe en annexe de la présente.

## 7. FINALITÉS ET BASE LÉGALES

Selon les cas, [nom de l'établissement ESR] traite notamment les données des salariés et agents publics pour les finalités suivantes :

- établir des documents officiels relatifs au parcours de l'étudiant (diplômes, rendez-vous officiels obligatoires, carte apprenante et tout autre document officiel) ;
- organiser le programme éducatif annuel et les sessions d'examen des étudiants ;
- garantir l'identification certaine de l'étudiant dans la gestion de son dossier et permettre l'établissement des documents officiels le concernant (diplômes, certificats, attestations...) ;
- assurer [nom de l'établissement ESR] de pouvoir contacter l'étudiant avec certitude dans le cadre de ses relations avec l'Université ;
- mettre à la disposition des étudiants des contenus éducatifs et pédagogiques, des informations administratives relatives à la vie scolaire, aux enseignements et au fonctionnement de l'établissement ainsi que de la documentation en ligne via un ENT ;
- analyser les usages faits de l'ENT afin de développer de nouveaux outils pédagogiques sur support numérique ;
- permettre à l'étudiant de créer un compte utilisateur en vue d'accéder à la plateforme pédagogique via l'ENT et/ou l'intranet de [nom de l'établissement ESR] ;
- permettre la sauvegardes de documents et travaux universitaires via l'ENT et/ou l'intranet;
- permettre la consultation du dossier pédagogique de l'étudiant (agenda, note, résultats examens, contacts professeurs) ;
- proposer des offres d'emploi ou débouchés professionnels en rapport avec les parcours des étudiants ;
- administrer un réseau des anciens permettant aux étudiants actuels de bénéficier des avantages octroyés par la communication avec d'anciens étudiants ;
- assister l'étudiant dans la procédure d'octroi d'une bourse d'étude et suivre son dossier ;
- fournir à l'étudiant une carte étudiant multiservices lui permettant d'accéder à plusieurs des services mis en œuvre par [nom de l'établissement ESR] ou ses partenaires ;
- sélectionner les candidats auprès de [nom de l'établissement ESR] par l'intermédiaire de Parcoursup ou de tout autre moyen de candidature à la disposition du candidat ;
- contrôler l'accès des étudiants aux locaux de [nom de l'établissement ESR] par l'intermédiaire de badges d'accès ;
- vidéosurveillance des abords de l'établissement afin de lutter contre les dégradations à l'extérieur de l'établissement ou à toutes tentatives d'intrusion dans ce dernier par des personnes non autorisées ;
- vidéosurveillance de certaines zones au sein de l'établissement à des fins de sécurité des étudiants et des biens et afin d'identifier les auteurs de vols, dégradations ou agressions éventuels ;
- réalisation d'états statistiques ;
- (Liste à compléter le cas échéant).

L'étudiant est informé que la collecte de ses données à caractère personnel est nécessaire à l'exécution d'une mission de service public ou d'une obligation légale de [nom de l'établissement ESR].

## 8. DESTINATAIRES DES DONNÉES – HABILITATION & TRAÇABILITÉ

[nom de l'établissement ESR] s'assure que les données ne soient accessibles qu'à des destinataires internes ou externes autorisés.

Les destinataires des données à caractère personnel des apprenants au sein de l'université sont soumis à une obligation de confidentialité spécifique.

[nom de l'établissement ESR] décide quel destinataire pourra avoir accès à quelle donnée selon une politique d'habilitation définie.

[nom de l'établissement ESR] n'est en aucun cas responsable des dommages de toute nature qui peuvent résulter d'un accès illicites aux données à caractère personnel.

Pourront notamment être destinataires de ces données à caractère personnel :

- les universités et écoles partenaires de [nom de l'établissement ESR];
- les éditeurs de contenus ou de services pédagogiques liés à [nom de l'établissement ESR] ou accessible via les ENT;
- les associations étudiantes internes à [nom de l'établissement ESR];
- les autorités de tutelles ;
- les organismes liés à la vie étudiante tels que le Cnous, le Crous, LMDE, SMERRA, - les partenaires [nom de l'établissement ESR] tels que [développer].

Par ailleurs, les données à caractère personnel pourront être communiquées à toute autorité légalement habilitée à en connaître. Dans ce cas, [nom de l'établissement ESR] n'est pas responsable des conditions dans lesquelles les personnels de ces autorités ont accès et exploitent les données.

## 9. DURÉE DE CONSERVATION [48]

La durée de conservation des données est définie par [nom de l'établissement ESR] au regard des contraintes légales et contractuelles qui pèsent sur elle et à défaut en fonction de ses besoins.

| Traitement concerné | Durée de conservation des données collectées |
|---|---|
| **Candidature et recrutement** | Destruction immédiate si le candidat n'est pas retenu ni pour le poste à pourvoir ni dans le cadre d'un futur recrutement.<br><br>Possibilité de conserver le CV pendant 2 ans après le dernier contact avec le candidat. |

[48] Possible de renvoyer à la politique de conservation des données selon le degré d'exhaustivité de celle-ci.

| | |
|---|---|
| **Gestion du dossier universitaire de l'étudiant** | Durée de l'inscription à [nom de l'établissement ESR] augmentée d'une période de deux ans.<br><br>Droits d'inscription : 10 ans, soit le délai de prescription des dettes éventuelles. |
| **Mise en œuvre d'un ENT** | Les données sont conservées jusqu'à ce que l'intéressée demande leur suppression, dans la mesure où l'étudiant a vocation à conserver son compte ENT à l'issue de sa formation.<br><br>Une demande explicite d'accord à la conservation de ses données devra être adressée une fois par an à chaque personne concernée qui n'est plus inscrite dans un établissement d'enseignement supérieur.<br><br>Les contributions personnelles laissées dans les espaces communautaires et espaces de stockage d'informations personnelles ou de publication ne peuvent, sauf opposition du contributeur lors de la fermeture de son compte ENT, être conservées par l'établissement qu'à des fins informatives. |
| **vidéosurveillance** | données conservées 1 mois. |

Passé les délais fixés, les données sont soient supprimées, soit conservées après avoir été anonymisées, notamment pour des raisons d'usages statistiques.

Il est rappelé aux apprenants que la suppression ou l'anonymisation sont des opérations irréversibles et que [nom de l'établissement ESR] n'est plus, par la suite, en mesure de les restaurer.

## 10. DROIT DE CONFIRMATION ET DROIT D'ACCÈS

L'étudiant ou le candidat dispose d'un droit de demander à [nom de l'établissement ESR] la confirmation que des données le concernant sont ou non traitées.

L'étudiant ou le candidat dispose également d'un droit d'accès, ce dernier étant conditionnée au respect des règles suivantes :

- la demande émane de la personne elle-même et est accompagnée d'une copie d'un titre d'identité ;
- être formulée par écrit à l'adresse suivante : [à compléter].

L'étudiant ou le candidat a le droit de demander une copie de ses données à caractère personnel faisant l'objet du traitement auprès de [nom de l'établissement ESR]. Toutefois, en cas de demande de copie supplémentaire, [nom de l'établissement ESR] pourra exiger la prise en charge financière de ce coût par l'étudiant ou le candidat.

Si l'étudiant ou le candidat présente sa demande de copie des données par voie électronique, les informations demandées lui seront fournies sous une forme électronique d'usage courant, sauf demande contraire.

L'étudiant ou le candidat est enfin informé que ce droit d'accès ne peut porter sur des informations ou données confidentielles ou encore pour lesquelles la loi n'autorise pas la communication.

Le droit d'accès ne doit pas être exercé de manière abusive c'est-à-dire réalisé de manière régulière dans le seul but de déstabiliser le service concerné.

## 11. MISE À JOUR – ACTUALISATION ET RECTIFICATION

Afin de permettre une mise à jour régulière des données à caractère personnel collectées par [nom de l'établissement ESR], celle-ci pourra solliciter l'apprenant qui aura pour obligation de satisfaire aux demandes de l'Université.

En cas de modification des informations de L'étudiant ou le candidat par [nom de l'établissement ESR], ce dernier en sera spontanément informé.

L'étudiant ou le candidat dispose également d'un droit à la rectification de ses données.

Pour ce faire, [nom de l'établissement ESR]:

- met à disposition des étudiants et candidats tous les moyens nécessaires en ligne ou hors ligne pour que ces derniers leur fassent part de toute modifications sur les données à caractère personnel détenues par [nom de l'établissement ESR]; les rectifications interviennent, sauf cas exceptionnel motivé, dans un délai qui ne saurait être supérieur à 8 jours ; - met à jour ses bases de données au début de chaque année universitaire.

L'étudiant ou candidat est informé que [nom de l'établissement ESR] ne procèdera à aucune modification dite de « confort », seules des modifications substantielles sur l'état civil, l'identité et les coordonnées de l'apprenant seront réalisées.

Dans la mesure du possible, [nom de l'établissement ESR] répercute ces rectifications auprès des personnes auxquelles il a transmis les données des apprenants. Cette obligation ne saurait toutefois s'imposer lorsqu'une telle démarche s'avère impossible ou exige des efforts disproportionnés.

## 12. DROIT À L'EFFACEMENT

Le droit à l'effacement de l'étudiant ou candidat ne sera pas applicable dans les cas où le traitement est mis en œuvre pour répondre une obligation légale.

En dehors de cette situation, l'étudiant ou candidat pourra demander l'effacement de ses données dans les cas limitatifs suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

- lorsque l'étudiant ou candidat retire le consentement sur lequel est fondé le traitement et qu'il n'existe pas d'autre fondement juridique au traitement ;
- l'étudiant ou candidat s'oppose à un traitement fondé sur l'exécution d'une mission d'intérêt public ou nécessaire aux fins des intérêts légitimes poursuivis par [nom de l'établissement ESR] et qu'il n'existe pas de motif légitime impérieux pour le traitement ;
- l'étudiant ou candidat s'oppose à un traitement de ses données à caractère personnel à des fins de prospection, y compris au profilage ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel [nom de l'établissement ESR] est soumise.

Conformément à la législation sur la protection des données à caractère personnel, l'étudiant ou candidat est informé qu'il s'agit d'un droit individuel qui ne peut être exercé que par la personne concernée relativement à ses propres informations : pour des raisons de sécurité, le service concerné devra donc vérifier son identité afin d'éviter toute communication d'informations confidentielles vous concernant à personne autre que celle-ci.

## 13. DROIT À LA LIMITATION

L'étudiant est informé qu'il ne dispose pas du droit à la limitation du traitement de ses données à caractère personnel dans la mesure où les traitements opérés par [nom de l'établissement ESR] sont licites et que toutes les données à caractère personnel collectées sont nécessaires à l'exécution de la relation entre [nom de l'établissement ESR] et les étudiants.

## 14. DROIT À LA PORTABILITÉ

Avant son départ de [nom de l'établissement ESR], l'étudiant pourra, sur demande, exercer son droit à la portabilité sur les seules données qu'il a lui-même communiqué à [nom de l'établissement ESR]. Ces données lui seront communiquées dans un format structuré, couramment utilisé et lisible par une machine.

## 15. DÉCISION INDIVIDUELLE AUTOMATISÉE

Si l'ÉTABLISSEMENTS ESR met en œuvre une DIE dans le cadre de la sélection des candidats via le dispositif Parcoursup, il convient de détailler ce dernier ici et de préciser s'il est ou non associé à une intervention humaine, étant précisé que le recours à une DIE est autorisé dans une telle hypothèse].

## 16. DROIT POST MORTEM

Les étudiants et candidats sont informés qu'ils disposent du droit de formuler des directives concernant la conservation, l'effacement et la communication de leurs données post-mortem. La communication de directives spécifiques post-mortem et l'exercice de leurs droits s'effectuent par courrier électronique à l'adresse [adresse e-mail] ou par courrier postal à l'adresse suivante [adresse de l'établissement], accompagné d'une copie d'un titre d'identité signé.

## 17. CARACTÈRE FACULTATIF OU OBLIGATOIRE DES RÉPONSES

L'étudiant est informé sur chaque formulaire de collecte des données à caractère personnel du caractère obligatoire ou facultatif des réponses par la présence d'un astérisque.

Dans le cas où des réponses sont obligatoires, [nom de l'établissement ESR] explique à l'étudiant les conséquences d'une absence de réponse.

## 18. DONNÉES ISSUES DES RÉSEAUX SOCIAUX

[nom de l'établissement ESR] s'interdit d'exploiter, sans l'accord préalable de l'étudiant ou du candidat, les données et les informations d'ordre privée, même si elles sont rendues publiques et diffusées par ce dernier sur les réseaux sociaux.

## 19. SOUS-TRAITANCE

[nom de l'établissement ESR] informe l'étudiant qu'elle pourra faire intervenir tout sous-traitant de son choix dans le cadre du traitement de ses données à caractère personnel.

Dans ce cas, [nom de l'établissement ESR] s'assure du respect par le sous-traitant de ses obligations en vertu du RGPD.

[nom de l'établissement ESR] s'engage à signer avec tous ses sous-traitants un contrat écrit et impose aux soustraitants les mêmes obligations en matière de protection des données qu'elle-même. De plus, [nom de l'établissement ESR] se réserve le droit de procéder à un audit auprès de ses sous-traitants afin de s'assurer du respect des dispositions du RGPD.

## 20. 20. ORIGINE DES DONNÉES COLLECTÉES

Les données collectées par [nom de l'établissement ESR] sont soit collectées directement par elle, soit collectées de manière indirecte.

### 20.1. DONNÉES COLLECTÉES DIRECTEMENT AUPRÈS DE L'APPRENANT

La collecte directe des données prend différentes formes :

- données collectées lors de l'inscription ou la réinscription administrative de l'étudiant auprès de [nom de l'établissement ESR] ;
- données collectées dans la préinscription ou l'inscription d'un candidat auprès de [nom de l'établissement ESR] ;
- données collectées par envoi ou remise d'une donnée personnelle par l'étudiant ou le candidat (courriel, lettre, carte de visites, etc.) ;
- données techniques (données de connexion ou de trafic) liées à l'usage des services informatique ou numérique de [nom de l'établissement ESR] [A développer si nécessaire].

### 20.2. DONNÉES COLLECTÉES DE MANIÈRE INDIRECTE

La collecte indirecte des données prend différentes formes :

- données collectées par le Cnous afin de payer les services de restauration du Crous de manière dématérialisée ;

- données collectées par les administrations et rectorat ;
- données collectées via d'autres universités ou écoles tierces à [nom de l'établissement ESR] ;
- données collectées via la plateforme Parcoursup dans l'hypothèse des candidatures auprès de [nom de l'établissement ESR] [A développer si nécessaire].

## 21. SÉCURITÉ

Il appartient à [nom de l'établissement ESR] de définir et de mettre en œuvre les mesures techniques de sécurité, physique ou logique, qu'elle estime appropriées pour lutter contre la destruction, la perte, l'altération ou la divulgation non autorisée des données de manière accidentelle ou illicite.

Pour ce faire, [nom de l'établissement ESR] peut se faire assister de tout tiers de son choix pour procéder, aux fréquences qu'elle estimera nécessaire, à des audits de vulnérabilité ou des tests d'intrusion.

Sauf cas d'urgence ou risque imminent, les services concernés seront informés préalablement à la réalisation de ces audits et seront tenus de prendre les mesures de protection adaptées qui leur seront notifiées au préalable.

En tout état de cause, [nom de l'établissement ESR] s'engage, en cas de changement des moyens visant à assurer la sécurité et la confidentialité des données à caractère personnel, à les remplacer par des moyens d'une performance supérieure. Aucune évolution ne pourra conduire à une régression du niveau de sécurité.

En cas de sous-traitance d'une partie ou de la totalité d'un traitement de données à caractère personnel, [nom de l'établissement ESR] s'engage à imposer contractuellement à ses sous-traitants des garanties de sécurité par le biais de mesures techniques de protection de ces données et les moyens humains appropriés.

## 22. VIOLATION DE DONNÉES

En cas de violation de données à caractère personnel, [nom de l'établissement ESR] s'engage à en notifier à la Cnil dans les conditions prescrites par le RGPD.

Si ladite violation fait porter un risque élevé pour les apprenants et que les données n'ont pas été protégées, [nom de l'établissement ESR] :

- en avisera les apprenants concernés ;
- communiquera aux apprenants concernés les informations et recommandations nécessaires.

## 23. DÉLÈGUE A LA PROTECTION DES DONNÉES

[nom de l'établissement ESR] a désigné un délégué à la protection des données.

Les coordonnées du délégué à la protection des données sont les suivantes : [A compléter].

En cas de mise en œuvre d'un nouveau de traitement de données à caractère personnel, [nom de l'établissement ESR] saisira préalablement le délégué à la protection des données.

Si l'étudiant ou candidat souhaite obtenir une information particulière ou souhaite poser une question particulière, il lui sera possible saisir le délégué à la protection des données qui lui donnera une réponse dans un délai raisonnable au regard de la question posée ou de l'information requise.

En cas de problème rencontré avec le traitement des données à caractère personnel, l'étudiant ou candidat pourra saisir le délégué à la protection des données désigné.

## 24. FLUX TRANSFRONTIÈRES

[nom de l'établissement ESR] se réserve seule le choix d'avoir ou non des flux transfrontières pour les données à caractère personnel qu'elle collecte et qu'elle traite.

En cas de transfert de données à caractère personnel vers un pays tiers à l'Union Européenne ou vers une organisation internationale, [nom de l'établissement ESR] en informera l'étudiant et s'assurera du bon respect de ses droits de ces mêmes personnes.

[nom de l'établissement ESR] s'engage si nécessaire à signer un ou plusieurs contrats permettant d'encadrer les flux transfrontières de données.

Les dispositions relatives aux flux transfrontières sont opposables à [nom de l'établissement ESR], sauf dans les cas dérogatoires prévus à l'article 49 du RGPD.

## 25. REGISTRE DES TRAITEMENTS

[nom de l'établissement ESR], en tant que responsable du traitement, s'engage à tenir à jour un registre de toutes les activités de traitement effectuées.

Ce registre est un document ou applicatif permettant de recenser l'ensemble des traitements mis en œuvre par [nom de l'établissement ESR] en tant que responsable du traitement.

[nom de l'établissement ESR] s'engage à fournir à l'autorité de contrôle, à première demande, les renseignements permettant à ladite autorité de vérifier la conformité des traitements à la règlementation informatique et libertés en vigueur.

## 26. DROIT D'INTRODUIRE UNE RÉCLAMATION AUPRÈS DE LA CNIL

L'étudiant ou candidat concerné par le traitement de ses données à caractère personnel est informé de son droit d'introduire une plainte auprès d'une autorité de contrôle, à savoir la Cnil, si celui-ci estime que le traitement de données à caractère personnel le concernant n'est pas conforme à la règlementation européenne de protection des données, à l'adresse suivante :

**Cnil** – Service des plaintes

3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07

Tél : 01 53 73 22 22

## 27. ÉVOLUTION

La présente politique peut être modifiée ou aménagée à tout moment en cas d'évolution légale, jurisprudentielle, des décisions et recommandations de la Cnil ou des usages.

Toute nouvelle version de la présente politique sera portée à la connaissance des étudiants et candidats par tout moyen défini par [nom de l'établissement ESR], en ce compris la voie électronique (diffusion par courrier électronique ou en ligne par exemple).

## 28. POUR PLUS D'INFORMATIONS

Pour toutes informations complémentaires, vous pouvez contacter les services suivants : [adresse email]

Pour toute autre information plus générale sur la protection des données personnelles, vous pouvez

# ANNEXE N°4 – MODÈLE DE POLITIQUE RGPD À DESTINATION DES SALARIÉS ET AGENTS PUBLICS

## 1. PRÉAMBULE

Le Règlement (EU) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personne et à la libre circulation de ces données, autrement appelé le Règlement général sur la protection des données (ci-après RGPD) fixe le cadre juridique applicable aux traitements de données à caractère personnel.

Le RGPD renforce les droits et les obligations des responsables de traitements, des sous-traitants, des personnes concernées et des destinataires des données.

Pour une bonne compréhension de la présente politique il est précisé que :

- le « responsable du traitement » s'entend de la personne physique ou morale, qui détermine les finalités et les moyens d'un traitement de données à caractère personnel. Au titre de la présente politique, le responsable du traitement est [ ] (ci-après désigné par « l'entreprise ») ;

- le « sous-traitant » s'entend de toute personne physique ou morale, qui traite des données à caractère personnel pour le compte du responsable du traitement. Il s'agit donc en pratique des prestataires avec lesquels l'entreprise travaille et qui interviennent sur les données à caractère personnel de l'entreprise ;

- les « personnes concernées » sont les personnes qui peuvent être identifiées, directement ou indirectement et leurs données à caractère personnel font l'objet d'une collecte par le responsable du traitement, c'est-à-dire l'ensemble des salariés de l'entreprise ;

- les « destinataires » des données s'entendent des personnes physiques ou morales qui reçoivent communication des données à caractère personnel. Les destinataires des données peuvent donc être aussi bien des salariés de l'entreprise que des organismes extérieurs (URSSAF, Mutuelle d'entreprise, établissement bancaire, centre des impôts, etc.).

Le RGPD, en son article 12, impose que les personnes concernées soient informées de leurs droits de manière concise, transparente, compréhensible et aisément accessible.

Par ailleurs l'article L. 1222-4 du Code du travail prescrit que « *aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ».

## 2. DÉFINITIONS

- « donnée à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou

plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

- « données enrichies » : les données à caractère personnel enrichies s'opposent à la notion de données à caractère personnel « brutes » fournies par la personne concernée. Il s'agit des données qui sont générées par le responsable du traitement, telles qu'un profil d'utilisateur créé par l'analyse des données brutes collectées à partir d'un compteur intelligent. Il peut également s'agir de données déduites et/ou dérivées créées par le responsable du traitement sur la base des données «fournies par la personne concernée».

- « traitement de données à caractère personnel » : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

- « violation de données à caractère personnel » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

## 3. OBJET

Pour satisfaire à son bon fonctionnement, [nom de l'établissement ESR] est tenue de mettre en œuvre et d'exploiter des traitements de données à caractère personnel relatifs aux salariés et agents publics qu'elle emploie.

La présente politique a pour objet de satisfaire à l'obligation d'information de [nom de l'établissement ESR] et ainsi de formaliser les droits et les obligations de ses salariés et agents publics au regard du traitement de leurs données à caractère personnel.

## 4. PORTÉE

La présente politique de protection des données à caractère personnel a vocation à s'appliquer dans le cadre de la mise en place du traitement des données à caractère personnel des salariés et agents publics de [nom de l'établissement ESR], quel que soit leur statut (CDI, CDD, autres formes de contrat, etc.). Le cas échéant, la présente politique s'applique également aux stagiaires intervenant au sein de [nom de l'établissement ESR].

La présente politique ne porte que sur les traitements dont [nom de l'établissement ESR] est responsable du traitement et ne vise donc pas les traitements qui ne seraient pas créés ou exploités par [nom de l'établissement ESR] elle-même (traitement dit « sauvages »).

Le traitement de données à caractère personnel peut être géré directement par [nom de l'établissement ESR] ou par le biais d'un sous-traitant spécifiquement désigné par [nom de l'établissement ESR].

Cette politique est indépendante de tout autre document pouvant s'appliquer au sein de [nom de l'établissement ESR], notamment les chartes des systèmes d'information, les chartes administrateur ou encore les chartes liées à la déconnexion ou au télétravail.

## 5. PRINCIPES GÉNÉRAUX

Aucun traitement n'est mis en œuvre dans [nom de l'établissement ESR] concernant des données de salariées s'il n'a pas été préalablement approuvé par la Direction générale et s'il ne répond pas aux principes généraux du RGPD.

Tout nouveau traitement, modification ou suppression d'un traitement existant sera porté à la connaissance des salariés et agents publics par tous moyens à la convenance de [nom de l'établissement ESR].

Une liste des traitements de données à caractère personnel existants est jointe en annexe de la présente.

## 6. FINALITÉS ET BASE LÉGALES

Selon les cas, [nom de l'établissement ESR] traite notamment les données des salariés et agents publics pour les finalités suivantes :

- gestion et suivi des candidatures ;
- évaluation de la capacité du candidat à occuper l'emploi proposé ;
- convocations à des entretiens ;
- embauches de stagiaires rémunérés ;
- gestion des fiches de renseignement des salariés ou agents publics ;
- gestion du personnel ;
- gestion des carrières ;
- gestion des congés ;
- évaluation du personnel ;
- gestion des accidents du travail et maladie professionnelle et suivi des visites médicales ;
- gestion des annuaires internes, organigrammes et agendas professionnels ;
- gestion des dotations individuelles en fournitures et équipements (ex : téléphonie mobile) ;
- gestion des élections professionnelles ;
- suivi et maintenance du parc informatique ;
- gestion de la messagerie électronique professionnelle ;
- gestion des réseaux privés virtuels internes permettant la diffusion ou la collecte de données des personnels (intranet) ;
- suivi des demandes de formation et des périodes de formation effectuées ;
- gestion des accords collectifs ;
- calcul et le paiement des rémunérations et accessoires et des frais professionnels ainsi que calcul des retenues déductibles ou indemnisables opérées conformément aux dispositions légales et conventionnelles applicables ;
- gestion des indemnités de départ à la retraite et calcul des engagements de départ ;
- réalisation des opérations résultant de dispositions légales, de conventions collectives ou de stipulations contractuelles concernant :
    - les déclarations à l'administration fiscale et aux organismes de protection sociale, de retraite et de prévoyance ;

    - le calcul des cotisations et versements donnant lieu à retenue à la source ;
    - la tenue des comptes individuels relatifs à l'intéressement et à la participation des travailleurs à l'entreprise ;
    - la réalisation de tous traitements statistiques non nominatifs, liés à l'activité salariée dans l'entreprise ;
    - la fourniture des écritures de paie à la comptabilité.
- contrôle individuel de l'accès pour sécuriser l'entrée dans les bâtiments ;
- contrôle individuel de l'accès pour sécuriser les locaux faisant l'objet d'une restriction de circulation ;
- gestion des horaires et des temps de présence ;
- contrôle de l'accès au restaurant d'entreprise et gestion de la mise en place d'un système de paiement associé ;
- réalisation d'états statistiques ;
- vidéosurveillance à des fins de sécurité des biens et des salariés et afin d'identifier les auteurs de vols, dégradations ou agressions éventuels - (Liste à compléter le cas échéant).

Le salarié ou agent public est informé que la collecte de ses données à caractère personnel est nécessaire à l'exécution de son contrat ou d'une obligation légale de [nom de l'établissement ESR].

## 7. DESTINATAIRES DES DONNÉES – HABILITATION & TRAÇABILITÉ

[nom de l'établissement ESR] s'assure que les données ne soient accessibles qu'à des destinataires internes ou externes autorisés.

Les destinataires des données à caractère personnel des salariés et agents publics au sein de [nom de l'établissement ESR] sont soumis à une obligation de confidentialité spécifique.

Pourront notamment être destinataires de ces données à caractère personnel :

- Interne : service de gestion du personnel, DSI, service financier, services généraux, délégués syndicaux, IRP, contrôleurs de gestion et audit.
- Externe : cabinet de recrutement, URSSAF, organismes de formation, organismes sociaux, organismes financiers, administration.

[nom de l'établissement ESR] décide quel destinataire pourra avoir accès à quelle donnée selon une politique d'habilitation définie.

La politique d'habilitation est régulièrement mise à jour et tient compte des arrivées et des départs des salariés et agents publics de [nom de l'établissement ESR] ayant accès aux données.

[nom de l'établissement ESR] n'est en aucun cas responsable des dommages de toute nature qui peuvent résulter d'un accès illicites aux données à caractère personnel.

Si un salarié ou agent public se rend compte qu'il dispose d'un accès à des données auxquelles il ne devrait pas avoir accès, il a pour obligation de prévenir sans délais la direction des systèmes d'information ou la direction des ressources humaines.

Les salariés et agents publics sont informés que tous les accès concernant des traitements relatifs à leurs données à caractère personnel font l'objet d'une mesure de traçabilité.

Par ailleurs, les données à caractère personnel pourront être communiquées à toute autorité légalement habilitée à en connaître. Dans ce cas, [nom de l'établissement ESR] n'est pas responsable des conditions dans lesquelles les personnels de ces autorités ont accès et exploitent les données.

## 8. DURÉE DE CONSERVATION[49]

La durée de conservation des données est définie par l'entreprise au regard des contraintes légales et contractuelles qui pèsent sur elle et à défaut en fonction de ses besoins.

| Traitement concerné | Durée de conservation des données collectées |
|---|---|
| **Candidature et recrutement** | Destruction immédiate si le candidat n'est pas retenu ni pour le poste à pourvoir ni dans le cadre d'un futur recrutement.<br>Possibilité de conserver le CV pendant 2 ans après le dernier contact avec le candidat. |
| **Gestion administrative des salariés et agents publics** | Les données sont conservées par les services gestionnaires pour la période d'emploi de la personne concernée.<br><br>Elles peuvent toutefois être conservées 5 ans en archivage intermédiaire à compter du départ du salarié. |
| **Gestion de la paie** | Gestion de la paie : **5 ans** à compter du versement de la paie (article L3243-4 du Code<br>du travail) ;<br><br>Les informations relatives aux motifs des absences ne sont pas conservées au-delà du temps nécessaire à l'établissement des bulletins de paie.<br><br>Les informations nécessaires à l'établissement des droits du personnel, notamment des droits à la retraite, peuvent être conservées sans limitation de durée. |

[49] Possible de renvoyer à la politique de conservation des données selon le degré d'exhaustivité de celle-ci.

| | |
|---|---|
| **Badges sur le lieu de travail** | Éléments d'identification des salariés : **5 ans** maximum après le départ du salarié de l'entreprise.<br><br>Éléments relatifs aux déplacements des personnes : pas plus de **trois mois**.<br><br>Si finalité de contrôle du temps de travail : **5 ans**.<br><br>Données relatives aux motifs d'absence : **5 ans**, sauf dispositions législatives contraires. |
| **Vidéosurveillance** | 1 mois à compter de la captation des images |
| **Données de connexion** | 6 mois |

Passé les délais fixés, les données sont soient supprimées, soit conservées après avoir été anonymisées, notamment pour des raisons d'usages statistiques.

Il est rappelé au salarié ou agent public que la suppression ou l'anonymisation sont des opérations irréversibles et que [nom de l'établissement ESR] n'est plus, par la suite, en mesure de les restaurer.

## 9. DROIT DE CONFIRMATION ET DROIT D'ACCÈS

Le salarié ou agent public dispose d'un droit de demander à [nom de l'établissement ESR] la confirmation que des données le concernant sont ou non traitées.

Le salarié ou agent public dispose également d'un droit d'accès, ce dernier étant conditionnée au respect des règles suivantes :

- la demande émane de la personne elle-même et est accompagnée d'une copie d'un titre d'identité ;
- être formulée par écrit à l'adresse suivante : [adresse physique et adresse e-mail].

Le salarié ou agent public a le droit de demander une copie de ses données à caractère personnel faisant l'objet du traitement auprès de l'entreprise. Toutefois, en cas de demande de copie supplémentaire, [nom de l'établissement ESR] pourra exiger la prise en charge financière de ce coût par le salarié.

Si le salarié ou agent public présente sa demande de copie des données par voie électronique, les informations demandées lui seront fournies sous une forme électronique d'usage courant, sauf demande contraire.

Le salarié ou agent public est enfin informé que ce droit d'accès ne peut porter sur des informations ou données confidentielles ou encore pour lesquelles la loi n'autorise pas la communication.

Le droit d'accès ne doit pas être exercé de manière abusive c'est-à-dire réalisé de manière régulière dans le seul but de déstabiliser le service concerné.

## 10. MISE À JOUR – ACTUALISATION ET RECTIFICATION

Afin de permettre une mise à jour régulière des données à caractère personnel collectées par [nom de l'établissement ESR], celui-ci pourra solliciter le salarié ou agent public qui aura pour obligation de satisfaire aux demandes de [nom de l'établissement ESR].

En cas de modification des informations du salarié ou de l'agent public par [nom de l'établissement ESR], ce dernier en sera spontanément informé.

Le salarié ou agent public est informé que [nom de l'établissement ESR] ne procèdera à aucune modification dite de « confort », seules des modifications substantielles sur l'état civil, l'identité et les coordonnées de la personne concernée seront réalisées.

## 11. DROIT À L'EFFACEMENT

Le salarié ou agent public est informé qu'il ne dispose pas du droit à l'effacement du traitement de ses données à caractère personnel dans la mesure où les motifs énoncés à l'article 17 du RGPD sont inopérants en l'espèce.

## 12. DROIT À LA LIMITATION

Le salarié ou agent public est informé qu'il ne dispose pas du droit à la limitation du traitement de ses données à caractère personnel dans la mesure où le traitement opéré par [nom de l'établissement ESR] est licite et que toutes les données à caractère personnel collectées sont nécessaires à l'exécution du contrat de travail.

## 13. DROIT À LA PORTABILITÉ

Le salarié ou agent public est informé qu'il ne dispose pas du droit à la portabilité de ses données à caractère personnel dans la mesure où le traitement opéré par [nom de l'établissement ESR] :

- N'est pas fondé sur le consentement du salarié ou de l'agent public, mais sur l'exécution du contrat de travail ou de mission ;
- N'est pas systématiquement effectué à l'aide de procédés automatisés.

## 14. DÉCISION INDIVIDUELLE AUTOMATISÉE

[nom de l'établissement ESR] ne procède à aucune décision individuelle automatisée concernant ses salariés ou agents publics.

## 15. DROIT POST MORTEM

Les salariés ou agents publics sont informés qu'ils disposent du droit de formuler des directives concernant la conservation, l'effacement et la communication de leurs données post-mortem. La communication de directives spécifiques post-mortem et l'exercice de leurs droits s'effectuent par courrier électronique à l'adresse [adresse e-mail] ou par courrier postal à l'adresse suivante [adresse postale], accompagné d'une copie d'un titre d'identité signé.

## 16. CARACTÈRE FACULTATIF OU OBLIGATOIRE DES RÉPONSES

Le salarié ou agent public est informé sur chaque formulaire de collecte des données à caractère personnel du caractère obligatoire ou facultatif des réponses par la présence d'un astérisque.

Dans le cas où des réponses sont obligatoires, [nom de l'établissement ESR] explique au salarié les conséquences d'une absence de réponse.

## 17. DROIT D'USAGE

[nom de l'établissement ESR] se voit conférer par le salarié ou agent public un droit d'usage et de traitement de ses données à caractère personnel pour les finalités exposées en annexe.

Toutefois, les données enrichies qui sont le fruit d'un travail de traitement et d'analyse de [nom de l'établissement ESR], autrement appelées les données enrichies, demeurent la propriété exclusive de [nom de l'établissement ESR] (analyse d'usage, statistiques, etc.).

## 18. DONNÉES ISSUES DES RÉSEAUX SOCIAUX

[nom de l'ÉTABLISSEMENTS ESR] s'interdit d'exploiter, sans l'accord préalable du salarié ou agent public, les données et les informations d'ordre privée, même si elle sont rendues publiques, diffusées par le salarié ou agent public sur les réseaux sociaux.

## 19. SOUS-TRAITANCE

[nom de l'établissement ESR] informe les salariés et agents publics qu'elle pourra faire intervenir tout sous-traitant de son choix dans le cadre du traitement des données à caractère personnel du salarié.

Dans ce cas, [nom de l'établissement ESR] s'assure du respect par le sous-traitant de ses obligations en vertu du RGPD.

[nom de l'établissement ESR] s'engage à signer avec tous ses sous-traitants un contrat écrit et impose aux sous-traitants les mêmes obligations en matière de protection des données qu'elle-même. De plus, [nom de l'établissement ESR] se réserve le droit de procéder à un audit auprès de ses sous-traitants afin de s'assurer du respect des dispositions du RGPD.

## 20. SÉCURITÉ

Il appartient à [nom de l'établissement ESR] de définir et de mettre en œuvre les mesures techniques de sécurité, physique ou logique, qu'elle estime appropriées pour lutter contre la destruction, la perte, l'altération ou la divulgation non autorisée des données de manière accidentelle ou illicite.

Pour ce faire, [nom de l'établissement ESR] peut se faire assister de tout tiers de son choix pour procéder, aux fréquences qu'elle estimera nécessaires, à des audits de vulnérabilité ou des tests d'intrusion.

Sauf cas d'urgence ou risque imminent, les salariés et agents publics seront informés préalablement à la réalisation de ces audits et seront tenus de prendre les mesures de protection adaptées qui leur seront notifiées au préalable.

En tout état de cause, [nom de l'établissement ESR] s'engage, en cas de changement des moyens visant à assurer la sécurité et la confidentialité des données à caractère personnel, à les remplacer par des moyens d'une performance supérieure. Aucune évolution ne pourra conduire à une régression du niveau de sécurité.

En cas de sous-traitance d'une partie ou de la totalité d'un traitement de données à caractère personnel, [nom de l'établissement ESR] s'engage à imposer contractuellement à ses sous-traitants des garanties de sécurité par le biais de mesures techniques de protection de ces données et les moyens humains appropriés.

## 21. VIOLATION DE DONNÉES

En cas de violation de données à caractère personnel, [nom de l'établissement ESR] s'engage à en notifier à la Cnil dans les conditions prescrites par le RGPD.

Si ladite violation fait porter un risque élevé pour les salariés et agents publics et que les données n'ont pas été protégées, [nom de l'établissement ESR] :

- en avisera les salariés et agents publics concernés ;
- communiquera aux salariés et agents publics concernés les informations et recommandations nécessaires.

## 22. DÉLÈGUE A LA PROTECTION DES DONNÉES

[nom de l'établissement ESR] a désigné un délégué à la protection des données.

Les coordonnées du délégué à la protection des données sont les suivantes :

- Nom :
- Adresse e-mail :
- Tél :

En cas de nouveau de traitement de données à caractère personnel, [nom de l'établissement ESR] saisira préalablement le délégué à la protection des données.

Si le salarié ou agent public souhaite obtenir une information particulière ou souhaite poser une question particulière, il lui sera possible saisir le délégué à la protection des données qui lui donnera une réponse dans un délai raisonnable au regard de la question posée ou de l'information requise.

En cas de problème rencontré avec le traitement des données à caractère personnel, le salarié ou agent public pourra saisir le délégué à la protection des données désigné.

## 23. FLUX TRANSFRONTIÈRES

[nom de l'établissement ESR] se réserve seul le choix d'avoir ou non des flux transfrontières pour les données à caractère personnel qu'il collecte et qu'il traite.

En cas de transfert de données à caractère personnel vers un pays tiers à l'Union Européenne ou vers une organisation internationale, [nom de l'établissement ESR] en informera les salariés et agents publics et s'assurera du bon respect des droits de ces mêmes personnes.

[nom de l'établissement ESR] s'engage si nécessaire à signer un ou plusieurs contrats permettant d'encadrer les flux transfrontières de données.

Les dispositions relatives aux flux transfrontières sont opposables à [nom de l'établissement ESR], sauf dans les cas dérogatoires prévus à l'article 49 du RGPD.

## 24. REGISTRE DES TRAITEMENTS

[nom de l'établissement ESR], en tant que responsable du traitement, s'engage à tenir à jour un registre de toutes les activités de traitement effectuées.

Ce registre est un document ou applicatif permettant de recenser l'ensemble des traitements mis en œuvre par [nom de l'établissement ESR] en tant que responsable du traitement.

[nom de l'établissement ESR] s'engage à fournir à l'autorité de contrôle, à première demande, les renseignements permettant à ladite autorité de vérifier la conformité des traitements à la règlementation informatique et libertés en vigueur.

## 25. DROIT D'INTRODUIRE UNE RÉCLAMATION AUPRÈS DE LA CNIL

Les salariés et agents publics concernés par le traitement de leurs données à caractère personnel sont informés de leur droit d'introduire une plainte auprès d'une autorité de contrôle, à savoir la Cnil, si ceux-ci estiment estime que le traitement de données à caractère personnel les concernant n'est pas conforme à la règlementation européenne de protection des données, à l'adresse suivante :

**Cnil** – Service des plaintes

3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07

Tél : 01 53 73 22 22

## 26. ÉVOLUTION

La présente politique peut être modifiée ou aménagée à tout moment en cas d'évolution légale, jurisprudentielle, des décisions et recommandations de la Cnil ou des usages.

Toute nouvelle version de la présente politique sera portée à la connaissance des salariés et agents publics par tout moyen défini par [nom de l'établissement ESR], en ce compris la voie électronique (diffusion par courrier électronique ou en ligne par exemple).

## 27. POUR PLUS D'INFORMATIONS

Pour toutes informations complémentaires, vous pouvez contacter les services suivants : [adresse email]

Pour toute autre information plus générale sur la protection des données personnelles, vous pouvez consulter le site de la CNIL www.cnil.fr.

# ANNEXE N°5 – MODÈLE DE POLITIQUE RGPD À DESTINATION DES PARTENAIRES[50]

## 1. PRÉAMBULE

Le Règlement (EU) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, autrement appelé le Règlement général sur la protection des données (ci-après RGPD) fixe le cadre juridique applicable aux traitements de données à caractère personnel.

Le RGPD renforce les droits et les obligations des responsables de traitements, des sous-traitants, des personnes concernées et des destinataires des données.

Dans le cas de notre activité nous sommes amenés à traiter des données à caractère personnel.

Pour une bonne compréhension de la présente politique il est précisé que :

- le « responsable du traitement » : [nom de l'établissement ESR];
- le « sous-traitant » : désigne toute personne physique ou morale qui traite des données à caractère personnel pour le compte de [nom de l'établissement ESR];
- les « personnes concernées » : désigne les partenaires de [nom de l'établissement ESR];
- les « destinataires » : désigne les personnes physiques ou morales qui reçoivent des données à caractère personnel de la part de [nom de l'établissement ESR]. Les destinataires des données peuvent donc être aussi bien des salariés ou agents publics de [nom de l'établissement ESR] que des organismes extérieurs (partenaires, exposants, établissement bancaire, intervenants, etc.).

Le RGPD, en son article 12, impose que les personnes concernées soient informées de leurs droits de manière concise, transparente, compréhensible et aisément accessible.

## 2. OBJET

La présente politique a pour objet de satisfaire à l'obligation d'information à laquelle [nom de l'établissement ESR] est tenue en application du RGPD (article 12) et de formaliser les droits et les obligations de ses partenaires au regard du traitement de leurs données à caractère personnel.

[50] Par « partenaires », il convient d'entendre les fournisseurs et tous les autres prestataires avec lesquels l'ÉTABLISSEMENTS ESR est amené à contracter pour l'exercice de son activité

## 3. PORTÉE

La présente politique a vocation à s'appliquer dans le cadre de la mise en place de l'ensemble des traitements de données à caractère personnel relatifs aux partenaires de [nom de l'établissement ESR].

[nom de l'établissement ESR] met tout en œuvre pour que les données soient traitées dans le cadre d'une gouvernance interne précise. Ceci étant précisé, la présente politique ne porte que sur les traitements dont [nom de l'établissement ESR] est responsable du traitement et ne vise donc pas les traitements qui ne seraient pas créés ou exploités en dehors des règles de gouvernance fixées par [nom de l'établissement ESR] (traitement dit « sauvages » ou shadow IT).

Le traitement de données à caractère personnel peut être géré directement par [nom de l'établissement ESR] ou par le biais d'un sous-traitant spécifiquement désigné par [nom de l'établissement ESR].

Cette politique est indépendante de tout autre document pouvant s'appliquer au sein de la relation contractuelle entre [nom de l'établissement ESR] et les partenaires.

## 4. TYPES DE DONNÉES COLLECTÉES

| | |
|---|---|
| **Données non techniques (selon les cas d'usage)** | ▯ Identité et identification (nom, prénom, numéro référence partenaire, raison sociale, code d'identification comptable, numéro SIREN)<br>▯ Coordonnées (e-mail, adresse postale, numéro de téléphone)<br>▯ Vie personnelle / professionnelle lorsque c'est nécessaire (notamment fonction, nom société)<br>▯ Données bancaires si nécessaire (en cas de souscription à un abonnement en ligne vente en ligne) |
| **Données techniques (selon les cas d'usage)** | ▯ Données d'identification (adresse IP)<br>▯ Données de connexion (logs) |

## 5. ORIGINES DES DONNÉES

Les données relatives à nos partenaires sont généralement collectées directement auprès d'eux (collecte directe).

## 6. FINALITÉS ET BASES LÉGALES

Selon les cas, [nom de l'établissement ESR] traite vos données pour les finalités suivantes : [à compléter][51]

Ces finalités reposent sur l'exécution de la relation contractuelle et commerciale entre [nom de l'établissement ESR] et ses partenaires.

Lorsque c'est nécessaire, [nom de l'établissement ESR] recueille le consentement des personnes (ex : newsletter).

## 7. DESTINATAIRES DES DONNÉES – HABILITATION & TRAÇABILITÉ

[nom de l'établissement ESR] s'assure que les données ne soient accessibles qu'à des destinataires internes ou externes habilités.

| Destinataires internes | Destinataires externes |
|---|---|
| - le personnel habilité de [nom de l'établissement ESR], des services chargés de traiter la relation partenaire, des services administratifs et comptables, des services logistiques et informatiques ainsi que leurs responsables hiérarchiques ;<br>- le personnel habilité des services chargés du contrôle (commissaire aux comptes, services chargés des procédures internes du contrôle, etc.) ; | - les partenaires, les sociétés extérieures ou les filiales d'un même groupe de sociétés ;<br>- les organismes, les auxiliaires de justice et les officiers ministériels, dans le cadre de leur mission de recouvrement de créances ; |

Les destinataires des données à caractère personnel des partenaires au sein de [nom de l'établissement ESR] sont soumis à une obligation de confidentialité.

[nom de l'établissement ESR] décide quel destinataire pourra avoir accès à quelle donnée selon une politique d'habilitation.

[51] Exemple de finalités susceptibles de figurer dans la dite politique en fonction des traitements mis en œuvre par l'ÉTABLISSEMENTS ESR : gestion de la relation contractuelle, gestion des commandes, gestion de la facturation et de la comptabilité, gestion d'un anniaire de contact, gestion du site web de l'ÉTABLISSEMENTS ESR, gestion du parc informatique de l'ÉTABLISSEMENTS ESR, envoi de newsletter, élaboration de statistiques, etc.

[nom de l'établissement ESR] n'est en aucun cas responsable des dommages de toute nature qui peuvent résulter d'un accès illicite aux données à caractère personnel.

Tous les accès concernant des traitements relatifs à des données à caractère personnel de clients et prospects font l'objet d'une mesure de traçabilité.

Par ailleurs, les données à caractère personnel pourront être communiquées à toute autorité légalement habilitée à en connaître. Dans ce cas, [nom de l'établissement ESR] n'est pas responsable des conditions dans lesquelles les personnels de ces autorités ont accès et exploitent les données.

## 8. DURÉE DE CONSERVATION

La durée de conservation des données est définie par [nom de l'établissement ESR] au regard des contraintes légales et contractuelles qui pèsent sur elle et à défaut en fonction de ses besoins et notamment selon les principes suivants :

| Traitement | Durée de conservation |
|---|---|
| **Données relatives aux Partenaires** | Pendant la durée des relations contractuelles augmentée de 3 ans à des fins d'animation et de prospection, sans préjudice des obligations de conservation ou des délais de prescription |
| **Données relatives aux contrats** | 5 ans à compter de leur conclusion |
| **Données techniques** | 1 an à compter de leur collecte |
| **Lutte contre le blanchiment** | 5 ans |
| **Gestion de la facturation et de la comptabilité** | 10 ans |
| **Cookies** | 13 mois |
| **Newsletter** | Jusqu'à désabonnement de la personne concernée |

Passés les délais fixés, les données sont soit supprimées, soit conservées après avoir été anonymisées, notamment pour des raisons d'usages statistiques. Elles peuvent être conservées en cas de précontentieux et contentieux.

Il est rappelé aux partenaires que la suppression ou l'anonymisation sont des opérations irréversibles et que [nom de l'établissement ESR] n'est plus, par la suite, en mesure de les restaurer.

## 9. DROIT DE CONFIRMATION ET DROIT D'ACCÈS

Les partenaires disposent d'un droit de demander à [nom de l'établissement ESR] la confirmation que des données le concernant sont ou non traitées.

Les partenaires disposent également d'un droit d'accès, ce dernier étant conditionné au respect des règles suivantes :

- la demande émane de la personne elle-même et est accompagnée d'une copie d'un titre d'identité, à jour ;

- être formulée par écrit à l'adresse suivante : [adresse] ou à l'adresse e-mail [adresse e-mail]. Les partenaires ont le droit de demander une copie de leurs données à caractère personnel faisant l'objet du traitement auprès de [nom de l'établissement ESR]. Toutefois, en cas de demande de copie supplémentaire, [nom de l'établissement ESR] pourra exiger la prise en charge financière de ce coût par les partenaires.

Si les partenaires présentent leur demande de copie des données par voie électronique, les informations demandées lui seront fournies sous une forme électronique d'usage courant, sauf demande contraire.

Les partenaires sont informés que ce droit d'accès ne peut porter sur des informations ou données confidentielles ou encore pour lesquelles la loi n'autorise pas la communication.

Le droit d'accès ne doit pas être exercé de manière abusive c'est-à-dire réalisé de manière régulière dans le seul but de déstabiliser le service concerné.

## 10. MISE À JOUR – ACTUALISATION ET RECTIFICATION

[nom de l'établissement ESR] satisfait aux demandes de mise à jour :

- automatiquement pour les modifications en ligne sur des champs qui techniquement ou légalement peuvent être mis à jour ;

- sur demande écrite émanant de la personne elle-même qui doit justifier de son identité.

## 11. DROIT À L'EFFACEMENT

Le droit à l'effacement des partenaires ne sera pas applicable dans les cas où le traitement est mis en œuvre pour répondre une obligation légale.

En dehors de cette situation, les partenaires pourront demander l'effacement de leurs données dans les cas limitatifs suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

- lorsque la personne concernée retire le consentement sur lequel est fondé le traitement et qu'il n'existe pas d'autre fondement juridique au traitement ;

- la personne concernée s'oppose à un traitement nécessaire aux fins des intérêts légitimes poursuivis par [nom de l'établissement ESR] et qu'il n'existe pas de motif légitime impérieux pour le traitement ;

- la personne concernée s'oppose à un traitement de ses données à caractère personnel à des fins de prospection, y compris au profilage ;

- les données à caractère personnel ont fait l'objet d'un traitement illicite.

Conformément à la législation sur la protection des données à caractère personnel, les partenaires sont informés qu'il s'agit d'un droit individuel qui ne peut être exercé que par la personne concernée relativement à ses propres informations : pour des raisons de sécurité, le service concerné devra donc vérifier votre identité afin d'éviter toute communication d'informations confidentielles vous concernant à une autre personne que vous.

## 12. DROIT À LA LIMITATION

Les partenaires sont informés de ce que droit n'a pas vocation à s'appliquer dans la mesure où le traitement opéré par [nom de l'établissement ESR] est licite et que toutes les données à caractère personnel collectées sont nécessaires à l'exécution de ses prestations.

## 13. DROIT À LA PORTABILITÉ

[nom de l'établissement ESR] fait droit à la portabilité des données dans le cas particulier des données communiqués par les partenaires eux même, sur des services en ligne proposés par [nom de l'établissement ESR] lui-même et pour les finalités reposant sur le seul consentement des personnes. Dans ce cas les données seront communiquées dans un format structuré, couramment utilisé et lisible par une machine.

## 14. DÉCISION INDIVIDUELLE AUTOMATISÉE

[nom de l'établissement ESR] ne procède pas à des décisions individuelles automatisées.

## 15. DROIT POST MORTEM

Les partenaires sont informés qu'ils disposent du droit de formuler des directives concernant la conservation, l'effacement et la communication de leurs données post-mortem. La communication de directives spécifiques post-mortem et l'exercice de leurs droits s'effectuent par courrier électronique à l'adresse [adresse e-mail] ou par courrier postal à l'adresse suivante [adresse], accompagné d'une copie d'un titre d'identité signé.

## 16. CARACTÈRE FACULTATIF OU OBLIGATOIRE DES RÉPONSES

Les partenaires sont informés sur chaque formulaire de collecte des données à caractère personnel du caractère obligatoire ou facultatif des réponses par la présence d'un astérisque.

Dans le cas où des réponses sont obligatoires, [nom de l'établissement ESR] explique aux partenaires les conséquences d'une absence de réponse.

## 17. DROIT D'USAGE

[nom de l'établissement ESR] se voit conférer par les partenaires un droit d'usage et de traitement de leurs données à caractère personnel pour les finalités exposées ci-dessus.

Toutefois, les données enrichies qui sont le fruit d'un travail de traitement et d'analyse de [nom de l'établissement ESR], autrement appelées les données enrichies, demeurent la propriété exclusive de [nom de l'établissement ESR] (analyse d'usage, statistiques, etc.).

## 18. SOUS-TRAITANCE

[nom de l'établissement ESR] informe ses partenaires qu'elle pourra faire intervenir tout sous-traitant de son choix dans le cadre du traitement de leurs données à caractère personnel.

Dans ce cas, [nom de l'établissement ESR] s'assure du respect par le sous-traitant de ses obligations en vertu du RGPD.

[nom de l'établissement ESR] s'engage à signer avec tous ses sous-traitants un contrat écrit et impose aux soustraitants les mêmes obligations en matière de protection des données qu'elle-même. De plus, [nom de l'établissement ESR] se réserve le droit de procéder à un audit auprès de ses sous-traitants afin de s'assurer du respect des dispositions du RGPD.

## 19. SÉCURITÉ

Il appartient à [nom de l'établissement ESR] de définir et de mettre en œuvre les mesures techniques de sécurité, physiques ou logiques, qu'il estime appropriées pour lutter contre la destruction, la perte, l'altération ou la divulgation non autorisée des données de manière accidentelle ou illicite.

Parmi ces mesures figurent principalement : [à compléter][52].

## 20. VIOLATION DE DONNÉES

En cas de violation de données à caractère personnel, [nom de l'établissement ESR] s'engage à en notifier à la CNIL dans les conditions prescrites par le RGPD.

Si ladite violation fait peser un risque élevé sur les partenaires et que les données n'ont pas été protégées, [nom de l'établissement ESR]:

- en avisera les partenaires concernés ;
- communiquera aux partenaires concernés les informations et recommandations nécessaires.

## 21. DÉLÉGUÉ À LA PROTECTION DES DONNÉES

[nom de l'établissement ESR] a désigné un délégué à la protection des données.

Les coordonnées du délégué à la protection des données sont les suivantes :

- Nom :
- Adresse e-mail :
- Tél :

En cas de nouveau traitement de données à caractère personnel, [nom de l'établissement ESR] saisira préalablement le délégué à la protection des données.

[52] A adapter selon les mesures mises en place par l'ÉTABLISSEMENTS ESR. Exemple de mesures susceptibles d'être mentionnées : conduite d'audits de sécurité, mise en œuvre d'une politique d'habilitation pour l'accès aux données, mesures de sauvegarde interne, adoption d'une PSSI, d'un PRA et/ou d'un PCA, utilisation de protocoles et/ou solutions sécurisées.

Si les partenaires souhaitent obtenir une information particulière ou souhaitent poser une question particulière, il leur sera possible de saisir le délégué à la protection des données qui leur donnera une réponse dans un délai raisonnable au regard de la question posée ou de l'information requise.

En cas de problème rencontré avec le traitement des données à caractère personnel, les partenaires pourront saisir le délégué à la protection des données désigné.

## 22. REGISTRE DES TRAITEMENTS

[nom de l'établissement ESR], en tant que responsable du traitement, s'engage à tenir à jour un registre de toutes les activités de traitement effectuées.

Ce registre est un document ou applicatif permettant de recenser l'ensemble des traitements mis en œuvre par [nom de l'établissement ESR], en tant que responsable du traitement.

[nom de l'établissement ESR] s'engage à fournir à l'autorité de contrôle, à première demande, les renseignements permettant à ladite autorité de vérifier la conformité des traitements à la règlementation informatique et libertés en vigueur.

## 23. DROIT D'INTRODUIRE UNE RÉCLAMATION AUPRÈS DE LA CNIL

Les partenaires concernés par le traitement de leurs données à caractère personnel sont informés de leur droit d'introduire une plainte auprès d'une autorité de contrôle, à savoir la Cnil en France, si celui-ci estime que le traitement de données à caractère personnel le concernant n'est pas conforme à la règlementation européenne de protection des données, à l'adresse suivante :

**Cnil** – Service des plaintes - 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07 - Tél : 01 53 73 22 22

## 24. ÉVOLUTION

La présente politique peut être modifiée ou aménagée à tout moment en cas d'évolution légale, jurisprudentielle, des décisions et recommandations de la Cnil ou des usages. Toute nouvelle version de la présente politique sera portée à la connaissance des partenaires par tout moyen défini par [nom de l'établissement ESR], en ce compris la voie électronique (diffusion par courrier électronique ou en ligne par exemple).

## 25. POUR PLUS D'INFORMATIONS

Pour toutes informations complémentaires, vous pouvez contacter les services suivants : [adresse email]. Pour toute autre information plus générale sur la protection des données personnelles, vous pouvez consulter le site de la CNIL www.cnil.fr.

## ANNEXE N°6 – LETTRE TYPE DE DEMANDE DE CONFORMITÉ AU RGPD À ADRESSER AU SOUS-TRAITANT

[en-tête de l'université]

**OBJET : Mise en conformité au RGPD**

Chère Madame, Cher Monsieur,

Vous n'êtes pas sans savoir qu'un nouveau Règlement européen sur la protection des données à caractère personnel entrera en vigueur au 25 mai 2018 prochain[53].

Notre université, en qualité de responsable du traitement, doit s'assurer que les sous-traitants auxquels elle recourt présentent des garanties suffisantes au regard de ce règlement.

Dans la mesure où vous agissez en tant que « sous-traitant » au sens du RGPD, notre université souhaite vous rappelez que l'ensemble des règles suivantes devront être respectées au plus tard le 25 mai 2018 :

- n'agissez que sur instructions documentées de notre part ;
- respectez les obligations de confidentialité des données à caractère personnel traitées ;
- prenez toutes les mesures requises en matière de sécurité des données à caractère personnel en vertu de l'article 32 du RGPD ;
- respectez la procédure de recrutement de vos sous-traitants ultérieurs ;
- engagez-vous à permettre la réalisation d'audits par notre université ou tout autre tiers habilité ;
- engagez-vous à assister notre université en cas de violation de données à caractère personnel ;
- dotez-vos d'un processus de suppression ou de transmission de données en fin de traitement ; - tenez un registre des activités de traitement.

Nous vous remercions donc de revenir vers nous pour nous expliquer les démarches que vous avez entreprises pour vous mettre en conformité avec le RGPD.

Pour notre part, nous vous adresserons, après un retour de votre part, notre propre politique RGPD.

Nous restons à votre disposition pour toute interrogation que vous auriez à ce sujet.

Je vous prie d'agréer, Chère Madame, Cher Monsieur, l'expression de mes sentiments distingués.

XXX (signature)

[53] Règlement (UE) 2016/679 du Parlement Européen et du Conseil en date du 27 avril 2016

## ANNEXE N°7 – AVENANT AU CONTRAT CONCLU ENTRE RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT

ENTRE

—

L'UNIVERSITÉ [ ]

[Forme sociale], dont le siège est situé [ ], prise en la personne de son Président Monsieur [ ], né(e) le [ ], à [ ] de nationalité [ ], demeurant [ ]

—

***Ci-après désigné le « … (CLIENT) »***

ET

—

LA SOCIÉTÉ [ ]

[Forme sociale] au capital de [ ], dont le siège social est situé [ ], inscrite au RCS de [ ], sous le numéro [ ], prise en la personne de son Président Monsieur [ ], né(e) le [ ], à [ ] de nationalité [ ], demeurant [ ]

—

***Ci-après désignée « [PRESTATAIRE] »***

—

***Ci-après désignés ensemble les « Parties »***

## 1. PRÉAMBULE

Les parties ont conclu un contrat de prestation de services le (à compléter) dont la mise en œuvre nécessite le traitement de données à caractère personnel.

À ce titre, le contrat de prestation de service contenait une clause spécifique à la protection des données à caractère personnel.

Néanmoins, l'entrée en application le 25 mai 2018 du 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 (ci-après « RGPD ») modifie en profondeur les relations entre (CLIENT) et [PRESTATAIRE].

L'article 28 du RGPD impose en effet que la relation entre (CLIENT) et [PRESTATAIRE] soit régi par un contrat ou par tout autre acte juridique précisant les différentes obligations de chacun ainsi que les instructions du (CLIENT) en matière de traitement des données à caractère personnel.

(CLIENT) a demandé par lettre RAR au sous-traitant s'il était bien conforme aux exigences du RGPD.

Option 1 : En réponse, [PRESTATAIRE] a confirmé au (CLIENT) être en conformité avec les exigences du RGPD.

Option 2 : En réponse, [PRESTATAIRE] a indiqué au (CLIENT) être actuellement en train de se conformer au RGPD et a garanti au (CLIENT) être prêt d'ici le 25 mai 2018.

Dès lors, afin d'assurer la continuité de leur collaboration dans le respect de la nouvelle règlementation applicable en matière de protection des données à caractère personne, (nom client) et [PRESTATAIRE] se sont rapprochés pour conclure le présent avenant

## 2. OBJET

Le présent avenant a pour objet de modifier les dispositions relatives à la protection des données à caractère personnel du contrat de prestation de service (.), conclu entre les parties le (.) (ci-après le « contrat »), afin d'être en conformité avec le RGPD.

Toutes les dispositions du contrat relatives à la protection des données à caractère personnel sont, par principe, remplacer par les dispositions prévues par le présent avenant.

Plus précisément, le présent avenant :

- modifie et remplace la clause relative à la protection des données à caractère personnel du contrat par une nouvelle clause conforme au RGPD ;
- intègre au contrat une annexe spécifique à la sous-traitance de données à caractère personnel conforme au RGPD ;

- intègre au contrat une annexe spécifique aux « mesures de sécurité » mises en œuvre par [PRESTATAIRE] dans le cadre de la prestation ;

Les autres clauses du contrat ne sont pas modifiées par le présent avenant. Néanmoins, en cas de contradiction entre les clauses du contrat et les clauses des nouvelles dispositions et annexes, les clauses des nouvelles dispositions et annexes prévaudront.

## 3. ENTRÉE EN VIGUEUR

Le présent avenant est applicable et fait partie intégrante du contrat dès sa signature par les parties qui doit intervenir au plus tard le 24 mai 2018.

## 4. CLAUSE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La clause (NUMERO) intitulée (.) du contrat est modifiée par la clause de protection des données suivante :

« (nom client) est responsable de traitement au sens de l'article 28 du Règlement (UE) 2016/679 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, [PRESTATAIRE] étant son sous-traitant en charge de la mise en œuvre de la prestation, objet du contrat.

Dans le cadre de l'exécution du contrat, [PRESTATAIRE] est amené à traiter des données à caractère personnel pour le compte et sur les instructions documentées du (CLIENT).

A ce titre, [PRESTATAIRE] s'engage à traiter les données à caractère personnel confiées par (nom client) dans le respect des instructions documentées et des dispositions prévues à l'annexe du présent contrat « Protection des données à caractère personnel » et ce, sans réserve. »

## 5. ANNEXES

L'annexe suivante est intégrée au contrat :

- annexe « RGPD ».

Pour [CLIENT] [date] [signature]

Pour [PRESTATAIRE] [date] [signature]

# ANNEXE N°8 – ANNEXE RGPD OPPOSÉE PAR LE RESPONSABLE DE TRAITEMENT À SON SOUS-TRAITANT

## 1. PRÉAMBULE

Dans le cadre du contrat de [préciser nom et/ou nature du contrat] d'[nom prestataire], le prestataire est sous-traitant au sens de l'article 28 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après « RGPD »).

À ce titre, le prestataire est informé que le respect de la règlementation en matière de protection des données à caractère personnel est un élément fondamental pour [Nom responsable du traitement].

Le prestataire déclare présenter les garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD.

Le prestataire s'engage à respecter, sans réserves, à l'ensemble des obligations prévues dans la présente annexe afin de se conformer aux dispositions de l'article 28 de la règlementation applicable en France et dans l'Union européenne dans le domaine de la protection des données à caractère personnel.

## 2. DÉFINITIONS

Pour la présente annexe, les termes ci-dessous ont entre les parties la signification suivante :

- « destinataire » : désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ;

- « données à caractère personnel » : désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

- « finalité » : désigne les objectifs principaux assignés au traitement et aux fonctions substantielles mises en œuvre ;

- « personne concernée » : désigne les personnes physiques identifiables ou identifiées dont les données à caractère personnel sont collectées et intégrées dans le traitement de données à caractère personnel ;

- « traitement de données à caractère personnel » : désigne toute opération ou ensemble d'opérations portant sur des données à caractère personnel, quel que soit le procédé utilisé telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

  « violation de données à caractère personnel » : désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

## 3. QUALIFICATION JURIDIQUE DES PARTIES

Au sens du RGPD et pour la bonne application des présentes :

- [Nom responsable du traitement] a la qualité de responsable de traitement ;

- le prestataire a la qualité de sous-traitant.

## 4. IDENTIFICATION DU TRAITEMENT [54]

Les éléments d'identification du traitement couverts par le présent avenant sont les suivants :

| | |
|---|---|
| **Objet du traitement** | |
| **Durée du traitement** | |
| **Nature du traitement** | |
| **Finalité du traitement** | Les finalités du traitement sont :<br>- [A COMPLÉTER] |
| **Type de données** | Les données collectées sont :<br>- [A COMPLÉTER] |

[54] Article 28 § 3 du RGPD

| | |
|---|---|
| **Catégorie de personnes concernées** | Les personnes concernées sont :<br><br>- [A COMPLÉTER] |

## 5. DÉCLARATION DU PRESTATAIRE[55]

Le prestataire est informé que le respect de la règlementation en matière de protection des données à caractère personnel est un élément fondamental pour [Nom responsable du traitement].

À ce titre, le prestataire déclare :

présenter toutes les garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée ; - disposer d'une politique informatique et libertés conforme au RGPD.

## 6. SOUS-TRAITANCE ULTÉRIEURE [56]

Option 1 (autorisation générale) Le prestataire est autorisé par [Nom responsable du traitement] à recruter d'autres sous-traitants dans le cadre du traitement.

Les autres sous-traitants recrutés par le prestataire sont listés en annexe 3 du présent avenant.

Dans tous les cas, le prestataire s'engage à :

- recruter un sous-traitant présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et du présent avenant mais également garantisse la protection des droits de la personne concernée ;

- signer avec l'autre sous-traitant un contrat faisant référence au présent avenant, et imposant à son sous-traitant les mêmes obligations en matière de protection des données à caractère personnel que celles fixées dans le présent avenant et au contrat ;

[55] Article 28 § 1 du RGPD
[56] Article 28 § 2 du RGPD

- tenir à la disposition d'[Nom responsable du traitement] la liste, annexées au présent avenant, des autres sous-traitants recrutés dans le cadre du contrat ayant accès à des données à caractère personnel ;

- informer [Nom responsable du traitement] de tout changement prévu concernant l'ajout ou le remplacement des autres sous-traitants, donnant ainsi à [Nom responsable du traitement] la possibilité d'émettre des objections et des réserves.

Le prestataire demeure pleinement responsable vis-à-vis d'[Nom responsable du traitement] et des tiers des actes de son propre sous-traitant. Il appartient donc au prestataire de prendre toutes les mesures nécessaires afin de garantir le respect par son sous-traitant des dispositions du RGPD, [Nom responsable du traitement] n'ayant aucun contrôle sur les autres sous-traitants.

Si le prestataire souhaite changer un ou plusieurs des autres sous-traitants, il doit en aviser préalablement [Nom responsable du traitement] avec un préavis minimum d'un (1) mois durant lequel [Nom responsable du traitement] peut émettre des « objections ».

En cas d'objections aux changements demandés, les parties s'engagent à se réunir et en discuter de bonne foi.

Si, à l'issue de cette réunion, [Nom responsable du traitement] maintien ses objections, il peut procéder à la résiliation du contrat moyennant un préavis de six (6) mois et ce, sans indemnité, lorsque :

l'autre sous-traitant est un concurrent d'[Nom responsable du traitement] ;
- [Nom responsable du traitement] est en précontentieux ou contentieux avec l'autre soustraitant ;
- [Nom responsable du traitement] apporte la preuve que le fait d'accepter l'autre sous-traitant lui ferait courir un risque de conflit d'intérêt ou un risque économique ou juridique.

Option 2 – (autorisation spécifique)

Le prestataire n'est autorisé à ne recruter d'autres sous-traitants dans le cadre du traitement mis en œuvre pour le compte d'[Nom responsable du traitement] qu'avec l'accord écrit et préalable de ce dernier.

En cas d'accord d'[Nom responsable du traitement], le prestataire s'engage à :

- recruter un sous-traitant présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et du présent avenant ;

- signer avec l'autre sous-traitant un contrat faisant référence au présent contrat et au présent avenant, et imposant à son sous-traitant les mêmes obligations en matière de protection des données à caractère personnel que celles fixées dans le présent avenant ;

- informer [Nom responsable du traitement] de tout changement prévu concernant l'ajout ou le remplacement des autres sous-traitants, donnant ainsi à [Nom responsable du traitement] la possibilité d'émettre des objections et des réserves.

Le prestataire demeure pleinement responsable vis-à-vis d'[Nom responsable du traitement] et des tiers des actes de son propre sous-traitant. Il appartient donc au prestataire de prendre les mesures nécessaires afin de garantir le respect par son sous-traitant des dispositions du RGPD, [Nom responsable du traitement] n'ayant aucun contrôle sur les sous-traitants du prestataire.

## 7. DROITS ET OBLIGATIONS DE [NOM RESPONSABLE DU TRAITEMENT][57]

[Nom responsable du traitement] s'engage à :

- fournir au prestataire toutes les informations et instructions documentées nécessaires à la bonne exécution du traitement ;

- indiquer au prestataire toute évolution des traitements ;

- fournir au prestataire les coordonnées de son interlocuteur ou, le cas échéant, de son délégué à la protection des données ;

- notifier les violations de données auprès de l'autorité compétente ;

- respecter ses obligations en matière de protection des données.

[Nom responsable du traitement] dispose du droit de :

demander au prestataire, à première demande, la communication de tout élément, pièce ou documentation permettant de garantir qu'il respecte les exigences du RGPD et du présent avenant ;

- formuler des objections et des réserves sur l'autre sous-traitant recruté par me prestataire;

- réaliser des audits ou des inspections auprès du prestataire afin de s'assurer du respect par ce dernier des exigences du RGPD et de l'avenant ;

- demander l'assistance du prestataire sur la mise en œuvre d'une étude d'impact et la mise en œuvre de l'exercice des droits des personnes concernées, sur la coopération avec la CNIL, sur la mise en œuvre des moyens de sécurité du traitement ou encore sur la mise en œuvre des notifications de violations de données auprès de la CNIL ou des personnes concernées.

[57] Article 28 § 3 du RGPD

## 8. INSTRUCTIONS DE [NOM RESPONSABLE DU TRAITEMENT] [58]

Le prestataire s'engage à ne traiter les données à caractère personnel dans le cadre du contrat que dans le respect des instructions documentées, communiquées par [Nom responsable du traitement] au fur et à mesure de l'exécution de la prestation.

Les instructions documentées sont communiquées au prestataire par écrit, sous toute forme choisie par [Nom responsable du traitement] telle que par document, courrier électronique ou compte rendu de réunion, sans que cette liste ne soit exhaustive.

Le prestataire informe immédiatement [Nom responsable du traitement] si, selon lui, une instruction d'[Nom responsable du traitement] constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données. Cette information doit être adressée par écrit et dans un temps compatible avec sa prise en compte par [Nom responsable du traitement]. [59]

## 9. FLUX TRANSFRONTIÈRES [60]

Aucun transfert de données à caractère personnel ne peut intervenir en dehors de l'Union européenne sans l'accord préalable, exprès et spécial d'[Nom responsable du traitement].

En cas d'accord d'[Nom responsable du traitement], le prestataire s'engage à respecter l'ensemble des obligations en matière de transfert de données à caractère personnel vers un pays tiers et notamment à conclure un acte juridique contraignant avec le destinataire des données comme des clauses contractuelles types ou des BCR et d'en justifier auprès d'[Nom responsable du traitement].

## 10. CONFIDENTIALITÉ RENFORCÉE [61]

Le prestataire s'engage à faire signer par toutes les personnes susceptibles d'accéder aux données à caractère personnel d'[Nom responsable du traitement] un engagement individuel de confidentialité conforme à l'annexe 1.

Le prestataire doit être en mesure de confirmer le respect de cette obligation auprès d'[Nom responsable du traitement], à première demande, en communiquant la liste des personnes susceptibles d'accéder aux données à caractère personnel, accompagnée des annexes signées par lesdites personnes.

[58] Article 23 § 3 a) du RGPD
[59] Article 28 § 3 a) du RGPD
[60] Article 23 § 3 a) du RGPD
[61] Article 23 § 3 b) du RGPD

Le prestataire s'engage à former les personnes susceptibles d'accéder aux données à caractère personnel d'[Nom responsable du traitement] sur les mesures de sécurité à mettre en œuvre. Le plan de formation annuel est communiqué à [Nom responsable du traitement].

Le prestataire s'engage à ce que ses éventuels sous-traitants ultérieurs soient également tenus par ces obligations spécifiques et soient en mesure d'en justifier auprès d'[Nom responsable du traitement], à première demande.

## 11. OBLIGATION DE SÉCURITÉ[62]

Le prestataire est tenu de mettre en œuvre les mesures organisationnelles et techniques de nature à lutter contre la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

À ce titre, le prestataire met en œuvre les mesures techniques et organisationnelles définies en annexe 2.

L'annexe 2 doit être maintenue à jour et tenir compte des évolutions technologiques. Aucune modification ne peut être apportée à l'annexe 2 qui n'ait été préalablement portée à la connaissance d'[Nom responsable du traitement] et approuvé par lui.

## 12. VIOLATION DE DONNÉES

Il appartient à [Nom responsable du traitement], et à lui seul, de notifier les éventuelles violations de sécurité à la CNIL.

Le prestataire s'engage à notifier à [Nom responsable du traitement], dans les meilleurs délais et, si possible au plus tard 48 heures après en avoir pris connaissance, toute violation de donnée à caractère personnel qu'il aurait subi.

En cas de retard dans la communication de la violation, le prestataire doit accompagner sa notification des motifs expliquant ce retard.

La violation de données est communiquée aux interlocuteurs désignés par [à [Nom responsable du traitement] ou, à défaut, au délégué à la protection des données désigné par à [Nom responsable du traitement]

La notification doit, au minimum, préciser :

[62] Article 28 § 3 c) du RGPD

- la nature de la violation des données, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernées ;
- le nom et les coordonnées du délégué à la protection des données du prestataire ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- les conséquences probables de la violation de données ;
- les mesures déjà prises ou celles qui sont proposées pour y remédier.

Si le prestataire est dans l'incapacité de fournir l'ensemble de ces informations au même moment, cela ne l'exonère pas de son obligation de notifier à [Nom responsable du traitement] la violation des données accompagnée de l'ensemble des informations à sa disposition, le reste devant être communiqué dès prise de connaissance.

En cas de violation de données, le prestataire prend, dès que possible, toutes les mesures nécessaires pour remédier et diminuer l'impact de la violation et informe [Nom responsable du traitement] des mesures prises et des résultats attendus et constatés.

Le prestataire s'engage à collaborer activement avec [Nom responsable du traitement] pour qu'elle soit en mesure de répondre à ses obligations réglementaires et contractuelles et notamment pour répondre aux interrogations de la CNIL.

## 13. AIDE ET ASSISTANCE DE [NOM RESPONSABLE DU TRAITEMENT][63]

### 13.1. AIDE ET ASSISTANCE CONCERNANT LE DROIT DES PERSONNES

Le prestataire s'engage à aider et assister [Nom responsable du traitement] par l'intermédiaire de mesures techniques et organisationnelles appropriées et en tenant compte de la nature du traitement à s'acquitter de l'obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits.

### 13.2. AIDE ET ASSISTANCE CONCERNANT LA SÉCURITÉ DU TRAITEMENT

Le prestataire est tenu d'aider et d'assister [Nom responsable du traitement] dans le cadre de la mise en œuvre des mesures techniques et organisationnelles appropriées de nature à satisfaire aux obligations de protection et de sécurisation des traitements.

Afin d'apporter une aide appropriée à [Nom responsable du traitement], le prestataire doit s'appuyer sur l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les personnes concernées.

[63] Article 28 § 3 e) f) h) du RGPD

[Nom responsable du traitement] reste le seul responsable de la mise en œuvre des propositions formulées par le prestataire.

Le prestataire informe sans délai [Nom responsable du traitement] en cas d'identification d'une vulnérabilité technique ou d'une défaillance organisationnelle.

### 13.3. AIDE ET ASSISTANCE CONCERNANT LA NOTIFICATION DE VIOLATIONS DE DONNÉES

Le prestataire s'engage à assister et aider [Nom responsable du traitement] en cas de violation de données afin qu'[Nom responsable du traitement] soit en capacité de communiquer l'ensemble des informations demandées par le RGPD dans le délai imparti, qu'il s'agisse de la notification à la CNIL ou aux personnes concernées.

Pour ce faire, le prestataire s'engage à fournir l'ensemble des informations qu'il dispose et toutes les informations demandées par le RGPD concernant le traitement et la violation de données.

En outre, le prestataire s'engage à apporter toute aide ou assistance technique dont pourrait bénéficier [Nom responsable du traitement] afin de limiter les effets de la violation de données ou d'interrompre ladite violation.

### 13.4. AIDE ET ASSISTANCE CONCERNANT L'ANALYSE D'IMPACT

Le prestataire informe [Nom responsable du traitement] dès lors qu'il a connaissance d'un type de traitement qui, compte tenu de sa nature, du contexte et des finalités, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Le prestataire s'engage à aider et assister [Nom responsable du traitement] dans la mise en œuvre de l'analyse d'impact en fournissant, à première demande, l'ensemble des informations dont [Nom responsable du traitement] a besoin pour réaliser cette analyse d'impact.

Le prestataire s'engage à aider et assister [Nom responsable du traitement] lorsque ce dernier décide de consulter la CNIL à la suite d'une analyse d'impact ayant indiqué que le traitement présenterait un risque élevé si le traitement ne fait pas l'objet d'une modification.

Le prestataire s'engage à fournir toutes les informations qu'il dispose ainsi qu'une aide et assistance technique afin de proposer des mesures d'atténuation des risques pour les droits et libertés des personnes physiques.

## 14. CONTRÔLE DE LA CNIL[64]

[Nom responsable du traitement] et le prestataire sont tenus de coopérer avec la CNIL, à la demande de celle-ci,

[64] Article 31 du RGPD

Dans le cas où le contrôle mené auprès du prestataire concernerait les traitements mis en œuvre au nom et pour le compte d'[Nom responsable du traitement], le prestataire s'engage à en informer immédiatement [Nom responsable du traitement] et à ne prendre aucun engagement pour elle.

En cas de contrôle de la CNIL auprès d'[Nom responsable du traitement] portant notamment sur les prestations délivrées par le prestataire, ce dernier s'engage à coopérer avec [Nom responsable du traitement] et à lui fournir toute information dont la CNIL pourrait avoir besoin.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le prestataire en tant que responsable du traitement, ce dernier fait son affaire du contrôle et s'interdit de communiquer ou de faire état des données à caractère personnel d'[Nom responsable du traitement].

Dans tous les cas, si le prestataire fait l'objet d'une mise en demeure, d'un avertissement ou d'une condamnation de la CNIL, même dispensée de publication, ce dernier est tenu d'en informer [Nom responsable du traitement] sans délai et au plus tard dans les 48h de la décision.

## 15. SORT DES DONNÉES À LA FIN DU CONTRAT

Option 1 – suppression

À l'expiration du contrat et au plus tard le dernier jour du contrat, le prestataire a pour obligation de supprimer toutes les données à caractère personnel et toutes copies existantes.

Il ne saurait y avoir de rétention de la part du prestataire pour quelque raison que ce soit.

Concomitamment à la destruction des données et des copies, le prestataire adresse à [Nom responsable du traitement] une attestation de destruction de toutes les copies existantes des données d'[Nom responsable du traitement].

Option 2 – restitution au responsable du traitement et attestation de suppression

À l'expiration du contrat et au plus tard le dernier jour du contrat, le prestataire a pour obligation de restituer l'ensemble de ses données à [Nom responsable du traitement]. Il ne saurait y avoir de rétention de la part du prestataire pour quelque raison que ce soit.

Concomitamment à la restitution des données, le prestataire adresse à une attestation de destruction de toutes les copies existantes des données d'[Nom responsable du traitement] [Nom responsable du traitement].

Option 3 – transfert de données vers un nouveau prestataire

À l'expiration du contrat et au plus tard le dernier jour du contrat, le prestataire s'engage à transférer toutes les données traitées dans le cadre du contrat vers le nouveau prestataire désigné par [Nom responsable du traitement].

Les parties définissent les conditions de réversibilité dans le cadre du plan annexé au présent avenant.

## 16. REGISTRE DES OPÉRATIONS DE TRAITEMENT

Option 1 [250 salariés: Au regard du nombre de ses employés], [option 2] Au regard de la qualité des données sous-traitées], le prestataire se doit de tenir un « registre des opérations de traitement » et le maintenir à jour.

Pour ce faire, [Nom responsable du traitement] communique au prestataire les éléments et informations qui lui seront demandés par le prestataire pour la bonne tenue de son registre.

Le prestataire est tenu de justifier de l'existence de son registre à première demande d'[Nom responsable du traitement] ou dans le cadre d'un audit.

Le registre est tenu à la disposition de la Cnil.

## 17. AUDIT

[Nom responsable du traitement] se réserve le droit de procéder à toute vérification qui lui paraitrait utile pour constater le respect des obligations précitées en procédant à un audit de sécurité auprès du prestataire ou directement auprès d'un de ses sous-traitants.

Le prestataire s'engage à répondre aux demandes d'audit d'[Nom responsable du traitement] ou d'un tiers de confiance qu'[Nom responsable du traitement] aura sélectionné, reconnu en tant qu'auditeur indépendant, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à [Nom responsable du traitement].

Les audits doivent permettre une analyse du respect par le prestataire de ses obligations au titre des présentes, ainsi qu'au titre de la règlementation applicable en matière de la protection des données à caractère personnel.

[Nom responsable du traitement] doit aviser le prestataire par écrit de son intention de faire procéder à un audit moyennant le respect d'un préavis minimum de trente (30) jours. [Nom responsable du traitement] ne peut réaliser un audit qu'une fois par an.

[Nom responsable du traitement] communique de la manière la plus précise et exhaustive possible le périmètre envisagé, la liste des opérations de contrôle et des outils de mesure qu'il envisage utiliser.

Le déploiement d'un outil est fait sous l'entière responsabilité d'[Nom responsable du traitement]. Le prestataire a le droit de faire analyser l'outil. Si un risque est identifié pour le système d'information et les données du prestataire, ce dernier est en droit de refuser l'utilisation d'un tel outil.

[Nom responsable du traitement] communique, le cas échéant, le nom de l'auditeur. Le prestataire a le droit de refuser l'auditeur pour un motif légitime. En cas de désaccord après une troisième proposition, le choix de l'auditeur est fixé par le tribunal compétent. [Nom responsable du traitement] est responsable des dommages causés par l'auditeur.

Le prestataire peut refuser l'accès aux zones confidentielles, sécurisées et mutualisées et effectue, dans ce cas, l'audit et en communique les résultats à [Nom responsable du traitement].

Les résultats de l'audit sont formalisés dans un rapport qui doit être adressé au prestataire pour qu'il puisse y insérer ses observations et réserves. Le rapport final doit nécessairement comprendre les observations du prestataire.

Si un désaccord survient concernant des écarts de conformité, [Nom responsable du traitement] est en droit de demander une mise en conformité. Toutefois, [Nom responsable du traitement] ne saurait invoquer la non-réalisation de la mise en conformité pour suspendre ses engagements.

La procédure d'audit se termine par la remise par [Nom responsable du traitement] d'une lettre clôturant l'audit même en cas d'audit favorable pour le prestataire.

## 18. RESPONSABILITÉ

Aux termes de l'article 82 du RGPD, le prestataire est tenu pour responsable du dommage causé par le traitement dès lors :

- qu'il n'a pas respecté les obligations prévues dans le RGPD qui incombent spécifiquement aux sous-traitants ou ;
- qu'il a agi en-dehors des instructions licites d'[Nom responsable du traitement] ou ; - qu'il a agi contrairement aux instructions licites d'[Nom responsable du traitement].

À ce titre, le prestataire est tenu à une obligation de résultat sur :

- le respect de l'annexe « mesures de sécurité » ;
- l'aide et l'assistance qu'il doit à [Nom responsable du traitement] ;
- sa réaction en cas de violation de sécurité ;
- ses obligations au titre du droit d'audit d'[Nom responsable du traitement] ;
- l'assistance due à [Nom responsable du traitement] en cas de contrôle de la part de la CNIL.

## 19. RÉPARATION DU PRÉJUDICE

Lorsque l'une des parties est individuellement responsable d'un dommage du fait du traitement, il est individuellement tenu responsable de ce dommage dans sa totalité afin de garantir aux personnes concernées une réparation effective.

Lorsque les parties sont conjointement responsables d'un dommage causé par le traitement, les parties sont également conjointement responsables du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

Aucune limitation de responsabilité ni aucun plafond de réparation ne sont applicables au titre de la réparation du préjudice des personnes concernées.

En cas de condamnation d'[Nom responsable du traitement] à une amende administrative ou à toute autre décision lui créant préjudice, le prestataire s'engage à la dédommager à hauteur des condamnations ou préjudices exposés.

## 20. RÉVISION

Toute évolution de la jurisprudence, décision de la CNIL ou toute nouvelle règlementation en matière de protection des données à caractère personnel, qui modifieraient l'une des dispositions du présent avenant implique nécessairement sa révision.

La révision doit emporter l'accord des deux parties.

En cas de désaccord sur la révision de l'avenant qui exposerait [Nom responsable du traitement] à un risque technique, économique ou juridique, le contrat peut être résilié sans indemnité ni pénalité par lettre RAR sous réserve de respecter un délai maximum de six (6) mois à compter de l'envoi de la demande de résiliation.

## 21. DÉSIGNATION D'UN REPRÉSENTANT [65]

Dans le cas où le prestataire ne serait pas localisé sur le territoire de l'Union européenne, il s'engage, dans le respect de la réglementation applicable, à désigner par écrit un représentant au sein de l'Union européenne.

Les coordonnées de ce représentant doivent être communiquées à [Nom responsable du traitement] à première demande.

## 22. DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Si [Nom responsable du traitement] et le prestataire désignent un délégué à la protection des données, les deux délégués se voient communiquer pour information le présent contrat. Par ailleurs les délégués à la protection des données se réunissent au moins une fois par an pour évoquer les améliorations pouvant être apportées au présent avenant.

[65] Article 27 du RGPD

## 23. DROIT APPLICABLE ET JURIDICTION COMPÉTENTE

Nonobstant toute disposition contraire du contrat, tout litige relatif à l'interprétation ou l'exécution du présent avenant relève du droit français et de la compétence exclusive des tribunaux du ressort de la Cour d'appel de Paris.

## 24. ANNEXES[66]

Le présent avenant est complété des annexes suivantes :

- Annexe 1 - « Engagement de confidentialité » ;
- Annexe 2 - « Mesures de sécurité mise en œuvre par Le prestataire» ;
- Annexe 3 - « Liste des sous-traitants ultérieurs au jour de la signature du contrat » ;
- Annexe 4 – « Réversibilité » uniquement si [Nom responsable du traitement] choisit l'option 3 de l'article 15

[66] L'annexe 1 correspond à l'annexe n°10 du présent document, intitulé « modèle de lettre d'engagement de confidentialité ». Quant aux autres annexes, elles doivent être élaborées au cas par cas par le sous-traitant, le cas échéant par le sous-traitant et le responsable de traitement agissant conjointement.

## ANNEXE N°9 – MODÈLE DE LETTRE D'ENGAGEMENT DE CONFIDENTIALITÉ

Dans le cadre des pourparlers engagés dès ce jour concernant [_____] et pour lesquels le Prestataire pourrait être amené à [décrire les prestations envisagées] au profit de l'Université [_____], le Prestataire va recevoir un certain nombre d'informations qui nécessitent bien entendu le respect de la plus entière confidentialité.

En conséquence, dès réception de ces documents, de nature commerciale, économique, sociale, juridique, judiciaire et financière, le Prestataire s'engage à garantir à l'Université [_____] le respect de la plus stricte confidentialité, concernant notamment :

- les informations écrites, orales ou visuelles de nature commerciale, financière, juridique et judiciaire ou de tout autre ordre communiquées par l'Université [_____] ou dont le Prestataire aurait eu connaissance à l'occasion de ces pourparlers ; dans la mesure où ces informations ne sont pas publiques ;

- que le Prestataire n'utilisera ces informations qu'aux fins de [décrire les prestations envisagées] ;

- que le Prestataire restituera tout document qui lui aurait été confié ainsi que toute copie de ces documents à l'issue de la présentation d'une offre éventuelle ;

- que le Prestataire ne conservera aucune copie, extrait, reproduction, enregistrement ou élément relatif aux informations qui lui auront été transmises ou dont il aurait eu connaissance ;

- que le Prestataire ne fera aucune utilisation pour son propre compte, directement ou indirectement, des informations qui lui auront été transmises ou dont il aurait eu connaissance ;

- que le Prestataire ne communiquera les informations qui lui auront été transmises ou dont ils auront eu connaissance qu'aux membres de son personnel expressément chargés de la préparation de l'offre et, le cas échéant de son exécution ;

- que le Prestataire prendra toutes les dispositions qui s'imposent pour que le personnel et/ou ses représentants légaux respectent le présent engagement.

Le présent engagement est valable pendant toute la durée de l'offre de ses suites et conséquences, y compris après la présentation de l'offre, et pendant trois années suivant la présentation de cette offre.

Tout non-respect de cet engagement pourra justifier l'engagement d'une procédure judiciaire visant à obtenir réparation des préjudices que ce non-respect pourra avoir causés.

Fait le [_____],
A [_____],
Signature des parties.

## ANNEXE N°10 – MODÈLE DE CLAUSE DONNÉE À CARACTÈRE PERSONNEL À OPPOSER AU SOUS-TRAITANT

«[nom de l'établissement ESR] est responsable de traitement au sens de l'article 28 du Règlement (UE) 2016/679 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, [PRESTATAIRE] étant son sous-traitant en charge de la mise en œuvre de la prestation, objet du contrat.

Dans le cadre de l'exécution du contrat, [PRESTATAIRE] est amené à traiter des données à caractère personnel pour le compte et sur les instructions documentées de [nom de l'établissement ESR].

À ce titre, [PRESTATAIRE] s'engage à traiter les données à caractère personnel confiées par [nom de l'établissement ESR] dans le respect des instructions documentées et des dispositions prévues à l'annexe du présent contrat « Protection des données à caractère personnel » et ce, sans réserve. »

## ANNEXE N°11 – MODÈLE DE REGISTRE DES TRAITEMENTS DU RESPONSABLE DE TRAITEMENT

Le présent registre est constitué vertu de l'article 30 du Règlement (UE) sur le protection des données n°2016-679 et de la loi française n° 78-17 (attention changement de numéro possible avec nouvelle loi).

Ce registre des traitements est obligatoire pour toute entreprise :

- [option 1] de plus de 250 salariés
- [option 2] de moins de 250 salariés souhaitant mettre en œuvre le respect du principe d'accountability
- [option 3] de moins de 250 salariés qui effectue un traitement non occasionnel susceptible de comporter un risque pour les droits et libertés des personnes concernées
- [option 4] de moins de 250 salariés qui traite de catégories particulières de données visées à l'article 9 du RGPD
- [option 5] de moins de 250 salariés qui traite de données à caractère personnel relatives à des condamnations pénales et infractions

, qu'elle agisse en qualité de responsable du traitement ou de sous-traitant.

Ce registre est mis en œuvre par [nom de l'université] en qualité de responsable du traitement.

Sur demande, ce registre sera mis à la disposition de l'autorité compétence à savoir la Cnil.

L'organisation et le maintien à jour de ce registre seront des étapes essentielles pour démontrer la conformité de l'entreprise à la règlementation informatique et libertés en vigueur.

Ce registre est placé sous l'autorité de :

- [option 1] DPO
- [option 2] toute personne désignée

C'est pourquoi il sera nécessaire de :

- recenser l'intégralité des traitements mis en œuvre par l'université ;
- désigner une personne en charge du recensement des données dans chaque service concerné ;
- sensibiliser et former le personnel en charge ;
- organiser périodiquement la remontée des informations par un calendrier établi afin de mettre à jour le registre le plus fréquemment possible (durée recommandée : mise à jour mensuelle).

**Rappel : Tous les traitements qui ne figurent pas dans ce registre sont considérés comme contraire à la politique RGPD de notre entreprise et pourra faire l'objet de sanction.**

**Date de création du registre : [xx/xx/xxxx]**

**Mis à jour le : [xx/xx/xxxx]**

racine
AVOCATS

# TRAITEMENT 1

| Traitement | Description |
|---|---|
| Nom du traitement | |
| Référence/numéro du traitement | |

| Traitement | Description |
|---|---|
| Nom de la personne responsable de la fiche | |
| Date de création de la fiche | |
| Mise à jour de la fiche | |

| Acteurs | Nom | Adresse | CP | Ville | Pays | Téléphone | Email |
|---|---|---|---|---|---|---|---|
| Responsable du traitement | | | | | | | |
| Responsable(s) conjoint(s) interne(s) ou soustraitant(s) | | | | | | | |
| Représentant du responsable du traitement | | | | | | | |
| Délégué à la protection des données | | | | | | | |

| Finalité(s) | Description |
|---|---|
| Finalité 1 | |
| Finalité 2 | |
| Finalité 3 | |

| Catégorie de personnes concernées | Description |
|---|---|
| Catégorie de personnes 1 | |
| Catégorie de personnes 2 | |

| | |
|---|---|
| Catégorie de personnes 3 | |

| Catégorie de données concernées | Description | Délai d'effacement |
|---|---|---|
| Données 1 | | |
| Données 2 | | |
| Données 3 | | |
| Données 4 | | |
| Données 5 | | |
| Données 6 | | |

| Catégorie de destinataires | Interne | Externe |
|---|---|---|
| Destinataires 1 | | |
| Destinataires 2 | | |
| Destinataires 3 | | |
| Destinataires 4 | | |

| Transfert de données hors UE | Destinataire | Type de garanties | Lien vers annexe justificative |
|---|---|---|---|
| Organisme destinataire 1 | | | |
| Organisme destinataire 2 | | | |

| Mesures de sécurité | Description |
|---|---|
| Mesures de sécurité techniques | |
| Mesures de sécurité organisationnelles | |

| Données sensibles[67] | Description | Délai d'effacement |
|---|---|---|
| Donnée sensible 1 | | |
| Donnée sensible 2 | | |
| Donnée sensible 3 | | |

[67] Attention, ne remplissez cette partie qu'à condition que vous traitiez effectivement ce type de données ; Si tel n'est pas le cas, merci de supprimer cette partie du registre.

# ANNEXE N°12 – MODÈLE DE PRÉREQUIS JURIDIQUES DE DÉVELOPPEMENT

## 1. PRÉAMBULE [68]

Même si l'obligation n'est pas formellement établie dans le RGPD, il est indispensable que les logiciels, progiciels ou autres applications (que nous appelons par commodité de langage « produit ») permettent à leur utilisateur (entreprise ou acteur public) de respecter les obligations posées par le RGPD.

Ces contraintes doivent être respectées aussi bien lorsque les développements sont réalisés par un prestataire externe (ESN) ou réalisés par les équipes internes (généralement la DSI). Il en va de même quel que soit l'ampleur du développement et/ou des développements spécifiques.

On peut distinguer 3 types de contraintes :

- les contraintes relatives au produit lui-même ;
- les contraintes relatives à l'usage du produit ;
- les contraintes relatives à la sécurité du produit.

Le présent document constitue des prérequis juridiques à destination des développeurs internes ou externes. Il fixe les règles à respecter en proposant de :

- présenter la contrainte et son référentiel dans le RGPD ;
- proposer des mesures de mise en œuvre.

Il ne s'agit ici que de propositions, le client étant seul à même de les mettre en œuvre ou de mettre en œuvre des solutions alternatives.

[68] Le présent modèle concerne l'hypothèse du développement d'un logiciel ou d'une application. Il peut toutefois être décliné à plusieurs autres hypothèses dans la mesure où les différents prérequis reprennent les exigences standard du RGPD.

Il s'agit essentiellement de contraintes endogènes, liées au produit lui-même.

## 2.1. PRÉREQUIS N°1 – MISE À JOUR DES DONNÉES

| | |
|---|---|
| **Référentiel RGPD** | **Art. 16 RGPD : Droit de rectification**<br><br>*« La personne concernée **a le droit** d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. »* |
| **Mise en œuvre** | 1. Le produit doit pouvoir permettre des mises à jour de l'ensemble des champs de données, sauf à justifier que les données ne doivent pas être modifiées pour des raisons juridiques.<br><br>2. Pour des services en ligne ou espace « membre » il est possible de prévoir que la mise à jour soit effectuée par l'internaute luimême.<br><br>3. Si possible, prévoir la traçabilité de la mise à jour (anticipation de contentieux).<br><br>4. Si la modification est réalisée directement par l'internaute, idéalement prévoir qu'il reçoive un message pour confirmer la mise à jour. |

## 2.2. PRÉREQUIS N°2 ACCÈS ET COPIE DES DONNÉES

| | |
|---|---|
| **Référentiel RGPD** | **Art. 15.1 RGPD : Droit d'accès de la personne concernée**<br><br>*« La personne concernée **a le droit** d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées (…) »*<br><br>**Art. 15.3 RGPD : Droit de copie**<br><br>*« Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement. Le responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement. »* |
| **Mise en œuvre** | 1. Prévoir un requêteur multicritères permettant de faire une recherche rapide et exhaustive pour répondre sans erreur au droit d'accès.<br><br>2. Prévoir une solution permettant la copie des données en question. Attention cette solution doit être de traiter toutes les données présentes sur différents traitements.<br><br>3. Prévoir l'accès sous forme de requête automatique par exemple, ou de simple requête auprès d'un administrateur qui devra fournir les données dans un délai raisonnable.<br><br>4. Prévoir également la possibilité de copie (extraction) sous forme de téléchargement d'un fichier |

## 2.3. PRÉREQUIS N°3 PORTABILITÉ DES DONNÉES

| | |
|---|---|
| **Référentiel RGPD** | **Art.20 RGPD : Droit à la portabilité des données**<br><br>*« 1. Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle,* lorsque:<br>*a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b);*<br>*b) le traitement est effectué à l'aide de procédés automatisés.*<br><br>*2. Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel ».* |
| **Mise en œuvre** | **ATTENTION**, le droit de copie n'est pas un « impératif », il ne s'applique que lorsque les 3 critères cumulatifs suivants sont présents :<br><br>Critère 1 – il s'agit d'un procédé automatisé, c'est-à-dire informatique. Il n'y donc pas de « portabilité » pour les traitements papier ; Critère 2 – les données sont saisies par la personne elle-même ; Critère 3 – le traitement est basé sur le « consentement ».<br><br>En pratique, il y a donc peu de cas où la portabilité s'applique.<br><br>1. Identifier les cas où la portabilité s'applique ;<br><br>2. Dans les cas où la portabilité s'applique, prévoir une fonction « export ». Les données doivent pouvoir être exportées dans un format commun et lisible. |

## 2.4. PRÉREQUIS N°4 PURGE TOTALE OU PARTIELLE

| | |
|---|---|
| **Référentiel RGPD** | **Art. 5 e) RGPD : suppression des données au terme d'un certain délai**<br><br>*« 1. Les données à caractère personnel doivent être :*<br><br>*conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation); »* |
| **Mise en œuvre** | 1. Prévoir une fonctionnalité permettant au client de paramétrer les durées de suppression automatique des données en fonction de sa politique de conservation.<br><br>2. À défaut d'une solution automatisée, prévoir dans tous les cas une fonction de purge des données.<br><br>**ATTENTION**, la durée de conservation doit être définie par le responsable de traitement et non par le prestataire. En interne, la durée doit être appréciée par les métiers et la direction juridique. |

## 2.5. PRÉREQUIS N°5 LIMITATION

| | |
|---|---|
| **Référentiel RGPD** | **Art.18 RGPD : Droit à la limitation du traitement**<br><br>1. La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :<br>a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel;<br>b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation;<br>c) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice;<br>d) la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.<br><br>La notion de « limitation » est explicitée à l'article 4 « définitions » du RGPD qui précise :<br><br>- « « limitation du traitement », le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur » |
| **Mise en œuvre** | 1. Prévoir la possibilité de taguer (marquer) des données ou par simplicité le compte d'un utilisateur pour lui appliquer une règle de limitation d'usage. |

## 2.6. PRÉREQUIS N°6 EFFACEMENT

| | |
|---|---|
| **Référentiel RGPD** | **Art. 17 RGPD : droit à l'effacement (« droit à l'oubli »)**<br><br>« *La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'appliquent :*<br>*a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière; 4.5.2016 L 119/43 Journal officiel de l'Union européenne ;*<br>*b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;*<br>*c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux (…)* » |
| **Mise en œuvre** | 1. Prévoir la possibilité d'effacer une ou plusieurs données où l'ensemble d'un compte utilisateur.<br>2. Prévoir la possibilité de prouver l'effacement (log ou autre).<br>3. Prévoir, si possible, l'envoi d'un message automatique à la personne concernée lorsque l'effacement a été réalisé. |

## 2.7. PRÉREQUIS N°7 CHAMP FACULTATIF OU OBLIGATOIRE

| | |
|---|---|
| **Référentiel RGPD** | Il ne s'agit pas d'une règle issue du RGPD, mais de l'article **32 I. 3 de la loi dite « informatique et libertés »**<br><br>*« La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant (…)*<br><br>***3°** Du caractère obligatoire ou facultatif des réponses (…)* |
| **Mise en œuvre** | 1. Prévoir, en présence d'un formulaire en ligne, la possibilité pour le responsable du traitement de paramétrer les champs de saisie obligatoire / facultatif et d'identifier les champs obligatoires par un (*).<br><br>2. Prévoir un espace spécifique sous le traitement pour l'information des personnes concernées. |

## 2.8. PRÉREQUIS N°8 COMPTE UTILISATEUR

| | |
|---|---|
| **Référentiel RGPD** | **Art. 13 et 14 RGPD : Information et accès aux données à caractère personnel**<br><br>Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit plusieurs informations dont :<br><br>- L'identité et les coordonnées du responsable de traitement (à défaut son représentant) ;<br>- Les finalités du traitement des données ;<br>- Les destinataires des données ;<br>etc. |
| **Mise en œuvre** | 1. Prévoir pour toute application en ligne permettant notamment l'ouverture d'un « compte utilisateur » un accès à la « politique de données personnelles ». |

## 2.9. PRÉREQUIS N°9 IDENTIFICATION DE DONNÉES SENSIBLES

| | |
|---|---|
| **Référentiel RGPD** | **Art. 9 RGPD : Traitement portant sur des catégories particulières de données à caractère personnel (données sensibles)**<br><br>Données qui concernent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, données génétiques, etc. |
| **Mise en œuvre** | Prévoir l'identification de ces données sous forme :<br><br>- soit de code couleur lorsqu'elles sont collectées dans un formulaire ;<br>- soit sous forme de pop-up signifiant leur caractère sensible au moment de la collecte ;<br><br>Lorsqu'elles apparaissent dans une zone de commentaires libres, prévoir une détection automatique de termes sensibles (répertoire). |

## 3. PRÉREQUIS RELATIFS À L'USAGE DU LOGICIEL

### 3.1. PRÉREQUIS N°1 - CONSENTEMENT

| | |
|---|---|
| **Référentiel RGPD** | **Art. 7 : Conditions applicables au consentement**<br><br>*« 1. Dans les 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 données à caractère personnel la concernant. »* |
| **Mise en œuvre** | **ATTENTION**, ce pré-requis ne s'applique que lorsque le traitement repose sur le recueil du consentement.<br><br>1. Prévoir la possibilité d'exprimer un consentement (clic ou autre) accompagné des mentions appropriées (renvoi à la « politique des données personnelles).<br><br>2. Prévoir la possibilité de garder la trace (log ou autre) d'un consentement de la part de la personne concernée. |

## 3.2. PRÉREQUIS N°2 ZONE DE SAISIE LIBRE (FONCTION BLOC NOTE)

| | |
|---|---|
| **Référentiel RGPD** | La problématique posée par les zones de saisie libre n'est pas formalisée en tant que tel dans le RGPD, mais elle fait partie des opérations de contrôle de l'autorité compétente. L'objectif est de vérifier si les zones de saisie libre sont « bien » utilisées et ne comportent pas de données à caractère personnel interdites (santé, situation de la personne, ….). |
| **Mise en œuvre** | **ATTENTION**, ce prérequis ne s'applique que si les personnes qui utilisent le produit (généralement les salariés ou les agents de l'entreprise) disposent d'un champ de saisie libre (souvent appelé zone bloc note).<br><br>1. Possibilité d'activer ou de désactiver la zone libre pour telle ou telle catégorie d'utilisateur.<br><br>2. Rappel des règles à respecter (sous forme de pop-up par exemple).<br><br>3. Possibilité de passer par un dictionnaire de données + actualisation du dictionnaire pour éviter la saisie de « mots interdits ». |

### 3.3. PRÉREQUIS N°3 – ACCÈS/INTERVENTION ADMINISTRATEURS

| | |
|---|---|
| **Référentiel RGPD** | Ce prérequis ne figure pas à proprement parler dans le RGPD, mais dans les recommandations de la Cnil qui souhaite que les actions/interventions des administrateurs puissent être identifiées (guide de la sécurité). |
| **Mise en œuvre** | 1. Identification particulière des accès et des actions des administrateurs (internes ou externes) |

### 3.4. PRÉREQUIS N°4 – TRAÇABILITÉ ET HISTORISATION

| | |
|---|---|
| **Référentiel RGPD** | Ce prérequis ne figure pas à proprement parler dans le RGPD (hormis l'historique du consentement), mais dans les recommandations de la Cnil qui souhaite que les actions/interventions des administrateurs puissent être identifiées (guide de la sécurité). |
| **Mise en œuvre** | 1. Prévoir une historisation des actions (log).<br>2. Prévoir la conservation dans des conditions de sécurisation adaptées des journaux d'historisation.<br>3. Limiter sur un plan logique l'accès aux journaux d'historisation.<br>4. Prévoir, en fonction de la politique de durée de conservation de l'entreprise, l'effacement régulier des journaux d'historisation. |

### 3.5. PRÉREQUIS N°5 HABILITATION

| | |
|---|---|
| **Référentiel RGPD** | Ce prérequis ne figure pas à proprement parler dans le RGPD, mais il participe aux mesures prises pour sécuriser et protéger les données, qui sont une exigence importante du RGPD. |
| **Mise en œuvre** | 1. Possibilité de créer des « profils » utilisateur du produit. |

### 3.6. PRÉREQUIS N°6 – OPT-IN / OPT-OUT

| | |
|---|---|
| **Référentiel RGPD** | Ce prérequis ne relève pas du RGPD, mais de la règlementation sur la prospection commerciale qui interdit la prospection commerciale à destination d'une personne (BtoC) qui n'a pas donné son consentement (opt-in) |
| **Mise en œuvre** | **ATTENTION**, ces mesures ne s'appliquent que dans le cas de collectes de données qui relèvent de l'opt-in (inscription à une newsletter par exemple)<br>1. Prévoir de taguer le compter utilisateur comme « opt-in » ou « optout ».<br>2. Prévoir la possibilité de changer de statut – opt-in vers opt-out et vice et versa.<br>3. Prévoir un moyen de conserver la trace du consentement (opt-in). |

# 4. PRÉREQUIS RELATIFS À LA SÉCURITÉ

## 4.1. PRÉREQUIS N°1 – CHIFFREMENT

| | |
|---|---|
| **Référentiel RGPD** | L'article 32 du RGPD « sécurité du traitement » précise que le responsable du traitement (client) et le sous-traitant (prestataire) mettent en œuvre les mesures techniques et opérationnelles appropriées pour garantir un niveau de sécurité adapté au risque.<br><br>Parmi les outils qui peuvent être déployés le RGPD évoque :<br><br>- « a) la pseudonymisation et le chiffrement des données à caractère personnel ». |
| **Mise en œuvre** | La mise en œuvre du chiffrement est préconisée par le RGPD, mais n'est pas une obligation en tant que tel.<br><br>1. En fonction de la sensibilité des données (à analyser avec le responsable du traitement), déploiement d'une solution de chiffrement. |

## 4.2. PRÉREQUIS N°2 CONDITIONS D'ACCÈS AU PRODUIT

| | |
|---|---|
| **Référentiel RGPD** | **Considérant 57 RGPD** :<br>« *L'identification devrait comprendre l'identification numérique d'une personne concernée, par exemple au moyen d'un mécanisme d'authentification tel que les mêmes identifiants utilisés par la personne concernée pour se connecter au service en ligne proposé par le responsable du traitement* ». |
| **Mise en œuvre** | 1. Prévoir la création d'un identifiant unique qui est propre à chaque utilisateur (sauf exception justifiée de codes collectifs).<br>2. Mot de passe de 8 caractères minimum comprenant lettre + chiffre + symbole (il est naturellement possible de prévoir d'autres mots de passe plus complexes et/ou d'autres moyens d'authentification).<br>3. Prévoir une périodicité adaptée pour exiger un changement de mot de passe.<br>4. Empêcher la réutilisation du même mot de passe.<br>5. Obliger l'utilisateur à changer le mot de passe attribué par défaut, et bloquer le compte lorsque ce dernier n'a pas été modifié.<br>6. Limiter le nombre de tentatives d'accès, en bloquant par exemple après 3 tentatives infructueuses.<br><br>La CNIL propose un outil (« PHRASE2PASSE » pour aider les utilisateurs à trouver un mot de passe le plus sécurisé possible : https://www.cnil.fr/fr/generer-un-mot-de-passe-solide ). Il faudrait donc proposer à l'utilisateur le lien pour l'assister afin d'éviter en amont les failles. |

### 4.3. PRÉREQUIS N°3 ACCÈS AUX JOURNAUX D'HISTORISATION

| | |
|---|---|
| **Référentiel RGPD** | **Art. 5 f) RGPD** : Traitement garantissant la sécurité des données, protection contre le traitement illicite et la perte. |
| **Mise en œuvre** | 1. Limiter et tracer l'accès aux journaux d'historisation. |

### 4.4. PRÉREQUIS N°4 – GESTION DES EXTRACTIONS EN MASSE

| | |
|---|---|
| **Référentiel RGPD** | **Art. 5 f) RGPD** : Traitement garantissant la sécurité des données, protection contre le traitement illicite et la perte. |
| **Mise en œuvre** | 1. Impossibilité de procéder à des extractions ou des exports en masse.<br>2. Alerte sur une extraction ou export de données en masse. |

## 4.5. PRÉREQUIS N°5 – SÉCURITÉ DU CODE

| | |
|---|---|
| **Référentiel RGPD** | **Art. 32 1. RGPD** :<br>« (…) *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (…)* » |
| **Mise en œuvre** | 1. Audit de sécurité sur le code du produit. |

## 4.6. PRÉREQUIS N°6 ABSENCE DE BACK DOOR

| | |
|---|---|
| **Référentiel RGPD** | **Considérant 39 RGPD** (dernière phrase) :<br>*« Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement. »*. |
| **Mise en œuvre** | 1. Interdiction d'intégrer et de livrer un produit comportant une back door ou un moyen d'accès sans en aviser préalablement le client. |

## 4.7. PRÉREQUIS N°7 – GESTION DES FAILLES DE SÉCURITÉ

| | |
|---|---|
| **Référentiel RGPD** | Obligation de sécurité du RGPD |
| **Mise en œuvre** | 1. Possibilité de passer des patchs de sécurité sans procéder à une nouvelle installation ni risquer d'affecter les données. |

## ANNEXE N°13 – MODÈLE DE CONTRAT DE RESPONSABILITÉ CONJOINTE[69]

ENTRE

—

**L'UNIVERSITÉ [nom de l'établissement ESR]**
[Forme sociale], dont le siège est situé [ ], prise en la personne de son Président Monsieur [ ], né(e) le [ ], à [ ] de nationalité [ ], demeurant [ ]

—

***Ci-après désigné « [nom de l'établissement ESR] »***

ET

—

**[NOM DU COCONTRACTANT]**

[Forme sociale] au capital de [ ], dont le siège social est situé [ ], inscrite au RCS de [ ], sous le numéro [ ], prise en la personne de son Président Monsieur [ ], né(e) le [ ], à [ ] de nationalité [ ], demeurant [ ]

—

***Ci-après désignée « [Nom de la partie 2] »***

—

***Ci-après désignés ensemble les « Parties »***

[69] Le présent modèle doit impérativement être personnalisé en fonction du rapport entretenu entre les parties en situation de responsabilité conjointe, car elles disposent de la liberté de se répartir les obligations qui s'imposent au responsable de traitement en s'assujettissant à certaines obligations seule ou de façon conjointe.

## 1. PRÉAMBULE

Dans le cadre de leurs missions, les Parties collectent et traitent des données à caractère personnel et déterminent conjointement les finalités et les moyens du/des traitement(s) mis en œuvre [ne pas hésiter à développer pour contextualiser le rapport de responsabilité conjointe].

En conséquence, les Parties sont conjointement responsables des traitements effectués dans le cadre de l'activité de la commune au sens de l'article 26 du 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 (ci-après le « RGPD »).

À ce titre, les Parties se sont rapprochées pour définir de manière transparente leurs obligations respectives en ce qui concerne l'exercice des droits des personnes concernées ainsi que leurs obligations respectives quant à la communication des informations à fournir aux personnes concernées.

## 2. OBJET DU CONTRAT

L'objet du contrat de responsabilité conjointe est de définir de manière transparente les obligations respectives des Parties en ce qui concerne l'exercice des droits des personnes concernées et la communication des informations à fournir aux personnes concernées dans le cadre des missions exercées par [nom de l'établissement ESR].

## 3. DURÉE DU CONTRAT

Le contrat entre en vigueur à compter de sa date de signature et reste en vigueur tant que les Parties poursuivent les missions pour lesquelles elles agissent réciproquement l'une aux côtés de l'autre [ne pas hésiter à développer pour contextualiser le rapport de responsabilité conjointe et la durée de conservation subséquente].

## 4. FINALITÉS DES TRAITEMENTS

### 4.1. PRINCIPE

Les Parties déterminent conjointement les finalités du traitement qui doivent être déterminées, explicites et légitimes.

Les données ne peuvent être traitées ultérieurement d'une manière incompatible avec les finalités déterminées conjointement par les Parties.

Un traitement effectué ultérieurement à des fins statistiques, à des fins de recherches historiques et scientifiques ou à des fins archivistiques dans l'intérêt public n'est pas considéré comme étant incompatible avec les finalités initiales.

### 4.2. DÉCISION CONJOINTE

Un nouveau traitement impliquant chacune des Parties ne peut être mis en œuvre sans avoir préalablement bénéficié de l'accord des deux parties.

En conséquence, si l'une ou l'autre des parties souhaite mettre en en œuvre un nouveau service impliquant un traitement de données à caractère personnel, il est nécessaire d'en informer préalablement l'autre partie afin d'obtenir son accord, cette communication pouvant intervenir par tous moyens.

## 5. MOYENS DES TRAITEMENTS

Les Parties déterminent conjointement les moyens techniques utilisés dans le cadre du traitement.

Les principaux moyens techniques du traitement sont : [à compléter][71].

## 6. DONNÉES À CARACTÈRE PERSONNEL TRAITÉES

La liste des données utilisées dans le cadre des traitements doit nécessairement répondre à l'exigence de minimisation, cette exigence étant assurée grâce à un effort conjoint des Parties, lesquelles arrêtent, d'un commun accord, la liste des données utilisées dans le cadre du traitement.

## 7. OPÉRATIONS DE TRAITEMENT

Les Parties se partagent les opérations des traitements qu'ils mettent conjointement en œuvre.

[nom de l'établissement ESR] est principalement en charge de [à compléter].

[Nom de la partie 2] est principalement en charge de [à compléter].

## 8. DURÉE DE CONSERVATION

Les Parties ne peuvent conserver des données à caractère personnel que pendant la durée nécessaire au traitement.

La politique de durée de conservation des données à caractère personnel est définie par [Nom de la partie 2] qui doit nécessairement en informer préalablement [nom de l'établissement ESR], accompagné d'une justification, de préférence, juridique et légale.

À l'expiration du délai ou lorsque le traitement n'est plus mis en œuvre, les Parties doivent, d'un commun accord, soit effacer soit anonymiser les données.

## 9. INFORMATION DES PERSONNES CONCERNÉES

Les Parties doivent informer la personne concernée de ses droits d'une façon concise, transparente, compréhensible et aisément accessible.

Les informations relatives aux droits des personnes concernées sont transmises à ces derniers par écrit ou par tout autre moyen y compris, lorsque cela est approprié, par email.

En conséquence, chacune des Parties publie une « politique » d'utilisation des données à destination des personnes concernées avec lesquelles elles sont en contact :

- une politique d'utilisation de données des étudiants et candidats pour [nom de l'établissement ESR] ;
- une politique d'utilisation des données des salariés pour [Nom de la partie 2].

En outre, afin de satisfaire aux obligations d'informations prévues par le RGPD et notamment à son article 26 point 2), des grandes lignes du présent contrat devront être mises à disposition des personnes concernées par chacune des parties.

## 10. DROIT DES PERSONNES CONCERNÉES

### 10.1. DROIT D'ACCES

Toute personne concernée a la possibilité d'obtenir soit de la part de l'une ou l'autre des Parties la confirmation que des données la concernant sont ou ne sont pas traitées.

À compter de la réception de la demande par l'une des Parties, l'autre Partie doit impérativement en être informée dans les plus brefs délais.

Dans l'hypothèse où des données sont effectivement collectées, les Parties doivent se concerter afin d'être en capacité de fournir à la personne concernée les informations suivantes :

- les finalités du traitement ;
- les catégories de données concernées par le ou les traitements ;
- les destinataires ou catégories de destinataires auxquels les données ont été communiquées
- si cela est possible, la durée de conservation des données envisagée ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée ;
- l'existence de la possibilité pour la personne concernée d'exercer ses droits ;
- le droit d'introduire une réclamation auprès de la CNIL ;
- si les données ne sont pas collectées par l'une ou l'autre des Parties, toute information quant à leur source ;
- si les données sont transférées en dehors de l'Union européenne, des garanties appropriées relatives au transfert.

En outre, les Parties doivent également fournir à la personne concernée, dans le cadre du droit d'accès, une copie des données le concernant faisant l'objet d'un traitement.

Toute demande d'une copie supplémentaire peut faire l'objet d'une facturation par l'une ou l'autre des Parties à la personne concernée à un montant correspondant aux coûts administratifs de la demande.

Il est recommandé de répondre aux demandes des personnes concernées dans un délai de 30 jours ouvrables.

La partie ayant reçu la demande de la part de la personne concernée demeure l'interlocuteur de la personne concernée et reste en charge de la réponse.

La réponse est fournie sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement.

### 10.2. DROIT DE RECTIFICATION

La personne concernée a le droit d'obtenir de [Nom de la partie 2], dans les meilleurs délais, la rectification de ses données qui seraient inexactes.

À compter de la réception de la demande, [Nom de la partie 2] doit vérifier que les données en sa possession relatives à la personne concernée sont exactes et tenues à jour.

Pour cela, [Nom de la partie 2] peut demander des informations complémentaires auprès de la personne concernée.

Dans l'hypothèse où les données ne seraient pas exactes ou tenues à jour, [Nom de la partie 2] doit compléter les données de la personne concernée qu'elle détient avec les nouvelles informations en sa possession.

En cas de doute, [Nom de la partie 2] peut demander confirmation directement auprès de la personne concernée.

La rectification doit intervenir dans un délai maximum de 15 jours ouvrables.

La personne concernée est informée par la commune de l'accomplissement de l'opération.

### 10.3. DROIT D'EFFACEMENT

Toute personne concernée a le droit d'obtenir auprès de l'une ou l'autre des Parties l'effacement, dans les meilleurs délais, des données le concernant.

Pour ce faire, les Parties doivent, à compter de la réception de la demande, s'informer respectivement de la demande et se communiquent les données concernant la personne concernée en leur possession.

Ensuite, les parties doivent, dans un premier temps, vérifier que les données objet de la demande sont effectivement soumises au droit à l'effacement.

En effet, le droit à l'effacement peut être refusé par les Parties lorsque le traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont sont investis les Parties ;
- pour des motifs d'intérêt public dans le domaine de la santé publique ;
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
- à la constatation, à l'exercice ou à la défense des droits en justice.

Si les données n'entrent pas dans ces exceptions alors les communes doivent, dans un second temps, vérifier si :

- les données ne sont plus nécessaires au regard des finalités pour lesquelles les données ont été collectées ou traitées ;
- la personne concernée a retiré son consentement au traitement ;
- la personne concernée s'est opposé au traitement ;
- les données ont fait l'objet d'un traitement illicite ;
- les données doivent être effacées pour respecter une obligation légale.

Si toutes les conditions sont remplies, les Parties ont l'obligation d'effacer les données de la personne concernée dans un délai de 15 jours ouvrables.

Chacune des parties fait son affaire de la suppression des données qu'elle détient, une partie ne pouvant être responsable du manquement de l'autre partie.

La personne concernée est informée par la partie saisie de l'accomplissement de l'opération.

### 10.4. DROIT À LA PORTABILITÉ

Les personnes concernées ont le droit de recevoir de la part de l'une ou l'autre des Parties les données les concernant dans un format structuré, couramment utilisé et lisible par machine et, ont le droit de transmettre ces données vers un autre responsable de traitement.

En cas de demande, les Parties doivent se concerter pour, dans un premier temps, vérifier que la personne concernée peut effectivement exercer son droit à la portabilité.

En effet, le droit à la portabilité peut être refusé par l'une ou l'autre des Parties lorsque le traitement est nécessaire à l'exercice d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont sont investis les Parties.

Si la personne concernée bénéficie d'un droit à la portabilité, les parties doivent, dans un second temps, se réunir pour recueillir l'ensemble des données relatives à la personne concernée et l'intégrer dans un format accessible par tous (CD-Rom ou transfert dématérialisé).

La portabilité doit intervenir dans un délai maximum de 30 jours ouvrables.

## 11. MESURES DE SÉCURITÉ

### 11.1. [NOM DE L'ÉTABLISSEMENT ESR]

[nom de l'établissement ESR] est en charge des mesures de sécurité de l'infrastructure système, réseau et des logiciels métiers (ex : traçabilité, chiffrement, pseudonymisation) de la commune ainsi que de leur maintenance et du stockage des données.

[nom de l'établissement ESR] est donc en charge à la fois de la sécurité numérique des infrastructures (mise à jour de logiciel, anti-virus, etc.) et de la sécurité physique de ces infrastructures (habilitation des accès aux serveurs, vidéo-surveillance, etc.).

### 11.2. [NOM DE LA PARTIE 2]

[Nom de la partie 2] est en charge des mesures de sécurité relatives à ses agents et notamment de la sécurité des postes et terminaux mis à la disposition des agents (ex : logiciel malveillant, modification et complexité des mots de passe, fermeture de compte des agents, etc.).

[Nom de la partie 2] doit veiller à ce que les agents respectent la charte des systèmes d'information qui leur est fournie et notamment doit veiller à ce que les agents utilisent les moyens techniques mis à leur disposition uniquement dans le cadre du travail et ne télécharge pas de logiciels ou données non-autorisés.

[Nom de la partie 2] est également en charge de la sécurité de ses locaux et de l'accès aux systèmes d'information situés dans ses locaux (ex : badge, vidéo-surveillance, etc.).

[nom de l'établissement ESR] peut notamment prévoir des audits de sécurité de [Nom de la partie 2] à tout moment.

## 12. COOPÉRATION AVEC LA CNIL

La Cnil peut effectuer des contrôles auprès de l'une ou l'autre des Parties. Dans le cas d'un contrôle, les parties doivent s'informer réciproquement des informations demandées par la Cnil et, le cas échéant, des réponses apportées.

Les Parties doivent se concerter afin de fournir l'ensemble des informations et documents demandées par la Cnil.

Les réponses seront apportées par chacune des parties en fonction des demandes de la Cnil.

En tout état de cause, la partie auditée communique à la Cnil le présent contrat.

## 13. REGISTRE

Si chacune des parties met en place un registre du traitement, tout traitement effectué conjointement par les Parties devra être intégré dans ledit registre.

Dans le cas où les parties mettent en œuvre un registre du traitement, la liste des traitements faisant l'objet d'un traitement conjoint par les Parties est établie en annexe.

La liste établie en annexe à vocation à évoluer et peut être librement modifiée sans qu'il soit nécessaire de conclure un avenant.

## 14. VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

Lorsqu'une Partie constate une violation des données à caractère personnel, elle doit en informer immédiatement l'autre Partie.

À la suite de la notification à l'autre Partie, les deux Parties doivent se concerter afin de limiter au maximum la propagation de la violation mais également afin d'évaluer la situation.

[nom de l'établissement ESR] peut proposer des mesures visant à remédier à la violation ou, le cas échéant, à atténuer les éventuelles conséquences négatives. En cas d'accord avec [Nom de la partie 2], les mesures doivent être mises en œuvre immédiatement.

À ce moment, les Parties doivent recueillir l'ensemble des informations devant être fournies à la Cnil et les communiquer entre elles réciproquement.

En outre, les Parties doivent décider, en fonction de la situation, qui sera en charge de la communication externe concernant la violation des données et, en tout état de cause, qui sera l'interlocuteur de la Cnil dans le cadre de la violation.

Lorsque les parties se sont mises d'accord, la partie en charge de la communication doit notifier cette violation à la Cnil dans les meilleurs délais et, si possible 72 heures au plus tard après en avoir pris connaissance.

Lorsque la notification à la Cnil n'a pas eu lieu dans les 72 heures, il est nécessaire que la notification soit accompagnée des motifs de retard.

La notification doit au minimum :

- décrire la nature de la violation de données y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- décrire les conséquences probables de la violation de données ;
- décrire les mesures prises ou que les Parties proposent de prendre pour remédier à la violation de données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si ces informations ne peuvent être délivrées en une seule fois dans le délai de 72 heures, elles peuvent néanmoins être communiquées de manière échelonnée sans autre retard indu.

La Partie désignée pour la communication externe doit, avec l'aide de l'autre Partie, réaliser un rapport documenté résumant l'ensemble de ces informations (faits, effets, mesures prises) afin de permettre à la Cnil de vérifier la conformité des parties à cette obligation.

En outre, lorsqu'une violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, la partie désignée communique la violation des données aux personnes concernées dans les meilleurs délais.

Pour ce faire, les parties se concertent afin de déterminer si la violation et les conditions d'un risque élevé sont réunies.

Si tel est le cas, la partie désignée devra notifier la violation à la personne concernée dans les 36 heures après avoir informé la Cnil de ladite violation.

En cas de doute sur le degré de risque, la partie en charge de la communication externe doit saisir la Cnil pour obtenir son assistance sur le sujet.

Si les parties n'ont aucun doute quant au degré de risque alors la communication de la notification doit intervenir en des termes clairs et simples, et doit contenir les informations suivantes :

- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- les conséquences probables de la violation de données ;

- les mesures prises ou que l'une ou l'autre des Parties propose de prendre pour remédier à la violation de données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

En revanche, la communication à la personne concernée n'est pas nécessaire lorsque :

- les Parties ont mis en œuvre les mesures de protection techniques et organisationnelles appropriées et que ces mesures ont été appliquées aux données affectées par la violation, en particulier lorsqu'est mis en œuvre une mesure rendant les données incompréhensibles pour toute personne non autorisée (ex : chiffrement) ;
- les Parties ont pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes n'est plus susceptible de se matérialiser ;
- la communication de la violation exigerait des efforts disproportionnées l'une ou l'autre des Parties (ex : coût trop élevé). Pour y remédier, les Parties doivent se concerter pour publier un communiqué de presse commun permettant aux personnes concernées d'être informées de manière tout aussi efficace.

## 15. TRANSFERT DE DONNÉES

[nom de l'établissement ESR] peut, dans le cadre de ses prérogatives, transférer des données vers des prestataires en dehors de l'Union européenne à la condition d'en informer préalablement [Nom de la partie 2] qui peut émettre des interrogations dans un délai de 15 jours à compter de la notification.

En cas d'interrogation de la part de [Nom de la partie 2], [nom de l'établissement ESR] doit répondre aux demandes d'information soulevées par la commune dans un délai raisonnable.

## 16. SOUS-TRAITANCE

[nom de l'établissement ESR] peut, dans le cadre de ses prérogatives, faire appel à des prestataires externes à la condition d'en informer préalablement la commune qui peut émettre des interrogations dans un délai de 15 jours à compter de la notification.

En cas d'interrogation de la part de [Nom de la partie 2], [nom de l'établissement ESR] doit répondre aux demandes d'information soulevées par la commune dans un délai raisonnable.

## 17. POINT DE CONTACTS

Les Parties peuvent être contactées par les personnes concernées pour toutes informations sur le traitement conjoint de leurs données aux coordonnées suivantes :

- Pour [nom de l'établissement ESR]: (CONTACT)
- Pour [Nom de la partie 2] : (CONTACT)

## 18. DOMICILATION

Pour l'exécution de la présente convention et sauf dispositions particulières, les Parties conviennent de s'adresser toute correspondance à leur siège social respectif.

## 19. LOI APPLICABLE ET JURIDICTION

Le présent contrat est régi par la loi française.

EN CAS DE LITIGE, COMPÉTENCE EXPRESSE EST ATTRIBUÉE AUX TRIBUNAUX COMPÉTENTS DU RESSORT DE LA COUR D'APPEL DE PARIS, NONOBSTANT PLURALITÉ DE DÉFENDEURS OU APPEL EN GARANTIE.

Fait à :

En deux exemplaires originaux.

| | |
|---|---|
| Pour [nom de l'établissement ESR] | Pour [Nom de la partie 2] |
| Nom | Nom |
| Qualité | Qualité |
| Date | Date |
| Signature | Signature |

## ANNEXE N°14 – CLAUSE D'INSCRIPTION A UNE NEWSLETTER

□ En cochant cette case, vous consentez à recevoir notre newsletter et vous reconnaissez avoir pris connaissance de notre Politique de protection des données personnelles accessibles ici (insérer un lien de renvoi vers la politique).

Vous êtes informé du fait que vous disposez du droit de vous désinscrire à tout moment de la présente newsletter grâce au lien de désinscription présent dans chaque newsletter que vous recevez.