Contribution

aux lignes directrices 07/2020 sur les concepts de
responsable de traitement et sous-traitant selon le RGPD

Le réseau SupDPO est le réseau national français des délégués à la protection des données (DPD-DPO) de l'enseignement supérieur, de la recherche et de l'innovation. Il est, à ce titre, partie à une convention renouvelée avec la Conférence des Présidents d'université (CPU) et la Commission nationale de l'informatique et des libertés (CNIL) et est désigné comme « tête de réseau » pour l'autorité de protection des données (APD) française[1].

Dans le cadre de ses travaux, le réseau SupDPO s'est saisi de diverses questions relatives à la sous-traitance et aux relations entre les acteurs d'un traitement de données, en particulier celle liée à l'intervention des partenaires privés dans la sphère de la mission d'intérêt public telle que déclinée dans le cadre des législations nationales et en particulier le Code de l'éducation français. Une demande de conseil auprès de la CNIL, basée sur une pré-instruction de plusieurs DPO, a été adressée le 16 janvier 2020 à l'ADP et s'intéresse plus particulièrement aux organismes de certification de langues. Cette demande concluait que le rapport entretenu avec les certificateurs de langue conduisait à un risque important de perte de maîtrise des données des populations liées à l'enseignement supérieur.

La présente contribution de SupDPO vise à faire part des éléments principaux de cette analyse pour préciser, le cas échéant, le projet de lignes directrices proposées par le Comité européen de la protection des données (CEPD).

En vue de la délivrance de certifications en langue à leurs étudiants, les établissements d'enseignement supérieur contractualisent avec des prestataires. Ces conventions, souvent imposées par lesdits prestataires sans marge de négociation, ne règlent pas les responsabilités des acteurs de manière satisfaisante, et peuvent prévoir des réexploitations des données traitées par le certificateur, le plus souvent acteur économique privé, qui s'arroge alors une qualification de responsable de traitement et de « propriétaire des données » pour l'ensemble des traitements concernés (certification objet de la convention, puis réexploitation des données à des fins commerciales).

A la lecture de votre projet de lignes directrices, **la relation entre les organismes certificateurs et l'enseignement supérieur pourrait, de notre point de vue, faire l'objet d'un éclairage distinct, ainsi que de cas d'usages et d'exemples précis afin de sécuriser les données des étudiants** européens et particulièrement ceux qui, selon leur droit applicable, peuvent rattacher l'objet de la convention à leurs missions[2] :

[1] http://www.cpu.fr/actualite/la-cnil-et-la-conference-des-presidents-duniversite-cpu-renouvellent-leur-convention-de-partenariat/
[2] Considérant 118, Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

- « 22. (…) *rather than directly appointing the controller or setting out the criteria for its appointment, the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task* ».

La jurisprudence Puškár[3] lie finalité et base légale. Le contrôleur européen à la protection des données, dans sa recommandation du 7 novembre 2019[4], estime que lorsque les moyens et les finalités du traitement sont basés sur une compétence particulière (explicite ou implicite) dévolue par la loi, l'organisme en charge est responsable de traitement.

En droit français, l'arrêté du 30 juillet 2018[5] relatif au diplôme national de licence par exemple a été modifié par l'arrêté du 3 avril 2020[6] relatif à la certification en langue anglaise. Cet arrêté impose une certification à tous les candidats inscrits aux diplômes nationaux de licence, de licence professionnelle et au diplôme universitaire de technologie : « *Pour certains parcours de formation, les établissements peuvent conditionner l'obtention du diplôme à un niveau minimum de certification. Cette certification concerne au moins la langue anglaise ; dans ce cas, elle fait l'objet d'une évaluation externe et est reconnue au niveau international et par le monde socio-économique. La justification de la présentation à cette certification conditionne la délivrance du diplôme* ».

Ces certifications sont donc selon la loi incluses dans le cursus des étudiants, intégrées dans les maquettes pédagogiques et leur obtention conditionne la diplomation.

- « *79. Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28 (10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions* ».

Dans ces conditions, les établissements d'enseignement supérieur paraissent effectivement responsables de traitement, les prestataires agissant uniquement sur leurs réquisitions (article 28 du Règlement général sur la protection des données RGPD). Ces derniers ne peuvent alors traiter les données au-delà du cadre initialement fixé.

Certains organismes certificateurs prévoient des dispositions exactement contraires à ces garanties en imposant contractuellement à l'établissement le principe d'une réutilisation des données estudiantines pour promouvoir ses activités de certificateur.

Il nous paraît donc effectivement indispensable de rappeler l'interdiction de réutilisation des données à d'autres fins, notamment lorsque les données étaient initialement traitées sur la base d'une obligation légale ou de l'exercice d'une mission d'intérêt public.

---

[3] http://curia.europa.eu

[4] https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

[5] Article 10 alinéas 1 et 2 *« Les modalités de contrôle des connaissances et des compétences (…) peuvent, sous la responsabilité des équipes pédagogiques, être adaptées (…) »*

[6] Arrêté du 3 avril 2020 relatif à la certification en langue anglaise pour les candidats inscrits aux diplômes nationaux de licence, de licence professionnelle et au diplôme universitaire de technologie

- « *164. (…) Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data* ».

  Il nous paraît aussi effectivement indispensable de rappeler cette interdiction de réutilisation des données à d'autres fins, notamment lorsque les données étaient initialement traitées sur la base d'une obligation légale ou de l'exercice d'une mission d'intérêt public, même dans l'éventualité où une responsabilité conjointe pourrait être retenue.

- « *65. Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities* ».

- « *66. (…) The use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing)* ».

- « *Example: Independent controllers when using a shared infrastructure* ».

  L'avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant » du groupe de travail « article 29 » sur la protection des données précisait qu' « *en cas de doute, d'autres éléments que les clauses d'un contrat peuvent servir à identifier le responsable du traitement, tel que le degré de contrôle réel exercé par une partie, l'image donnée aux personnes concernées et les attentes raisonnables que cette visibilité peut susciter chez ces dernières (…). Cette catégorie est particulièrement importante puisqu'elle permet d'examiner les responsabilités et de les attribuer également en cas de comportement illicite consistant à traiter des données contre les intérêts et la volonté de certaines des parties* ».

  Il semble nécessaire de rappeler de tels éléments d'appréciation dans les nouvelles lignes directrices.

  Toutefois, il convient de noter que l'existence de quasi-monopole ou de situations privilégiées de certains opérateurs dans les certifications de certaines langues, qui proposent la même infrastructure pour leurs activités de B2C et B2B, tendra potentiellement à identifier des situations de responsabilité conjointe entre l'établissement universitaire qui souhaite permettre la certification de ses étudiants, et le prestataire administrateur de la plateforme au sein de laquelle les données sont traitées.

  Dans cette hypothèse, il conviendrait de rappeler qu'une responsabilité conjointe ne confère pas aux responsables de traitement le droit de traiter les données des personnes sans préalablement avoir respecté leurs droits (tel que leur consentement et/ou leur information) et que des responsables conjoints ne peuvent contractuellement consentir pour les personnes à des traitements de données manifestement excessifs et contraire à leur intérêt.

Comments

on the Guidelines 07/2020 on the concepts
of controller and processor in the GDPR.

SupDPO is the French national association of data protection officers (DPO) in higher education, research and innovation. As such, it is party to a renewed agreement with the Conference of University Presidents (CPU) and the National Commission for Informatics and Liberties (CNIL) and is designated as the "network head" for the french Data Protection Authority (DPA).

As part of its work, SupDPO has taken up various questions relating to processing and the relations between the actors of data processing, in particular that related to the intervention of private partners in the sphere of the public interest mission as defined within the framework of national legislation and in particular the french Education Code. A request for advice has been sent to CNIL, based on a pre-instruction from several DPOs, on January 16, 2020 and is particularly interested in language certification bodies. This request concluded that the relationship maintained with the language certifiers led to a significant risk of loss of control over the data of populations linked to higher education.

This SupDPO contribution aims to enlight the main elements of this analysis to specify, when useful, the draft guidelines proposed by the European Data Protection Board (EDPB).

In order to issue language certifications to their students, higher education institutions enter into contracts with service providers. These agreements, often imposed by service providers without any room for negotiation, do not settle the responsibilities of actors in a satisfactory manner, and may provide for re-use of the data processed by the certifier, most often a private economic actor, who then arrogates to himself a qualification of data controller and "owner of data" for all the processing operations concerned (certification covered by the agreement, then re-use of the data for commercial purposes).

On reading your draft guidelines, the relationship between certification bodies and higher education could, from our point of view, be the subject of a separate enlightment, as well as use cases and precise examples, in order to secure the data of European students and particularly those who, according to their applicable law, may relate the subject of the agreement to their missions:

> - « 22. (…) *rather than directly appointing the controller or setting out the criteria for its appointment, the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task* ».

The Puškár case links purpose and legal basis. The European Data Protection Supervisor (EDPS), in his recommendation of November 7, 2019, considers that when the means and purposes of processing are based on a particular competence (explicit or implicit) devolved by law, the body in charge is the controller.

In French law, the decree of July 30, 2018 relating to the national "license" diploma (Bachelor's degree), for example, was amended by the decree of April 3, 2020 relating to certification in the English language. This decree imposes certification on all candidates registered for the national license, professional license and university diploma in technology: "*For certain training courses, establishments may make obtaining the diploma subject to a minimum level of certification. This certification concerns at least the English language; in this case, it is subject to an external evaluation and is recognized internationally and by the socio-economic world. The justification of the presentation for this certification conditions the delivery of the diploma*".

These certifications are therefore by law included in the students' curriculum, integrated into the educational models and their achievement is a condition for graduation.

- « *79. Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28 (10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions* ».

  Under these conditions, higher education establishments appear to be effectively data controllers, with service providers acting only on their requisitions (article 28 of the General Data Protection Regulation GDPR). Those providers cannot then process the data beyond the framework initially set.

  Some certification bodies have standard contract that stand exactly contrary to these guarantees by contractually imposing on the establishment the principle of reuse of student data to promote its activities as certification body.

  We therefore believe it is essential to recall the prohibition on re-use of data for other purposes, in particular when the data were initially processed on the basis of a legal obligation or the exercise of a public interest mission.

- « *164. (…) Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data* ».

  We also believe it is essential to recall this ban on the reuse of data for other purposes, in particular when the data were initially processed on the basis of a legal obligation or the exercise of a public interest mission, even in the event that joint controllership could be retained.

- « *65. Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities* ».

- « *66. (…) The use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing)* ».

- « *Example: Independent controllers when using a shared infrastructure* ».

  It seems necessary to recall such considerations in the new guidelines.

  However, it should be noted that the existence of an almost monopoly or privileged situations of some operators in the certifications of certain languages, which offer the same infrastructure for their B2C and B2B activities, will potentially tend to identify situations of joint controllership between the university which wishes to allow the certification of its students, and the service provider administrator of the platform within which the data is processed.

  In this case, it should be remembered that joint controllership does not give data controllers the right to process personal data without first having respected their rights (such as their consent and/or information) and that joint controllers cannot contractually consent for individuals to data processing that is manifestly excessive and contrary to their interests.