□1

t

CNPD

National Data Protection Commission

RESOLUTION/2021/622

I. Report

1. The National Data Protection Commission (CNPD) received a participation against

regarding the use of the "Respondus Lockdown Browser" and "Respondus Meritor" applications to carry out the remote assessment of students.

2. The use of such technological tools is provided for in a Rector's Dispatch

paia v gorar in the scões of the apprenticeships to the distsnes rno school 2020/2021,

thus imposing a rapid analysis of the case by the CNPD, in order to be able to adopt a decision in good time, that is, before the beginning of the evaluations, giving effectiveness to its action.

3. Since there is only the decision of the iH to use briefly the "Respondus" applications, as these are not yet fully operational, the CNPD essentially based its analysis on the compliance of the data processing carried out through these applications with the RGPD, in the conditions of use and technical description of each of the applications, in the contractual terms of their licensing, in the guidelines given by the Rector's Dispatch, in the impact assessment on data protection (AIPD) carried out by^|and in the information made available to students on the website of ^^^^^|

II. facts

4. The Dean of the ^Birooffered the Dispatch'

At the

Considering, among others, the CNPD guidelines, of April 8, 2020, on the use of technologies to support distance learning1 and the conclusions of the Respondus impact assessment study carried out by the person in charge of

1 https://www.cnpd.pt/media/1encswse/orientacoesjecnologias.de.suporte_ao_ensino_a.distancia.pdf

T (+351) 213 928 400

F (+351) 213 6/9 832

geral@cnpd.pt

www.cnpd.pt

r

8. As described in the AIPD, the assessment system analyzed is composed of two components: a specific Internet browser, the "Respondus Lockdown Browser" (BLR), which prevents students from using other applications on their computer while taking the exam , and a surveillance system that records student behavior during the exam, the "Respondus Monitor".

9. These applications were created and developed by Respondus, Inc.", a company that provides technology and software services for the educational area, particularly in the field of online tests or exams, based in the United States of America.

10. When contracting the service with Respondus, Inc., the entity, in this case, is

licensed to use the subscribed applications, that is, the BLR and the supplementary application “Respondus Monitor”. This licensing agreement includes a data processing agreement (Data Processing Agreement - DPA2), effective as of August 2020, between the licensed institution and Respondus, Inc., according to which it is acknowledged that the licensed institution is responsible for the processing of [student] data and that Respondus, Inc. is the processor that processes the personal data on behalf of the controller and under documented instructions.

11. Regarding the operation of specific applications, the BLR application is a product that can be integrated with various learning management systems (LMS3) already existing in institutions (eg Moodle), through which teachers design and provide proof of evaluation.

12. In order to access the test, the student installs the BLR application, which contains its own browser (òrowser), which blocks access to other Internet pages and any other areas or resources of the device used by the student. , until the exam is finally submitted (the computer is in "kiosk" mode).

two

3

Leaming Management System

0

two

r

CNPD

National Data Protection Commission

13. According to the official description of the product4, the proof is displayed in full-screen mode, without it being possible to minimize the respective browser.

14. The menu as well as other browser options are disabled (with the exception of: rewind; forward; refresh; stop) and the following options are inhibited: printing; screenshot; 'copy' and/or 'paste'; right mouse button; hotkeys; run the task manager; access to messaging applications, screen sharing, remote connection and even running in a virtual environment.

15. As for the "Respondus Monitor" application, it is presented as a leading product in automated surveillance (“proctoring”), preventing fraud in carrying out an exam, through the use of a video camera (webcam) and industry-leading video".

16. Still checking the official website of this application5, it is possible to establish a sequence of operations prior to carrying out the evaluation, namely:

The. Webcam check - verification of the student's audio and video conditions;

B. Additional Instructions - instructions for carrying out the test;

ç. Guidelines + Tips - previous instructions;

d. Student Photo - asks the student to fit in with the webcam capture area, to collect the photo;

and. Show ID - requests display of student identification and framing, with the capture area, for photographic collection;

f. Environment Check - the student films the surrounding area;

g. Facial Detection Check - student's facial detection, after which the assessment test begins.

17. The first and last options listed above are mandatory, and the verification of the remaining steps is defined by the teacher, when creating the test in the LMS system.

18. With the beginning of the test, the recording of the student's image through the webcam begins, a process that ends when the student finishes the test, through his submission.

4 How LockDown Browser Works", available at: https://web.respondus.com/he/lockdownbrowser/

5 How Respondus Monitor Works", available at: https://web.respondus.com/he/monitor/ and Video demo of pre-exam

operations: https://www.youtube.com/watch?v=7J1 K8- R20ao

Av. D. Carlos 1,134.1°

1200*651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

19. The "Respondus Monitor" analysis is performed every second, through three concurrent vectors:

The. use face detection, movement and lighting to analyze the student and the exam environment;

B. gathering information from the student's device (keyboard activity, mouse movements, hardware changes, etc.) for pattern identification;

ç. analysis of student interaction with the exam, including question-by-question comparison between students on the same exam, the response time spent on each question, or if the answer is changed.

20. The application in question records the student's activity, through video and sound. The sound capture can be disabled by the user and, in accordance with the guidelines set out in the Rector's Dispatch, it can only occur for interaction between the student and the teacher or for exceptional reasons that result in the indispensability of sound recording, through favorable ruling by the Pedagogical Council (cf. points 2 and 3 of the guidelines in Annex I). The system is not, however, configured so that, by default, there is no sound recording. In the absence of an action on the part of the student, sound is captured and recorded.

21. During an examination session, a wide variety of personal data is automatically processed. The webcam recording itself goes through an automated post-processing step that uses «facial detection and facial recognition technology6» to determine: if the student remained in the frame of the video; whether there were several people appearing in that frame; whether the person appearing in the video frame is the same person who started the exam; and qua the position of the user's face in relation to the video camera.

22. Additionally, “Respondus Monitor” tracks and monitors the applications and processes running on the examinee's computer during the assessment, including the quality of the Internet connection and the time and duration of connection drops.

23. Subsequently, a report is delivered to the teacher with the analysis of the evaluation session of each student, including a chronology of relevant events, being generated automatically, based on the

However, in additional clarifications requested by |

Respondus, it was stated that there is no processing of biometric data to identify the student (cf. contained in the AIPD).

representative of

CNPD

National Data Protection Commission

information collected, a value about the exam session to help the teacher to determine the risk of occurrence of violations7.

24. Under the terms of the specific use of this application for students8, students, in order to access "Respondus Monitor" to carry out the exams, are obliged to accept all the conditions imposed by the company, including the terms related to the processing of personal data, being advised that you use the application at your own risk, and you agree that Respondus, Inc. will not be responsible for the occurrence of any data breaches. In each access to the application, the student must individually accept these conditions of use.

25. As contractually provided for in the DPA, Respondus, Inc. processes personal data within the scope of the provision of the service, in the form of storage, on its servers, which are located outside the European Economic Area, the licensed institution recognizing that there is an international transfer of personal data, being therefore responsible for establishing the basis legal for such a transfer.

26. The Licensee further acknowledges under the DPA that Respondus, Inc. that host the licensed applications and the respective personal data processed, are controlled and operated by a (sub-)subcontractor, Amazon Web Services (AWS)9, giving its authorization for this purpose.

27. Also with regard to international data transfers, it is expressly stated in the terms of the contract that personal data are transferred to the United States of America to an entity certified under the Privacy Shield Principles or to a recipient under of standard contractual clauses approved by the European Commission. Attached to the contract is a data transfer contract for the US between the licensed institution, as a data exporter, and Respondus, Inc., as a data importer, still under Directive 95/46/EC ( Data Protection Directive).

28. As described in the contract between the controller and the processor, within the scope of the international transfer of data

to the USA, attached to the DPA, personal data of the following categories of data subjects are transferred: customer employees (in this case, the H); students enrolled at the client's institution.

8 Available at: https://web.respondus.com/tou-monitor-student/

9 See Annex 2 à$ contractual clauses for the international transfer of data to the USA.

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351 >213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

29. Also under the terms of the contractual clauses, the following categories of personal data are transferred: authentication data (username); identification data (first and last name); contact details (email-optional, in case of technical support request); unique ID numbers and signatures (Student ID card is optional depending on the operating requirement of the licensed institution); pseudonymized identifiers (student identification code assigned by the LMS, if applicable); photos, video and audio (video/audio recording of examinee; photograph of examinee is optional depending on license requirements); educational data (exam surveillance analysis: examination session analytical data); device identification (IP address).

30. Respondus, Inc. further reserves the right, at any time, to disclose any information or data retained, whether of the institution, the student or any other user (including recordings), to comply with the law, a regulation or a governmental request10.

31. In the institution-specific terms of use11 of the "Respondus Monitor" application, Respondus, Inc. It also collects personal data from students, through "random samples of video and/or audio recordings", with the purpose of improving the company's ability to provide services, and such data may be shared with researchers (including biometrics experts).

32. According to the description of the processing operations contained in the AIPD, a^B provides that the capture of an image of the surrounding environment, for the preservation of privacy, as well as, as a general rule, the capture (with the exceptions determined in the Annex to the Rector's order and described above in point 20). If a photograph of a student ID card is taken, it is expected to be the student card.

33. Bases the processing of personal data in the context of Respondus applications in pursuit of the legitimate interest of the person responsible, cf. Article 6(1)(f) of the GDPR, citing its legitimate interest in 'assessing student performance in a fair and equitable manner,

10 According to US surveillance legislation, in particular Section 702 of the FISA (Foreign Intelligence Surveillance Act), both the subcontractor Respondus, Inc., and the sub(subcontractor) AWS are companies that, by their activity, are directly subject to subpoenas from US authorities to give massive access to the personal data they have in their possession, custody or custody, being legally prohibited from informing their customers of such requests (as is expressly determined in the contractual clauses ).

11 httos://web.resoondus.com/tou-monitor-admin/

12 As stated in the

with respect to Respondus, Inc. applications.

CNPD

National Data Protection Commission

34. The documents that support the terms of use of "Respondus

Monitor" for institutions and the DPA.

35. In the impact assessment, the data processing in question is justified by the indispensability of carrying out distance assessment tests due to the pandemic situation, the danger of contagion, the significant number of displaced students, national and international (cf. point 4.1 of the IAPD).

36. The data protection officer agrees with the grounds of legitimacy invoked for the processing of data and sanctions the justification given for that purpose (cf. point 2.1 of his opinion on the IAPD).

37. The data protection officer concludes, in his opinion,

adequately protects the rights and freedoms of students". However, in point 3 of its opinion, it raises the question of whether, in the 'Respondus Monitor' surveillance system, "data on the student's behavior,

student consent has not been obtained.

38. The expected start date of treatment was|

the opinion of the person in charge of

data protection to the IAPD is dei

|and the date of approval of the AIPD by the Rector da^Hé de|

39. Exam season has not started yet, but Respondus applications have

are available on the ^^^^^l website, and their early installation is encouraged to allow students to test them and thus become familiar with how they work.

III. Right

40. The CNPD is competent under the terms of subparagraphs a) and h) of paragraph 1 of article 57 and also of paragraph 2 of article 58 of Regulation (EU) 2016/679, of 27 April 2016 - General Data Protection Regulation (GDPR), in conjunction with article 3, paragraph 2 of article 4, and subparagraph b) of paragraph 1 of article 6, all of the Law No. 58/2019, of August 8 - GDPR Enforcement Law.

41. The participated entity is responsible for the processing of personal data, within the meaning of point 7) of article 4 of the GDPR, since it defines the purpose of the treatment - surveillance of tests carried out at a distance, with the purpose of guaranteeing the its credibility and legitimacy - as well as the means to achieve this end - resorting to the combined use of the "Respondus Lockdown Browser" and 'Respondus Monitor" applications, through the

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

subcontracting services to the company "Respondus, Inc.", which acts as a subcontractor, within the meaning of Article 4(8) of the GDPR.

42. In addition to the CNPD guidelines of April 8, 2020, mentioned in the Rector's Order and generally intended for distance learning platforms, the CNPD issued, on May 21, 2020, specific guidelines aimed at higher education precisely in the context of remote assessments13.

43. First of all, it should be noted that, according to the rector's order, student assessments must be

made preferably through the institutional platform, the same on which the

distance teaching and learning activities and presumably assessments from the previous school year and the first semester of the current school year. It is left to the decision of each coordinator

identify the situations in which the use of Respondus applications will be imposed, given that no specific circumstances or weighty criteria justify the use of this second option.

44. This is a key issue for two reasons. On the one hand, the justification of the data processing associated with the use of the two Respondus applications,

it is limited to the need to carry out assessments remotely and with integrity (which the system is supposed to ensure ■■■■), and no concrete arguments are presented for the use of Respondus tools. Furthermore, since they are two different applications, and the "Respondus Lockdown Browser" can work by itself, there are no reasons to use the "Respondus Monitor" application, in addition to the BLR application. Therefore, from the point of view of the purpose of the data processing, it is not sufficiently specific and explicit, as required by Article 5(1)(b) of the GDPR, in order to provide predictability as to situations where, as an alternative to the institutional platform^^^^H, it will be necessary to use Respondus applications. In effect, this is a decision that is left to the discretion of the coordinators of the organic units, without specifying which criteria can be met to support such a decision. Thus, the use or not of those applications, which imply an increased processing of personal data and a high degree of intrusion on students' privacy, is not subject to objective, uniform and scrutable criteria. For that reason, it generates discrimination.

45. On the other hand, the lack of specificity of the aims in view and the absence of pre-defined criteria result in the inexistence of precise and homogeneous instructions for the entire University regarding the concrete application of the guidelines contained in the Rector's Dispatch to the various operations of the " Respondus Monitor", leaving a margin of discretion to each teacher, which may imply the processing of additional data, such as

13 Available at https://www.cnpd.pt/media/Omwfxdcp/orientacoes_avaliacao.distancia_ensino.superior.pdf.



the student's photograph and the student's photograph together with an identity card14 (cf. steps described in point 16, subparagraphs d) and e), of this determination). It follows that the principle of data minimization, recognized in article 5 ,

paragraph 1(c) of the GDPR is put in crisis.

46. As regards the lawfulness ground of data processing, on the basis of Article 6(1),

point f) of the GDPR, it is first of all important to point out that invoking the legitimate interest of the person in charge as a legal basis for the processing of data resulting from the use of Respondus applications is not an obvious path. This is because, although a public foundation subject to a regime of law

as defined in paragraphs 1 and 2 of article 9 and paragraph 1 of article 134 of the Legal Regime for Higher Education Institutions, approved by Law n.° 62/2007, of 10 September, this institution's mission is clearly to pursue the public interest, as paragraph 2 of article 134 of the same law underlines.

47. Thus, the interests invoked by the^^^^^^^^^^B are only the public interests legally established, in particular by the Legal Regime of Higher Education Institutions and, to that extent, it seems to be forbidden to invoke interests legitimate under Article 6(1)(f) of the GDPR, pursuant to the second subparagraph of that provision.

48. However, even if that were not the case, it would always have to be recognized that the requirements of Article 6(1)(f) of the GDPR are not met here.

49. First, even assuming an interest on the part of the controller to carry out remote assessments through a credible process that ensures the legitimacy of the evidence, this would always depend on demonstrating the impossibility of carrying out the assessment by any other means. (in person, or by other alternative means that do not involve the processing of personal data described above)15.

50. Furthermore, the pursuit of the legitimate interest of the person responsible could only be a condition of lawfulness of data processing, if the interests, rights and freedoms of the data subjects did not prevail. However, that weighting test was not carried out and, therefore, it was not demonstrated by the controller, as would be his obligation, in accordance with the combined provisions of Article 5(2) and Article

14 The AIPD suggests that it is the student card, but no concrete instructions on the matter were found.

15 Furthermore, in this case, the supervening reasons of an extraordinary nature that could lead to the use of a subsidiary system such as Respondus instead of the institutional platform that is presented as preferential are not advanced (cf. Despachn^^^^Bf, thus not allowing to evaluate properly the interests at stake.

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

24, paragraphs 1 and 2, of the GDPR, that the interest of the person responsible prevailed over the rights and freedoms of the holders

51. With regard to the considerations made in the IAPD regarding the rights and freedoms of the holders, in the sense that the intrusion on their privacy would be mitigated by the adoption of some measures, they clearly sin by default and did not take into account the full dimension and extent of the processing of personal data. So, let's see.

52. Although it is granted that there may be no processing of biometric data, within the meaning of Article 4(14) of the GDPR, relying on the clarifications provided by the company - despite the fact that in the contractual clauses it is mentioned that there is detection and "facial recognition" -, there is clearly the application of biometric patterns in the use of the mouse, keyboard or student's body movements, which are not transparent or resonate with the user, but which nevertheless contribute to the construction of a student's profile.

53. The granular level of monitoring and surveillance of the "Respondus Monitor" application actually allows intensive data collection in order to define, by fully automated means, a profile of the examinee, to which a value is assigned. And yet, an assessment was not made on the adequacy, necessity and proportionality of collecting so much personal data to achieve the general objective of credibility and integrity of the evidence. The choice and weighting of the parameters used for the definition of profiles are equally opaque, and it is not known what role they play, so it is not possible to ascertain their suitability for the purpose in view.

54. When data relating to student behavior is at stake and processed in an analytical context through algorithms, it can only be concluded that there is a treatment of special sensitivity. In the absence of due and demonstrated reasoning, the treatment in question proves to be unnecessary and excessive, in breach of the principle set out in Article 5(1)(c) of the GDPR16.

55. On the other hand, the fact that it is stated that there are no automated decisions, because the teacher, based on the "value" presented to him for each student, makes his decision, thus introducing the factor of human intervention, is not , by

itself, sufficient. Again, the absence of specific guidelines regarding the interpretation to be given to these values and the lack of guiding criteria for teachers to make coherent and transparent decisions can generate discrimination and allow the teacher to validate the automatic decision of the system. And the data subject, who may be negatively affected in their sphere

16 The data protection officer, in point 3 of his opinion to the AIPD, states that student behavior data, such as the time of response to each question and changes to the answers given, are not necessary for the assessment.



/

CNPD

National Data Protection Commission

legal system, has no way of reacting, insofar as the right provided for in Article 22 of the

56. Also with regard to contractual conditions with Respondus, Inc., ^Accepts that the company collects video and audio recordings from students, not in the context of providing the service and performance of the contract, but expressly for its own purposes (of product improvement and research), assuming the responsibility for further processing, without such processing being subject to the student's consent.

57. In this regard, it should be noted that the student is required to consent to the terms of use of the "Respondus' applications, individually and each time he authenticates himself. In order to take the assessment test, the student must agree with the conditions of use in general, including the subsequent processing of data by Respondus, Inc., in the role of controller. This (mandatory) consent is obviously contrary to the provisions of the GDPR, as consent must constitute an unequivocal, specific and free, and none of these requirements are met in this context, as no alternatives are offered to the student, so this 'consent' is not legally relevant (cf. Article 4, paragraph 11), and Article 7, no. 2 and 4). It follows that this further processing of data from the students' video and audio recordings has no basis of legitimacy, and is therefore unlawful, in breach of the principle enshrined in Article 5. , paragraph 1(a) of the GDPR.

58. Indeed, neither the IAPD appreciates this additional data processing or the

conditions imposed on students to accept the terms of use of Respondus applications.

59. As for the BLR application, there was also no assessment of the level of intrusion on privacy that it represents, when the student's computer is under the full control of a third party, be it a^or a company acting on its behalf. There is clearly

interference in the device's communications with the outside, as well as in its internal use, blocking all types of access and not allowing certain software to be installed (e.g., virtualization software).

60. It further follows from the contractual terms between Respondus, Inc. that the data

personal data are transferred to the US to be processed and hosted on servers controlled by AWS. The legal instrument used for the international transfer is based on article 46(2)(c), in conjunction with paragraph 5 of the same article, that is, on a model contract approved by the European Commission to transfer data between responsible processing in the European Economic Area and subcontractor established in a third country.

GDPR

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213976832

geral@cnpd.pt

www.cnpd.pt

61. Although the aforementioned standard contractual clauses generally offer appropriate guarantees for the international transfer of data, it is necessary to assess whether the legislation in the country of destination conflicts, in any way, with the level of protection provided by such clauses, jeopardizing the guarantees of adequacy contained therein. However, in the opinion of the Court of Justice of the European Union (CJEU), in the Judgment that invalidated the Decision on the adequacy of the Privacy Shieldv, the surveillance legislation for US national security purposes, which overrides instruments of a contractual nature, does not allows a level of data protection essentially equivalent to that of the EU to be guaranteed.

62. Therefore, data transfers to that country based on article 46 of the GDPR could only take place if effective supplementary measures are adopted, if any, to prevent, by technical and/or organizational means, massive access by the northern authorities -Americans to the transferred personal data. Which did not happen in the present case. Therefore, the personal data of students (and University workers) cannot be transferred to the USA, in accordance with the jurisprudence of the CJEU, interpreting the GDPR in the light of the Charter of Fundamental Rights.

63. The remote assessment tests using the "Respondus Lockdown Browser" and "Respondus Monitor" applications have not

yet started, so there has been no processing of personal data in this context for the time being. available for installation on the University website and students were encouraged to test them in advance, and their installation involves data processing, it is likely that some personal data is already processed by Respondus, Inc.

64. In this way, as the CNPD is urgent to act in order to guarantee the safeguarding of the right to the protection of personal data, the CNPD, making use of its powers of correction provided for in subparagraphs a) and d) of no. Article 58 of the GDPR, in conjunction with subparagraph b) of paragraph 1 of article 6 of Law No. 58/2019, of 8 August, determines:

The. Warn the controller, in the sense that the processing of personal data that he intends to carry out, resulting from the use of the two Respondus applications, is likely to violate the provisions of the GDPR;

B. Order the controller to request from the processor Respondus, Inc. to erase all personal data that may have been collected, in case some students have already installed the applications, and must draw up the proper data destruction notice and send it to the person responsible for the treatment.

17 Judgment of July 16, 2020, in case C-311/18, Schrems II case, points 92,93 and 165.





65. Considering the need to give immediate effect to these measures, due to the approximation of the date of the assessment tests, the hearing of interested parties is waived, under the terms of subparagraph a) of paragraph 1 of article 124 of the Civil Code. Administrative Procedure.

IV. Conclusion

66. On the grounds set out above, pursuant to Article 58(2)(a) and d) of the GDPR and Article 6(1)(5) of Law No. 58/ 2019, of August 8, the CNPD resolves:

The. Warn against the combined use of "Respondus Lockdown" applications

Browser" and "Respondus Monitor", within the scope of distance assessment of students, is likely to violate the principles of lawfulness, purpose, data minimization and proportionality, enshrined in article 5, paragraph 1, subparagraphs a), b) and cj, of the GDPR.

B. Order to give instructions to Respondus, Inc. for

that immediately destroys all personal data collected in the context of installing the applications by students, and must issue a data destruction notice and send it

67. Without prejudice to the right to file a lawsuit, this decision is subject to a complaint, under the terms of article 191 of the Code of Administrative Procedure, within 15 days of this notification.

68. Notify yourself, in the person of your legal representative, of the content of this

Deliberation.

Approved at the meeting of May 11, 2021

Filipa Calvão (President)

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T (+351 >213 928 400

F (+351) 213 6/9 832

geral@cnpcl.pt

www.cnpd.pt